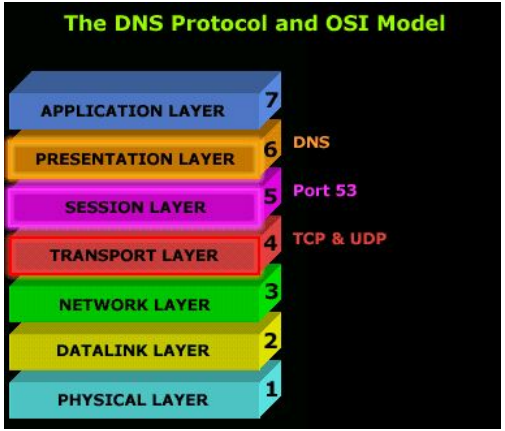
DNS / Revproxy

vaktas & lionofinterest

Domain Name System

Domain Name System



- Un ordinateur ça ne comprend que des nombres.
- DNS : Annuaire géant qui associe des noms de domaines à des IP.
- Service informatique qui tourne sur des serveurs, on parle de Domain Name Server !
- Requête port 53

Au niveau de l’ordinateur

Le fichier contenant les hôtes :

Windows : C:/Windows32/drivers/etc/hosts

Linux : /etc/hosts

Le fichier qui s’occupe de la résolution :

