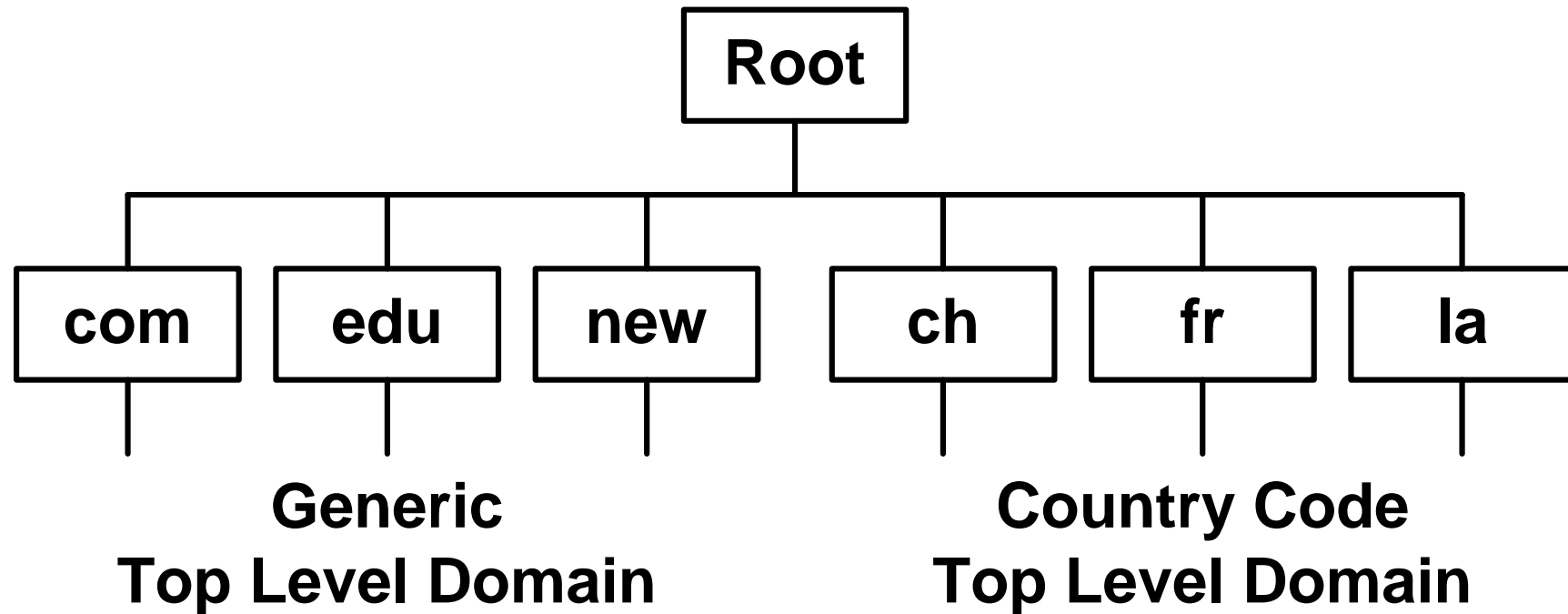


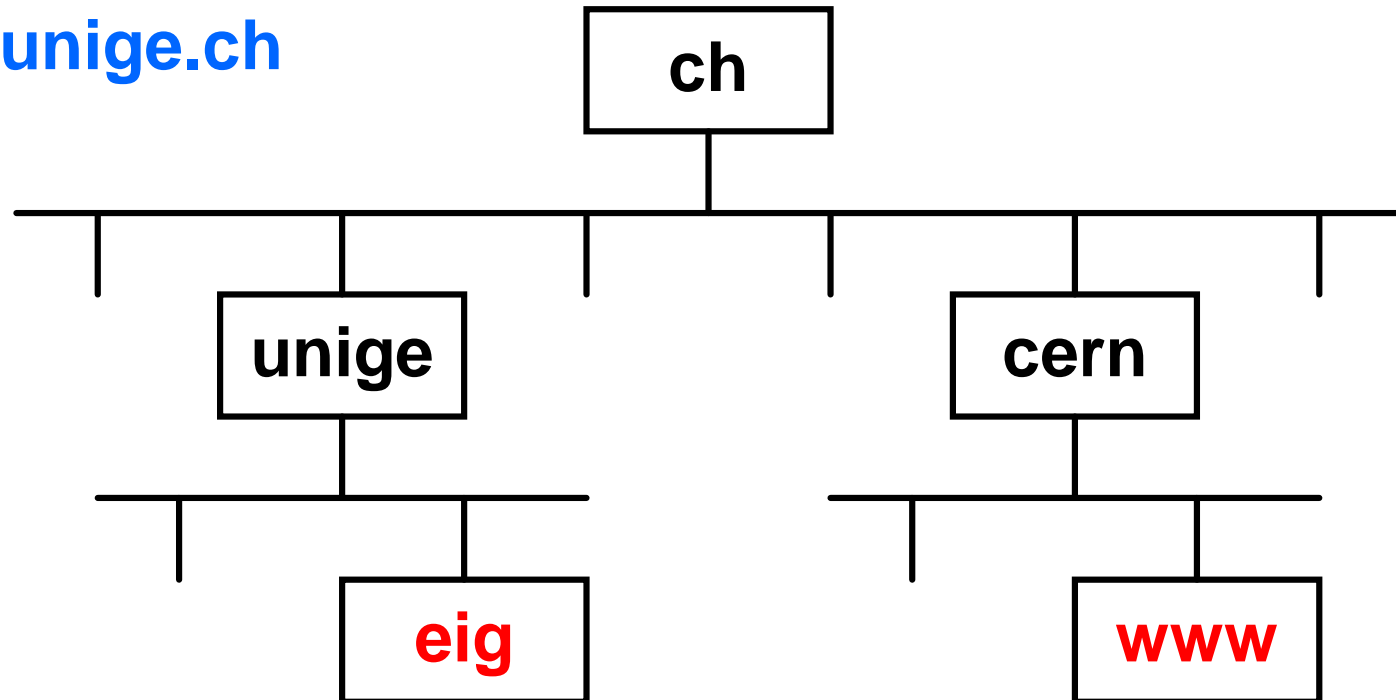
- **Rappel**
- **Cache du client**
- **Zone et types de serveurs**
- **Configuration du labo**
- **Réponses autoritaires, requêtes itératives et récursives**
- **nslookup**

