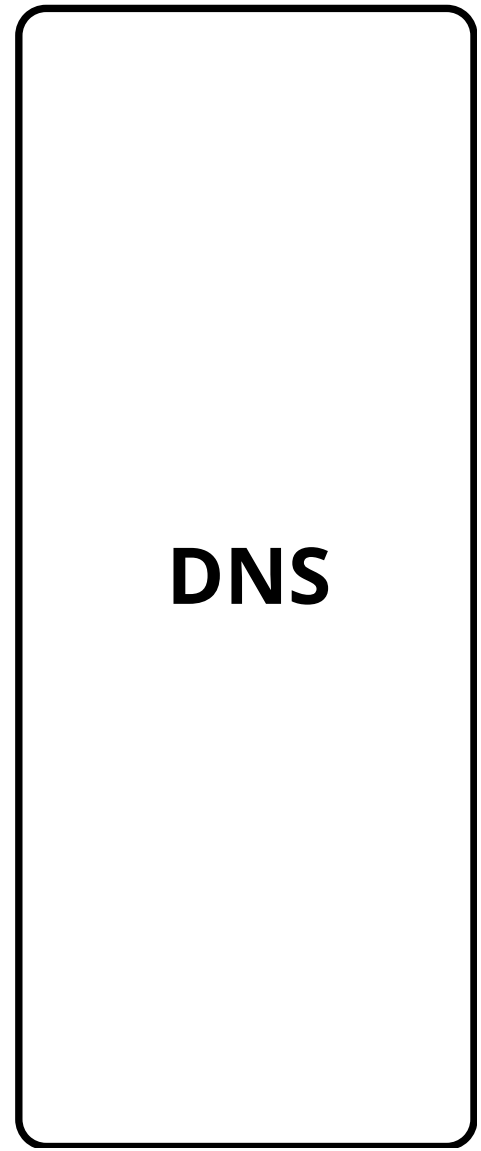
Impact of secure DNS transports on resolver performance

Etienne LE LOUËT, Antoine BLIN, Julien SOPENA

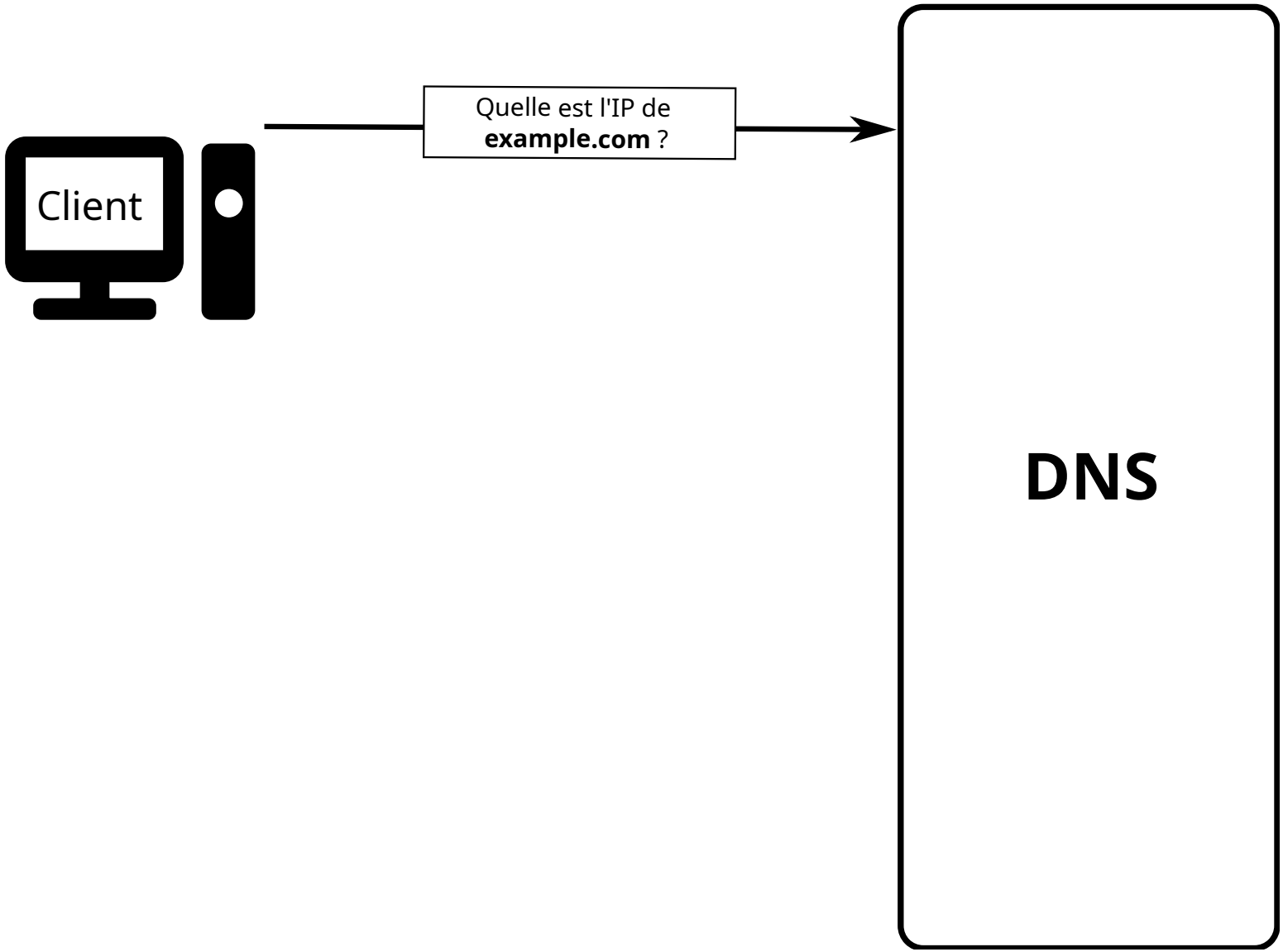
Gandi, LIP6

2023

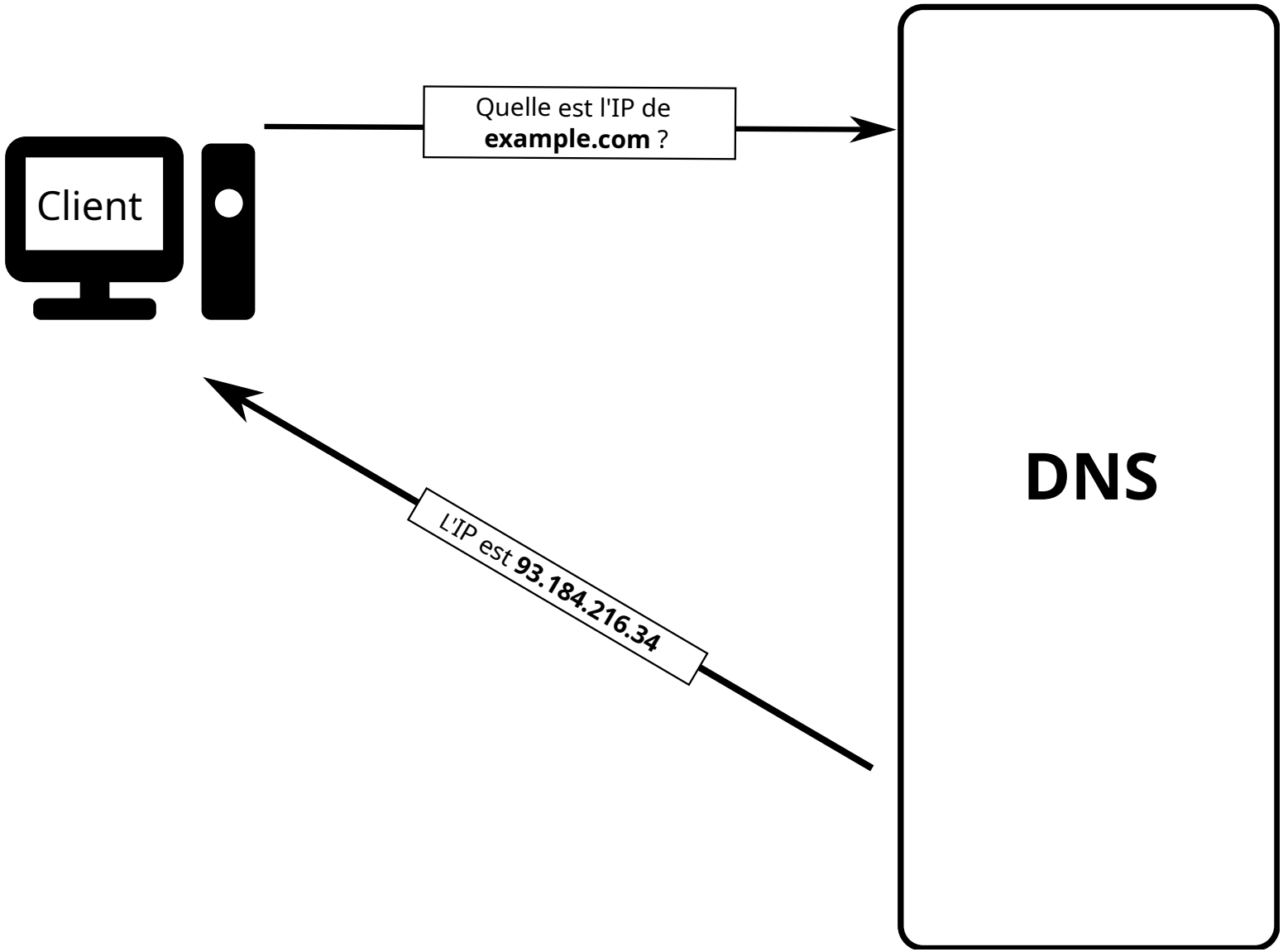
DNS - Architecture



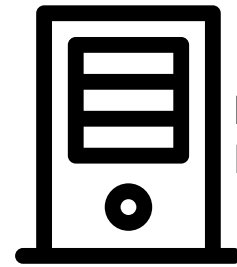
DNS - Architecture



DNS - Architecture



DNS - Architecture

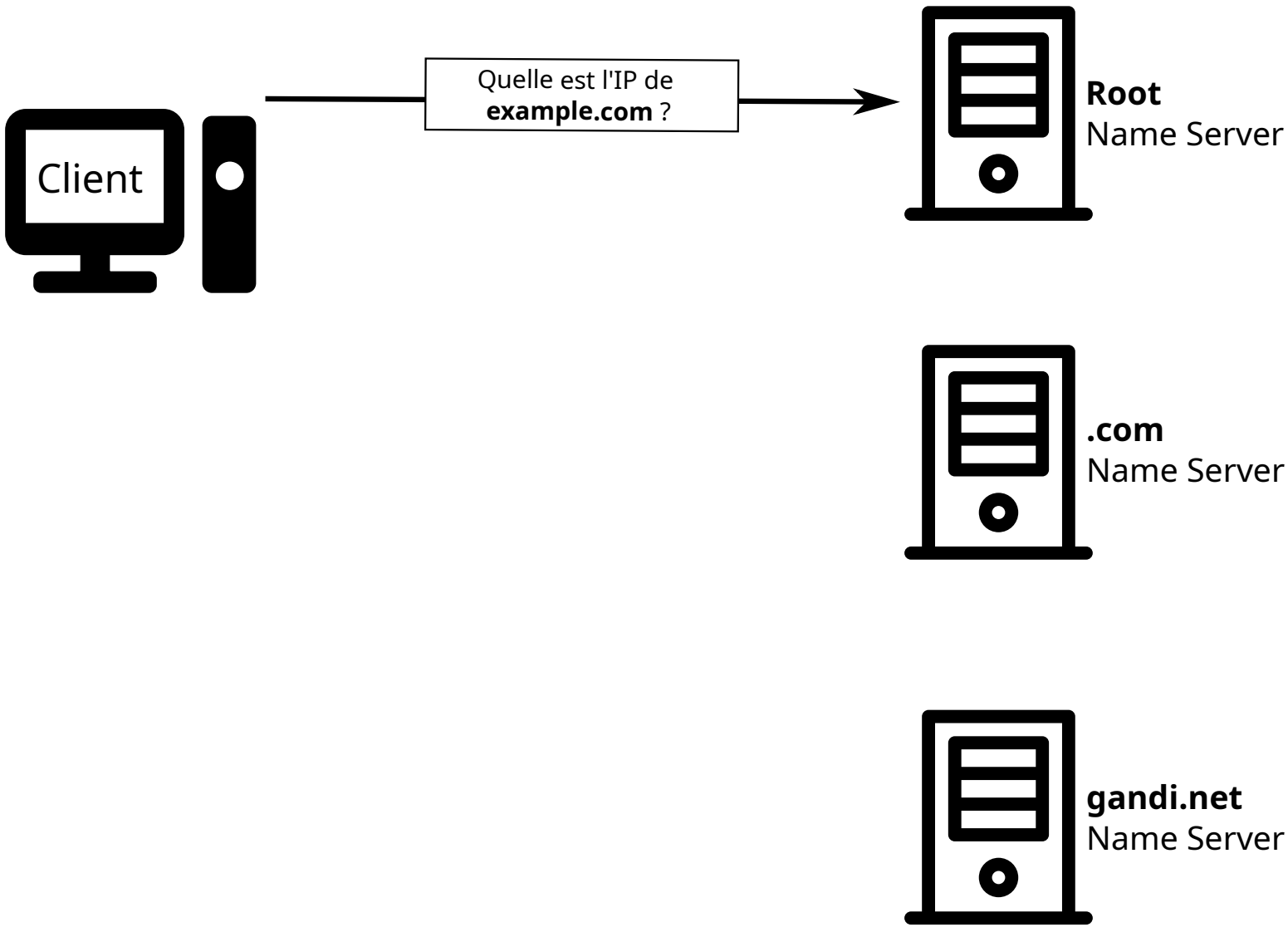


Root
Name Server

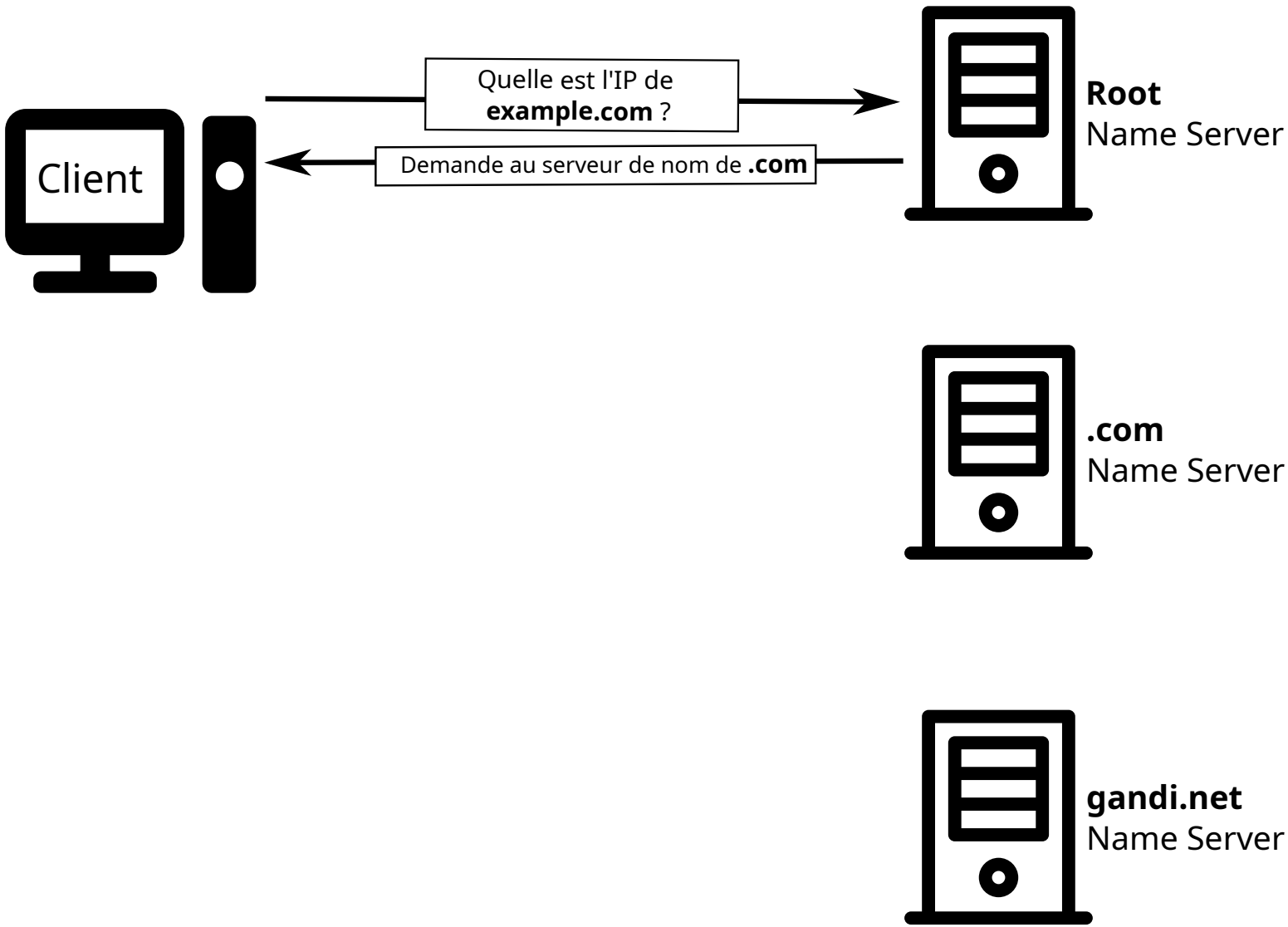
.com
Name Server

gandi.net
Name Server

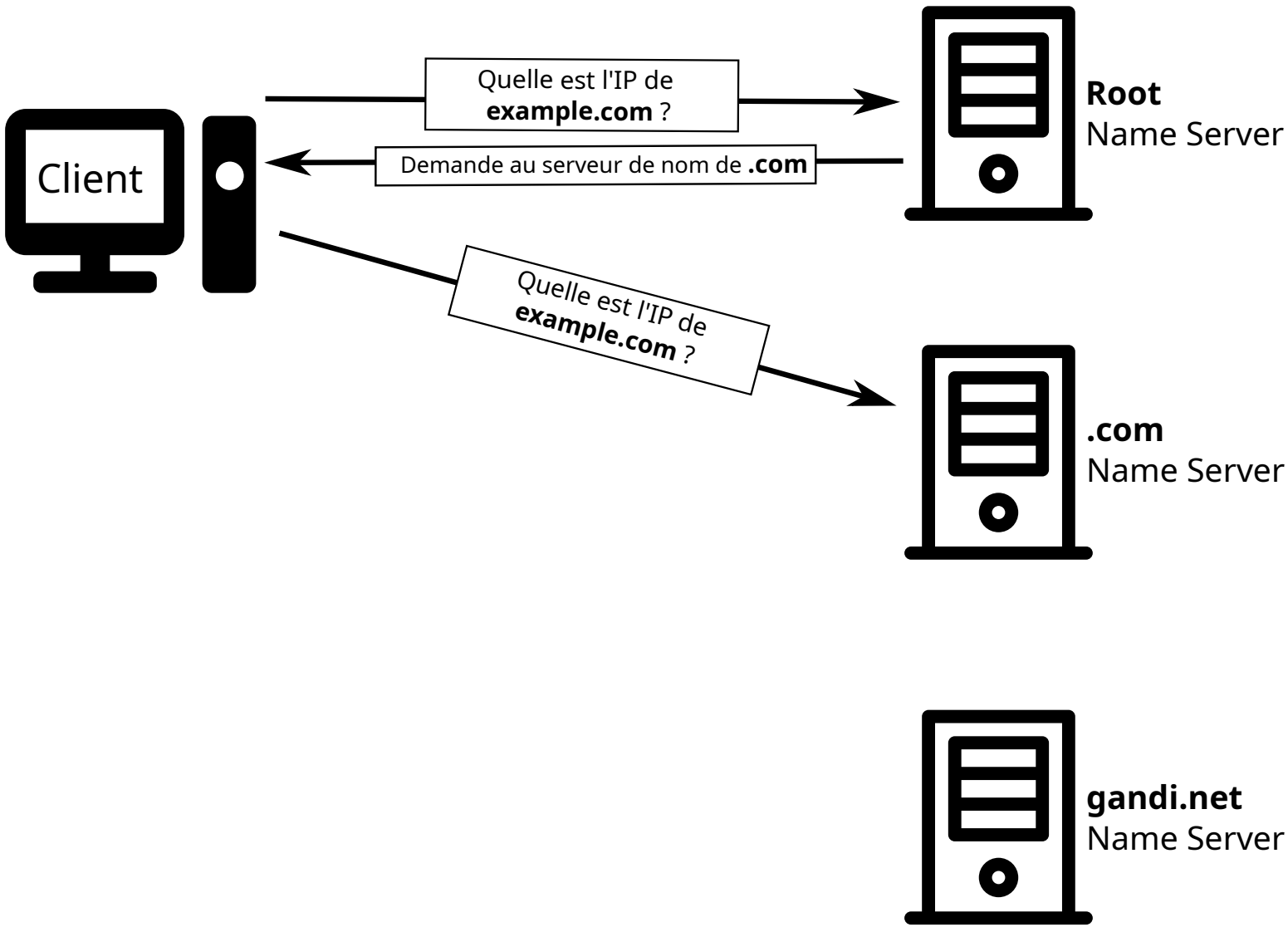
DNS - Architecture



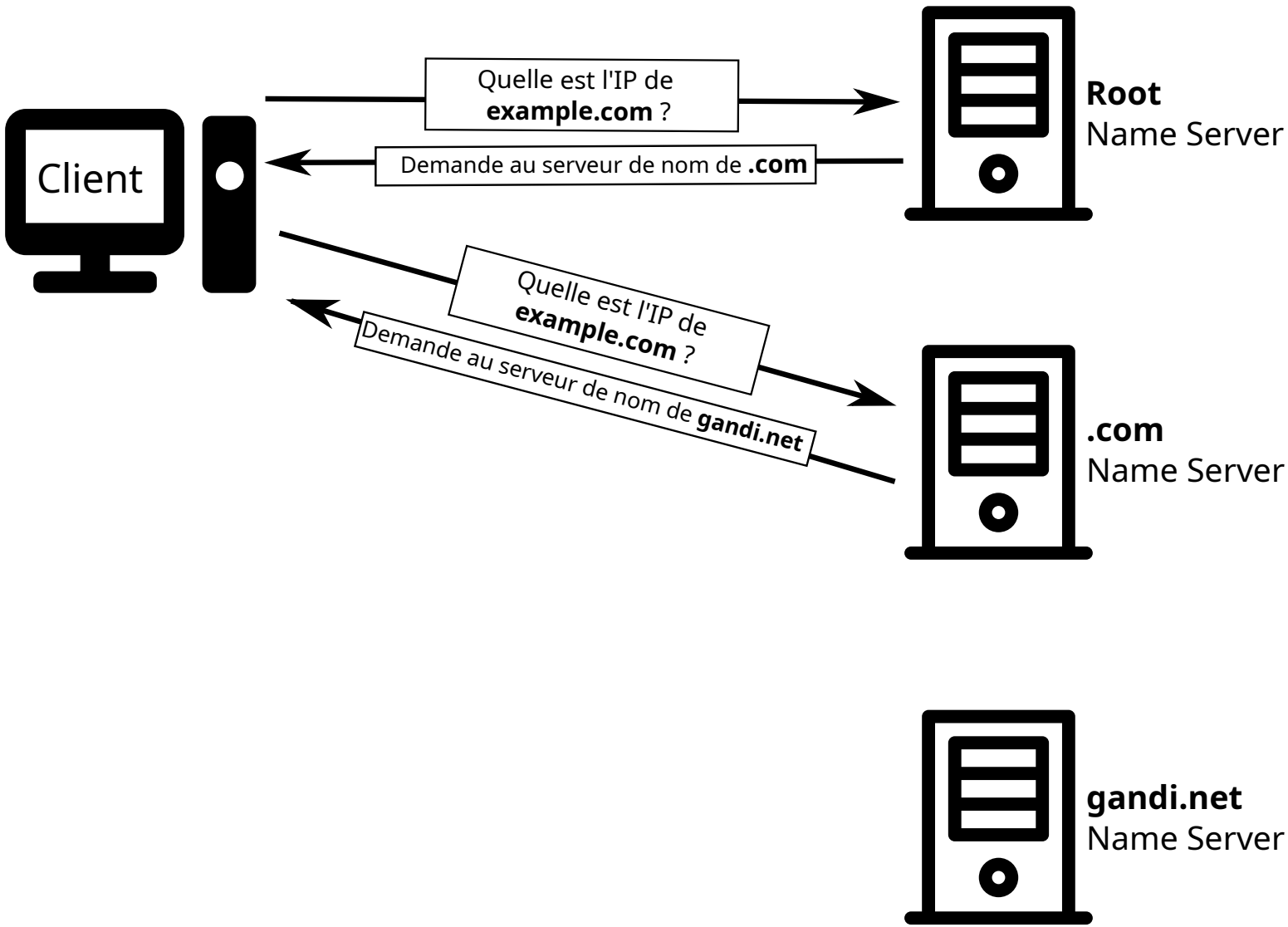
DNS - Architecture



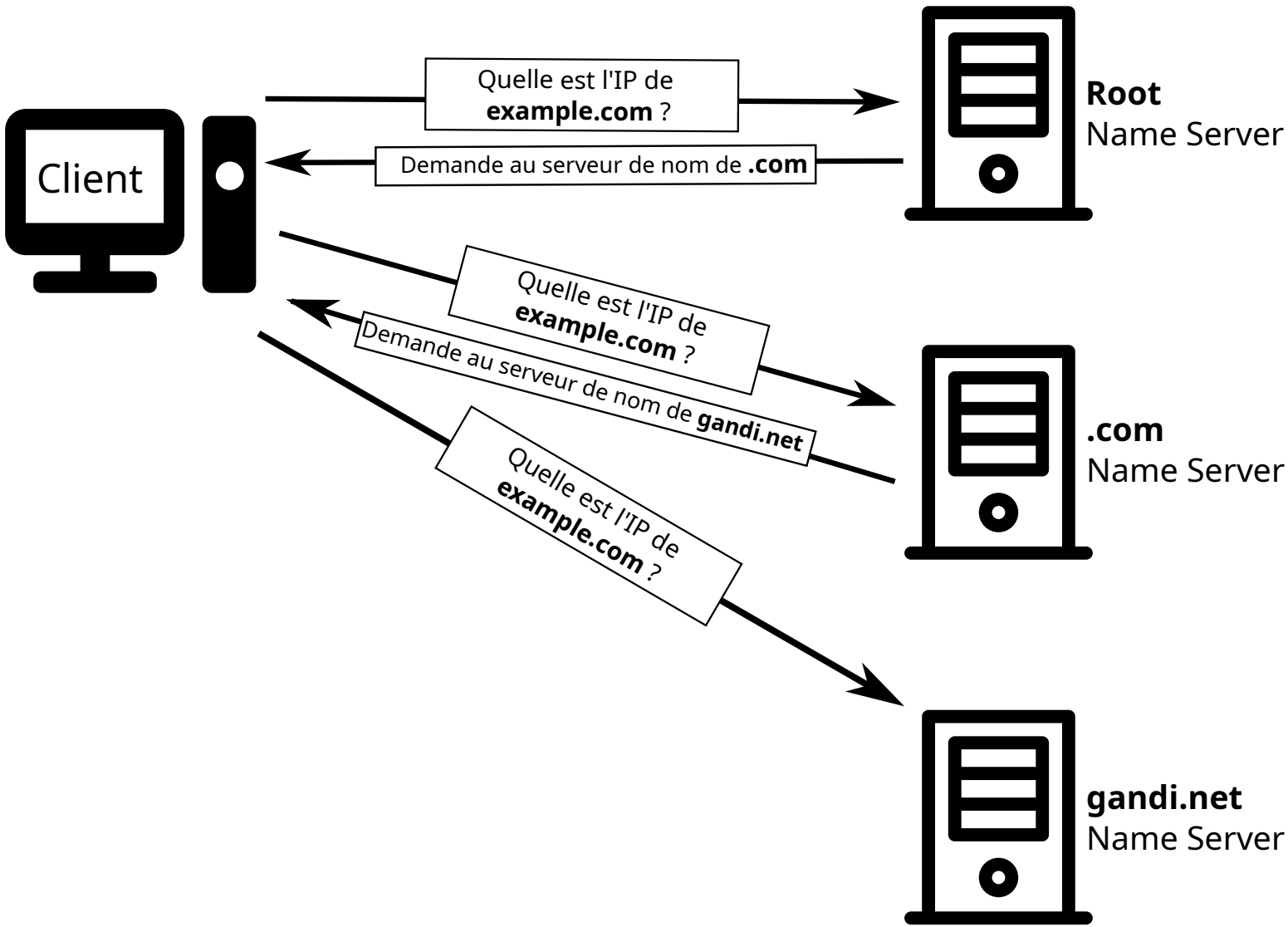
DNS - Architecture



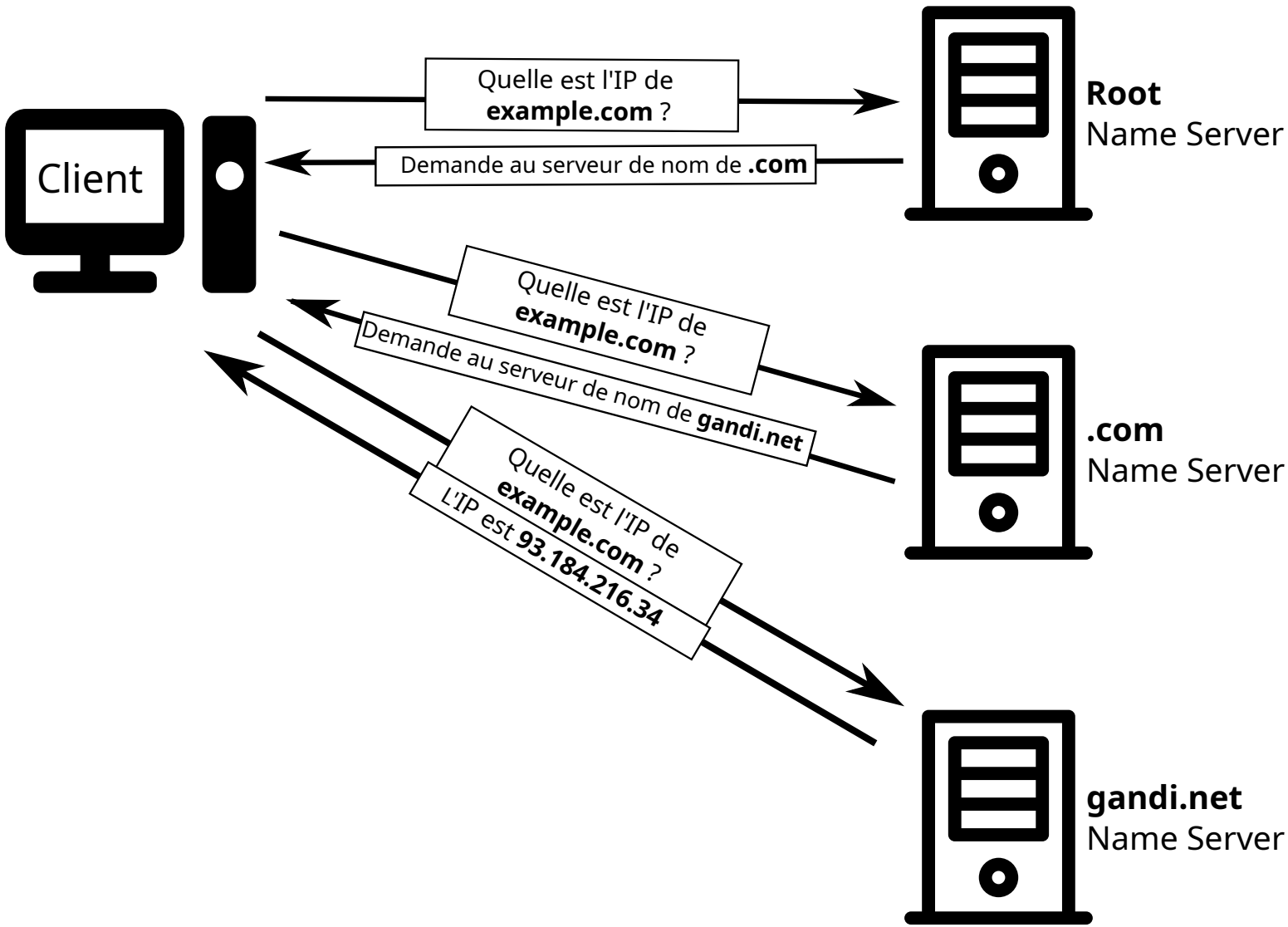
DNS - Architecture



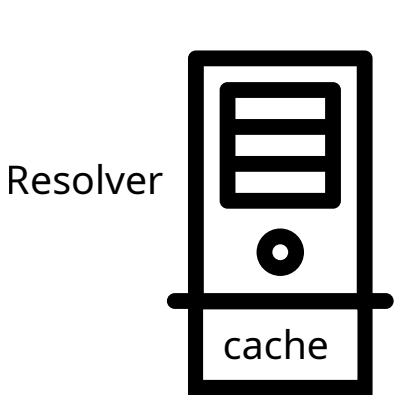
DNS - