DNS

Gaétan Richard
gaetan.richard@unicaen.fr

M1 Informatique

I. Base du DNS

Contenu du DNS

Contenu : Le DNS contient :

- Des informations sur le gestionnaire du domaine (champ *SOA*) ;
- Des serveurs de nom de domaine (champ *NS*) ;
- Des adresses IPv4 correspondant au nom des machines (champ *A*) ;
- Des adresses IPv6 (champ *AAAA*) ;
- Des alias (champ *CNAME*) ;
- Des noms correspondant à des adresses (champ *PTR*) ;
- Des serveurs de mail (champ *MX*) ;
- …

Principe du DNS

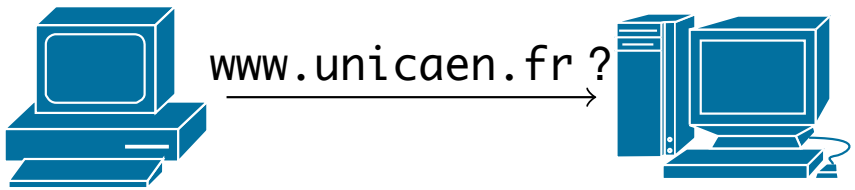
dns

dns racine

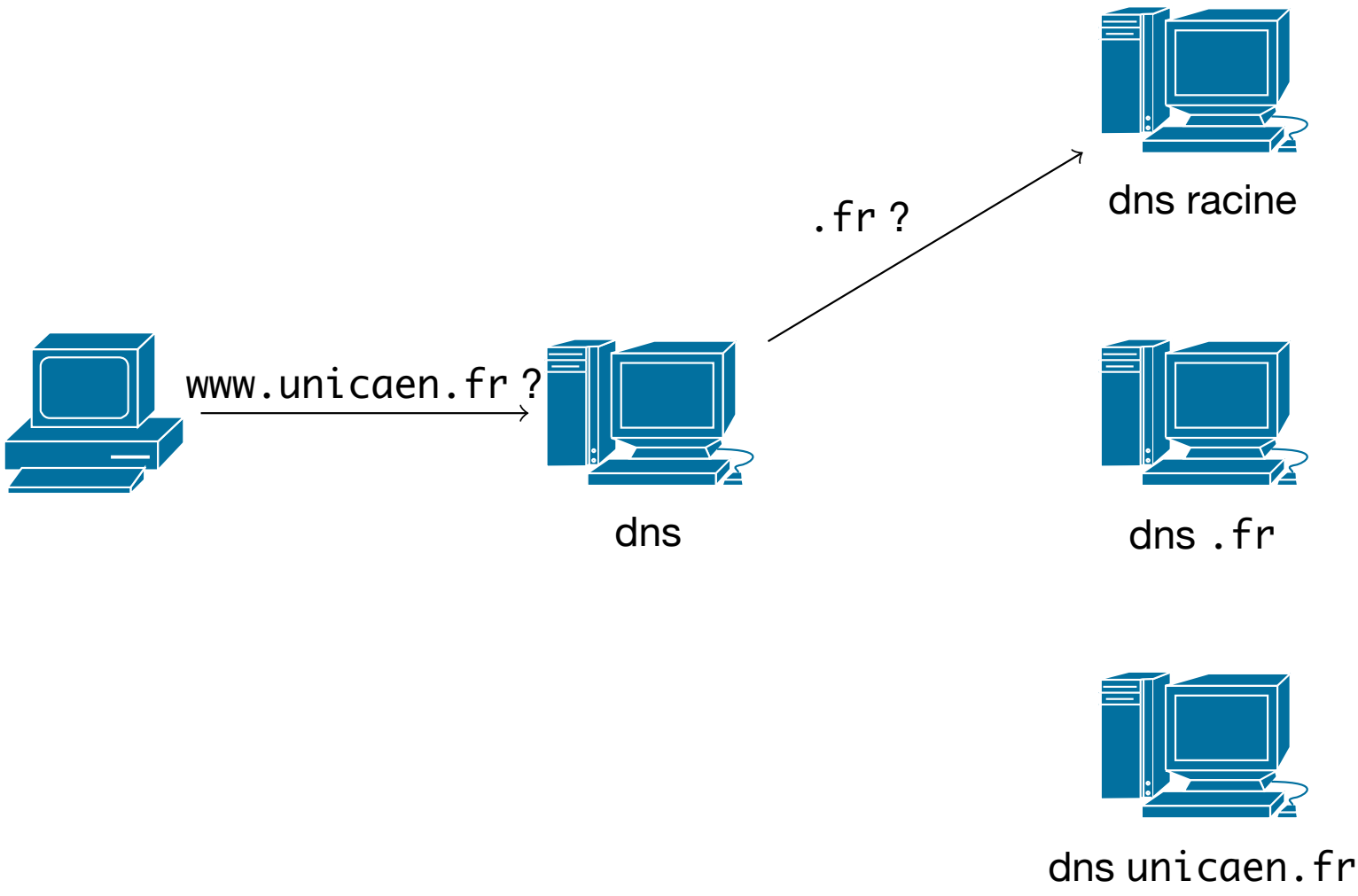