- Le *Domain Name System* est une base de données distribuée

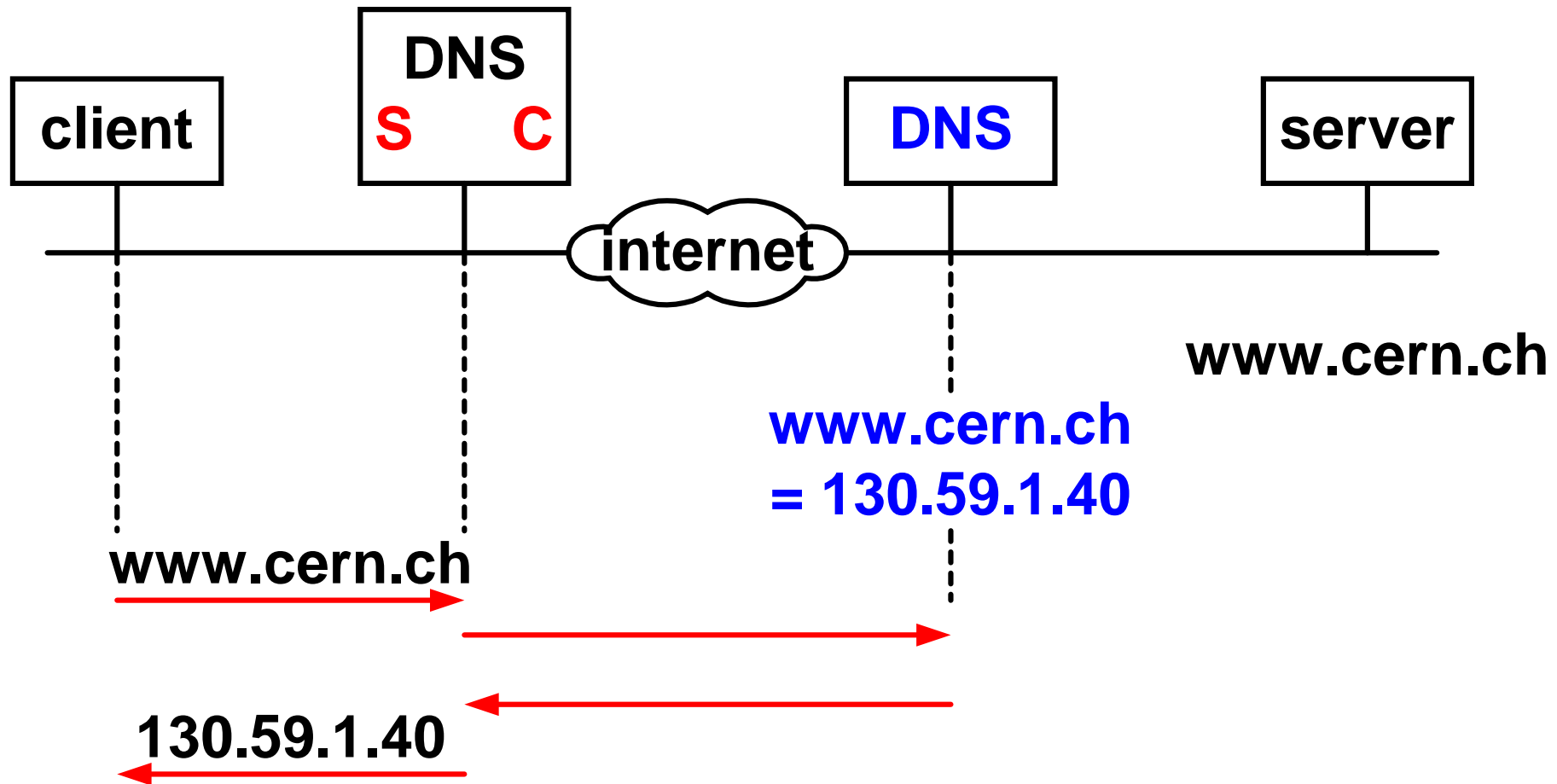


DNS : FQDN est unique

- FQDN : **host**.domain
www.cern.ch
eig.unige.ch



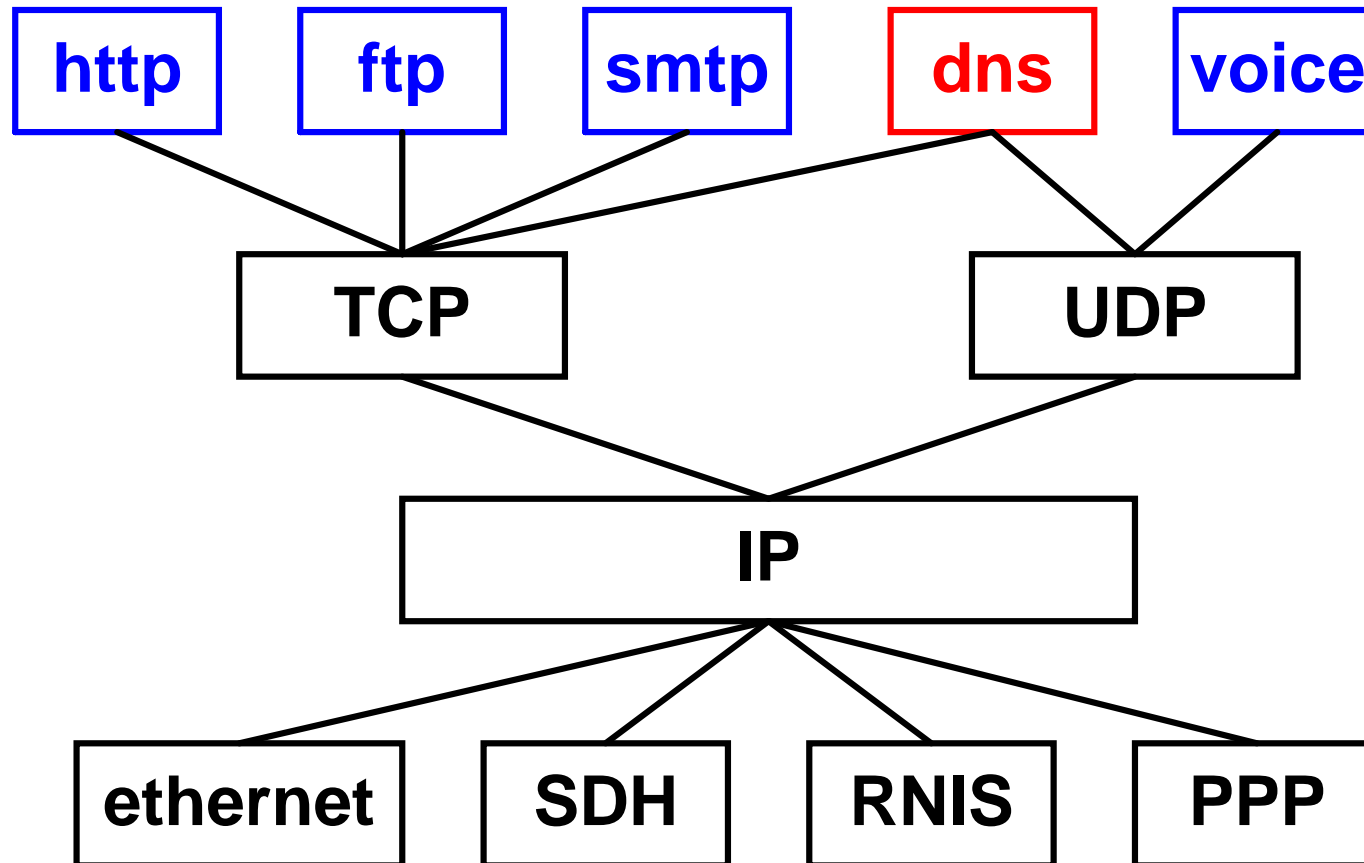
- FQDN est unique
- Unige peut déléguer l'autorité à **td.unige.ch**



- Echange du type client (*resolver*) – serveur (*name server*)
- Mémoire cache dans client et serveurs DNS

DNS : caractéristiques

- **Gestion décentralisée**
Administration des ressources locales (serveurs, ...)
Accès à toutes les ressources d'*internet*
Fonction vitale : plus de DNS → panne générale
- **Systeme de mémoire cache (durée de vie)**
Mémoriser les résolutions précédentes
Gain de temps
Eviter les surcharge inutile du réseau
Tolère des pannes DNS
- **Modifications pas instantanées**



- **Resolver** accessible applications IE, ftp, ...



- `ipconfig /displaydns`
`localhost 127.0.0.1`

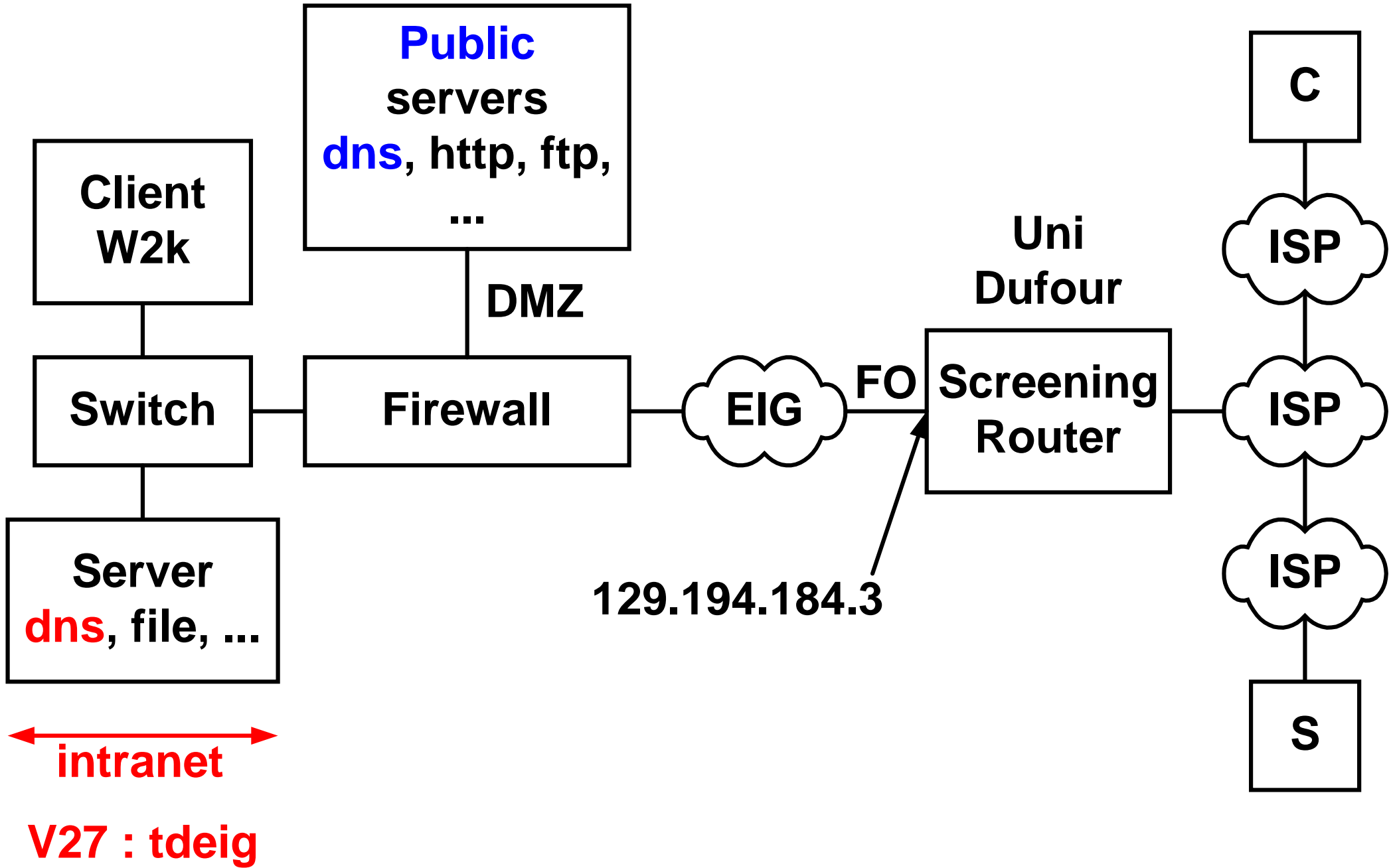
affiche le contenu du cache

- `ipconfig /flushdns`

efface le cache

DNS : définitions

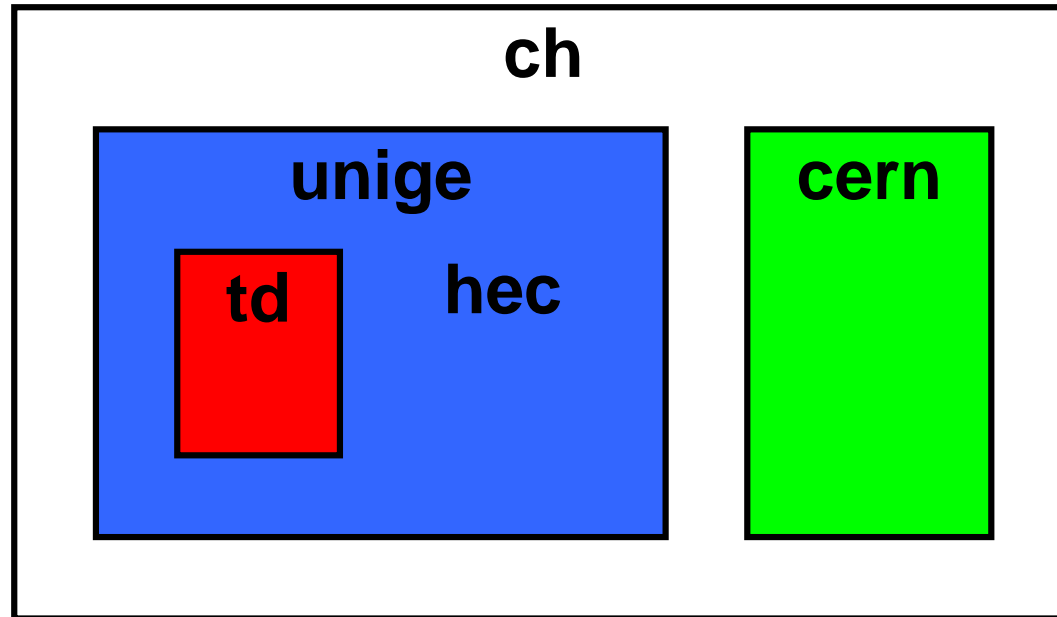
- ***Naming structure*** espace de noms hiérarchique
Root domain – arborescence
Full Qualified Domain Name (FQDN)
- ***Public namespace***
unige.ch cern.ch
- ***Private namespace***
eig eivd company



DNS : types de serveurs

- **Zone** : sous-arbre administré séparément
- **Primary Name Server**
possède une zone avec accès en lecture et écriture
- **Secondary Name Server** facultatif
possède une zone avec accès en lecture
- **Primary & secondary are authoritative**
- **Caching only Name Server**

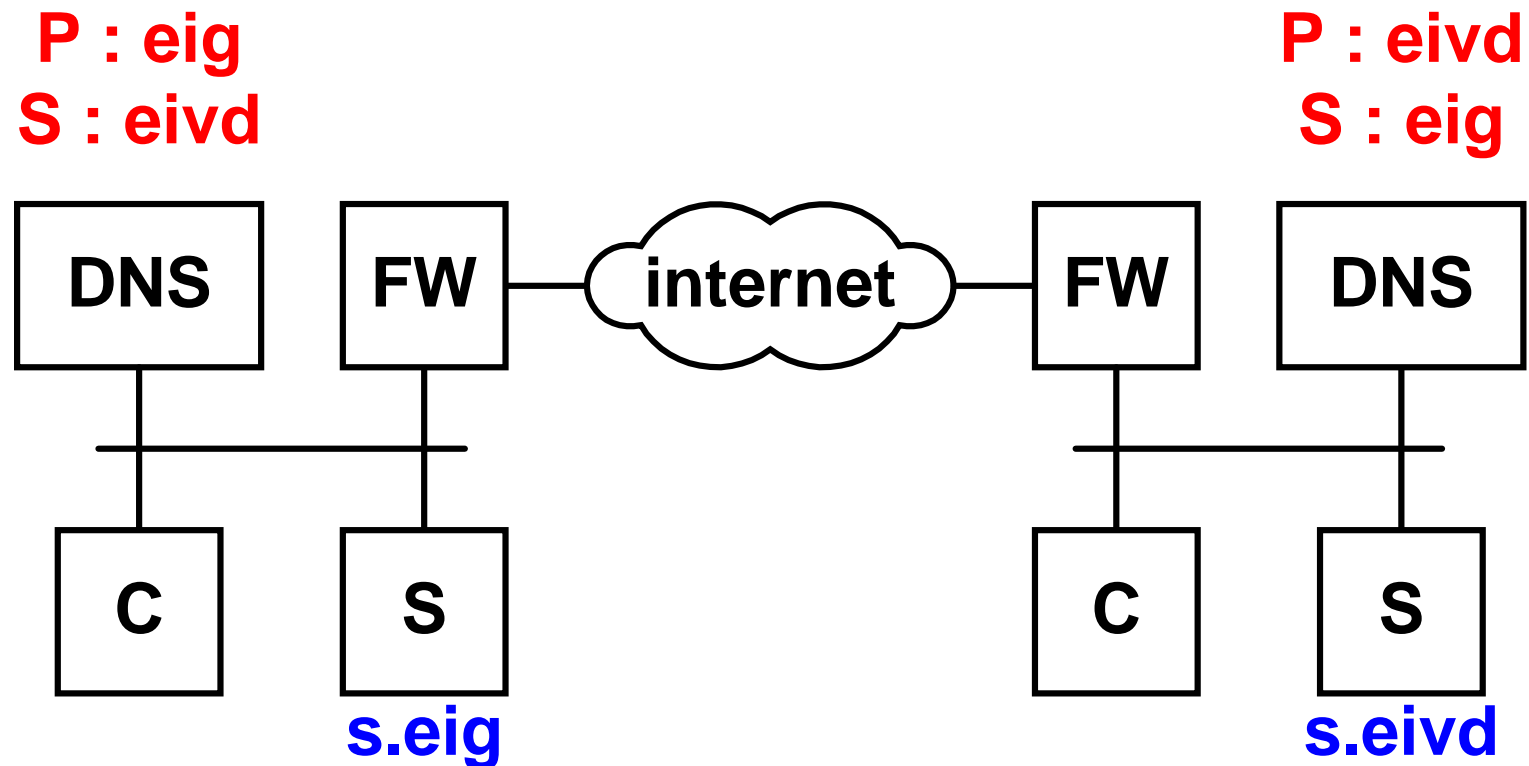
- Espace de noms est découpé en zones



- Zone sous l'autorité d'un *Name Server*
- *Name Server* peut avoir l'autorité sur plusieurs zones

Illustration avec VPN EIG - EIVD

- Réseau privé virtuel (*Virtual Private Network*)
- Zones eig et eivd (*private namespace*)



- + Zones publiques (*public namespace*)

Gère la zone td.unige.ch

W2k Server SP4

Name	Type	Data
	Start of Authority	v19.td.unige.ch.
	Name Server	v19.td.unige.ch.
v19	Host	129.194.184.212
v20	Host	129.194.184.80
www	Alias	v20.td.unige.ch.
ftp	Alias	v20.td.unige.ch.
hpxw	Host	129.194.184.81
secure	Alias	hpxw.td.unige.ch.
ca	Alias	hpxw.td.unige.ch.

Zone inverse

Name	Type	Data
	Start of Authority	v19.td.unige.ch.
	Name Server	v19.td.unige.ch.
129.194.184.212	Pointer	v19.td.unige.ch.
129.194.184.80	Pointer	v20.td.unige.ch.
129.194.184.81	Pointer	hpxw.td.unige.ch.

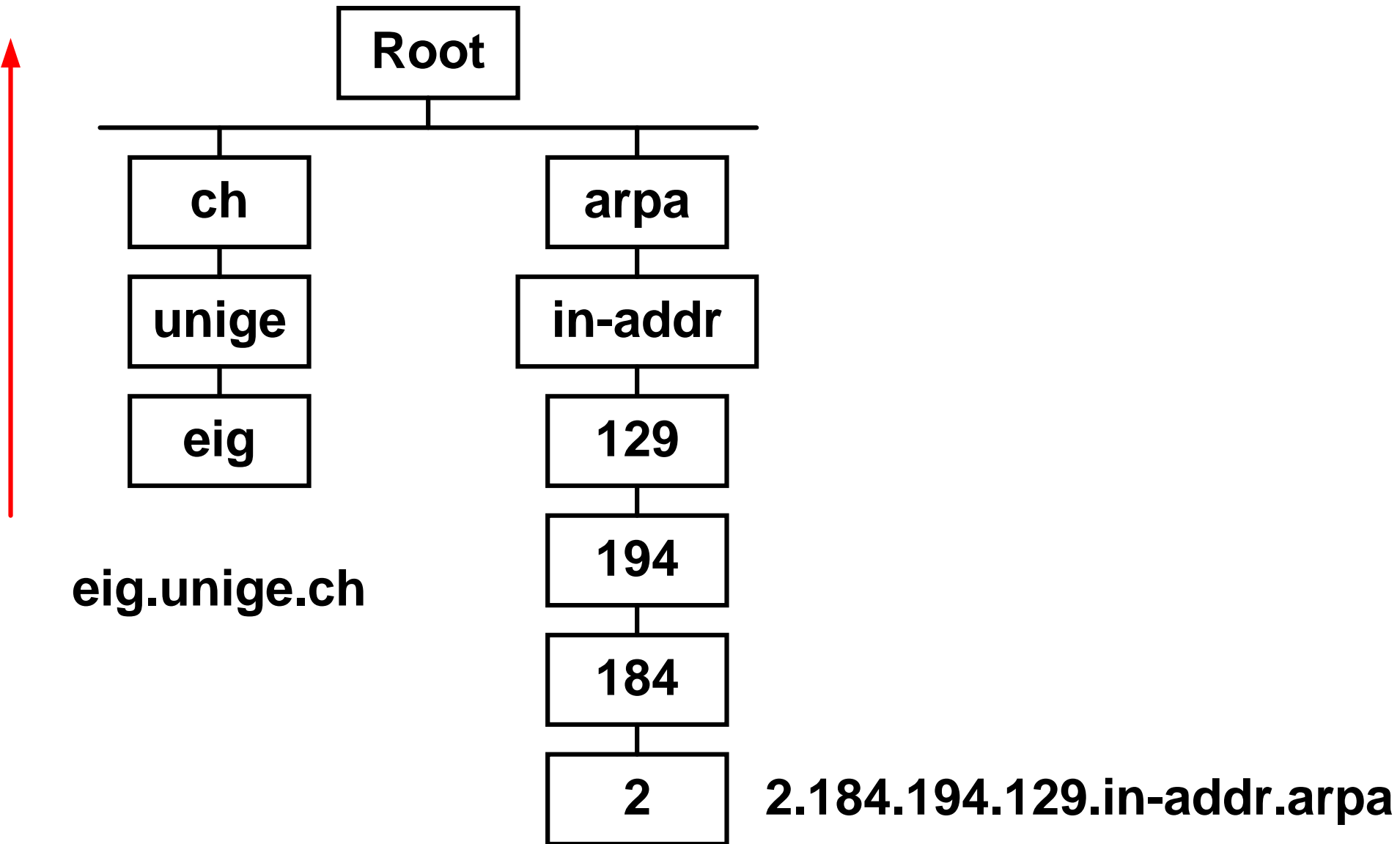
Types définis de la classe Internet (IN) selon RFC 1700 :

- **SOA** *marks the **start of zone of authority***
- **NS** *an **authoritative name server***

- **A** *a **host address***

- **CNAME** *the **canonical name for an alias***

- **PTR** *a **domain name pointer***
- **MX** ***mail exchange***

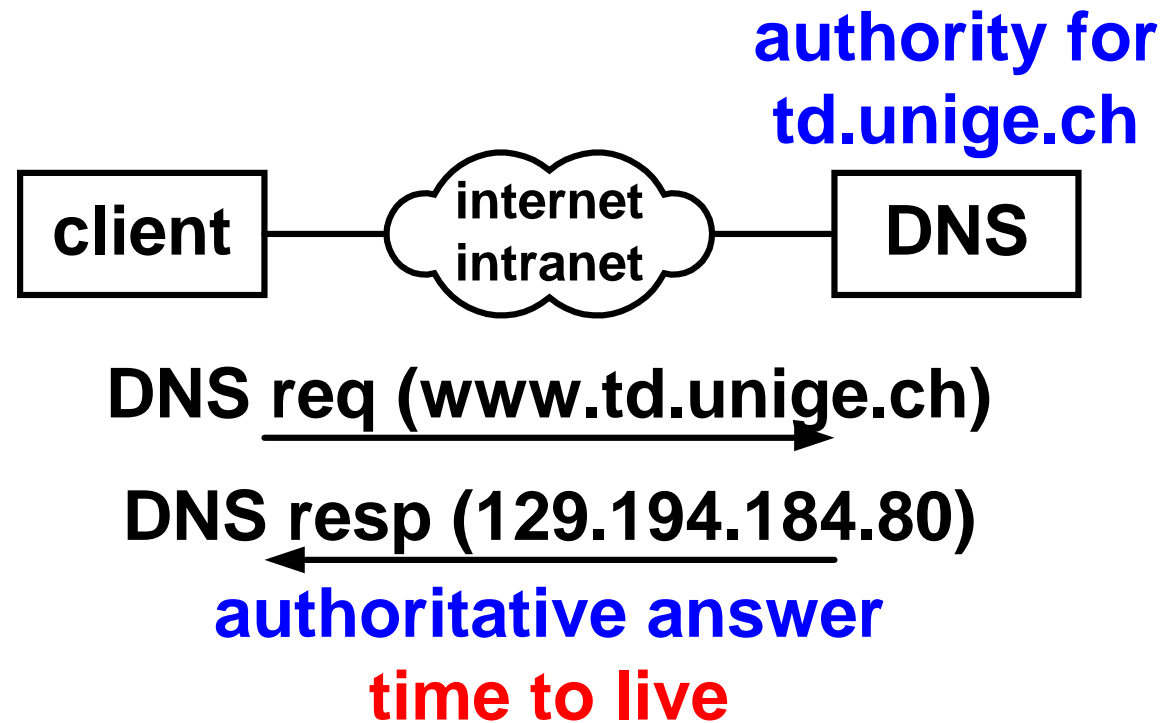


Gère la zone **tdeig**

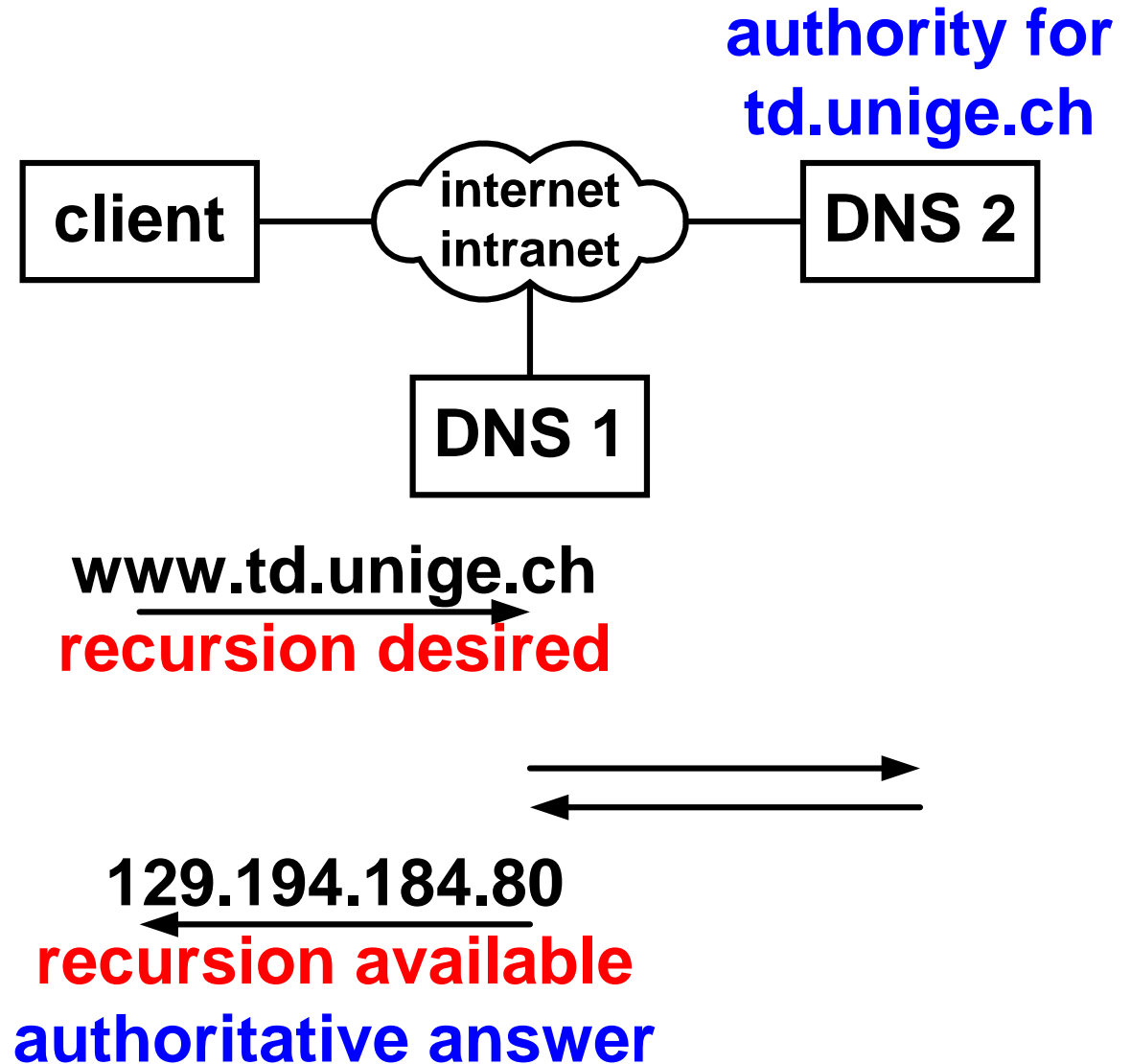
W2k Server SP4

Name	Type	Data
	Start of Authority	dc1.tdeig.
	Name Server	dc1.tdeig.
dc1	Host	10.1.1.10
e1	Host	10.1.4.1
e2	Host	10.1.4.2
...
e10	Host	10.1.4.10
s1	Host	10.1.1.1
s2	Host	10.1.1.2
ftp	Alias	s2.tdeig.

- Le serveur DNS possède l'autorité sur la zone td.unige.ch

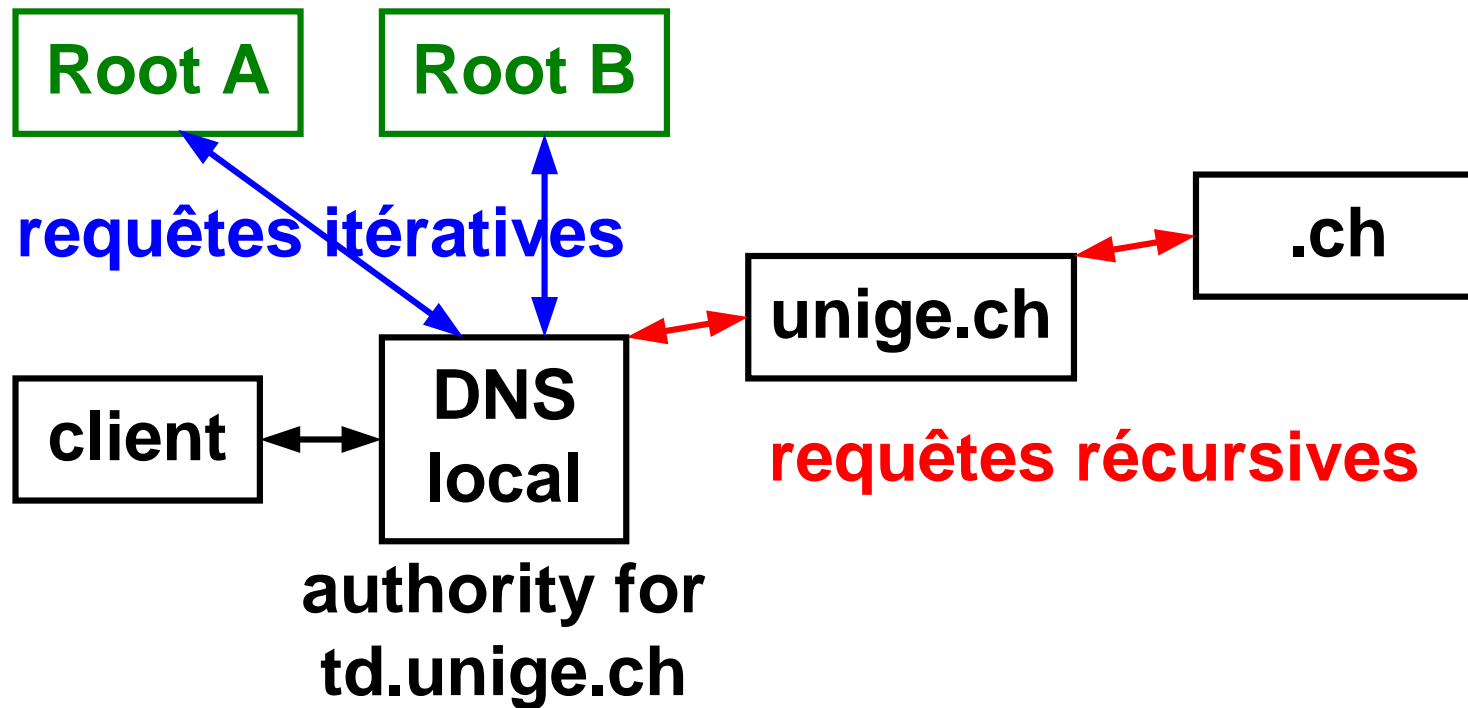


- Durée de vie dans un cache = 1h (min TTL = 3600)

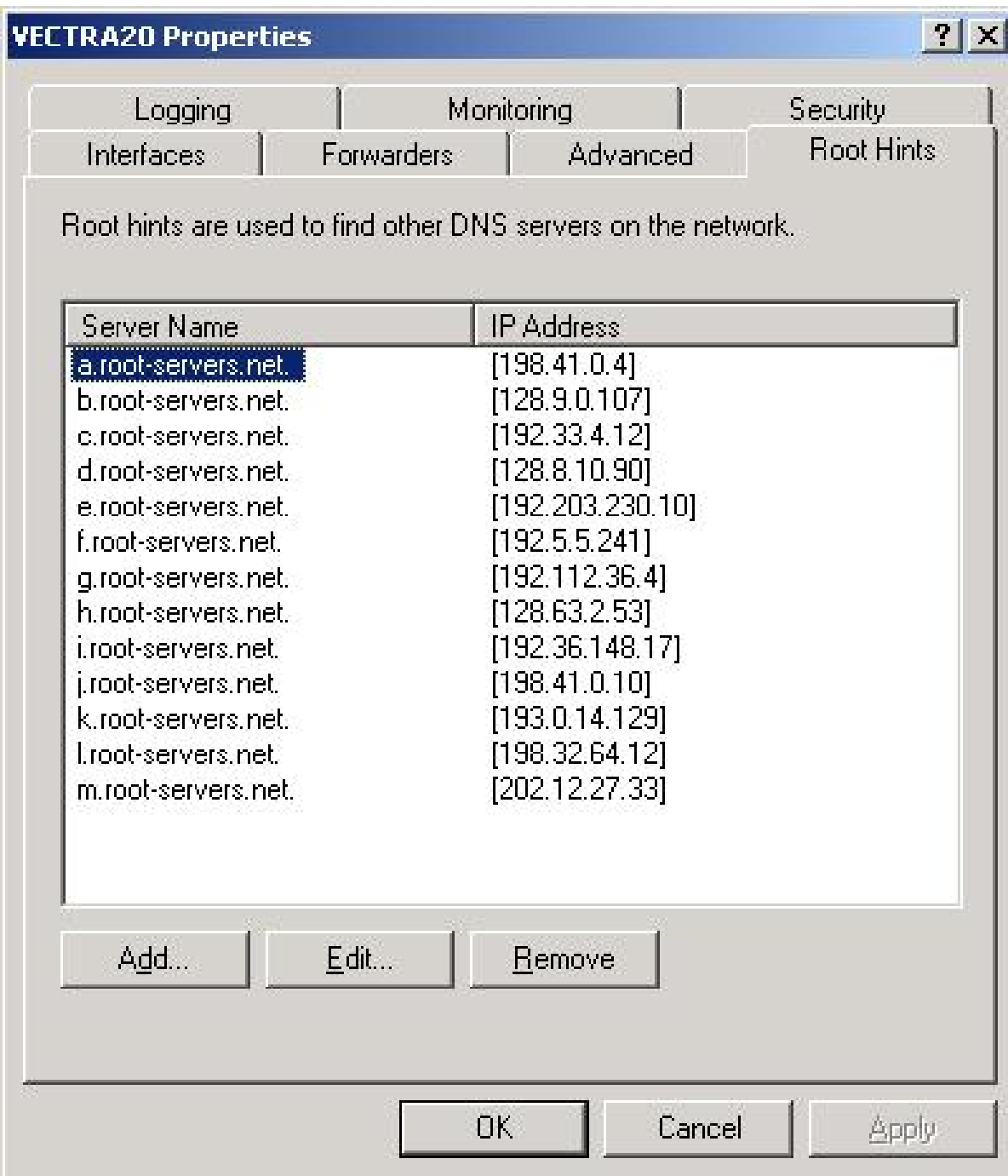


- Le client adresse la requête à son serveur DNS local
- DNS1 est capable de rechercher
- Mise en mémoire cache

- *Root servers (A, B, ...)*



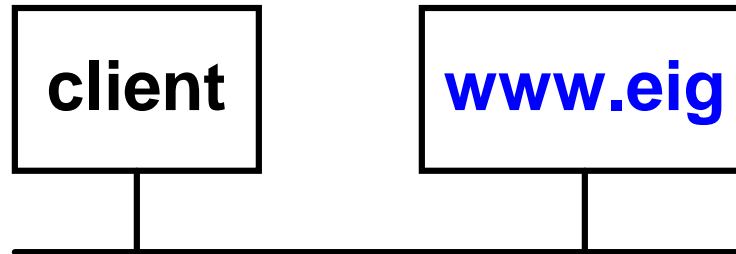
- *Root servers ne supportent pas la récursivité*



10 **USA**
2 **Europe**
1 **Japon**
13 **Total**

**21 oct 02 : 7 serveurs
down suite à DDoS
*Distributed Denial of Service***

- Illustration avec FQDN = **www.eig** (intranet)



- Client - fichier `\winnt\system32\drivers\etc\hosts`
`10.0.0.8 www.eig`

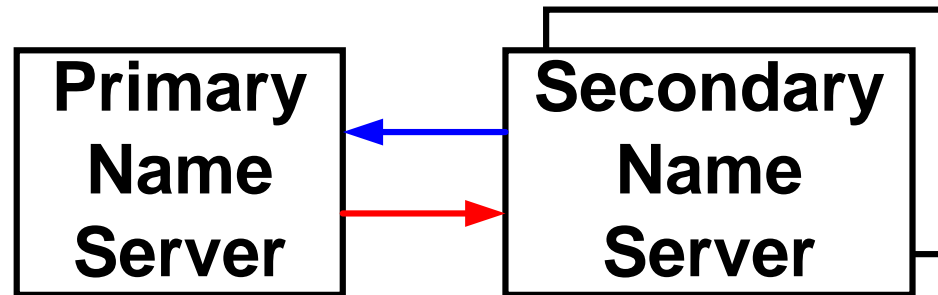
DNS : round-robin

Name	Type	Data
www	Host	129.194.184.200
www	Host	129.194.184.201
www	Host	129.194.184.202

- Principe du tourniquet
- Répartition de la charge (*load balancing*)
- Application exigeant une haute disponibilité

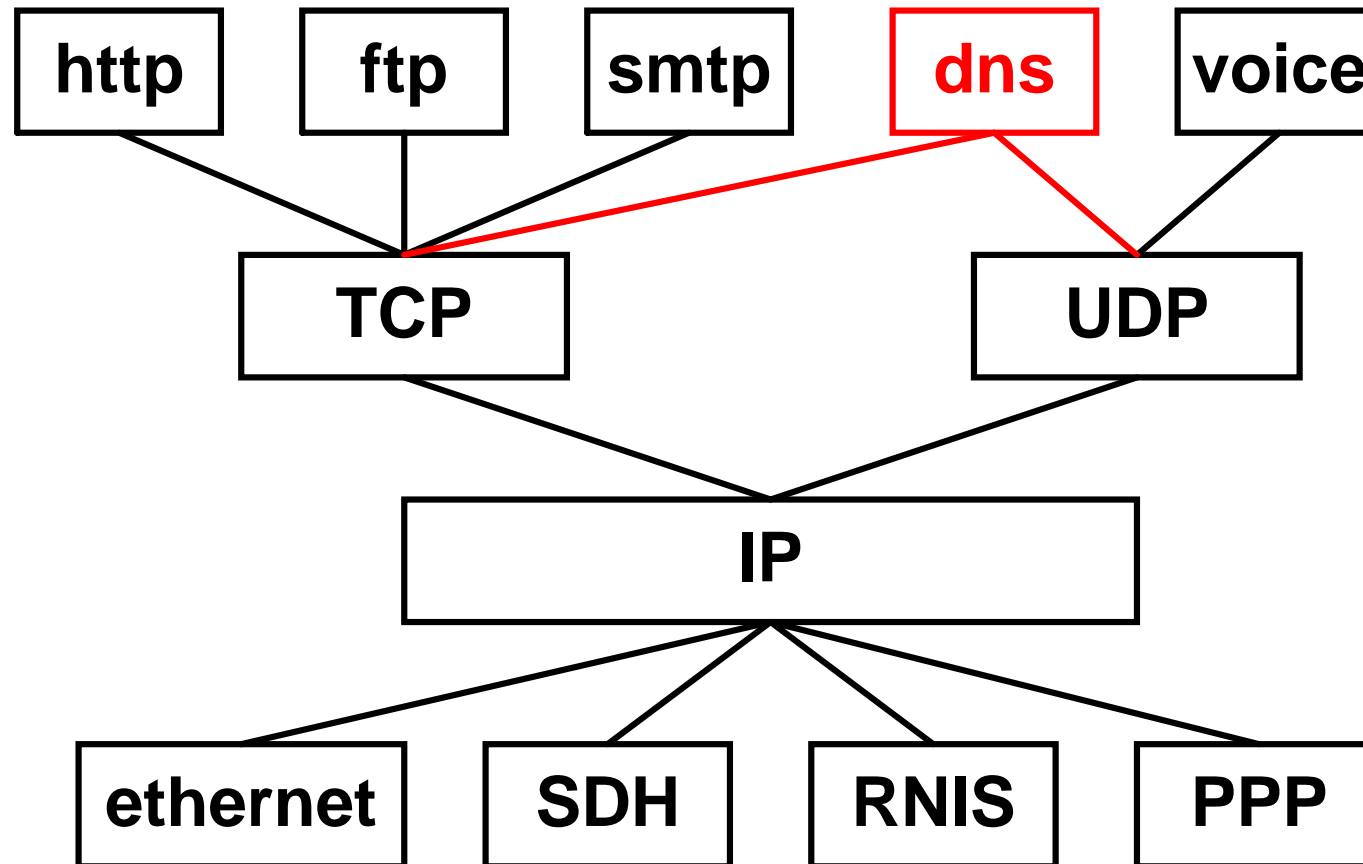
DNS : secondary name server

- Illustration avec le fichier `td.unige.ch.dns`
 - 3600 (1h) refresh intervalle entre 2 **requêtes de transfert**
 - 600 (10') retry intervalle si pas de réponse
 - 86400 (1j) expire *sec. name server* répond alors que *prim. name server est down*



zone transfers

- Utiliser également par des gens malintentionnés



- Transfert de zone via TCP – port 53
- *Resolver – Server* via UDP – port 53

```
C:\>nslookup
```

```
Default Server:   XXX
```

```
Address:  YYY
```

```
> set type=ns
```

```
> unige.ch
```

```
sns2-tss2.unige.ch
```

```
IP = 129.194.8.7
```

```
dns93.unige.ch
```

```
IP = 129.194.4.6
```

```
uni2b.unige.ch
```

```
IP = 129.194.4.32
```

```
> set type=all
```

```
> unige.ch
```

Config. par défaut

Name Server

Zone

Tous les paramètres

Zone

nslookup (2)

```
C:\>nslookup
```

```
Default Server:   XXX
```

```
Address:  YYY
```

Config. par défaut

```
> set type=all
```

```
> switch.ch
```

**Tous les paramètres
Zone**

```
scsnms.switch.ch
```

```
IP = 130.59.1.30
```

```
> server scsnms.switch.ch
```

Set default server

```
...
```

```
> td.unige.ch
```

Zone

```
C:\>nslookup
```

```
Default Server:   XXX
```

Config. par défaut

```
Address:   YYY
```

```
> server v19.td.unige.ch
```

Set default server

```
...
```

```
> ls -d td.unige.ch
```

List all records

```
*** Can't list domain td.unige.ch: Query refused
```

Test d'un serveur DNS

- <http://www.intodns.com/>
- [Report_unige.ch.htm](http://unige.ch/Report_unige.ch.htm)
- [Report_td.unige.ch.htm](http://unige.ch/Report_td.unige.ch.htm)

IP database - Whois

- Permet l'identification de l'adresse IP démon
- Réseaux IP Européens (RIPE)
www.ripe.net/ripe/about/
<http://www.ripe.net/whois> Query the RIPE Database
- *American Registry for Internet Numbers (ARIN)*
www.arin.net
- *Asia Pacific Network Information Center (APNIC)*
www.apnic.net
- www.uwhois.com (Universal)

- **Organisme d'attribution des noms de domaine**

Unicité du nom de domaine

www.switch.ch, www.nic.ch

www.nic.fr

Network Information Center

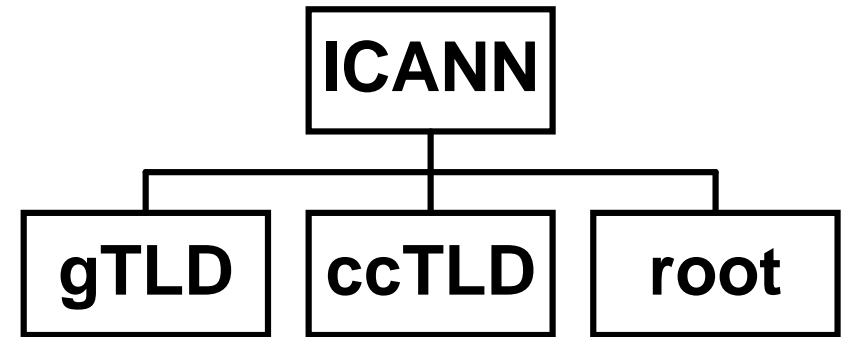
www.networksolutions.com

- **Résolution des conflits**

<http://www.wipo.int/amc/en/index.html> , www.itu.int

- www.icann.org

*Internet Corporation for
Assigned Names and Numbers*



- <http://www.iana.org/gtld/gtld.htm>

Generic Top Level Domain : com, biz, aero, ...

- www.iana.org/cctld

Country Code Top Level Domain : ch, fr, ...

- www.root-servers.org

- 1 nslookup**
- 2 Demandes récursives**
- 3 Demande itératives**
- 4 Divers (répartition de charge, ...)**