Windows : Windows + R -> ncpa.cpl -> Clic droit sur votre interface -> IPv4

Linux : /etc/resolv.conf

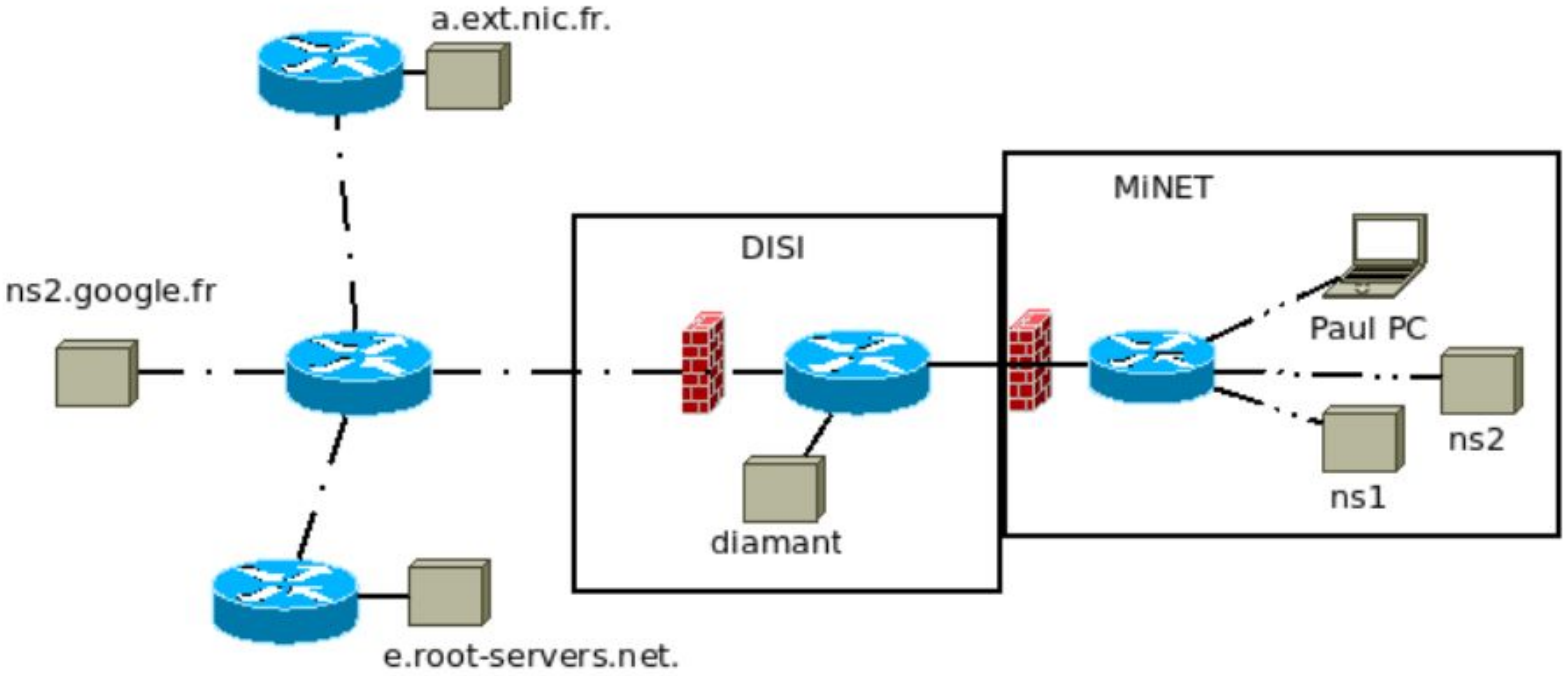
Quelques DNS

Bind9 utilisé à MiNET

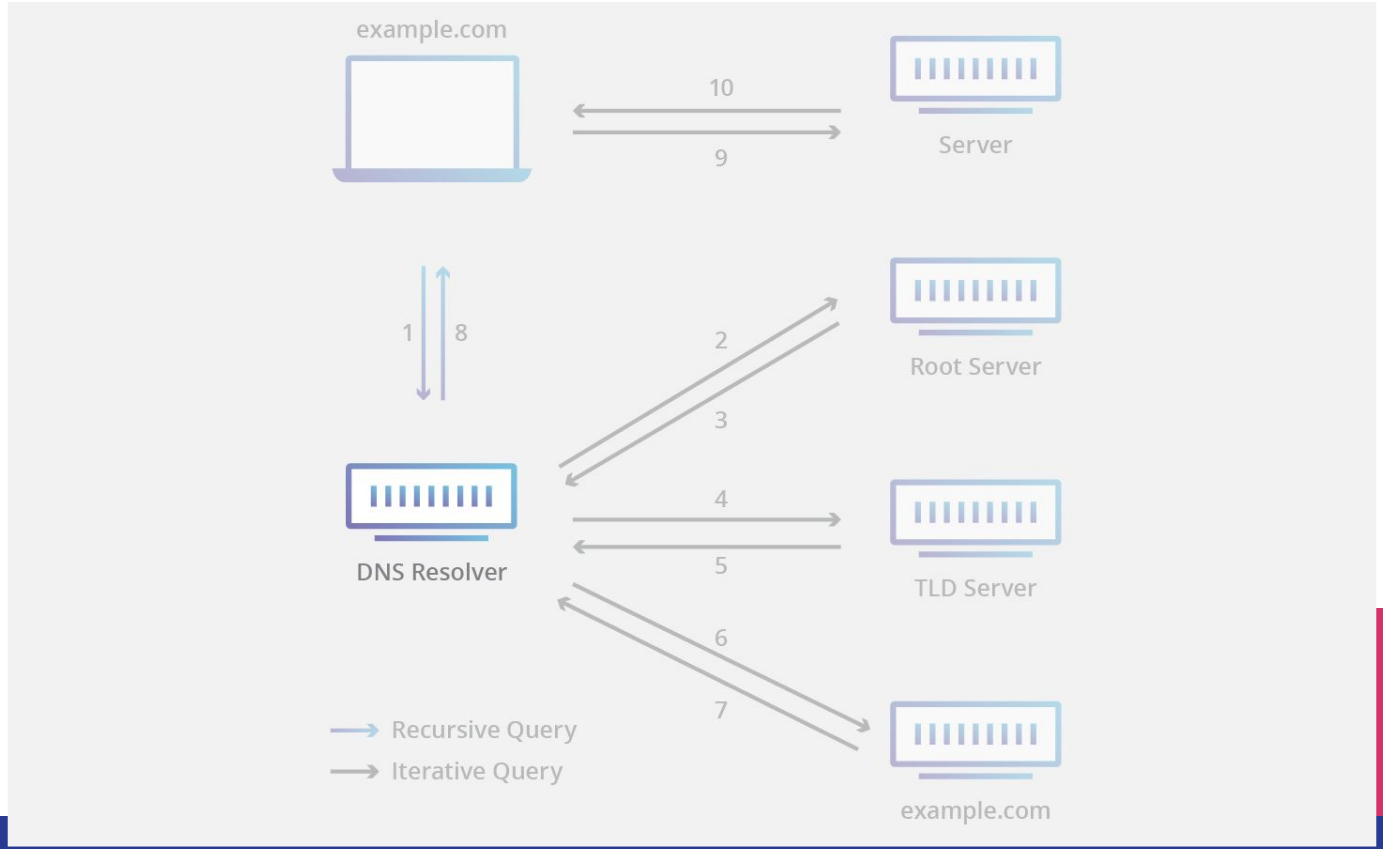
Dnsmasq

Microsoft DNS

Infrastructure MiNET (merci sowarks)



La résolution DNS comment ça marche ?



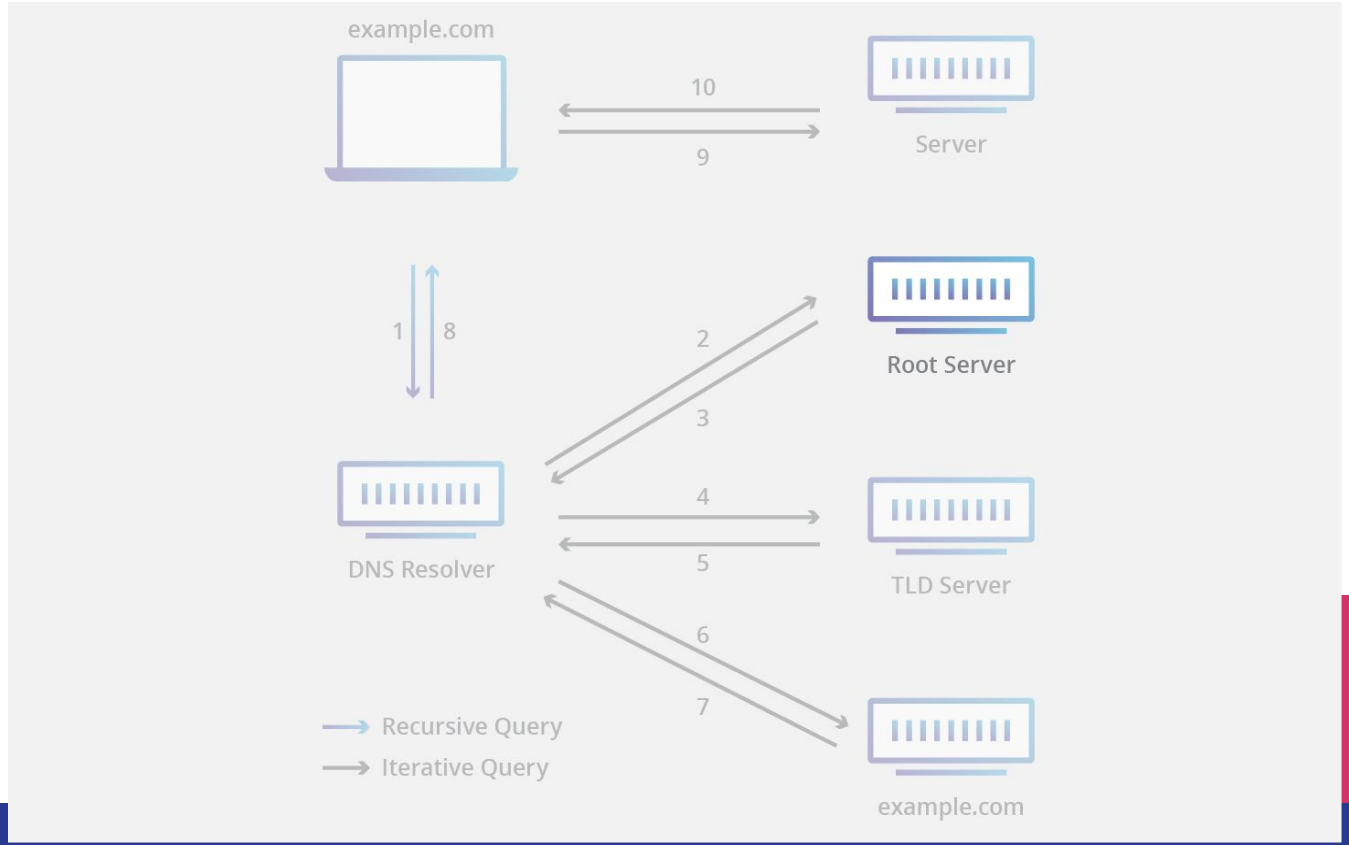
Récurseur DNS

- L’intermédiaire entre le client et le serveur DNS.

- S’il dispose de la réponse en cache, il la renvoie immédiatement.

- Sinon, il fait une requête au…

La résolution DNS comment ça marche ?



Serveur racine .

Domaine originel noté .

13 IPs notées, les root servers

à contacter en priorité.

```
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;           file                /domain/named.cache
;           on server           FTP.INTERNIC.NET
;       -OR-                    RS.INTERNIC.NET
;
;       last update:    February 17, 2016
;       related version of root zone:   2016021701
;
; formerly NS.INTERNIC.NET
;
.                        3600000      NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.      3600000      AAAA  2001:503:ba3e::2:30
;
; FORMERLY NS1.ISI.EDU
;
.                        3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000      A     192.228.79.201
B.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:84::b
;
; FORMERLY C.PSI.NET
;
.                        3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.      3600000      A     192.33.4.12
C.ROOT-SERVERS.NET.      3600000      AAAA  2001:500:2::c
;
; FORMERLY TERP.UMD.EDU
```

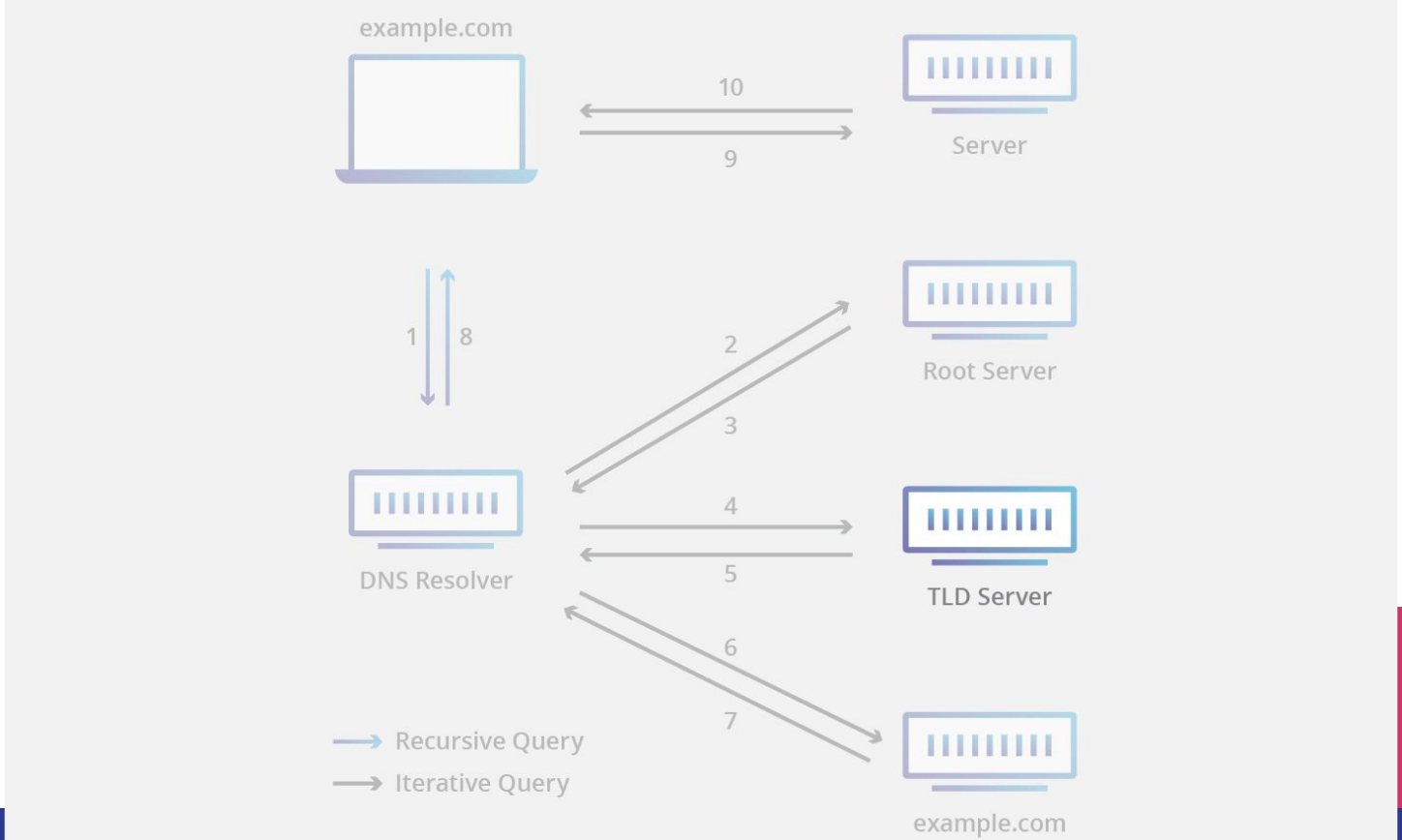
Serveur racine

- Reçoit la requête du récurseur.

- 13 serveurs “connus” par chaque récurseur.

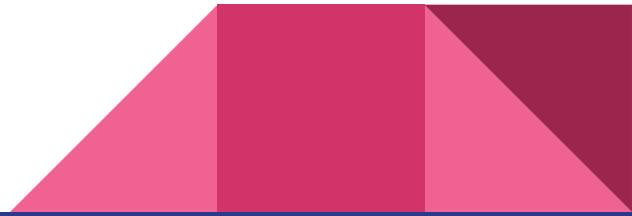
- Il renvoie … au récurseur.

La résolution DNS comment ça marche ?

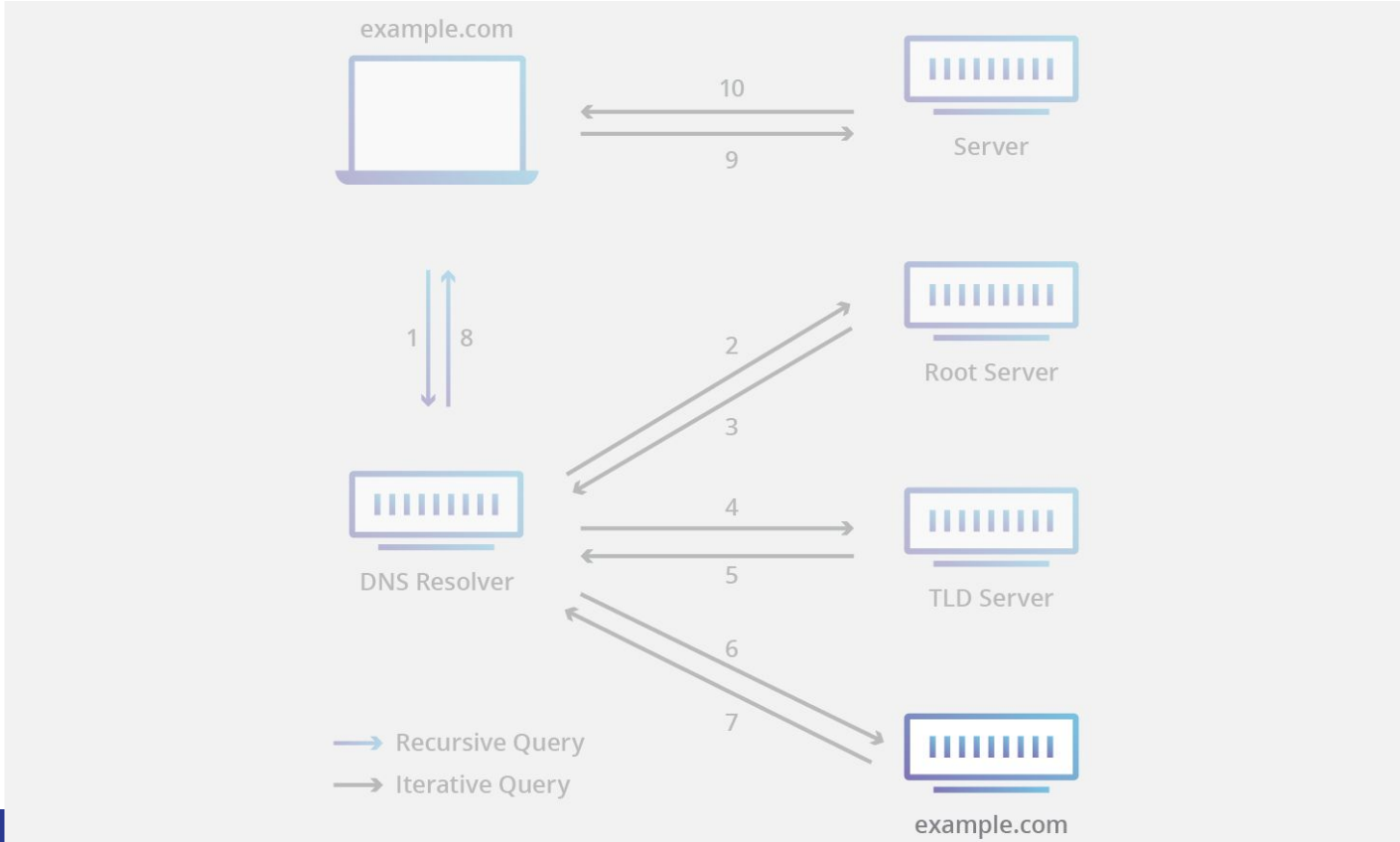


Top Level Domain

- Reçoit la requête du récurseur.
- Contient les informations relatives à une extension de domaine (.com, .net…)
- Generic Top-Level Domain & Country code top-level domains
- Il répond en pointant … au récurseur.



La résolution DNS comment ça marche ?



Authority Nameserver

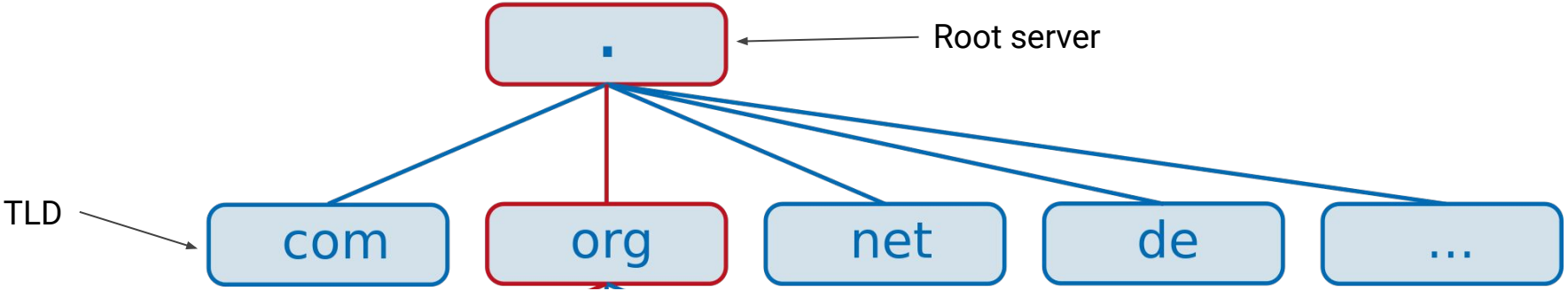
- Reçoit la requête du récurseur.

- Rempart final avant l’association IP <-> nom de domaine !

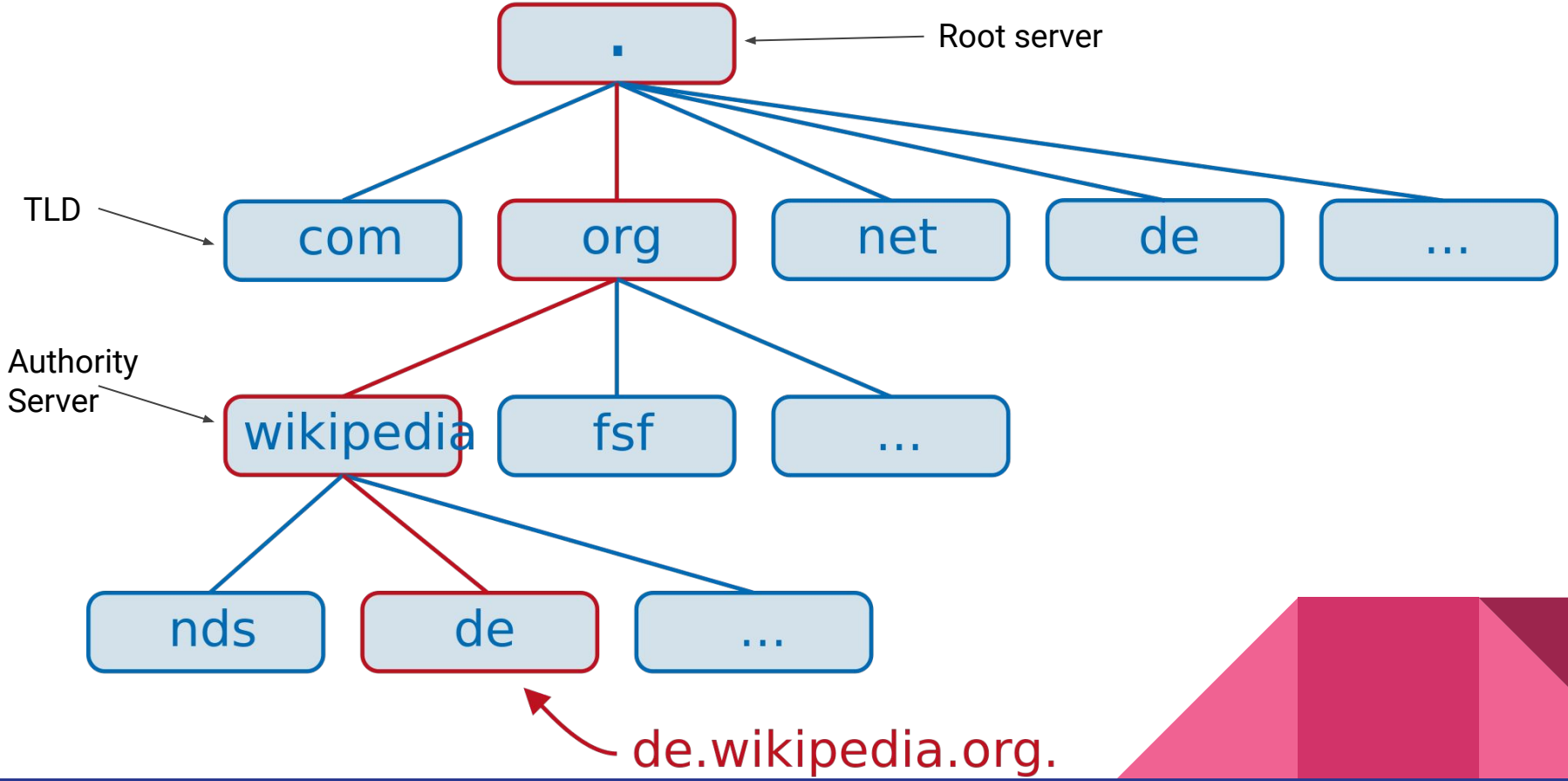
- Il renvoie la requête au récurseur, et revient vers le client.

Cheminement de la requête DNS

Cheminement de la requête DNS

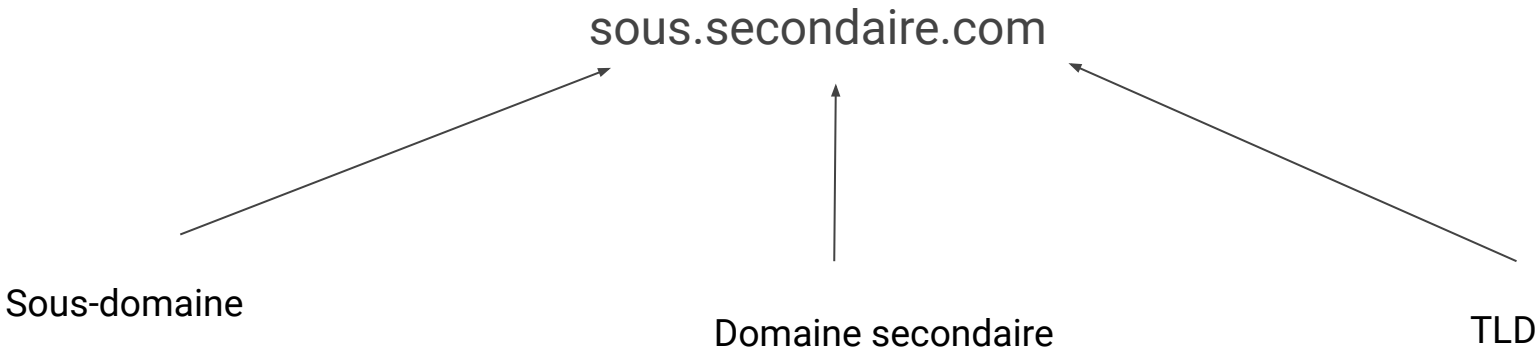


Cheminement de la requête DNS



Zoom sur l’Authority Nameserver

Zones DNS



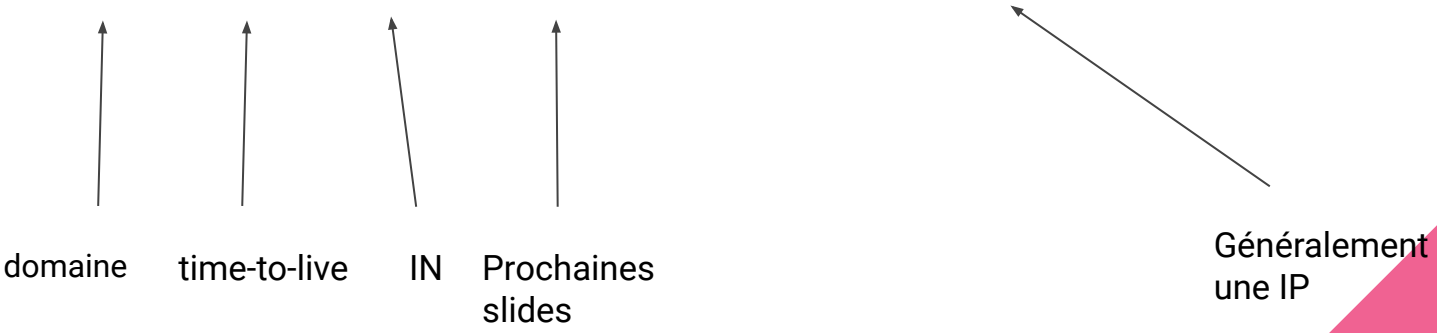
Gestion du **namespace**

Zones et enregistrements DNS

Zone DNS : Fichier contenu dans le serveur, qui liste tous les enregistrements pour tous les domaines de la zone.

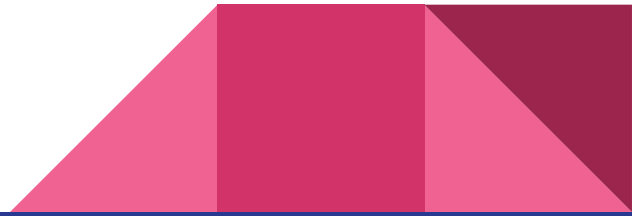
Structure organisée pour regrouper les domaines.

<name> <ttl> <class> <type> <rdlength> <radata>



Types de zones DNS

- Primary : RW
- Secondary : RO
- Active Directory-integrated
- Stub : SOA



Petite zone posée

```
gateway         IN      A       157.159.40.1
                IN      A       157.159.40.241
                IN      A       157.159.40.253
gateway-disi    IN      A       157.159.40.254
                IN      A       157.159.40.242
vpndev          IN      A       157.159.40.14
nmap            IN      A       157.159.40.15
smtp            IN      A       157.159.40.18
                IN      AAAA    2001:660:3203:422::A18
vpn             IN      A       157.159.40.19
                IN      A       157.159.40.20
vpn1            IN      A       157.159.40.19
vpn2            IN      A       157.159.40.20
mx              IN      A       157.159.40.25
                IN      A       157.159.40.26
mx1             IN      A       157.159.40.25
;               IN      AAAA    2001:660:3203:422::A25
mx2             IN      A       157.159.40.26
;               IN      AAAA    2001:660:3203:422::A26
listes          IN      A       157.159.40.103
listes          IN      MX 10   mx1.minet.net.
listes          IN      MX 10   mx2.minet.net.
lites           IN      MX 10   mx1.minet.net.
lites           IN      MX 10   mx2.minet.net.
imap            IN      A       157.159.40.27
```

Architecture d’une zone

Start Of Authority (SOA) record, pour être conforme à l’IETF.

host -t SOA minet.net (plus synthétique)

dig SOA minet.net

Architecture d’une zone

Start Of Authority (SOA) record, pour être conforme à l’IETF.

host -t SOA minet.net (plus synthétique)

dig SOA minet.net

RNAME : dns@minet.net

Numéro de série

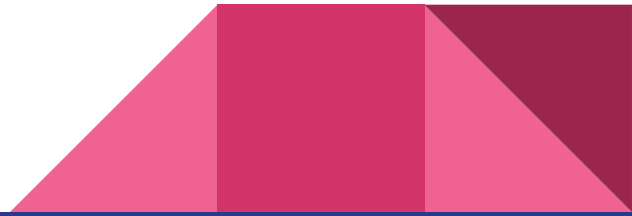
MNAME : serveur principal

Enregistrements DNS

A record	Associe une IPv4 à un domaine
AAAA record	Associe une IPv6 à un domaine
CNAME record	Forward vers un domaine ou sous-domaine existant
MX record	Redirige les mails vers un serveur mail
NS record	Enregistre le nom du serveur DNS
SOA record	Retiens des informations admin sur un domaine
PTR record	Donne une IP sur une résolution inverse

Les différentes données trouvées dans le DNS

champs A, AAAA, TXT, SRV, DMARC, etc.



PTR : Résolution inverse

Nécessité d’avoir l’enregistrement PTR, sans lequel ça ne marcherait pas.

PTR enregistre l’IP, l’inverse et y rajoute un domaine spécial : in-addr.arpa

Utilité : les serveurs de mail font des résolutions inverses pour vérifier l’authenticité d’un mail.

dig -x 157.159.40.103

```
;; ANSWER SECTION:
103.40.159.157.in-addr.arpa. 86400 IN   PTR     revproxy.minet.net.
```

Comment sécuriser le DNS

DNSSEC

DNS over TLS/DNS over HTTPS

Quelques manipulations 1/2

Le serveur DNS utilisé par notre ordinateur :

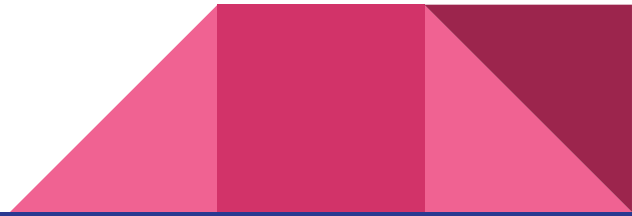
Windows : nslookup

Linux : nslookup minet.net

Avoir plus de détails sur le DNS contacté :

Linux : dig google.com +short

Linux : dig -x 8.8.8.8 +short



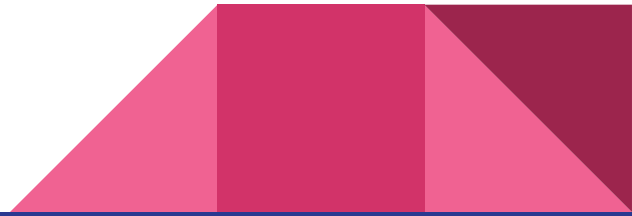
Quelques manipulations 2/2

Information sur le registrar : whois minet.net

Hosts définis : getent hosts

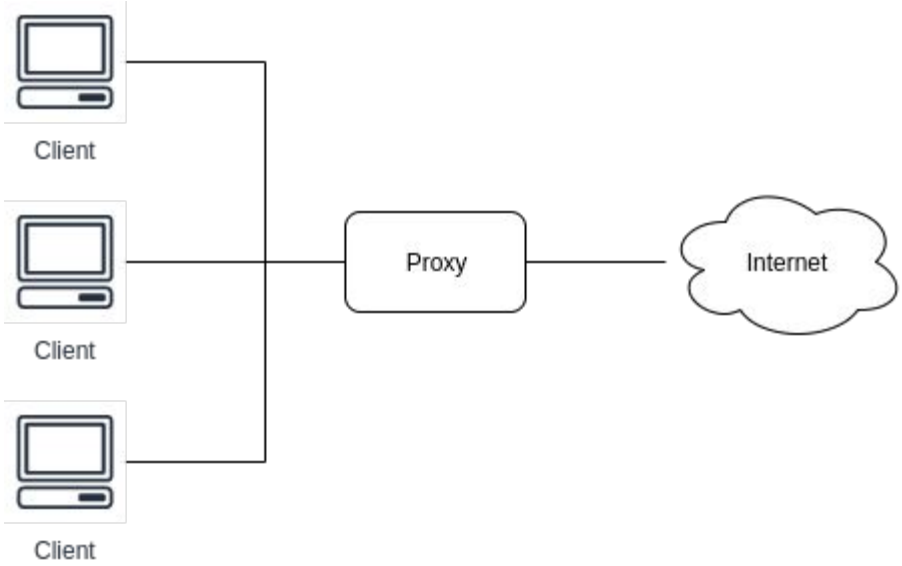
Requête spécifique depuis un DNS : dig @<ip_dns_server> minet.net NS

Visualisation du cache : dig example.com, à taper deux fois

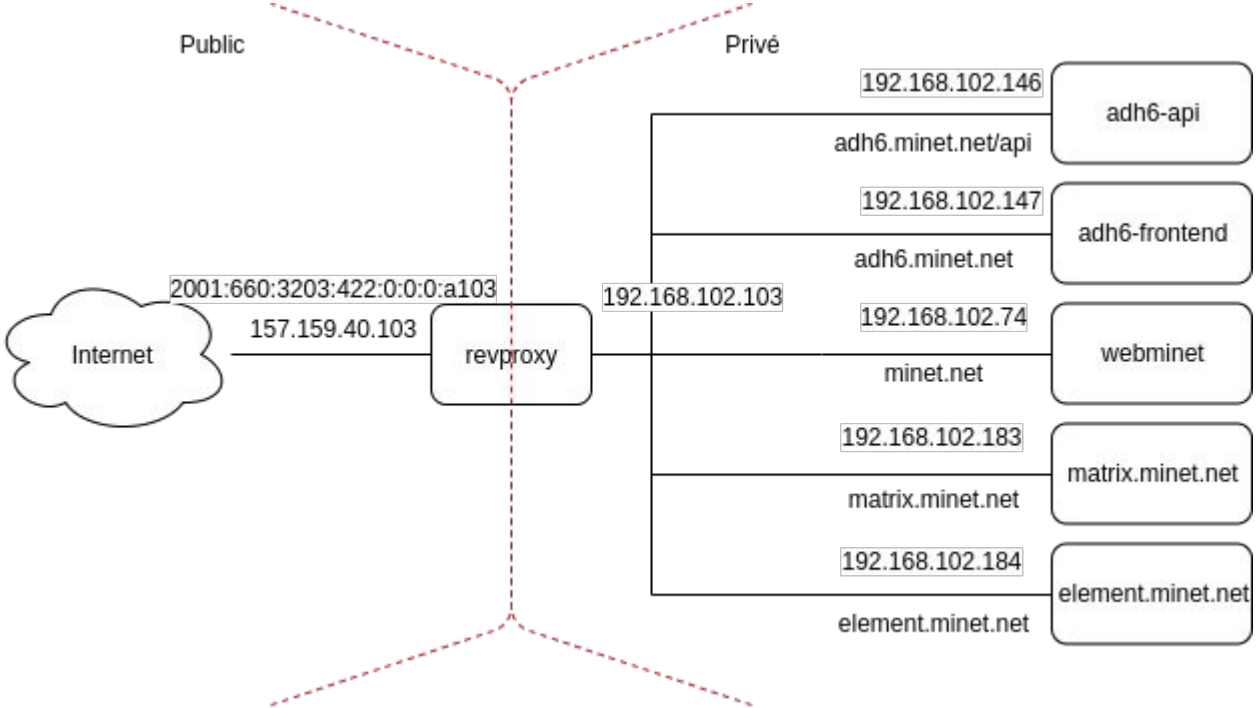


Reverse Proxy

Késako ?



Késako ?

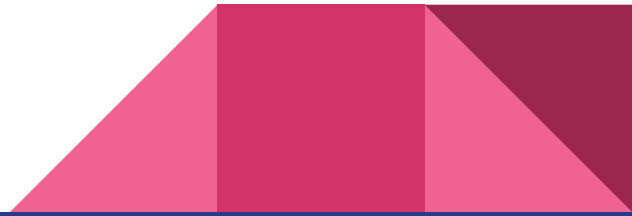

Public
Privé
192.168.102.146
adh6-api
adh6.minet.net/api
192.168.102.147
adh6-frontend
adh6.minet.net
2001:660:3203:422:0:0:0:a103
192.168.102.103
157.159.40.103
Internet
revproxy
192.168.102.74
webminet
minet.net
192.168.102.183
matrix.minet.net
matrix.minet.net
192.168.102.184
element.minet.net
element.minet.net

Plusieurs solutions

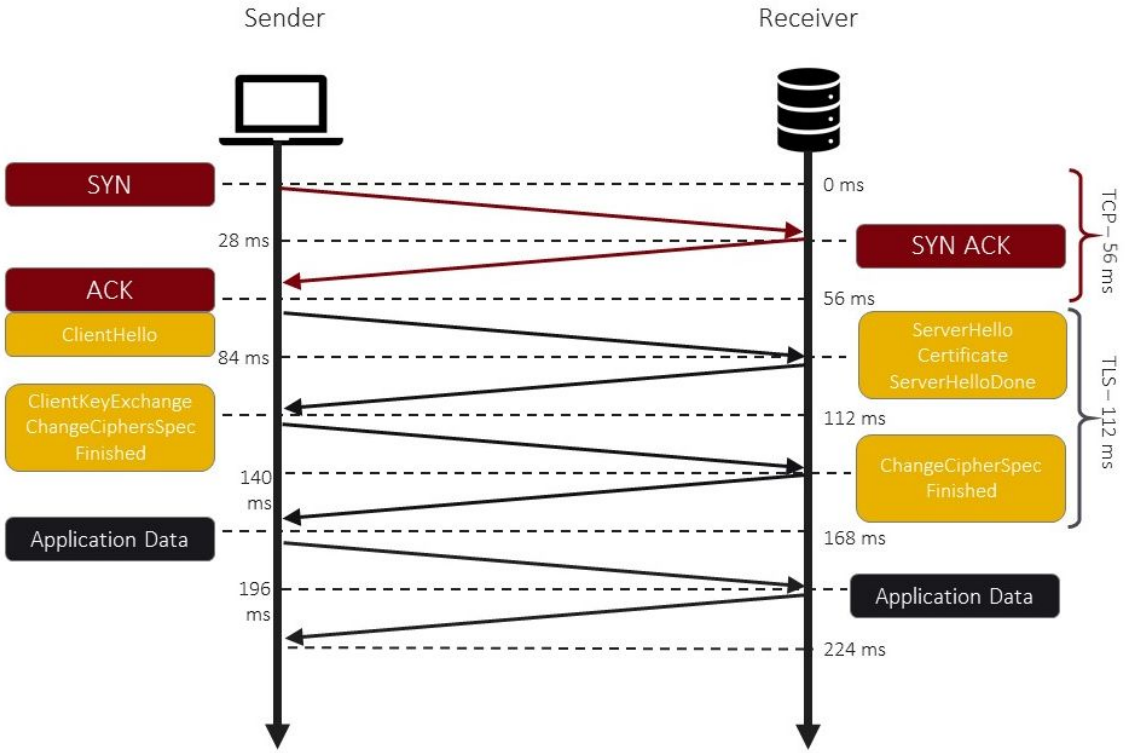
- nginx
- traefik
- apache

Comment faire une config ?

- redirection de http vers https avec un code 301
- Si possible: supporter l’ipv6

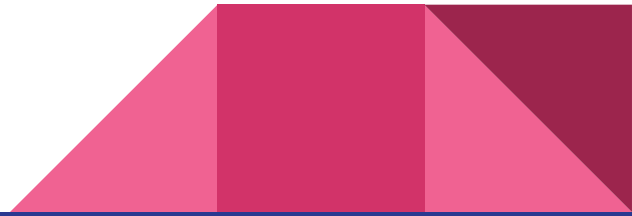


HTTPS


Sender
Receiver
SYN
0 ms
28 ms
SYN ACK
TCP – 56 ms
ACK
56 ms
ClientHello
84 ms
ServerHello
Certificate
ServerHelloDone
ClientKeyExchange
ChangeCiphersSpec
Finished
112 ms
TLS – 112 ms
ChangeCipherSpec
Finished
140 ms
Application Data
168 ms
196 ms
Application Data
224 ms

Une bonne config HTTPS

- NE PAS UTILISER TLS1.1
- être au minimum à TLS1.2 voire 1.3
- Avoir un certificat valide (sauf pour les tests)



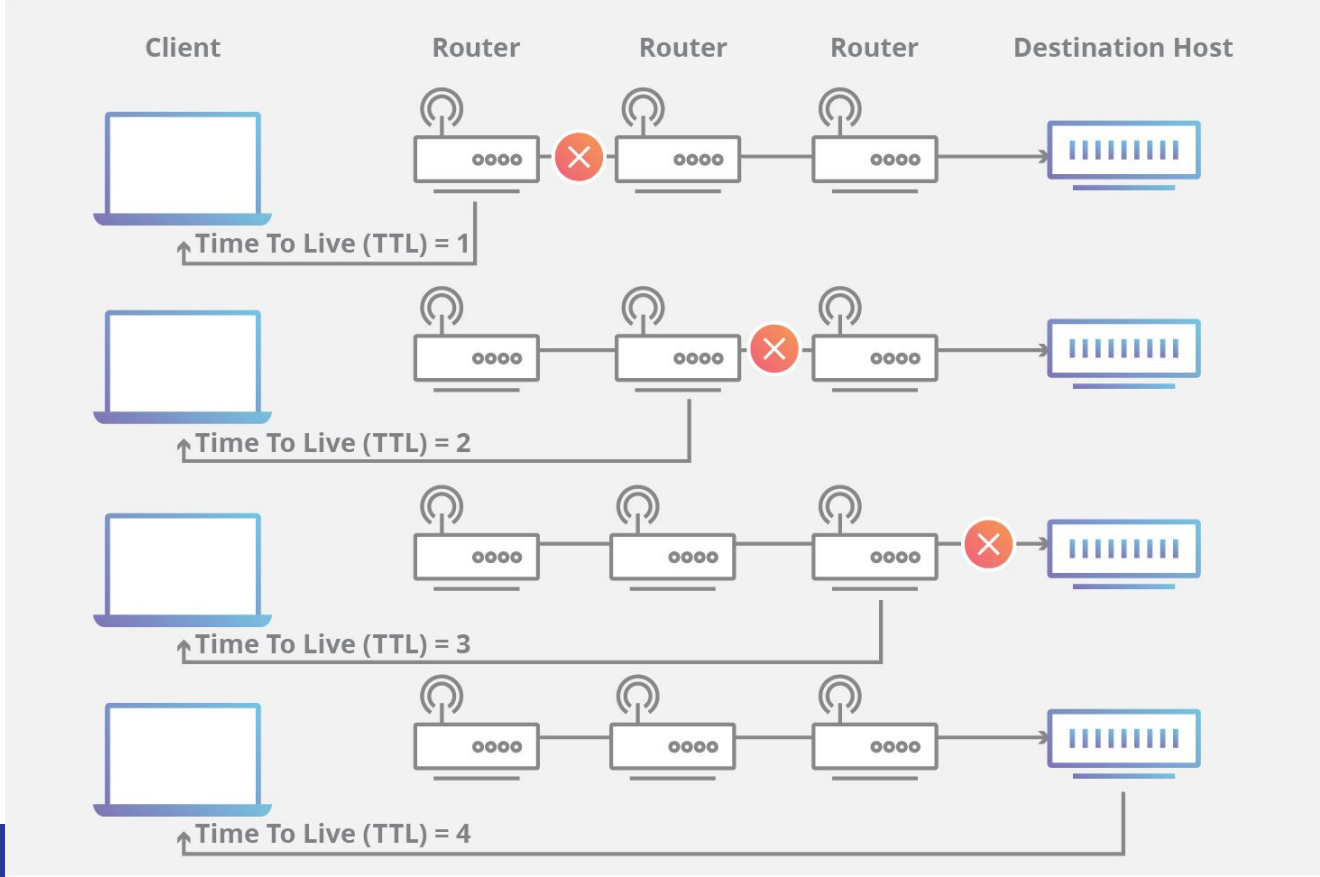
Quelques outils pour une bonne config HTTPS

- https://ssl-config.mozilla.org/
- certbot: https://eff-certbot.readthedocs.io/en/stable/intro.html

TP

Annexe

Annexe TTL


Client
Router
Router
Router
Destination Host
Time To Live (TTL) = 1
Time To Live (TTL) = 2
Time To Live (TTL) = 3
Time To Live (TTL) = 4