INTRODUCTION À DNS

Jérôme Andrieu

Déroulement

- Cours 1h45
- Pause
- TD 1h45
  - Fonctionnement de base
  - Configuration d'un serveur
  - Etude de cas
  - Partie #1 à rendre en fin de séance
  - Partie #2 peut être rendu au plus tard dimanche 4 mars.

  - Adresse mail: jerome.andrieu@cea.fr (zip, gz, … des documents si possibles).

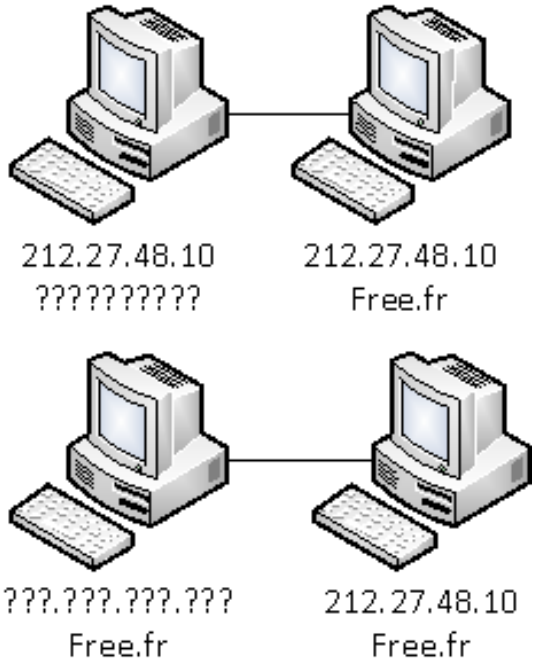
Sommaire

- Contexte
- Généralité
- Administration/Configuration
- HPC
  - Cache
  - Réplication
  - Zones
  - Délégation
  - Sécurité

GÉNÉRALITÉ

Contexte

- Les machines ont des adresses IP (v4 ou v6) qui sont uniques sur internet
  - 82.232.102.55 ? Qui c'est ?
  - http://www.free.fr ? Ou est-ce que ?
  - Il est difficile de se rappeler d'une IP
  - Un nom peut indiquer la fonction
    - http://webmail.free.fr



- Un exemple:
  - Annuaire téléphonique/Annuaire inversé.
    - 06 12 34 56 78 ?
      - Si pas de nom: Qui c'est ?
    - Contact: Emmanuel Macron ?
      - Si pas de numéro dans le contact: Comment je l'appelle ?

Contexte

Forme d'une adresse DNS:

www.yahoo.fr.

fr.: Top Level Domain

yahoo.: Domain

www.: sub domaine

Requête:

- www.yahoo.fr dans DNS donne une adresse 124.108.115.101 (Champ A)
- Dans l'annuaire Emmanuel Macron donne 06 01 23 45 67
- Les noms se résolvent par la droite (comme le tri postal: pays, département, ville, …)

mail.yahoo.fr.

Requête:

- Mail.yahoo.fr donne un autre nom rc.yahoo.fr (Champ CNAME)
- Dans l'annuaire on cherche Président de la France, réponse: Emmanuel Macron
- Alias

Contexte

Forme d'une adresse DNS:

www.yahoo.fr.

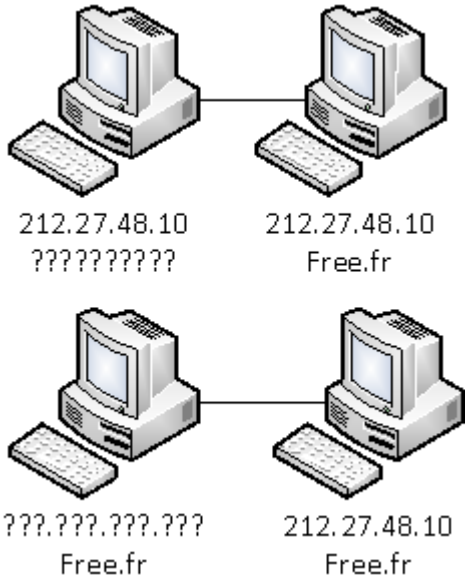
fr.: Top Level Domain

yahoo.: Domain

www.: sub domaine

- Un domaine désigne un domaine, sous domaine, …
- Le DNS est insensible à a case. (WWW.yahoo.fr ou www.yahoo.fr)
- Dans la forme d'un nom DNS, on ne peut pas différencier une machine d'un domaine.

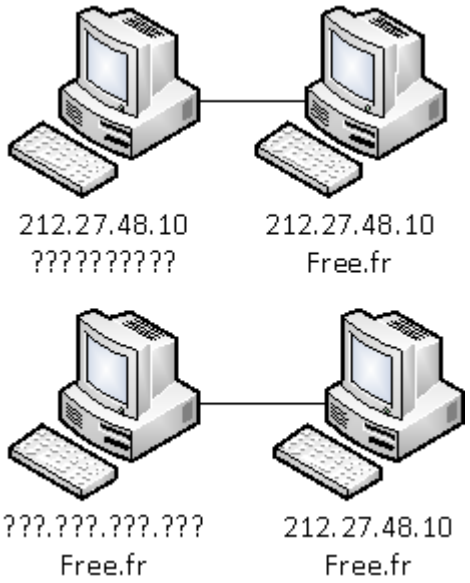
Contexte



- Au début on utilisé un fichier plat
  - /etc/hosts
  - Il était recopié sur toutes les machines
    - Pas facile a maintenir
    - Problèmes de cohérence
  - Toujours utilisé
    - Pour certains cas particuliers
  - Difficilement utilisable avec beaucoup d'entrées

```
82.103.55.32    machine1
83.54.43.23     station2
72.23.92.3      serveur0
194.12.34.12    www
82.232.43.1     mail
```

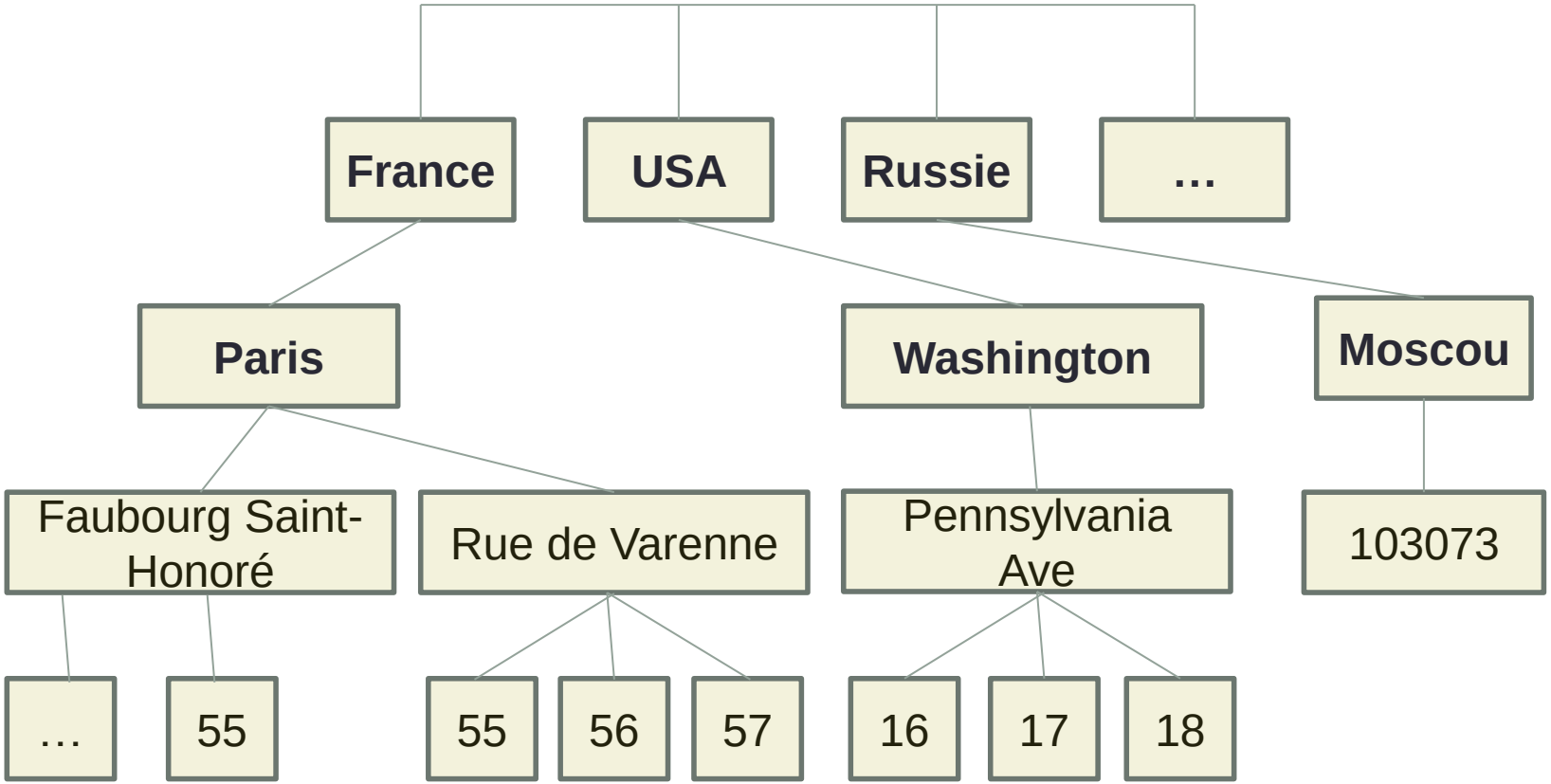
Contexte



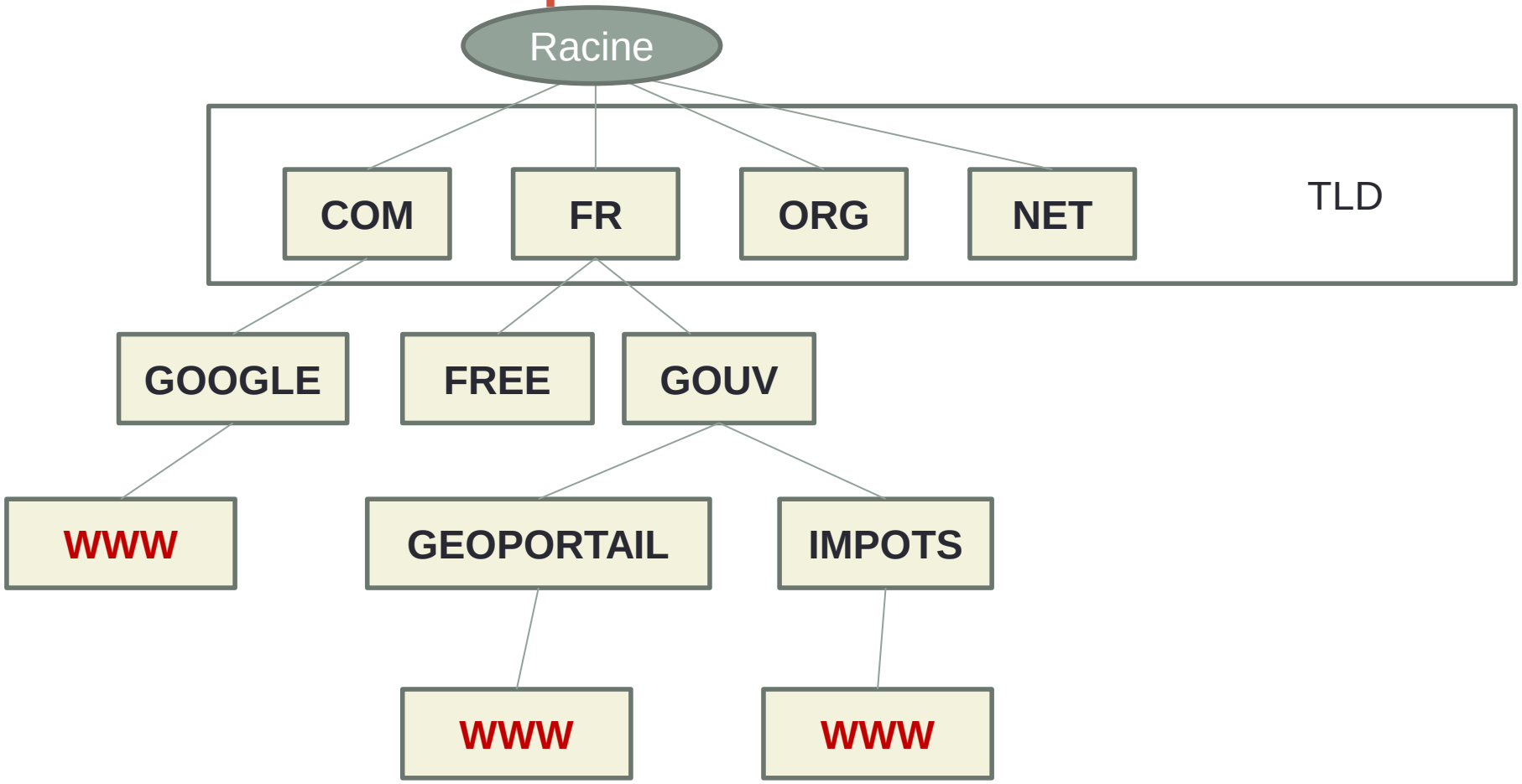
- Mise en place de DNS en 1984
  - première RFC en 1983 à demande de la DARPA).
- En France géré par l'AFNIC
  - dans le monde ICANN.

- Domain Name System
- Defense Advanced Research Projects Agency
- Association française pour le nommage Internet en coopération
- Internet Corporation for Assigned Names and Numbers

Contexte: Espace de nom



Contexte: Espace de nom



Contexte: Serveurs racine

- Répond aux requêtes pour les TLD (Top Level Domain)
- Désigne un des serveurs gérés par l'ICANN
- Il existe des serveurs alternatifs

- Contacté pour avoir une mise à jour des serveurs racine
- Contacté pour la liste des serveurs des TLD (com, fr, …)

Contexte: Top Level Domain TLD

- Com, org, fr, …
  - Com: entreprises commerciales
  - Org: organisations
  - fr/de/…: TLD par code pays à 2 lettre (ISO 3166).
- Arpa est réservé a des fin techniques
  - Sert pour les reverses
    - 06 12 34 56 78 -> Nom
- IP6 technique
  - Sert pour les reverses ipv6

Top Level Domain TLD

- Les TLDs sont mis en gestion chez des entreprises
  - IANA fourni une db
    - https://www.iana.org/domains/root/db
    - .com generic VeriSign Global Registry Services
    - .fr country-code Association Française pour le Nommage Internet en Coopération (A.F.N.I.C.)
    - .weather generic International Business Machines Corporation
    - .paris generic City of Paris
    - .ファッション generic Amazon Registry Services, Inc.
  - Les gestionnaires vendent les sous domaines et les délègues
    - Free.fr
    - bienvenue.paris
  - L'acheteur du sous domaine peut refaire des sous domaines, …
    - User.free.fr
  - Il est courant d'acheter des noms de domaines pour les revendre (ex: fillon-président.fr)

Généralité

- Distribué, hiérarchique et redondant

- Il y a des millions de serveurs DNS dans le monde
  - Dans des boxs, des isps, …
  - Tous ne sont pas maîtres de zones
    - Certaines ne font que du cache, du transfert, …
- Il y a seulement 13 serveurs racine
- Deux types de serveurs
  - Récursif
    - Cherche un obtenir la réponse
  - Itératif
    - Se contente de transmettre la demande

Généralité: Résumé

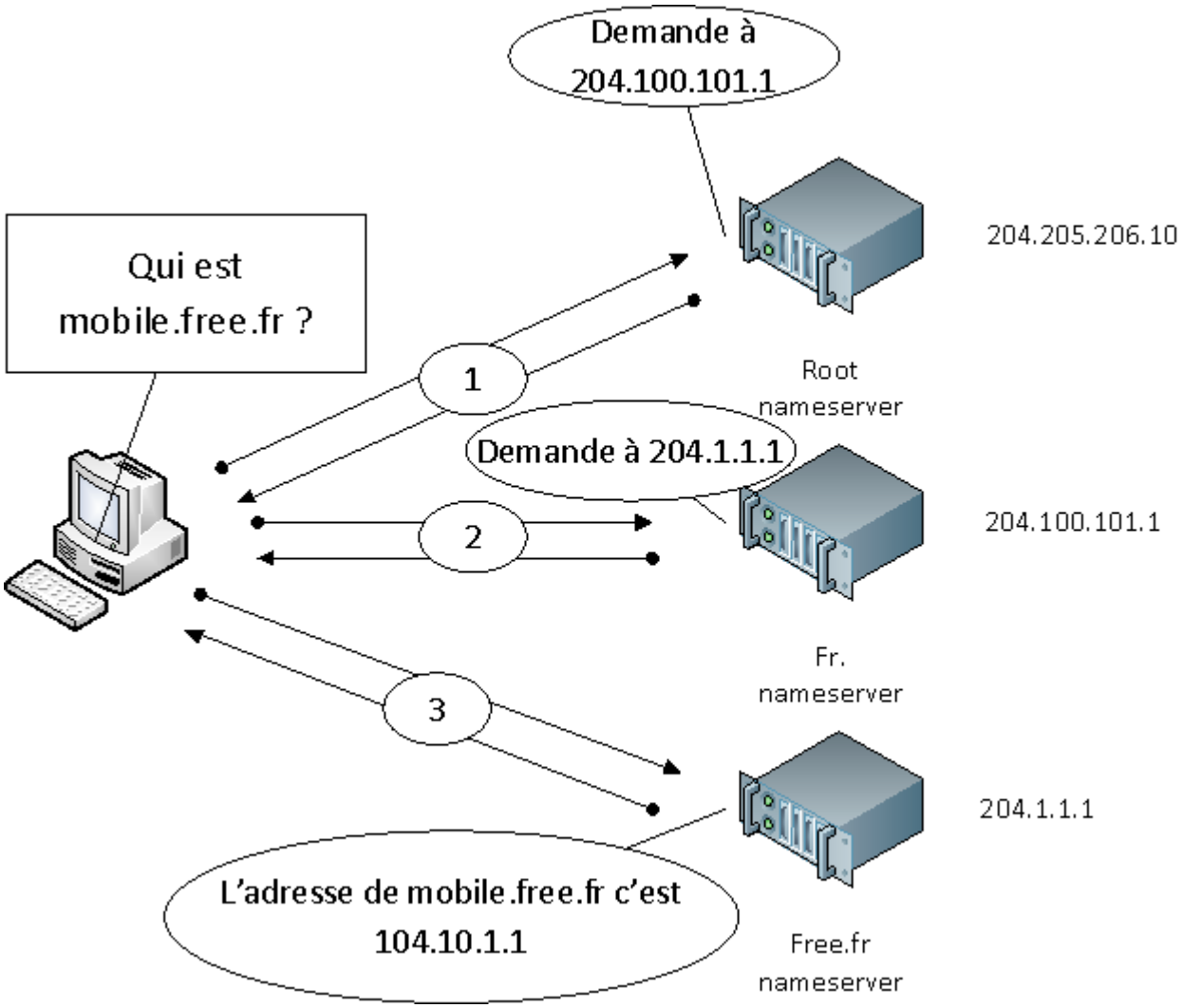
- FQDN (Fully Qualified Domain Name)
  - Machine.sousdomaine.domaine.tld != machine
- TLD (Top Level Domain)/Serveurs racine
  - com/fr/org/…
- 63 char. par élément, 255 char. max au total
- Résolution directe
  - Free.fr -> 212.27.48.10
- Résolution inverse
  - 212.27.48.10->Free.fr

Généralité

- Dynamic update
  - Laisse une machine s'enregistrer (utilisé dans l'univers microsoft)
- DNSSEC
  - DNS Security Extension
    - Permet de vérifier les records (nécessite d'en ajouter)
- Protocoles
  - UDP quand c'est possible (port 53) si paquet < 512octets
    - Si le paquet est perdu on réessaye, change de serveur, ..
  - TCP (Transfert de zones, …) port 53

FONCTIONNEMENT

Fonctionnement



Records

- A record: ipv4
- AAAA record: ipv6
- CNAME: Canonical name (Alias)
- MX: Mail eXchanger (adresse SMTP du domaine)
- PTR: Lien vers un autre domaine, utilisé pour les résolutions inverses
- NS: Name serveur, nom d'un serveur d'un autre domaine, utilisé pour les délégations
- SOA: Start Of Authority (Informations sur la zone, nom du serveur primary, mail, ttl, …)
- SRV: Service (utilisé par Active Directory par exemple)
- TXT: Champ text

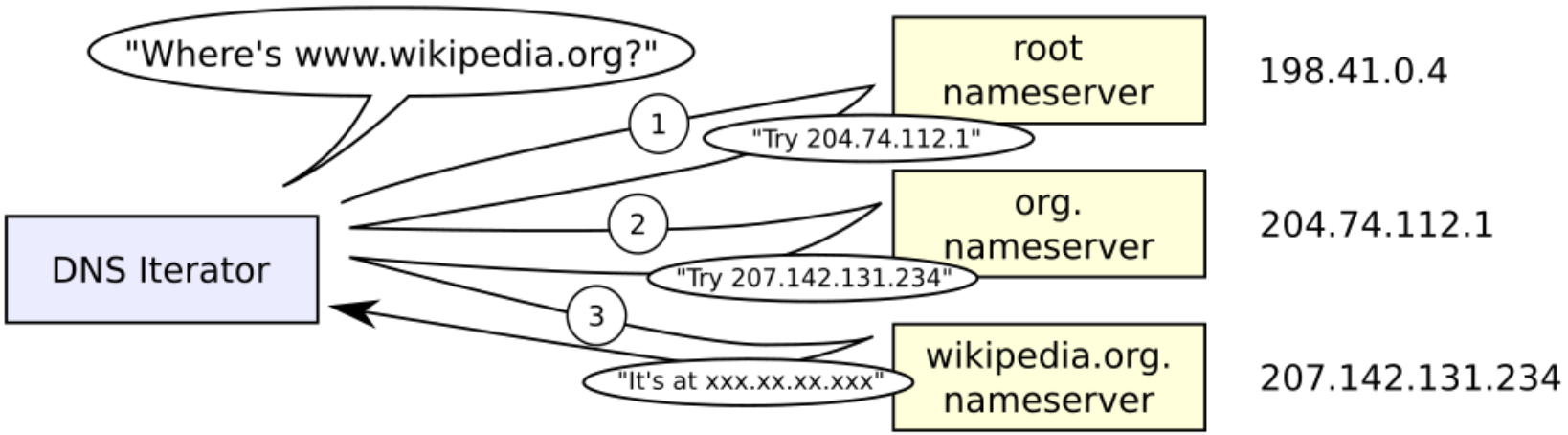
Records: exemples

- Pour free.fr
  - NS
    - Free.fr NS freens1-g20.free.fr.
    - Free.fr NS freens2-g20.free.fr.
  - A
    - Free.fr IN A 212.27.48.10
  - CNAME
    - Pop3 CNAME pop3.free.fr.

Records: SOA

- free.fr
- origin = freens1-g20.free.fr
- mail addr = hostmaster.proxad.net
- serial = 2018021501
- refresh = 10800
- retry = 3600
- expire = 604800
- minimum = 86400

Fonctionnement

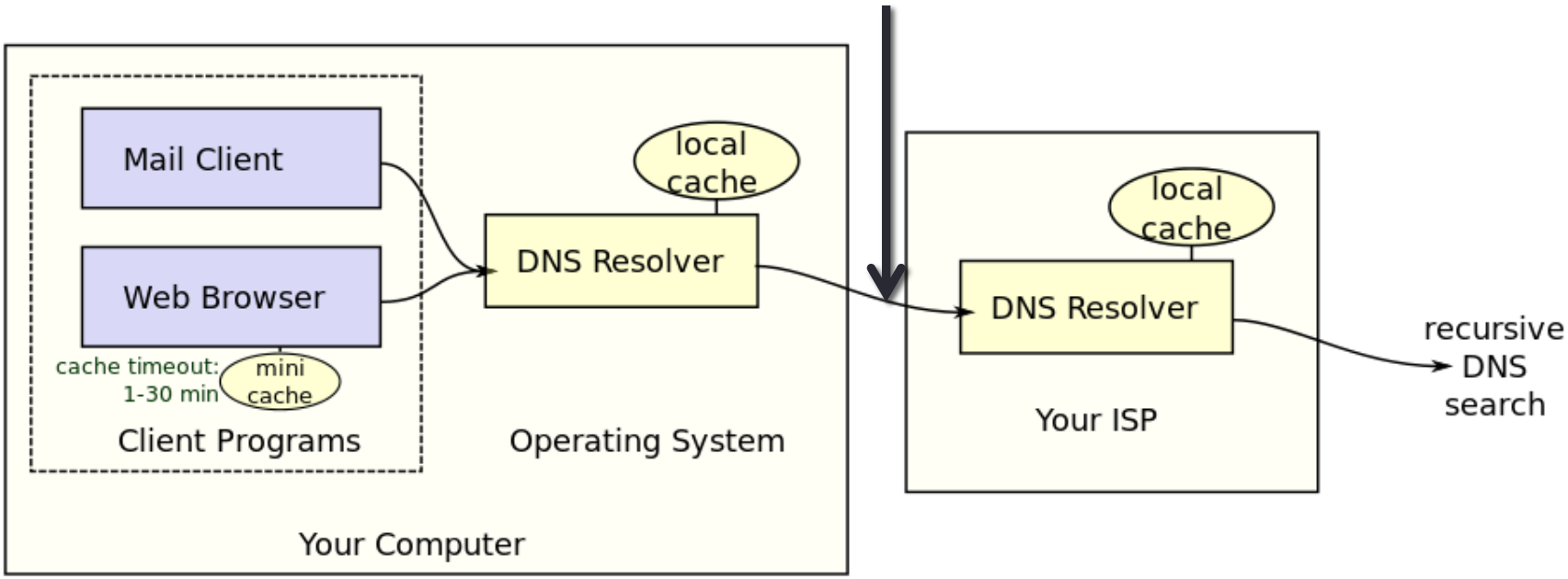


Récursif, une question peut retourner une réponse ou une autre référence pour poser la question

Fonctionnement

En pratique à la maison

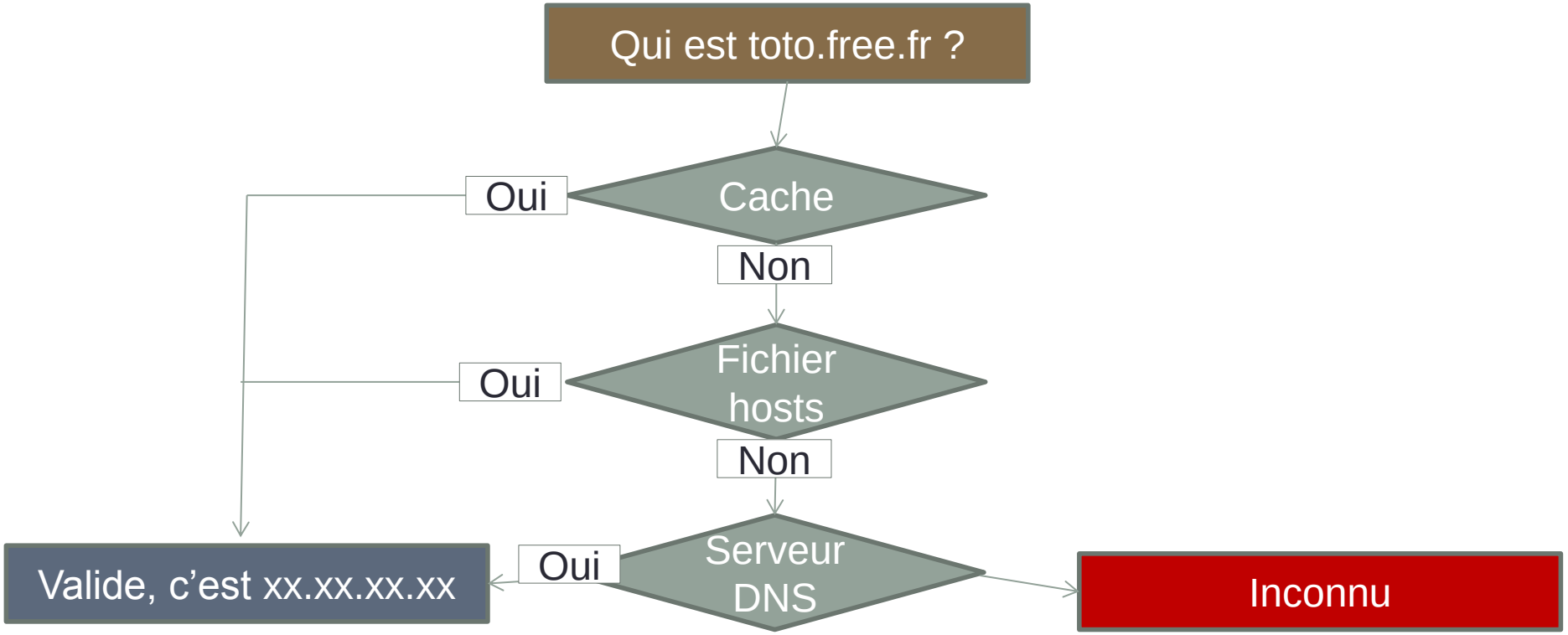
Itératif:
Une requête, une réponse attendu