dns `.fr`

dns `unicaen.fr`

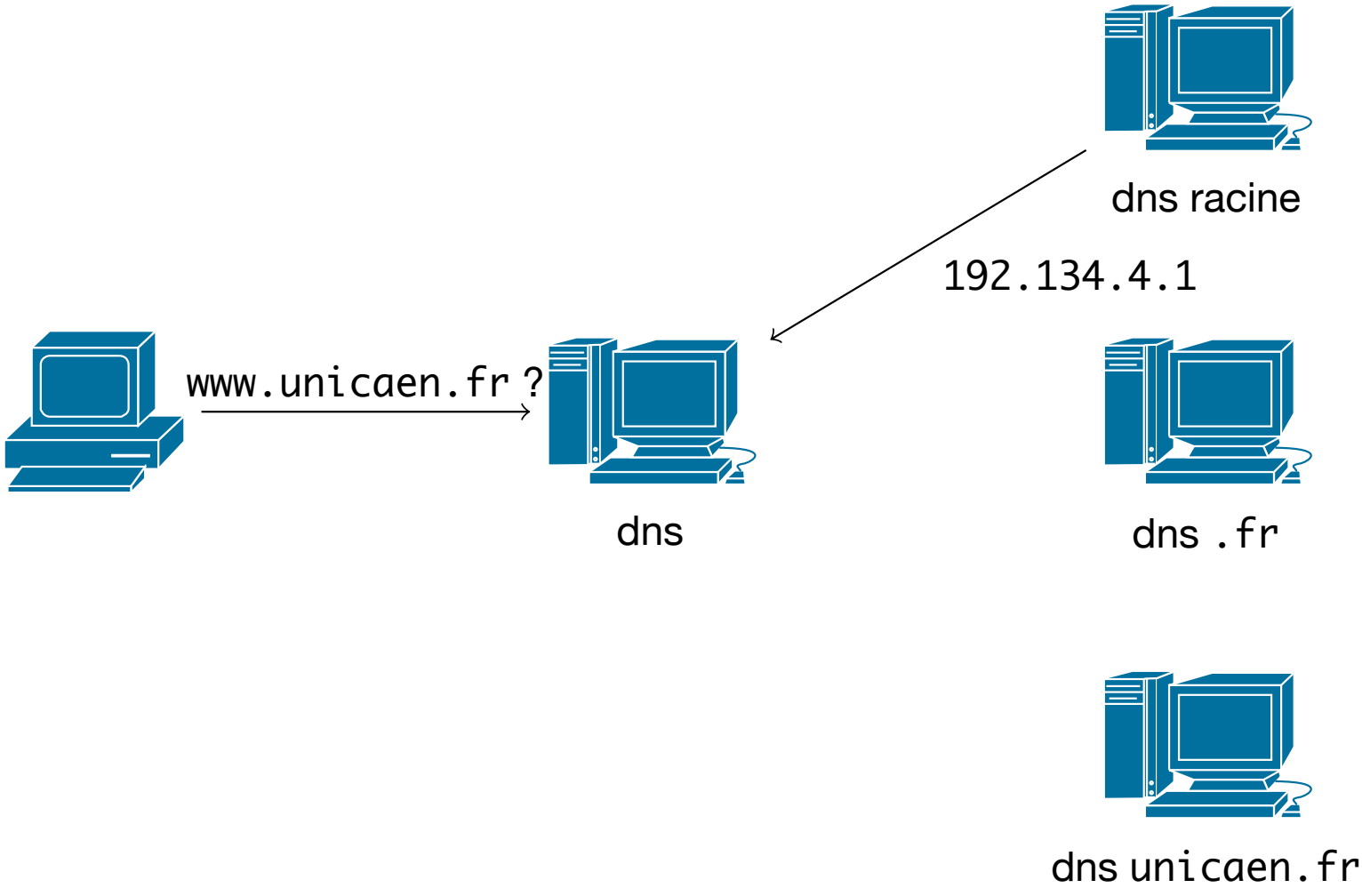
Principe du DNS



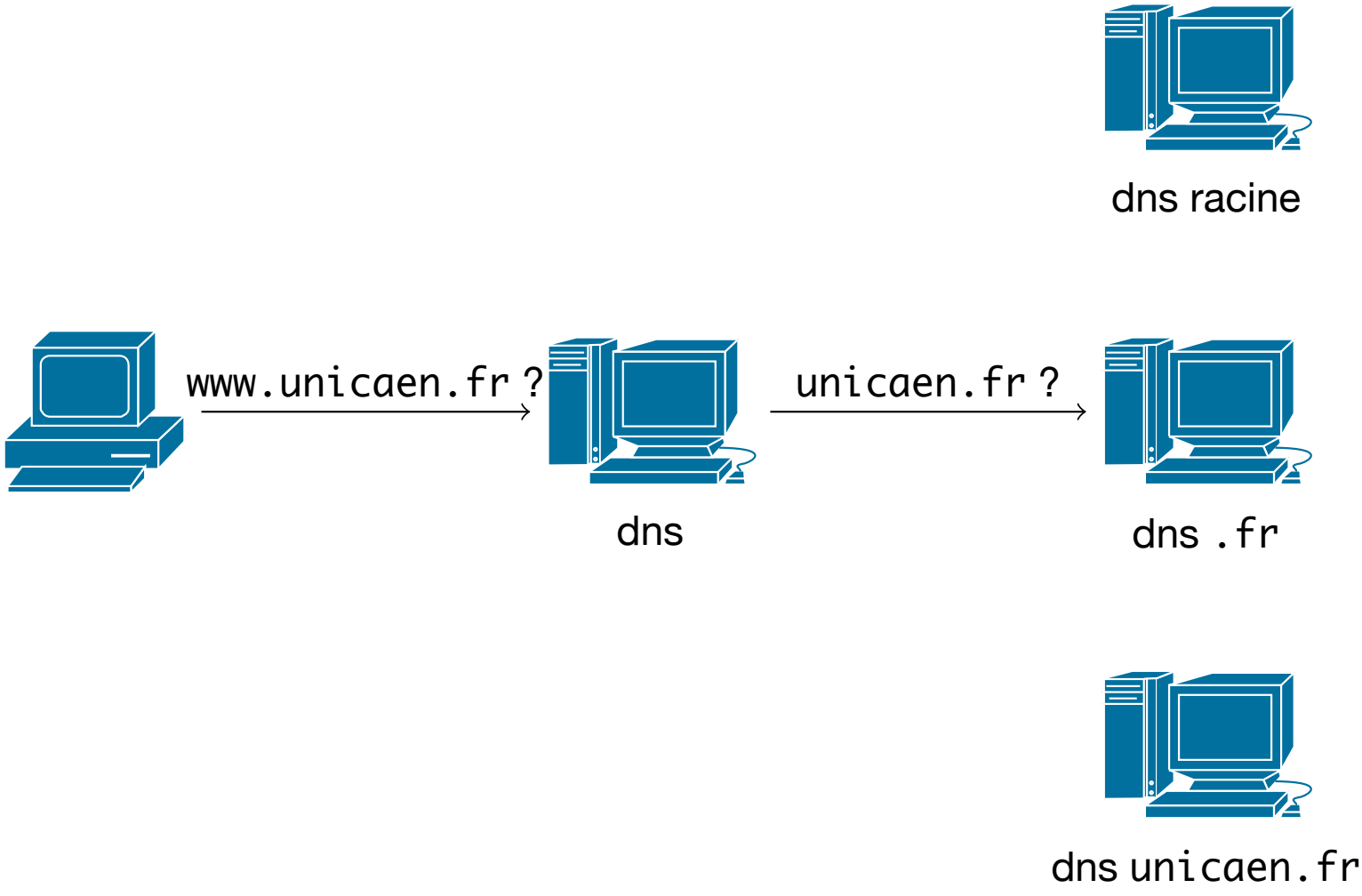
Principe du DNS



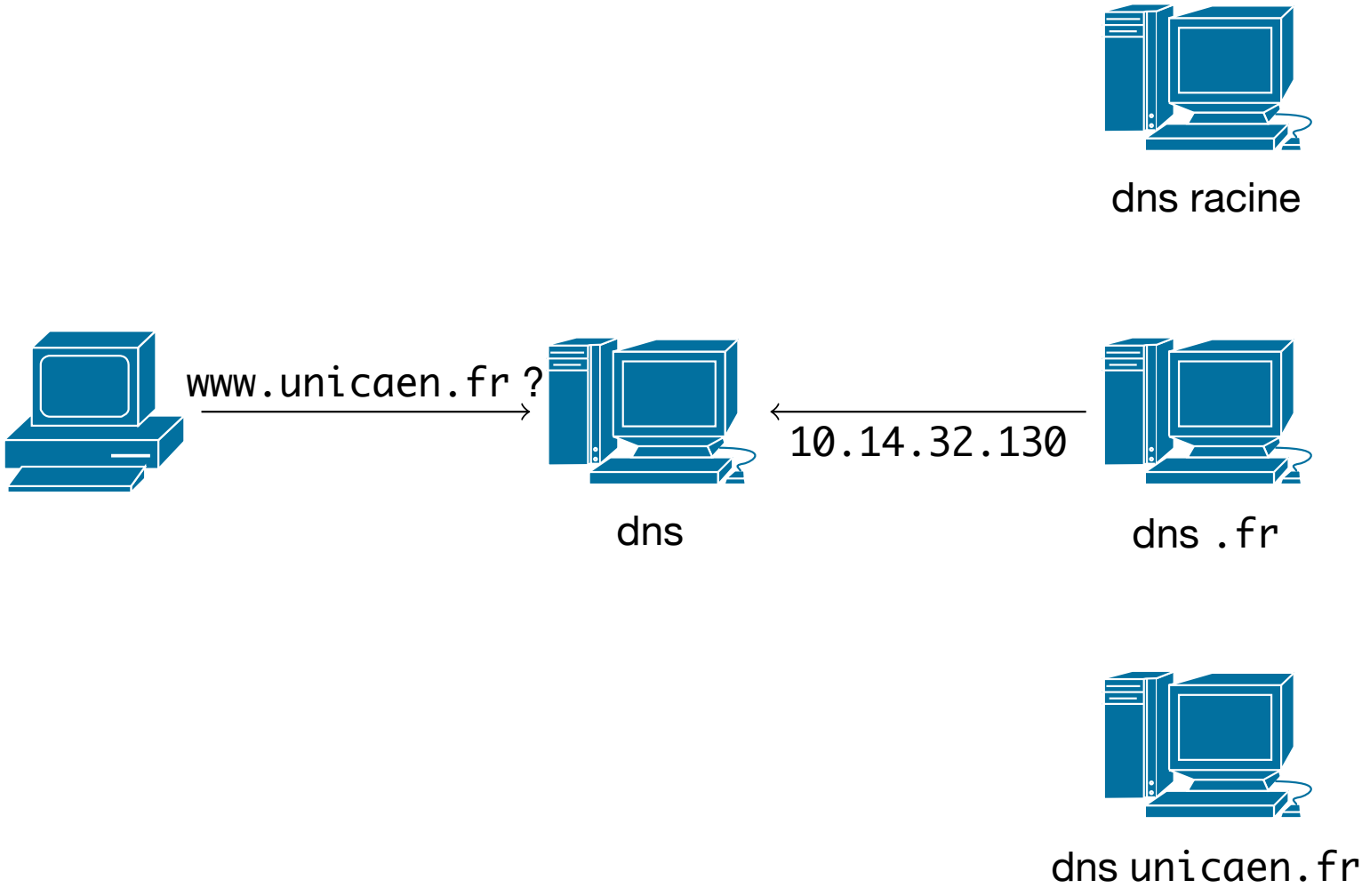
Principe du DNS



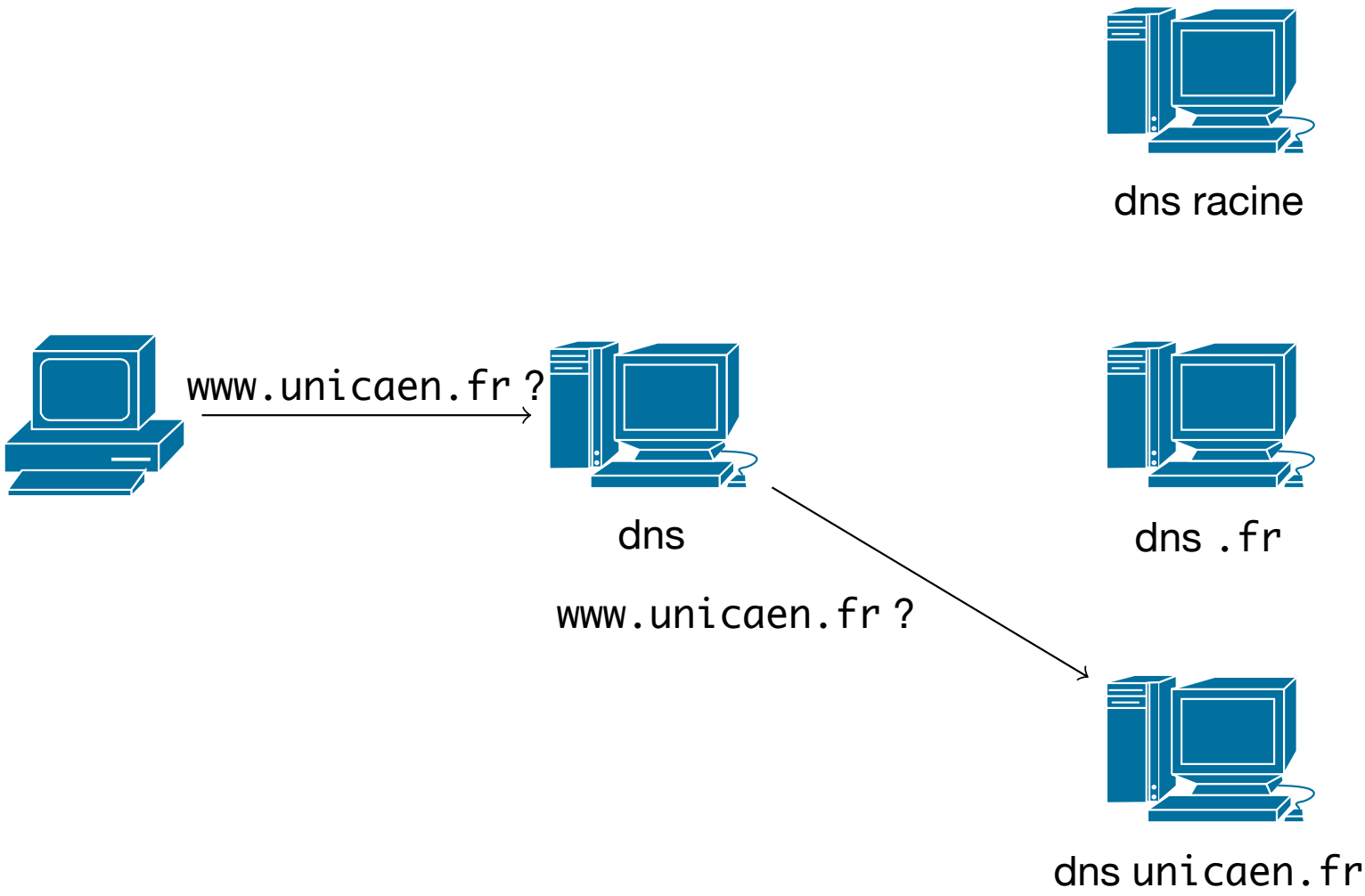
Principe du DNS



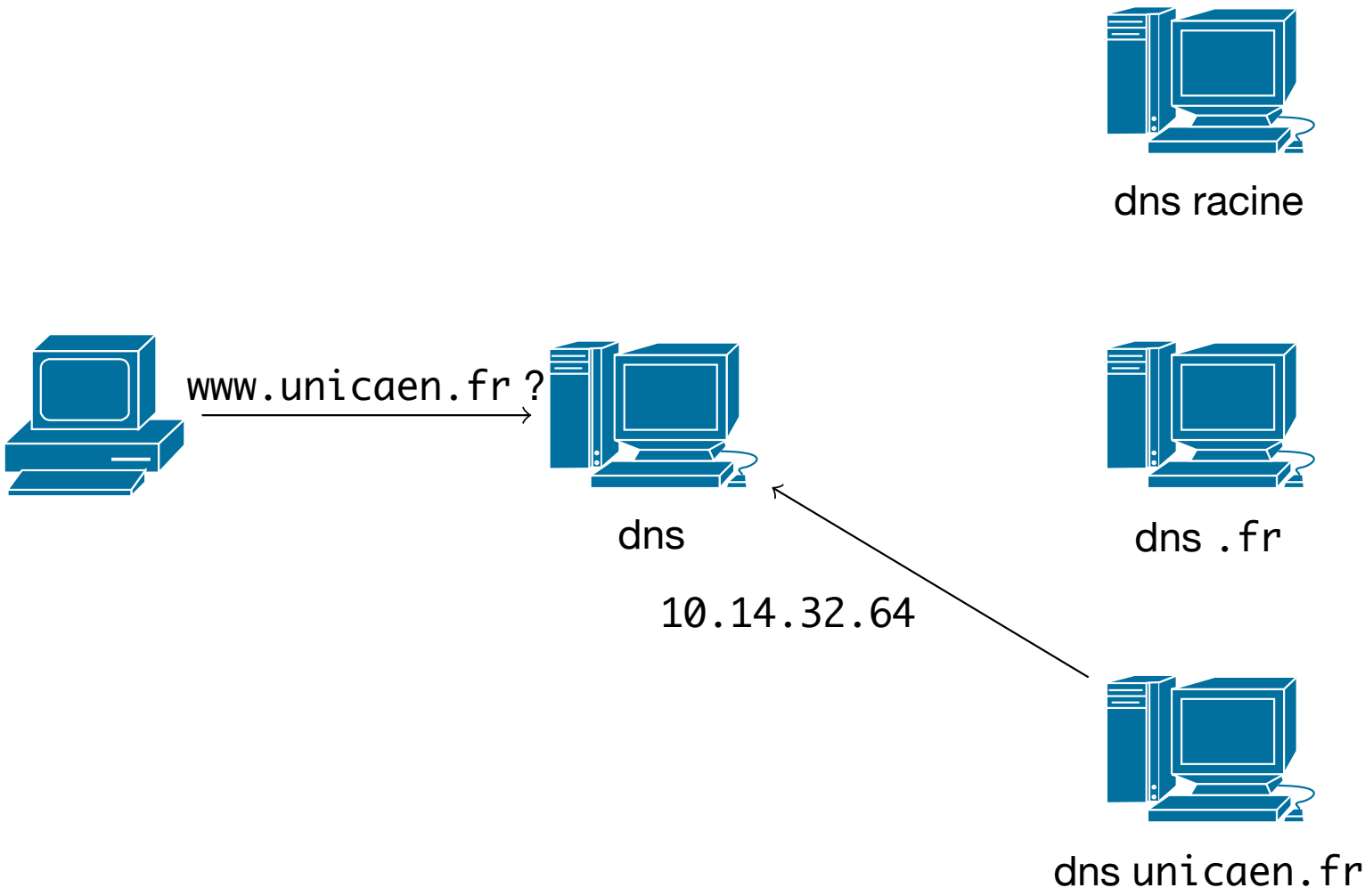
Principe du DNS



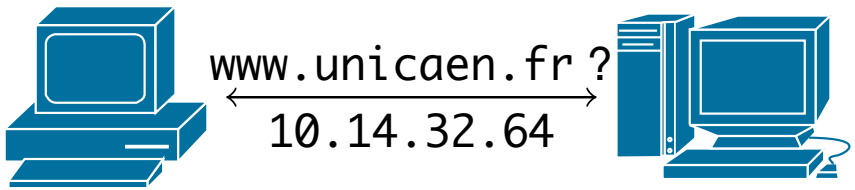
Principe du DNS



Principe du DNS



Principe du DNS



Configuration d'un DNS

Principe : Le logiciel *bind* se configure à l'aide d'un fichier global de configuration `/etc/bind/named.conf` et à l'aide de fichiers contenant les informations (de la forme `/etc/bind/db.x`).

Exemple :

```
TTL    604800
@       IN      SOA     zoneZZ.tp.info.unicaen.fr. root.zoneZZ.tp.info.unicaen.fr. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
@       IN      NS      dns
@       IN      MX      m3

dns     IN    A     192.168.1.2
dns      IN    AAAA    2001 :660 :7101 :ZZ :1 ::2
m1     IN    A     192.168.1.1
m2     IN    A     192.168.1.2
m3     IN    A     192.168.1.3
m4      IN      CNAME   m3
```

Configuration d'un DNS

Principe : Le logiciel *bind* se configure à l'aide d'un fichier global de configuration `/etc/bind/named.conf` et à l'aide de fichiers contenant les informations (de la forme `/etc/bind/db.x`).

Exemple :

```
@       IN      SOA     zoneZZ.tp.info.unicaen.fr. root.zoneZZ.tp.info.unicaen.fr.
...

@    IN    NS    dns.zoneZZ.tp.info.unicaen.fr.
1.1    IN    PTR    m1.zoneZZ.tp.info.unicaen.fr.
2.1    IN    PTR    m2.zoneZZ.tp.info.unicaen.fr.
3.1     IN    PTR    m3.zoneZZ.tp.info.unicaen.fr.

...
```

En cas d'erreur

Attention : En cas d'erreur dans un des fichiers de données, le serveur *dns* "saute" ce fichier et ne le marque que dans le fichier de log `/var/log/daemon.log`.

Bonne pratique : Créer un script qui relance le serveur puis affiche la fin du fichier de log pour vérifier le bon déroulement.

Cache : Une donnée erronée peut persister plusieurs heures dans le réseau.

2. Problèmes de DNS

UDP *vs* TCP

Attention : Certaines requêtes (listing ou nom très long) nécessitent le protocole TCP au lieu de l'habituel UDP.
Ceci sert à éviter les attaques DOS par rebond.

Filtrage : le DNS du FAI est le point actuellement privilégié pour effectuer du filtrage administratif (compromis coût / efficacité / effets indésirables).

Redondance

Importance : le DNS est un service critique puisque quasi tous les autres services en dépendent.

Redondance : Il est possible de créer un serveur dns redondant à l'aide du mode maître-esclave.
Très souvent, ce serveur est mis sur un autre site géographiquement séparé.

Faille du dns

Kaminsky : une faille critique découverte en 2005.

Solution : DNSSEC authentification des requêtes DNS.

3. DNS et mail

Authentification du mail

SPF *Sender Policy Framework* est un protocole de vérification du nom de domaine de l'expéditeur d'un courrier électronique.

Il utilise le champ TXT du dns pour indiquer quels serveurs sont autorisés à envoyer des mails du domaine.

Il nécessite que le domaine de réception est activé son support et que les utilisateurs du domaine initial aient configuré correctement leur serveur smpt (et utilisent une authentification).

Exemple de SPF

host -t TXT ietf.org :

```
ietf.org descriptive text ”v=spf1 ip4 :12.22.58.0/24
ip4 :64.170.98.0/24 ip4 :4.31.198.32/27
ip4 :209.208.19.192/27 ip4 :72.167.123.204
ip6 :2001 :1890 :123a ::/56
ip6 :2001 :1890 :126c ::/56
ip6 :2001 :1900 :3001 :0011 ::0/64
ip6 :2607 :f170 :8000 :1500 ::0/64 -all”
```