Fonctionnement

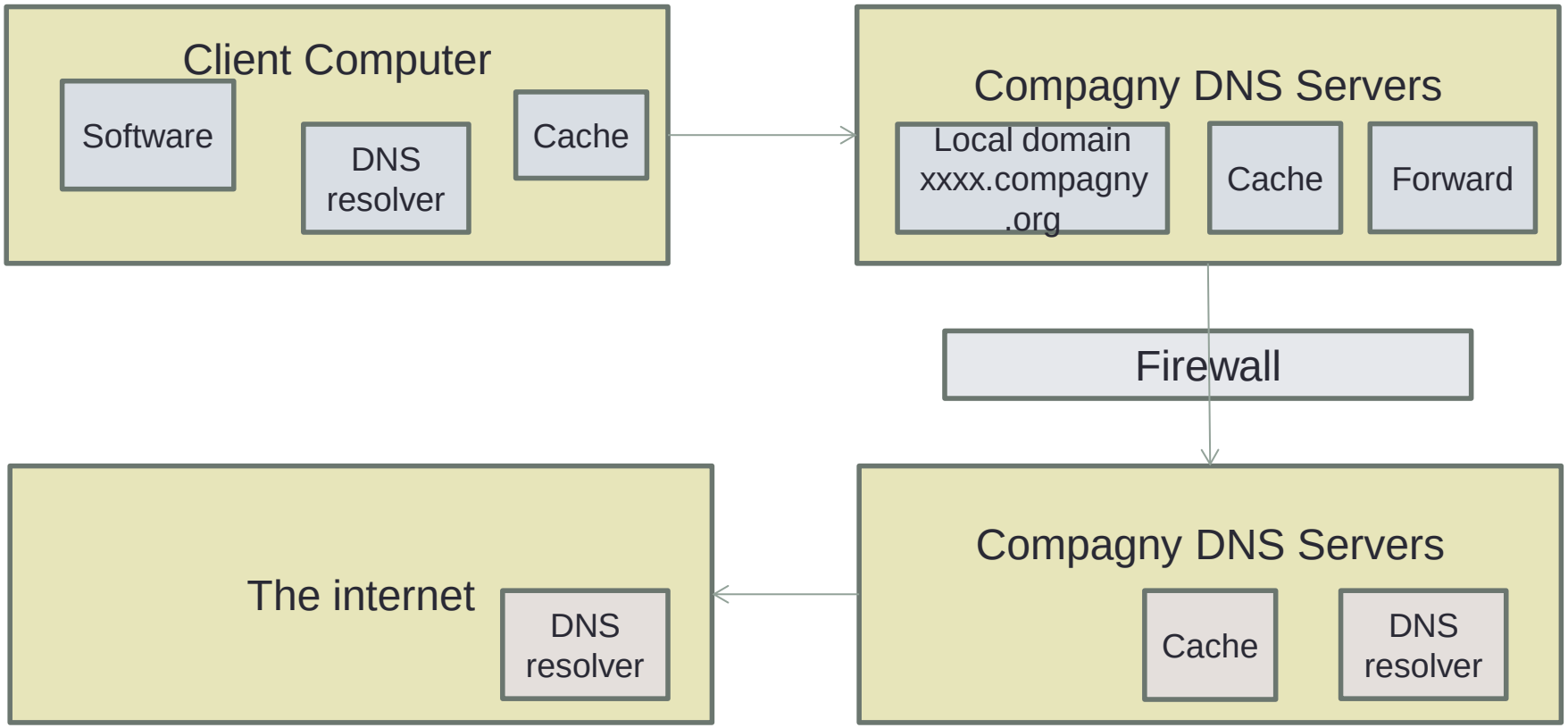
- Quand un DNS fait du récursif, il garde en mémoire la réponse qu'il obtient
- Quand on lui demande une information qu'il a en cache, il donne la réponse de son cache.
  - Il indique aussi qu'il ne fait pas autorité sur la réponse (Non-authoritative answer).
  - Il indique ou on peut avoir une réponse d'un serveur qui a délégation sur la zone.
- Le cache à une durée de vie (TTL, time to live) et se vide automatiquement
- Attention aux effets de caches et aux temps de propagation.

Fonctionnement par ‘défaut’

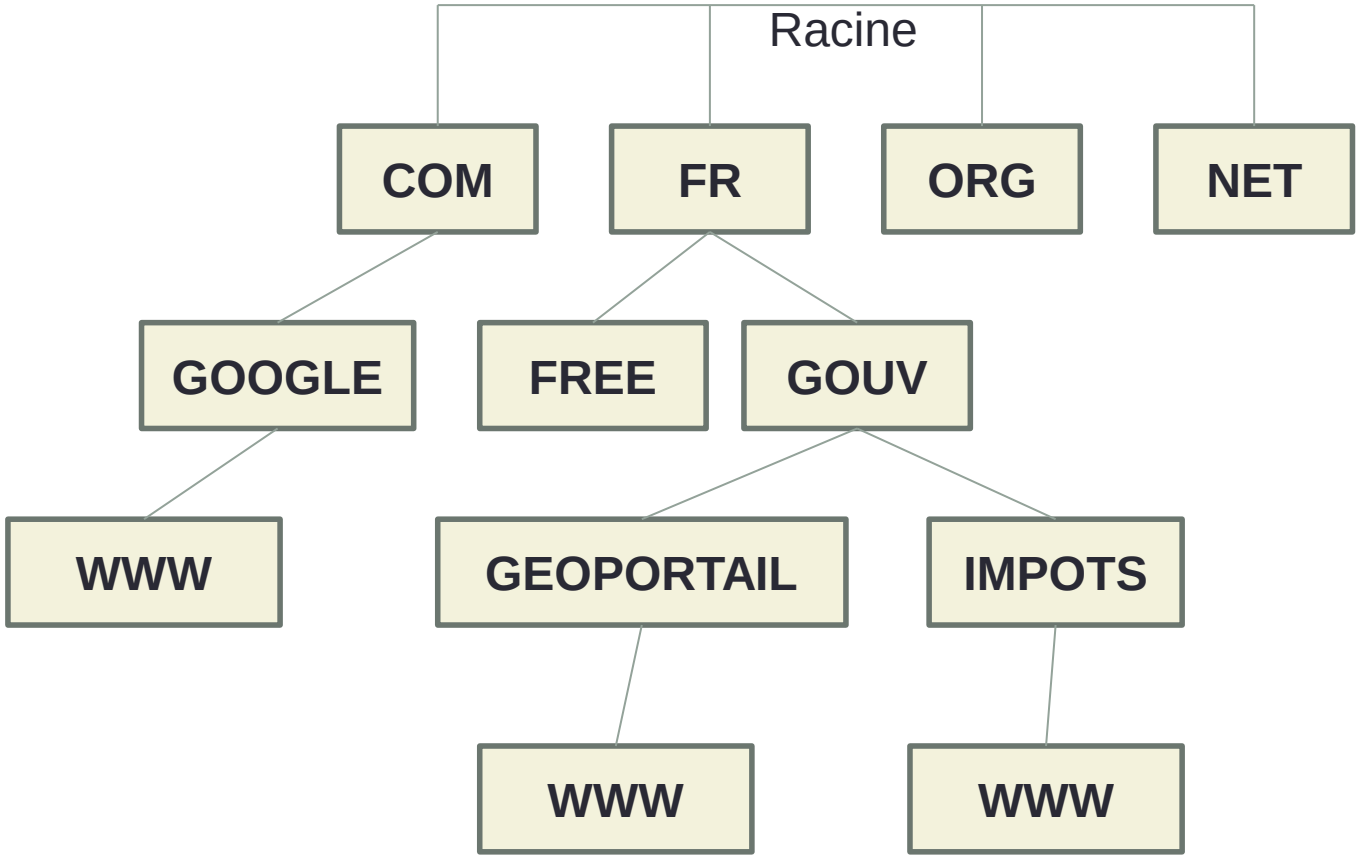


Fonctionnement

- Pratique en entreprise



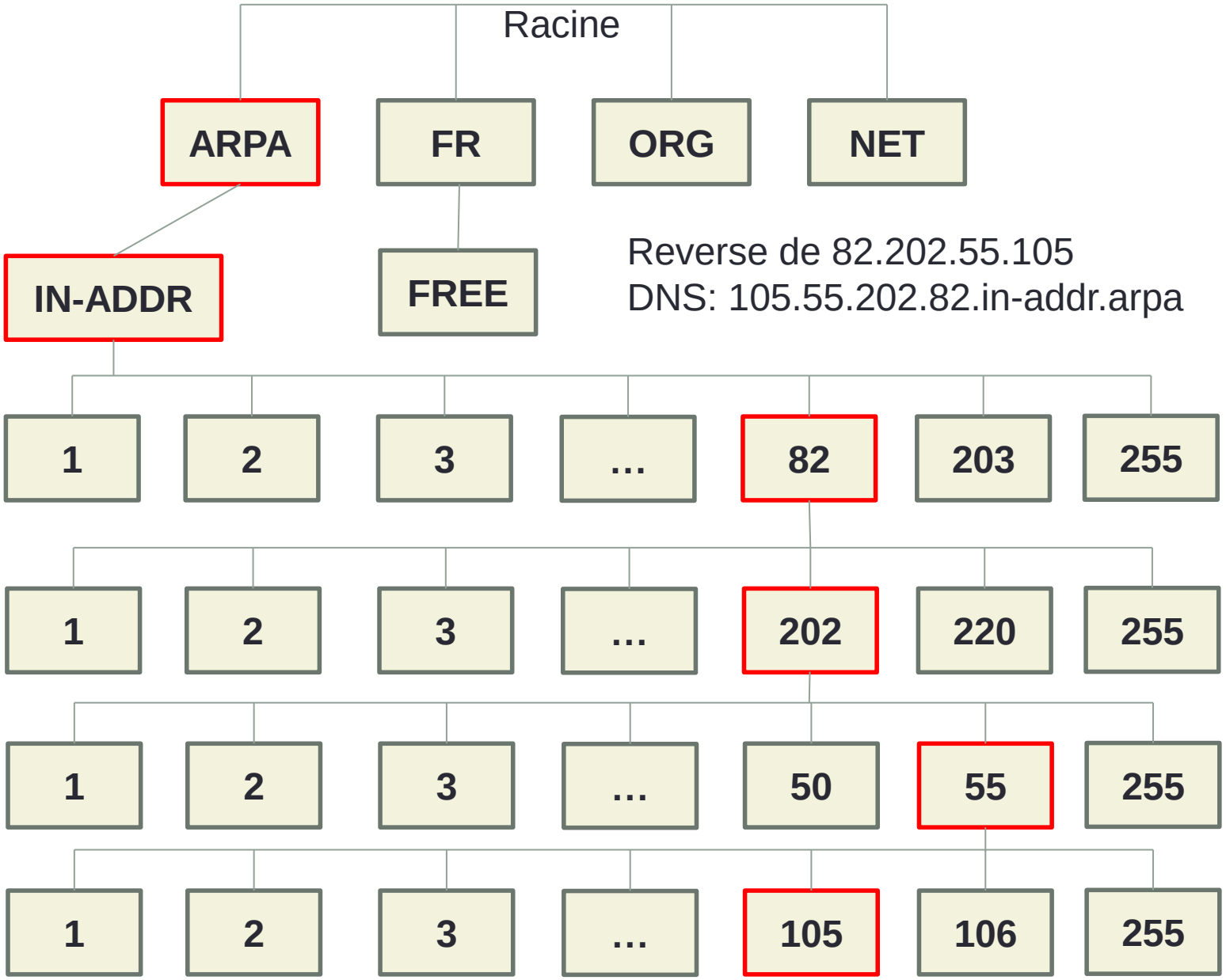
Fonctionnement direct



Fonctionnement reverse

- Mécanisme
  - Transforme l'ip en nom DNS dans in-addr.arpa.
  - 1.2.3.4 deviens 4.3.2.1.in-addr.arpa
- On demande le champs PTR
- Déroulement
  - Demande à
    - . Qui est arpa
    - Arpa. Qui est in-addr.arpa
    - In-addr.arpa qui est 1
    - 1.in-addr.apa qui est 2
    - …
    - 3.2.1.in-addr.arpa qui est 4
  - Le serveur réponds avec le nom « toto.free.fr »

Fonctionnement reverse



Dig +trace

- 20.60.27.212.in-addr.arpa@8.8.8.8 (Google):

.	219524	IN	NS	c.root-servers.net.
.	219524	IN	NS	g.root-servers.net.
.	219524	IN	NS	a.root-servers.net.
.	219524	IN	NS	j.root-servers.net.
.	219524	IN	NS	k.root-servers.net.
.	219524	IN	NS	l.root-servers.net.
.	219524	IN	NS	f.root-servers.net.
.	219524	IN	NS	m.root-servers.net.
.	219524	IN	NS	e.root-servers.net.
.	219524	IN	NS	d.root-servers.net.
.	219524	IN	NS	b.root-servers.net.
.	219524	IN	NS	i.root-servers.net.
.	219524	IN	NS	h.root-servers.net.

- ;; Received 228 bytes from 8.8.8.8#53(8.8.8.8) in 4 ms

in-addr.arpa.	172800	IN	NS	a.in-addr-servers.arpa.
in-addr.arpa.	172800	IN	NS	b.in-addr-servers.arpa.
in-addr.arpa.	172800	IN	NS	c.in-addr-servers.arpa.
in-addr.arpa.	172800	IN	NS	d.in-addr-servers.arpa.
in-addr.arpa.	172800	IN	NS	e.in-addr-servers.arpa.
in-addr.arpa.	172800	IN	NS	f.in-addr-servers.arpa.

- ;; Received 419 bytes from 199.7.83.42#53(199.7.83.42) in 3 ms

212.in-addr.arpa.	86400	IN	NS	pri.authdns.ripe.net.
212.in-addr.arpa.	86400	IN	NS	sec3.apnic.net.
212.in-addr.arpa.	86400	IN	NS	sns-pb.isc.org.
212.in-addr.arpa.	86400	IN	NS	tinnie.arin.net.
212.in-addr.arpa.	86400	IN	NS	ns3.lacnic.net.
212.in-addr.arpa.	86400	IN	NS	ns3.afrinic.net.

- ;; Received 207 bytes from 193.0.9.1#53(193.0.9.1) in 321 ms

60.27.212.in-addr.arpa.	172800	IN	NS	ns0.proxad.net.
60.27.212.in-addr.arpa.	172800	IN	NS	ns1.proxad.net.

- ;; Received 89 bytes from 199.212.0.53#53(199.212.0.53) in 222 ms

60.27.212.in-addr.arpa.	86400	IN	SOA	ns0.proxad.net. hostmaster.proxad.net. 2017100302 21600 3600 1209600 86400

- ;; Received 104 bytes from 212.27.32.130#53(212.27.32.130) in 106 ms

Serveurs

- BIND
  - Le plus commun, la référence
- NSD
  - Ne sert que des serveurs qui font autorité, ne peut pas en interroger d’autres
- Dnsmasq
  - Commun, utilisé dans plein de cas « particuliers »
- Microsoft DNS Server
  - Utilisé dans les entreprises « full windows »

Configuration serveur

- Linux
  - /etc/named.conf
    - configuration
  - /var/named
    - Base de données par défaut
  - Gestion du service
    - systemctl
    - Initd
    - …

Clients/Outils

- NSCD (Named Server Caching Daemon)
- Nslookup (utilise ses propres fonctions)
- Dig (utilise les libs standards)
- Host –d –t

- Appel système
  - Gethostbyname
  - Getaddrinfo

Configuration du client

- Configuration résolution DNS
  - /etc/resolv.conf
    - Searchdomain
    - Server
- Providers
  - /etc/nsswitch.conf
    - Hosts: files dns

Gethostbyname (deprecated)

```
#include <netdb.h>
struct hostent *gethostbyname(const char *name);
struct  hostent {
        char    *h_name;        /* official name of host */
        char    **h_aliases;    /* alias list */
        int     h_addrtype;     /* host address type */
        int     h_length;       /* length of address */
        char    **h_addr_list;  /* list of addresses from name server */
};
```

getaddrinfo

```
#include <sys/types.h>
#include <sys/socket.h>
#include <netdb.h>

int getaddrinfo(const char *node, const char *service,
                const struct addrinfo *hints,
                struct addrinfo **res);

void freeaddrinfo(struct addrinfo *res);

const char *gai_strerror(int errcode);

struct addrinfo {
    int              ai_flags;
    int              ai_family;
    int              ai_socktype;
    int              ai_protocol;
    size_t           ai_addrlen;
    struct sockaddr *ai_addr;
    char            *ai_canonname;
    struct addrinfo *ai_next;
};
```

CONFIGURATION

Configuration de named.conf

- Acl (access control list)

```
acl calc1 {172.20.10.0/24;};
acl calc2 {172.20.20.0/24;};
acl servext {172.20.30.0/24;};
acl servint {172.20.31.0/24;};
acl stock1 {172.20.40.0/24;};
acl ZA {172.40.10.0/24;};
```

Configuration de named.conf

- Options

```
options {
        listen-on port 1053 { 127.0.0.1; };
        directory ""/var/named/";
        dump-file "/var/named/data/cache_dump.db";
        pid-file        "/var/run/named/named.pid";
forwarders{
                127.0.0.1:3053;
                127.0.0.1:4053;
        };
        forward only;
        also-notify    {127.0.0.1 2053; };
        allow-transfer 127.0.0.1 2053; };
        allow-query {127.0.0.1; calc1; calc2; servext; servint; stock1; ZA;};
        allow-query-cache {127.0.0.1; calc1; calc2; servext; servint; stock1; ZA;};
        version « You don’t need to know. »;
};
```

Configuration de named.conf

```
logging {
        channel my_file {
        file "/var/log/named/named.log";
        severity dynamic;
        print-category yes;
        print-severity yes;
        print-time yes;
                };
        channel my_syslog {
        syslog local4;
        severity info;
        print-category yes;
        print-severity yes;
        print-time yes;
                };
        category default { my_syslog; my_file; };
        category general { my_syslog; my_file; };
        category client { my_syslog; my_file; };
        category config { my_syslog; my_file; };
        category database { my_syslog; my_file;};
        category dnssec { my_syslog; my_file; };
        category lame-servers { my_syslog;
        my_file; };
        category network { my_syslog; my_file; };
        category notify { my_syslog; my_file; };
        category queries { my_syslog; my_file; };
        category resolver { my_syslog; my_file; };
        category security { my_syslog; my_file; };
        category update { my_syslog; my_file; };
        category xfer-in { my_syslog; my_file; };
        category xfer-out { my_syslog; my_file; };
                };
```

Déclaration d’une zone dans named

```
zone "localhost" IN {
        type master;
        file "primary/localhost";
        forwarders {};
};

zone "ccc.cdc.fr" IN {
        type master;
        file "primary/ccc.cdc.fr";
        forwarders {};
};
```

Déclaration d’une zone dans named

```
zone "localhost" IN {
        type master;
        file "primary/localhost";
        forwarders {};
};

zone "ccc.cdc.fr" IN {
        type master;
        file "primary/ccc.cdc.fr";
        forwarders {};
};
```

primary/localhost

```
$TTL 24h        ; TTL
@       IN      SOA     localhost.      root.localhost. (
                2010110500 ; serial
                8h ; refresh
                1h ; retry
                1w ; expire
                1d ; default_ttl
                )
@       IN      NS      primary-ns.ccc.cdc.fr.
@       IN      NS      backup-ns.ccc.cdc.fr.

localhost.      IN      A       127.0.0.1
```

primary/ccc.cdc.fr

```
$TTL 24h                ; TTL
@       IN      SOA     primary-ns.ccc.cdc.fr.      root.serv1.cdc.cea.fr. (
                2018022201; serial
                4h ; refresh
                1h ; retry
                1w ; expire
                1d ; default_ttl
        )
@       IN      NS      primary-ns.ccc.cdc.fr.
@       IN      NS      backup-ns.ccc.cdc.fr.

serv1           IN      A       172.20.31.1
serv2           IN      A       172.20.31.2
serv3           IN      A       172.20.31.3
primary-ns      IN      A       172.20.31.1
backup-ns       IN      A       172.20.31.2
ntpserv1        IN      CNAME   serv1.ccc.cdc.fr.
```

Déclaration d’un slave/reverse

```
zone “calc1.ccc.cdc.fr" IN {
        type slave;
        file "secondary/calc1.ccc.cdc.fr";
        masters { 127.0.0.1 2053; }; //en vrai 172.20.10.x
        forwarders {};
};
zone “10.20.172.in-addr.arpa" IN {
        type slave;
        file "secondary/172.20.10.calc1.ccc.cdc.fr";
        masters { 127.0.0.1 2053; }; //en vrai 172.20.10.x
        forwarders {};
};
```

Admin

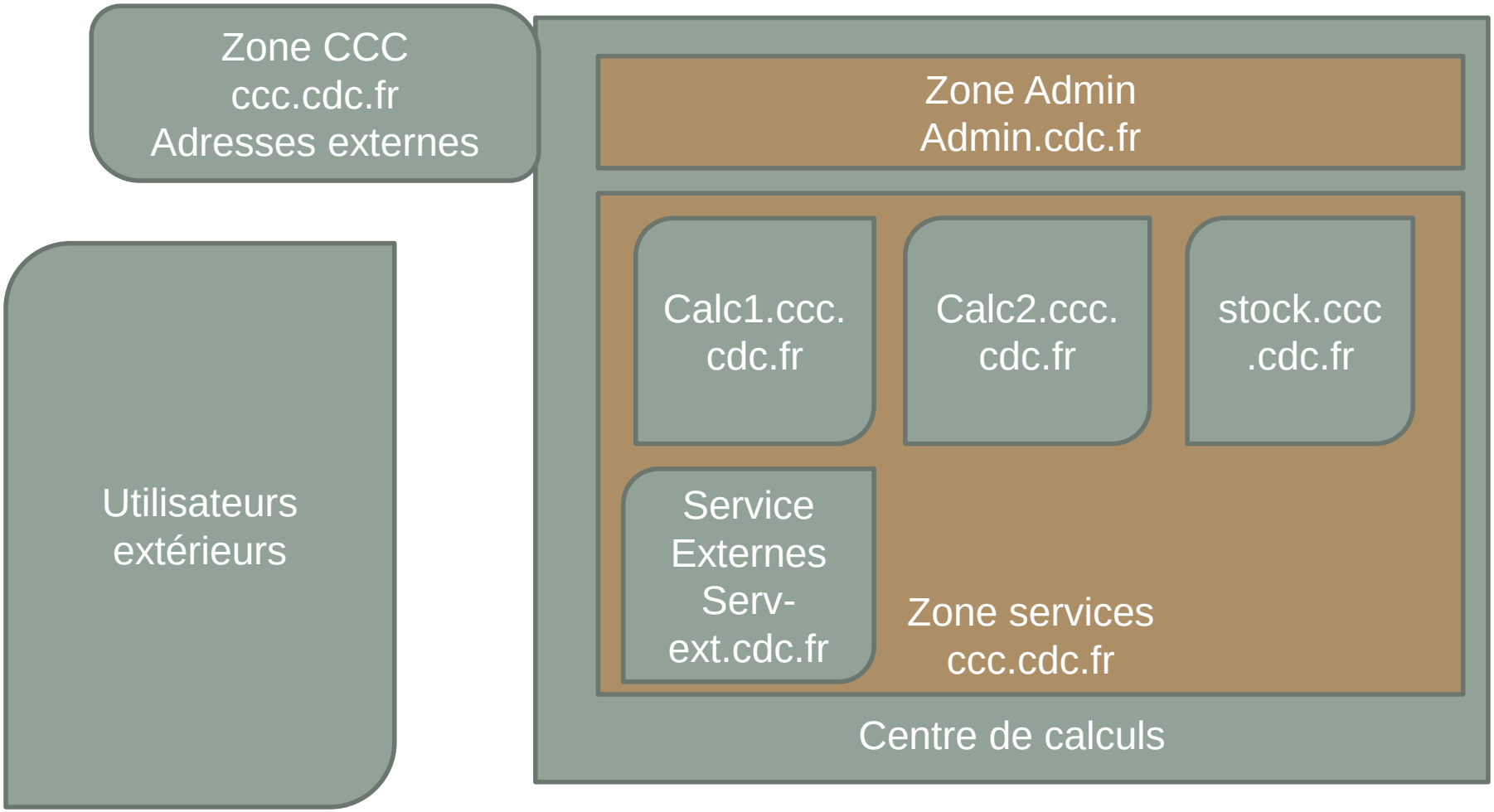
- Nslookup
  - The 'help' command is not yet implemented
  - Server nomduserver
  - Set type=type (any/soa/a/…)
- Dig
  - Man dig

Resolv.conf

- Searchdomain
  - Complète automatiquement une recherche DNS si elle n'existe pas
  - Search domain tata.toto.fr, toto.fr
    - Si on cherche titi tout court:
      - Titi
      - Titi.tata.toto.fr
      - Titi.toto.fr
  - Pratique, mais peut être source d'erreur
- Server
  - Configure le, ou les serveurs à utiliser

CENTRE DE CALCUL

Les zones


Zone CCC
ccc.cdc.fr
Adresses externes
Utilisateurs extérieurs
Zone Admin
Admin.cdc.fr
Calc1.ccc.cdc.fr
Calc2.ccc.cdc.fr
stock.ccc.cdc.fr
Service Externes Serv-ext.cdc.fr
Zone services
ccc.cdc.fr
Centre de calculs

HAUTE DISPO

Cache

- Mise en mémoire temporaire d'une information pour ne pas la redemander
- Coté client
  - NSCD
  - Attention à bien régler la durée de vie
    - Surtout problématique lors de l'installation de nouvelles machines, …
- Côté serveur
  - Attention à la durée et aux numéros de versions des tables
  - Essentiel au bon fonctionnement
    - Que ce passerait t'il si tout le monde demande à chaque fois des informations aux 13 serveurs racine.
- Dans les deux cas:
  - Attention aux effets de cache en cascade
  - Attention au cache négatif !

Replication slave/secondaire

- Réplication
  - A l'initiative du slave
  - Une fois la première réplication faite, le slave redemande toutes les XXXXX secondes (durée définie dans le SOA de la zone)
  - Le master peut faire un NOTIFY aux slaves connus pour initier une mise à jour de zone
  - Types de transferts
    - AXFR (complet)
    - IXFER (incrémental)
  - Permet d'avoir plusieurs serveurs autoritatifs sur une zone

HA et Pacemaker/DRBD

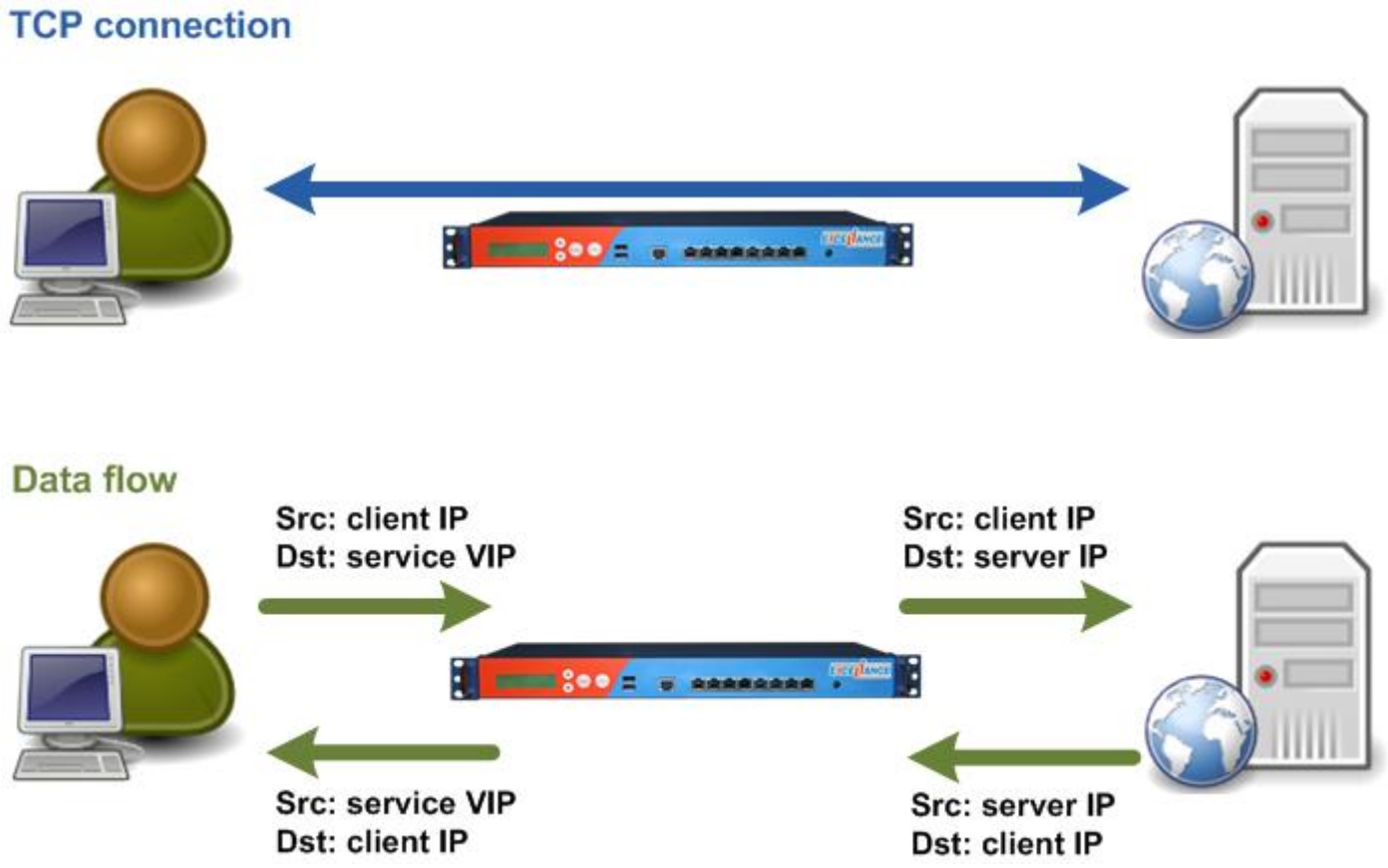
- DRBD
  - Disque commun entre deux machine synchronisé
    - Les serveurs doivent être proches
    - Sujet aux « split brain »
- Pacemaker
  - Permet de basculer des services d'une machine a une autre
    - Groupe de services qui bascule quand un est en panne
- Il est possible de palier à des pannes avec ces systèmes
  - Balance risque/gain
    - Souvent contre ces solutions pour des services tel le DNS et LDAP
    - La complexité de pacemaker/drbd ajoute un risque technique
    - Maintient en condition opérationnel/sécurité couteux
    - Plutôt utilisé quand il n'y a pas de redondance intégrée.

Load Balancer

- Hardware (HLB ou HLD (Hardware Load balancer Device)) ou « *layer 4-7 router* »
  - *Cisco (deprecated)*
  - *Kemp*
  - *…*
- Software (SLB)
  - HA Proxy
  - NGINX
  - …

SLB, SNAT

SLB qui DNAT/SNAT (Network Address Translation)



Round-Robin

- Déclaration
  - fr.pool.ntp.org. 150 IN A 88.190.208.249
  - fr.pool.ntp.org. 150 IN A 88.191.228.144
  - fr.pool.ntp.org. 150 IN A 193.55.167.2
  - fr.pool.ntp.org. 150 IN A 5.135.152.40
- Renvoie les 4 adresses en décalant l’ordre d’un cran a chaque requête

Round Robin (yahoo)

- $date && nslookup yahoo.fr
- mer. nov. 8 09:47:14 CET 2017
- Server: xxxx
- Address: xxxx

- Non-authoritative answer:
- Name: yahoo.fr
- Address: 106.10.212.24
- Name: yahoo.fr
- Address: 98.137.236.24
- Name: yahoo.fr
- Address: 74.6.50.24
- Name: yahoo.fr
- Address: 77.238.184.24
- Name: yahoo.fr
- Address: 124.108.105.24

$date && nslookup yahoo.fr
mer. nov. 8 09:47:15 CET 2017
Server: xxxx
Address: xxxx

Non-authoritative answer:
Name: yahoo.fr
Address: 98.137.236.24
Name: yahoo.fr
Address: 74.6.50.24
Name: yahoo.fr
Address: 77.238.184.24
Name: yahoo.fr
Address: 124.108.105.24
Name: yahoo.fr
Address: 106.10.212.24

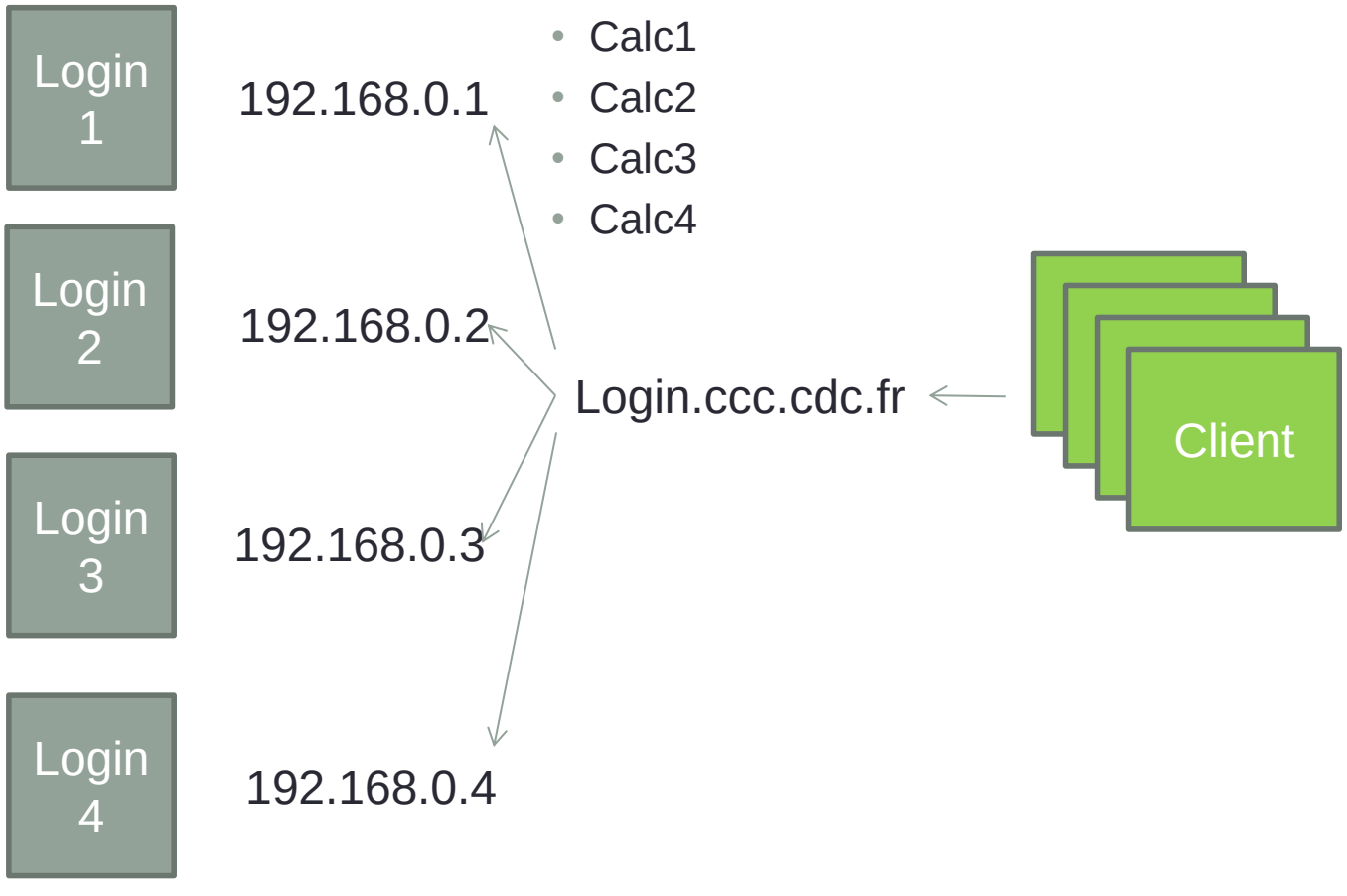
Round-Robin

- $ping -c 1 yahoo.fr
- PING yahoo.fr (98.137.236.24) 56(84) bytes of data.
- ^C
- --- yahoo.fr ping statistics ---
- 1 packets transmitted, 0 received, 100% packet loss, time 2309ms

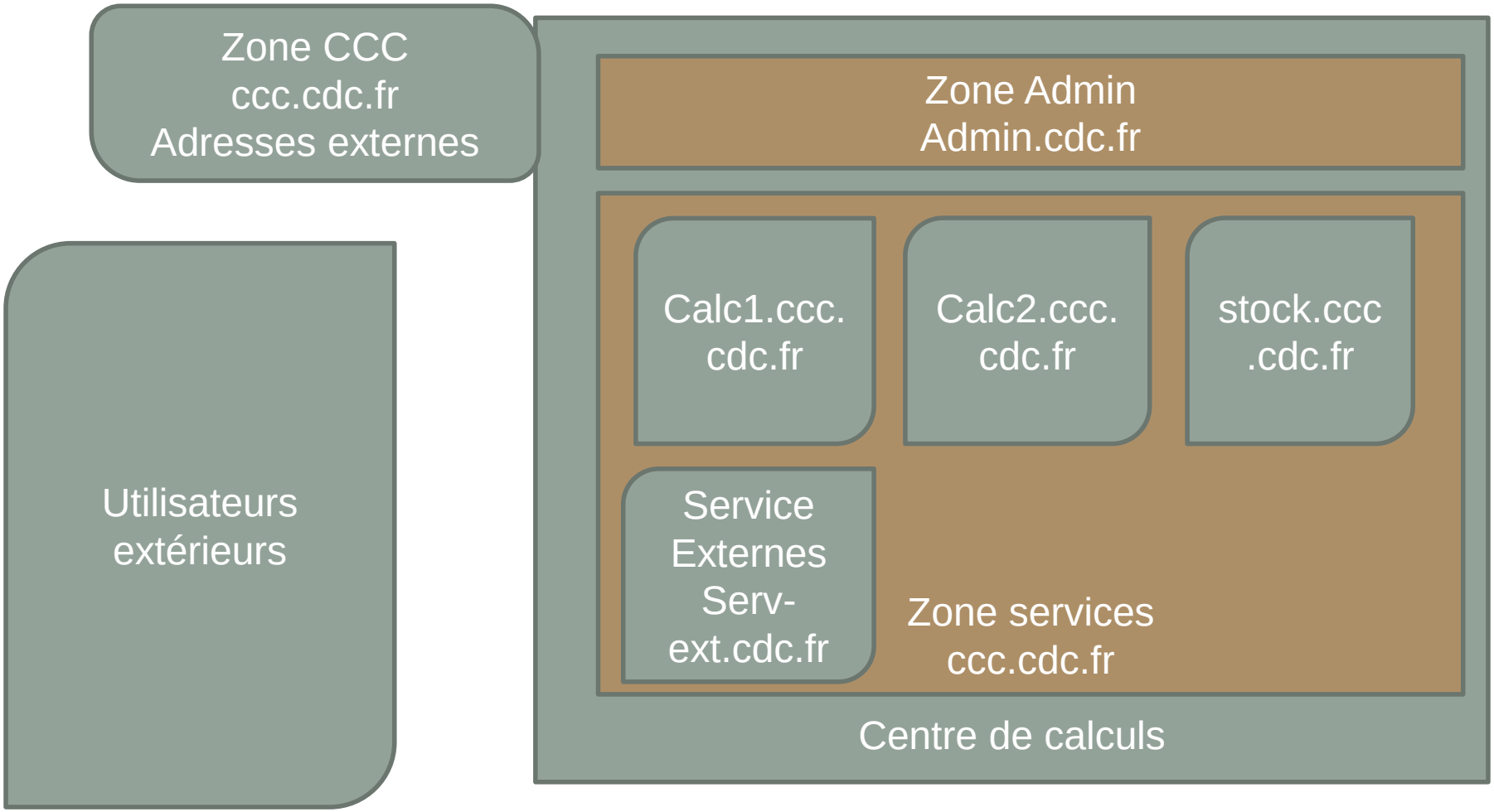
- $ping -c 1 yahoo.fr
- PING yahoo.fr (74.6.50.24) 56(84) bytes of data.
- ^C
- --- yahoo.fr ping statistics ---
- 1 packets transmitted, 0 received, 100% packet loss, time 494ms

Usages en pratique

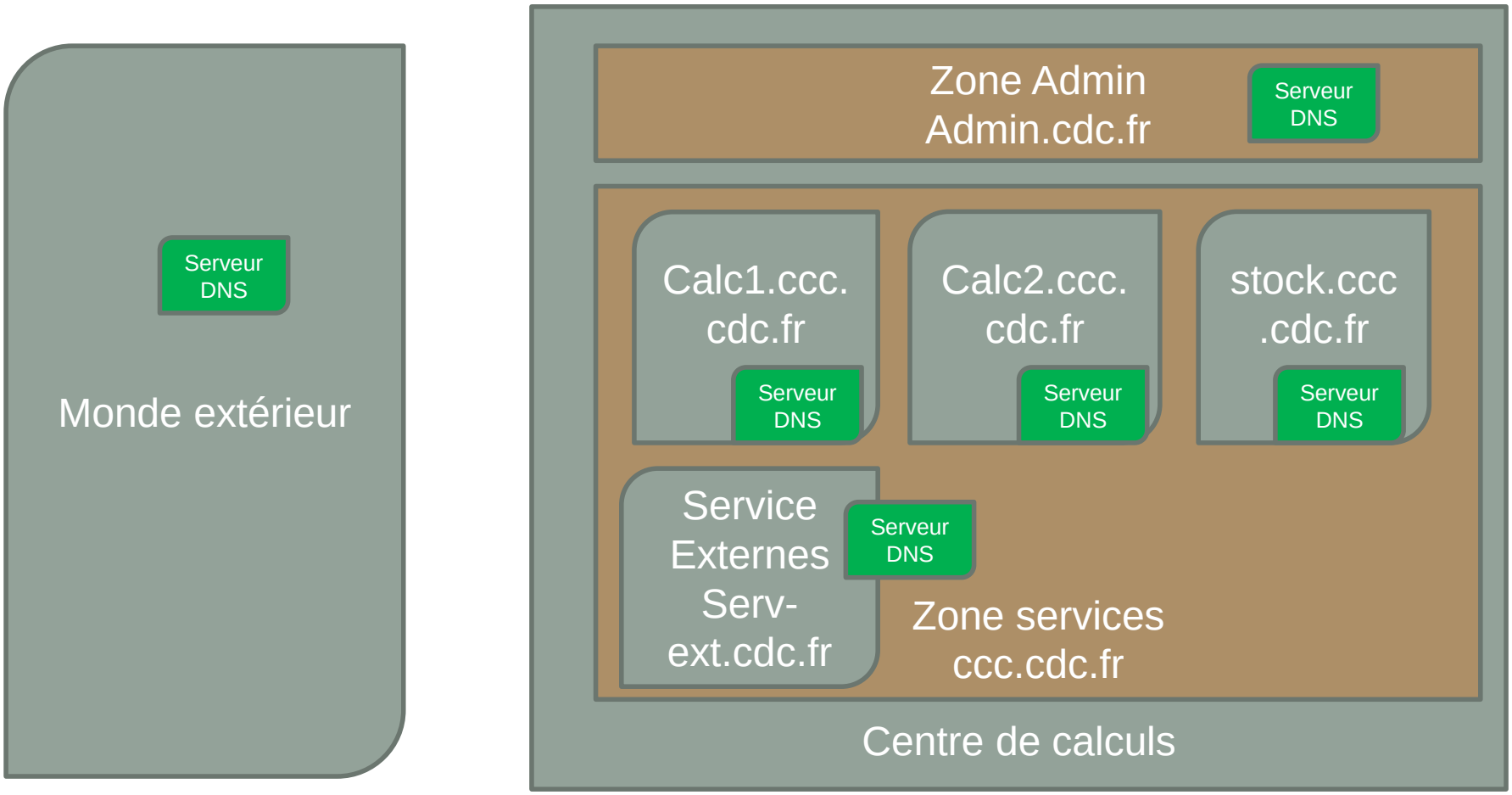
- Nœud de login
  - Round Robin pour la connexion aux nœuds interactif
    - Ssh calculateur.ccc.cdc.fr
      - Calc1
      - Calc2
      - Calc3
      - Calc4



Les zones

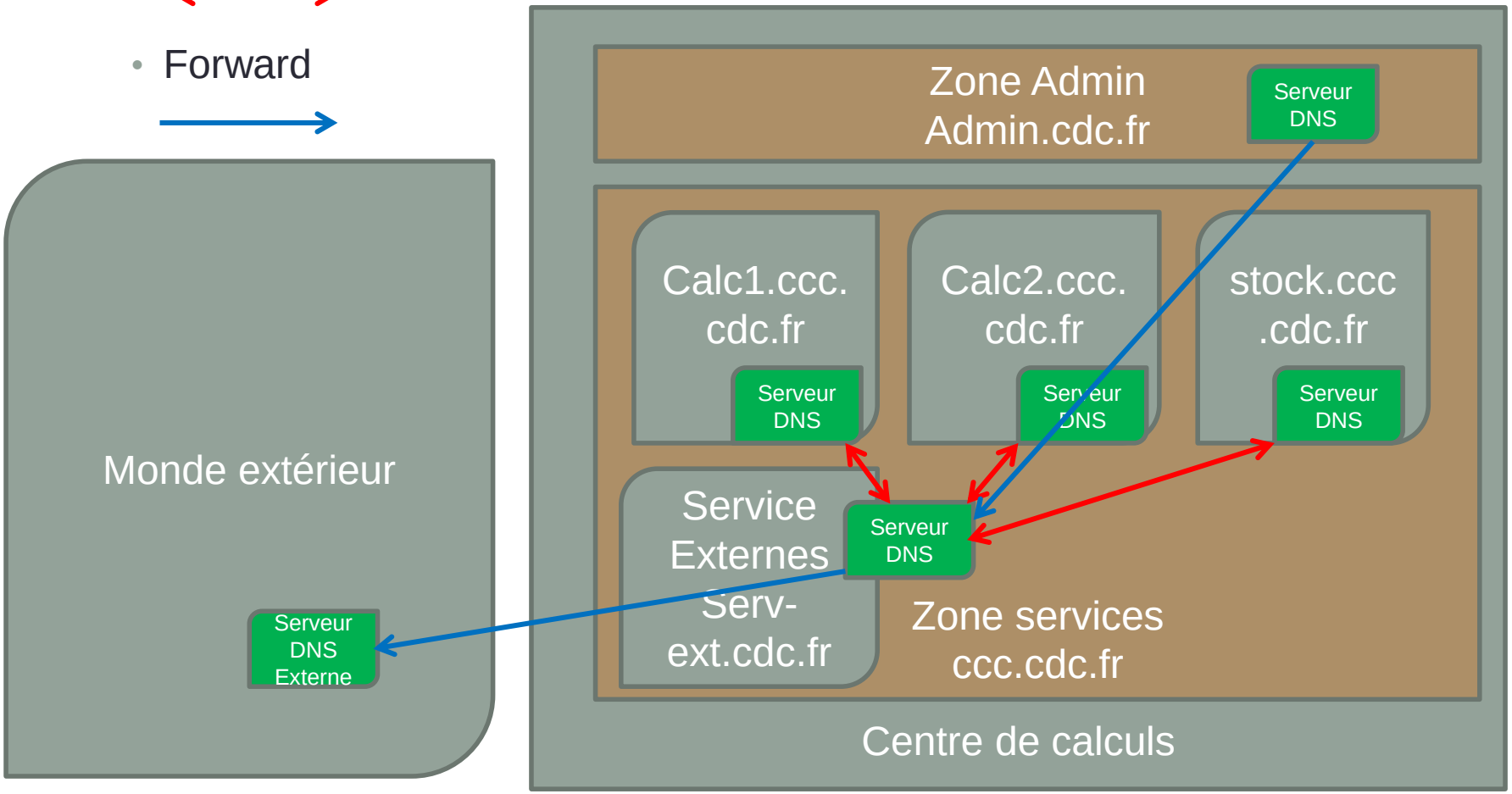

Zone CCC
ccc.cdc.fr
Adresses externes
Utilisateurs extérieurs
Zone Admin
Admin.cdc.fr
Calc1.ccc.cdc.fr
Calc2.ccc.cdc.fr
stock.ccc.cdc.fr
Service Externes Serv-ext.cdc.fr
Zone services
ccc.cdc.fr
Centre de calculs

Les zones et serveurs



Les zones et serveurs solution #1

- Replication zones
- Forward



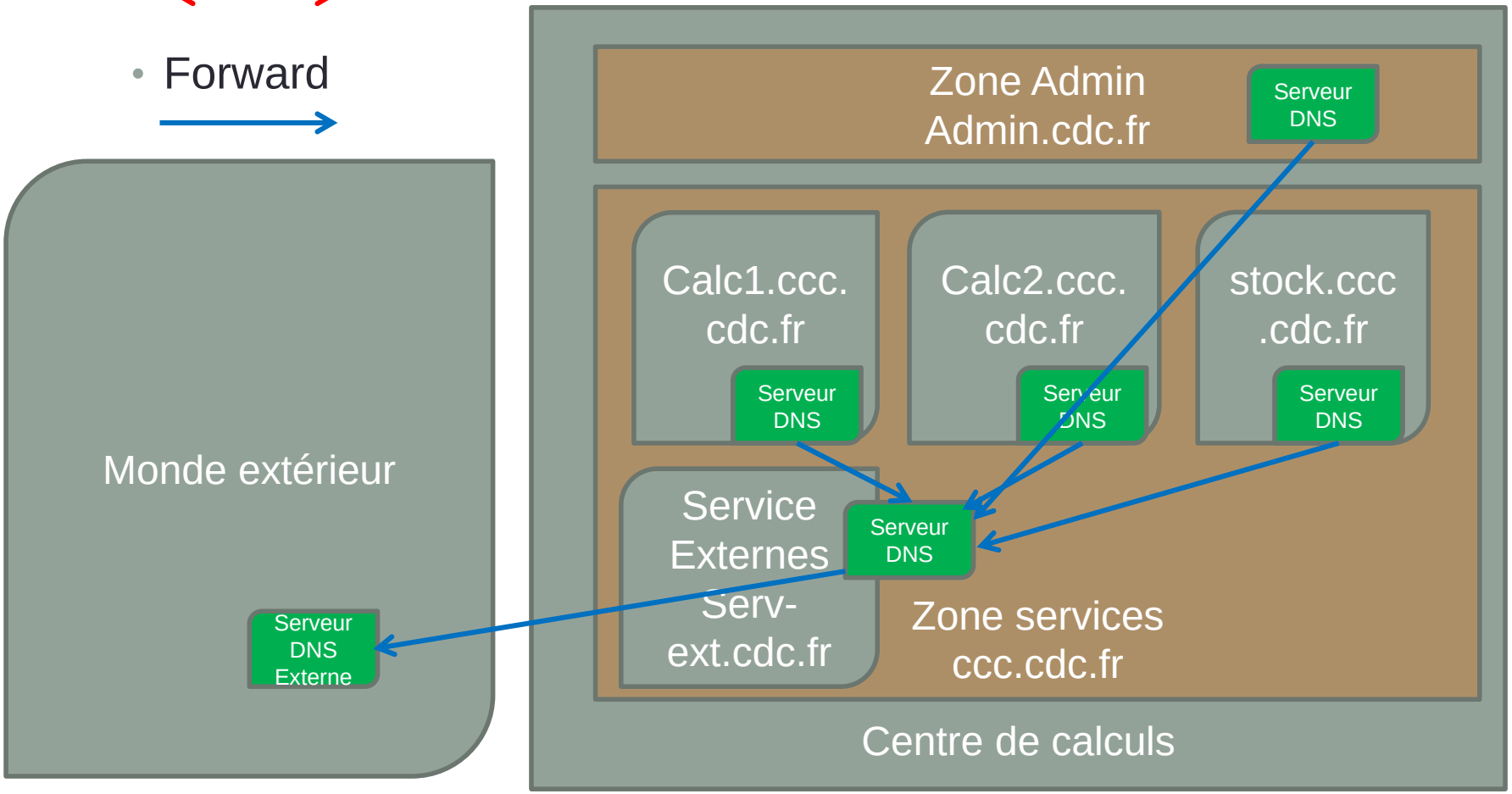
Les zones et serveurs solution #1

- Pour
  - Permet de séparer les périmètre
  - On peut déléguer entièrement une zone à un calculateur qui est autonome dessus.

- Contre
  - Complexité des réplications
  - Attention aux erreurs de configuration et aux tables qui expires

Les zones et serveurs solution #2

- Replication zones
- Forward



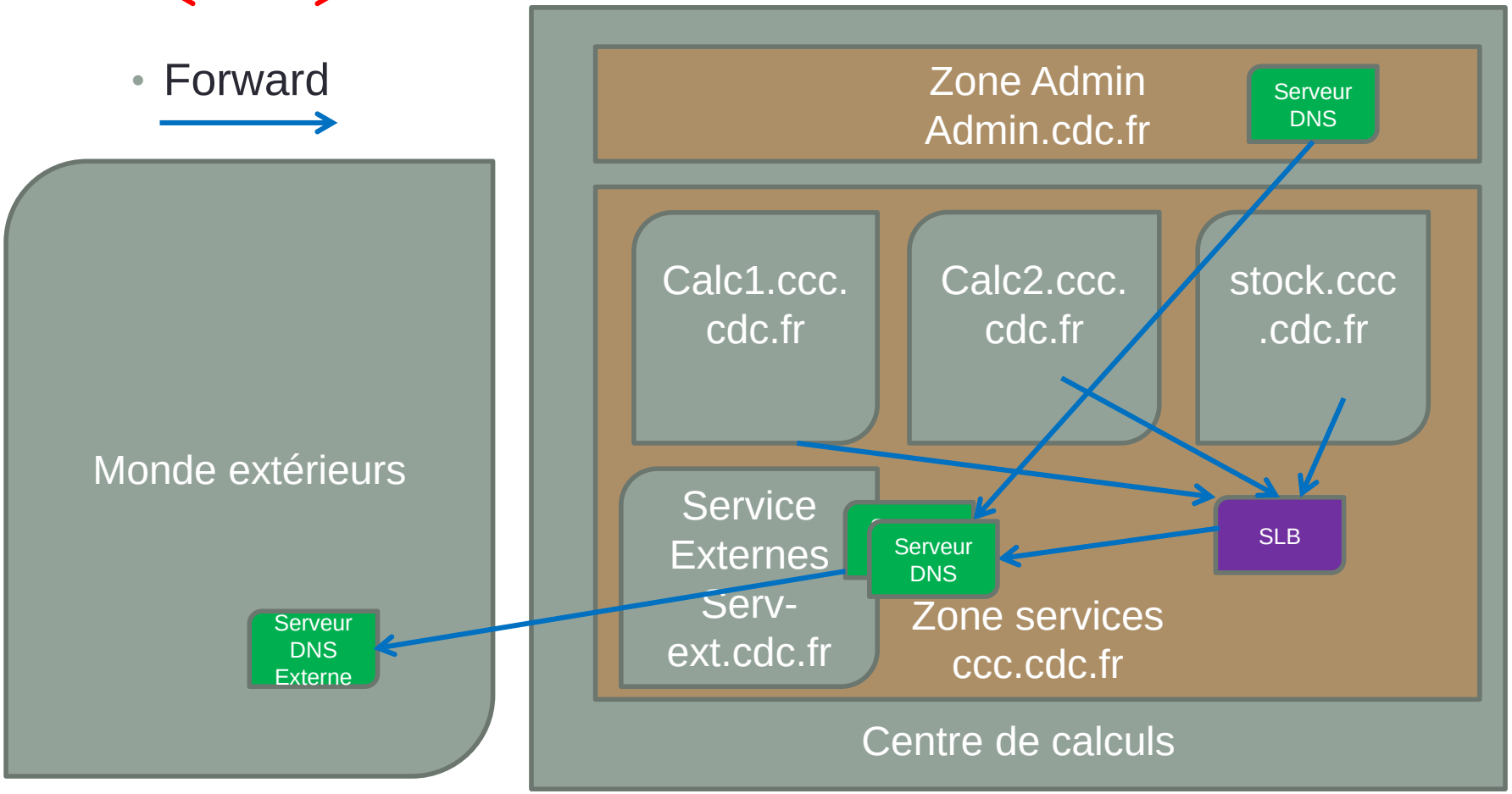
Les zones et serveurs solution #2

- Pour
  - Solution simple qui utilise le cache client et serveur
  - Choix facile de ce que l'on expose ou pas à l'extérieur

- Contre
  - Les déclarations de la zone sont potentiellement déclaré sur deux serveurs
  - Moyen niveau performance et haute disponibilité

Les zones et serveurs solution #3

- Replication zones
- Forward



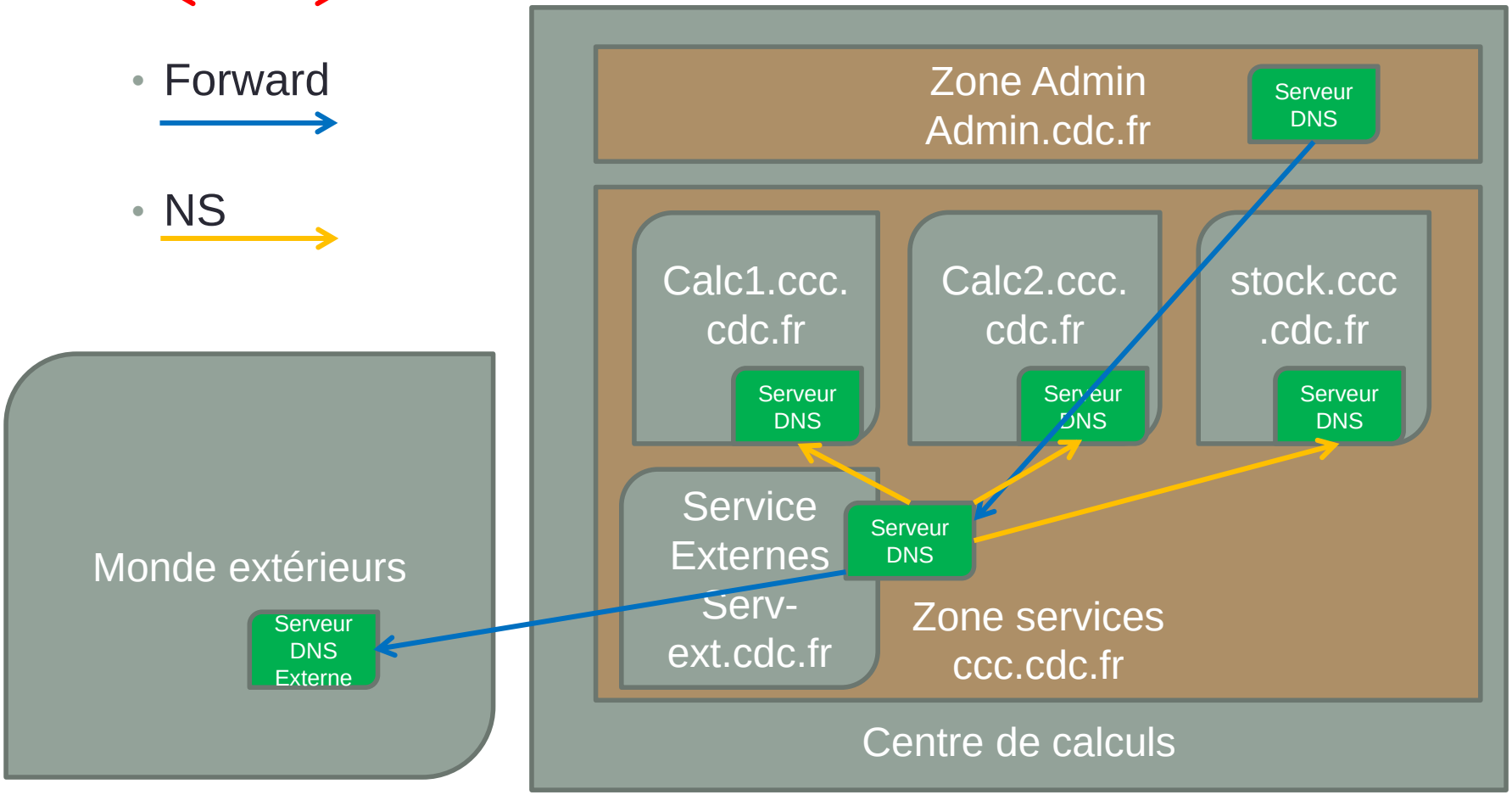
Les zones et serveurs solution #3

- Pour
  - Solution simple qui utilise le cache client et serveur
  - Répartir la charge entre plusieurs serveurs
  - Choix facile de ce que l'on expose ou pas à l'extérieur

- Contre
  - Les déclarations de la zone sont potentiellement déclaré sur deux serveurs
  - Meilleurs niveau performance et hautre dispo, mais ajouté un equipement et potentiellement un SPOF.

Les zones et serveurs solution #4

- Replication zones
- Forward
- NS



Les zones et serveurs solution #4

- Pour
  - Permet de séparer les périmètre
  - On peut déléguer entièrement une zone à un calculateur qui est autonome dessus.

- Contre
  - Complexité des réplications
  - Attention aux erreurs de configuration et aux tables qui expires
  - Beaucoup d’ouvertures de fluxs

Usage

- Activer le query log
  - Permet de détecter les logiciels qui essayent de se mettre à jour ou d’accéder à l’extérieur.
- Toujours surveiller la réplication des zones, une erreur est très vite arrivée.

Sécurité

- Attention a ce que l'on forward à l'exterieur
  - On ne veut pas exposé la topologie interne d'un centre de calcul
- Proxy over DNS
  - NSTX (disponible sur sourceforge) permet d'encapsuler de l'IP dans des requêtes DNS
- DNS ID Spoofing
  - Capture un paquet et on répond avant le destinataire
- DNS Cache Poisoning
  - Un serveur DNS répondu avec plusieurs d'informations fausses qui vont être mise en cache

QUESTIONS ?

Class ip

Classful addressing definition [edit]

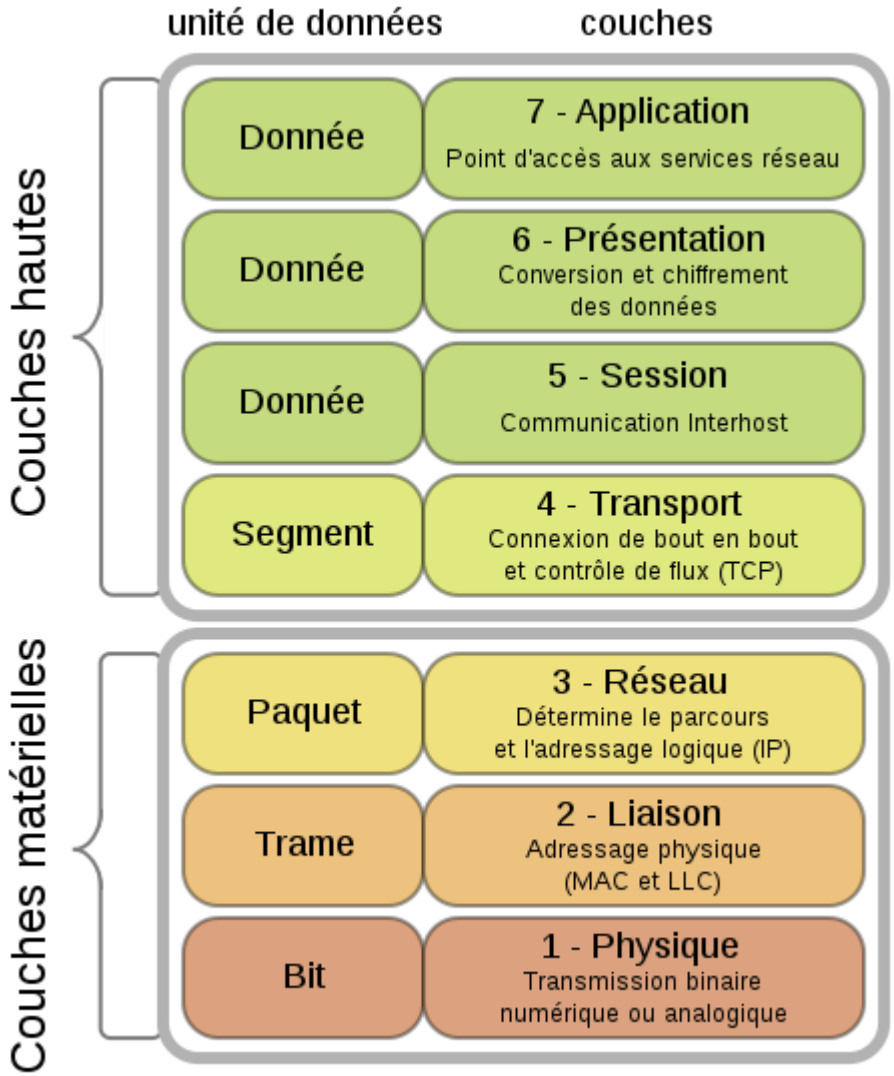
Class	Leading bits	Size of *network number* bit field	Size of *rest* bit field	Number of networks	Addresses per network	Total addresses in class	Start address	End address	Default subnet mask in dot-decimal notation	CIDR notation
Class A	0	8	24	128 (2^7)	16,777,216 (2^{24})	2,147,483,648 (2^{31})	0.0.0.0	127.255.255.255[a]	255.0.0.0	/8
Class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	1,073,741,824 (2^{30})	128.0.0.0	191.255.255.255	255.255.0.0	/16
Class C	110	24	8	2,097,152 (2^{21})	256 (2^8)	536,870,912 (2^{29})	192.0.0.0	223.255.255.255	255.255.255.0	/24
Class D (multicast)	1110	not defined	not defined	not defined	not defined	268,435,456 (2^{28})	224.0.0.0	239.255.255.255	not defined	not defined
Class E (reserved)	1111	not defined	not defined	not defined	not defined	268,435,456 (2^{28})	240.0.0.0	255.255.255.255	not defined	not defined

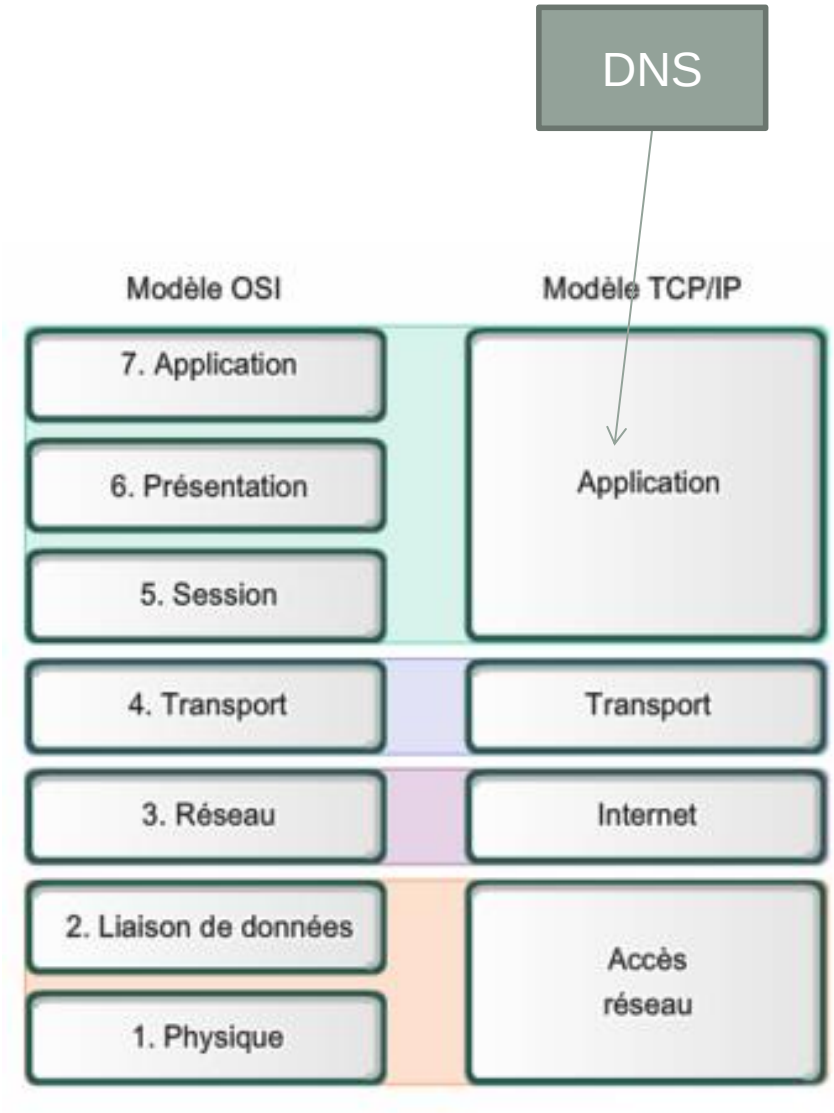
Non routable

Préfixe	Plage IP	Nombre d'adresses
10.0.0.0/8	10.0.0.0 – 10.255.255.255	2^{32-8} = 16 777 216
172.16.0.0/12	172.16.0.0 – 172.31.255.255	2^{32-12} = 1 048 576
192.168.0.0/16	192.168.0.0 – 192.168.255.255	2^{32-16} = 65 536

Source wikipedia

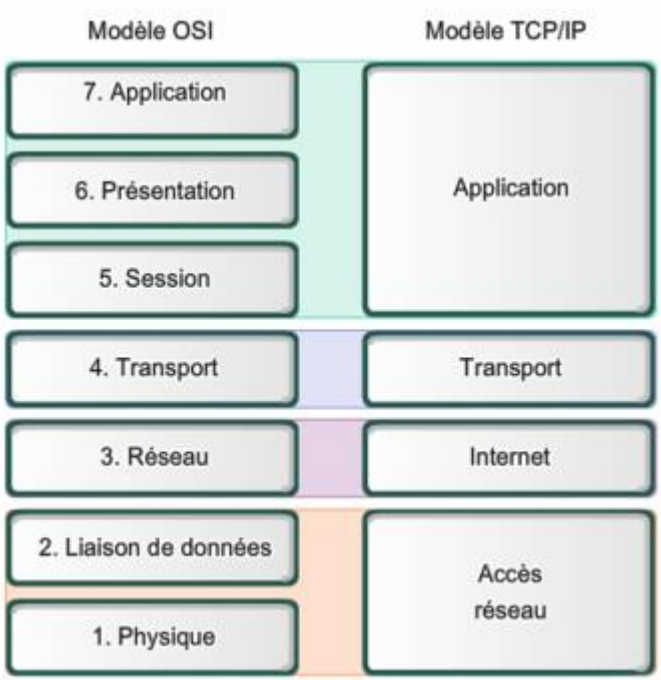
Modèle OSI





Source wikipedia

Load Balancer HLB/HLD



HLD/HLB

Routeur IP

Switch

Source wikipedia

Software Load Balancer

- Développement actif
  - **version 1.8** : multi-threading, HTTP/2, cache, on-the fly server addition/removal, seamless reloads, DNS SRV, hardware SSL engines, ...
  - **version 1.7** : added server hot reconfiguration, content processing agents, multi-type certs, ...
  - **version 1.6** : added DNS resolution support, HTTP connection multiplexing, full stick-table replication, stateless compression, ...
  - **version 1.5** : added SSL, IPv6, keep-alive, DDoS protection, ...
  - **version 1.4** : the most stable version for people who don't need SSL. Still provides client-side keep-alive

Software Load Balancer

- Plusieurs type de HA
  - **Layer 4 Load Balancing (IP)**
    - **Round Robin sur IP**
    - **Hash IP+PORT**
    - **…**
  - **Layer 7 Load Balancing (Applicatif)**
    - **Basé sur le contenu de la requête**
  - **Algorithmes**
    - **Round Robin**
    - **« Leastconn », le nœud avec le moins de connexions**
    - **Source**
    - **Health Check**
    - **…**

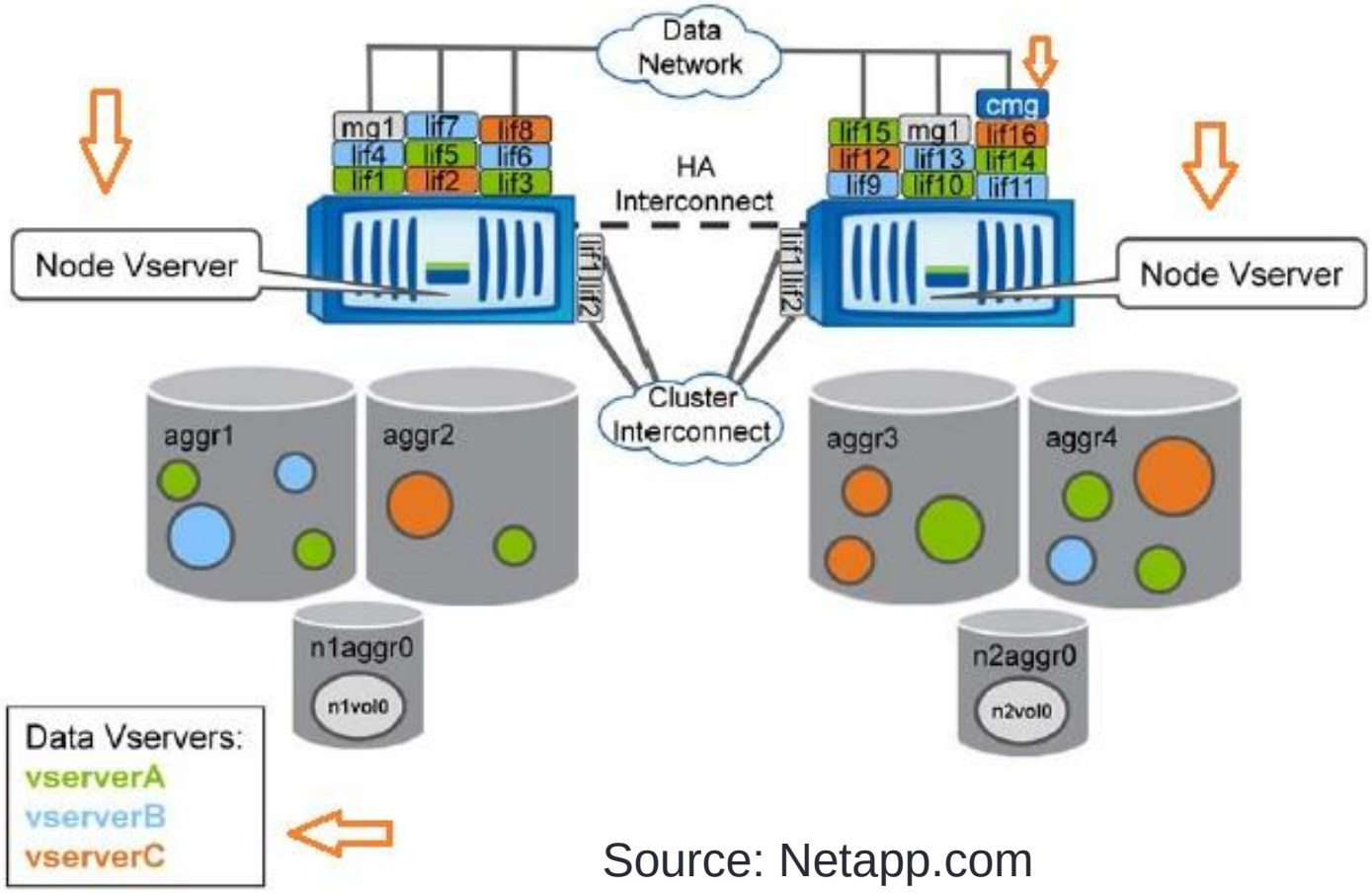
Round Robin pour le HPC ?

- On a 4 serveurs dédié physique avec des interfaces réseau
- Ces serveurs physiques hébergent des instances virtuelles
- Les instances virtuelles ont des interfaces réseau logiques qui peuvent être associées aux serveurs physiques

- L'instance virtuelle a donc 4 adresses d'accès qui peuvent être montées de façon aléatoire par les nœuds du calculateur et qui accèdent à la même ressource

Round Robin pour le HPC ?

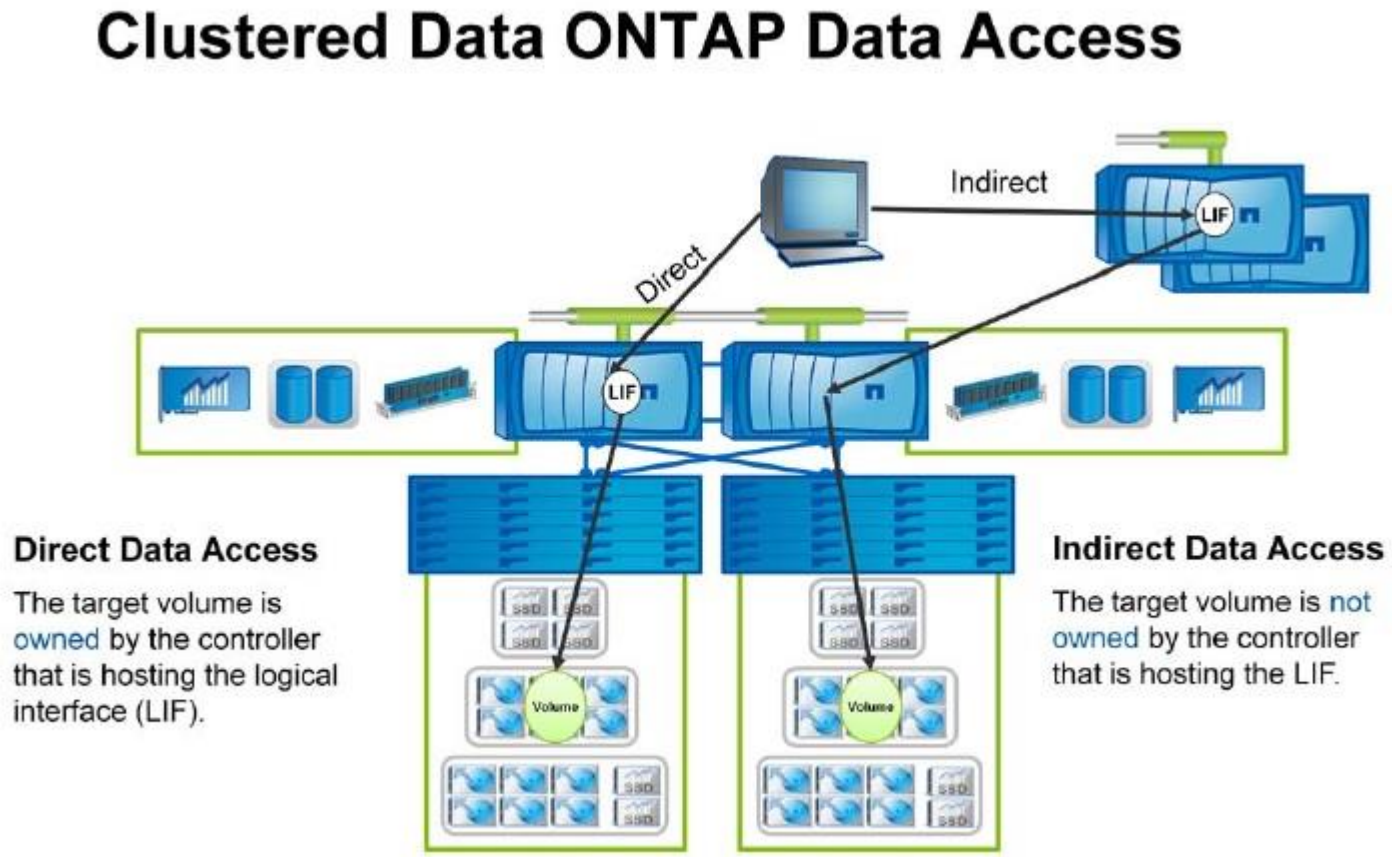
Avec une Appliance Netapp



Source: Netapp.com

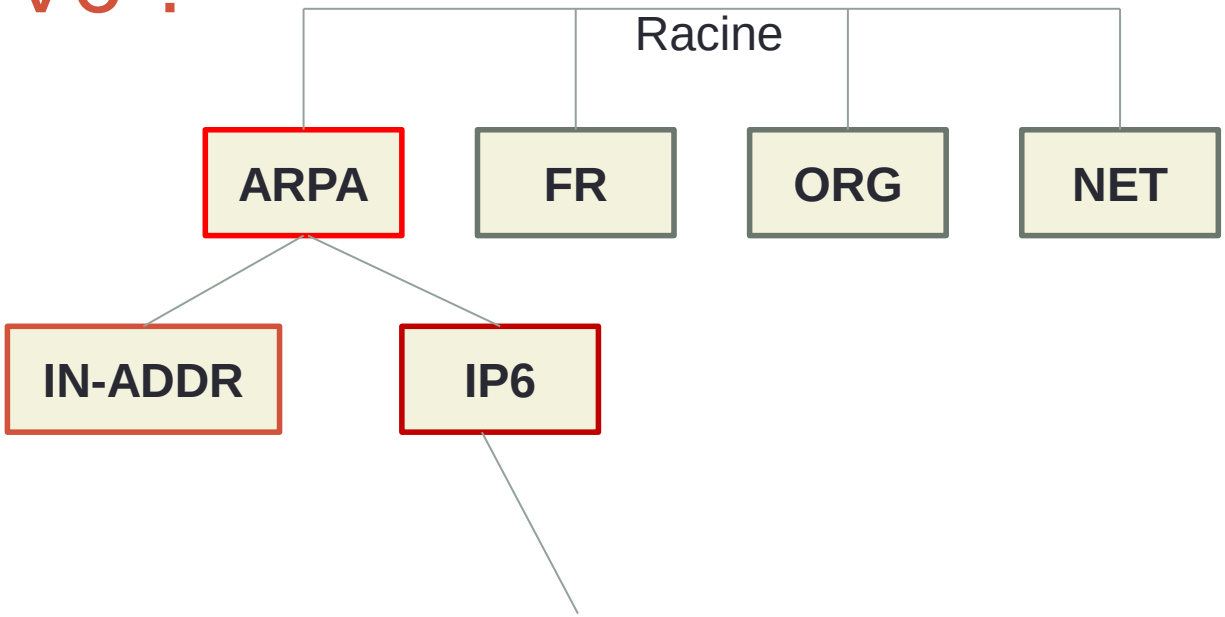
Round Robin pour le HPC ?

Avec une Appliance Netapp

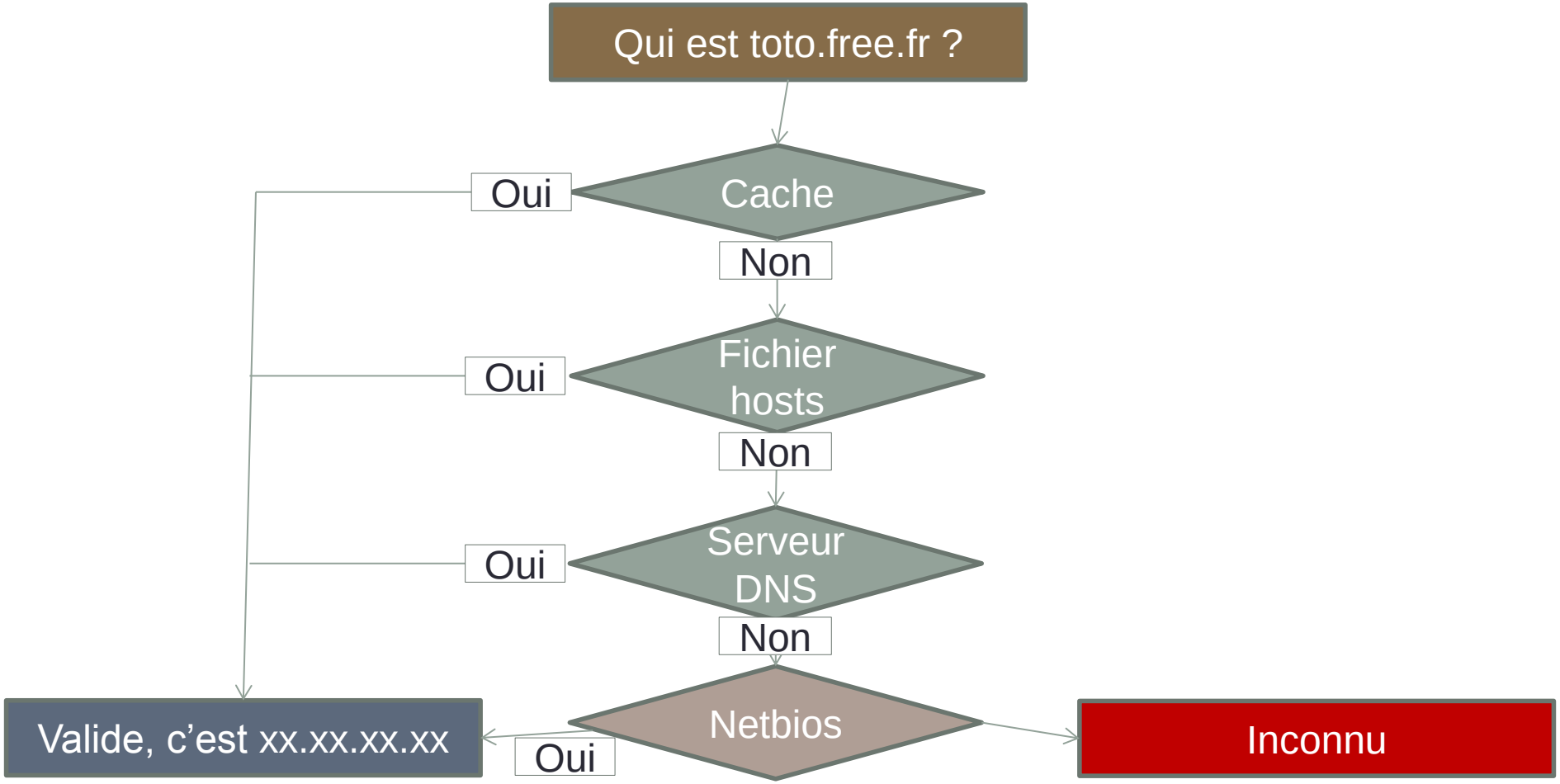


Source: Netapp.com

IPV6 ?



Fonctionnement par ‘défaut’ Chez Bill

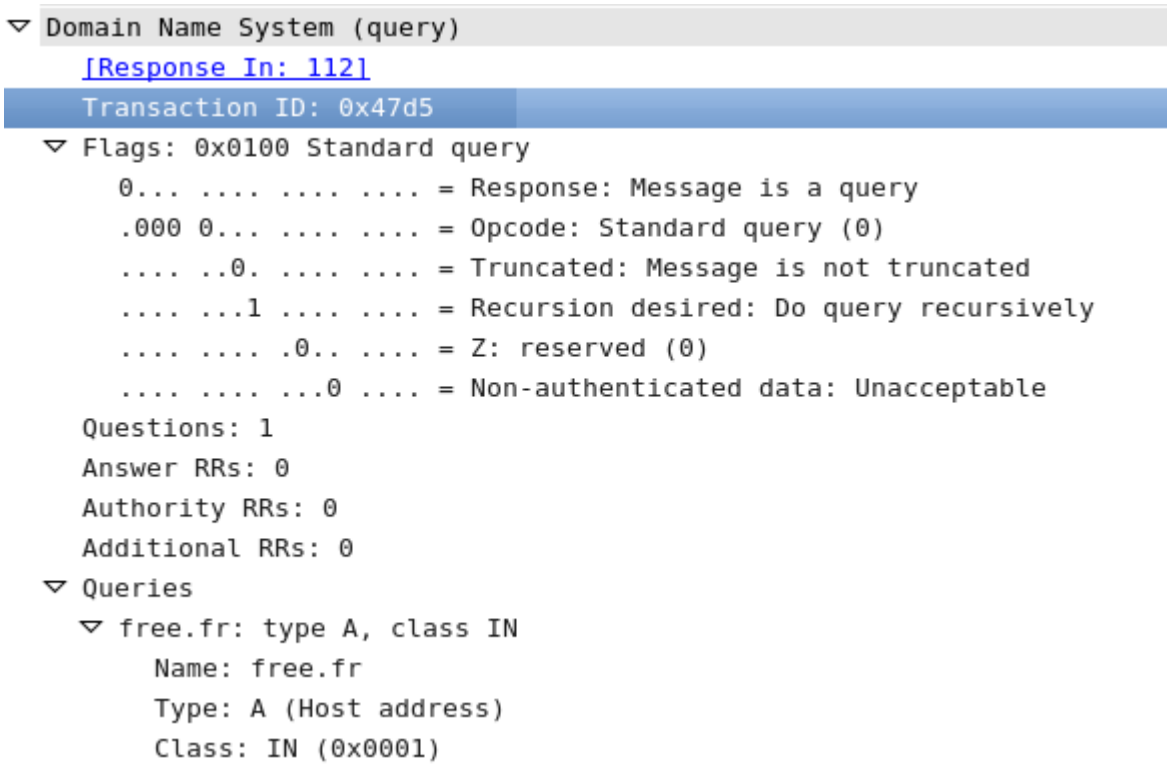


Protocole

#Nslookup free.fr
Server:172.X.X.X
Address:172.X.X.X#53

Non-authoritative answer:
Name:free.fr
Address: 212.27.48.10

Protocole


Domain Name System (query)
[Response In: 112]
Transaction ID: 0x47d5
Flags: 0x0100 Standard query
0... .... = Response: Message is a query
.000 0... .... = Opcode: Standard query (0)
.... ..0. .... = Truncated: Message is not truncated
....1 .... = Recursion desired: Do query recursively
.... .0.. .... = Z: reserved (0)
....0 .... = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
free.fr: type A, class IN
Name: free.fr
Type: A (Host address)
Class: IN (0x0001)

Protocole

```
▽ Domain Name System (response)
    [Request In: 110]
    [Time: 0.000686000 seconds]
    Transaction ID: 0x47d5
  ▽ Flags: 0x8180 Standard query response, No error
      1... .... .... .... = Response: Message is a response
      .000 0... .... .... = Opcode: Standard query (0)
      .... .0.. .... .... = Authoritative: Server is not an authority for domain
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... 1... .... = Recursion available: Server can do recursive queries
      .... .... .0.. .... = Z: reserved (0)
      .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
      .... .... ...0 .... = Non-authenticated data: Unacceptable
      .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 2
    Additional RRs: 4
  ▽ Queries
    ▽ free.fr: type A, class IN
        Name: free.fr
        Type: A (Host address)
        Class: IN (0x0001)
  ▽ Answers
    ▷ free.fr: type A, class IN, addr 212.27.48.10
  ▽ Authoritative nameservers
    ▷ free.fr: type NS, class IN, ns freens1-g20.free.fr
    ▷ free.fr: type NS, class IN, ns freens2-g20.free.fr
  ▽ Additional records
    ▷ freens2-g20.free.fr: type A, class IN, addr 212.27.60.20
    ▷ freens2-g20.free.fr: type AAAA, class IN, addr 2a01:e0c:1:1599::23
    ▷ freens1-g20.free.fr: type A, class IN, addr 212.27.60.19
    ▷ freens1-g20.free.fr: type AAAA, class IN, addr 2a01:e0c:1:1599::22
```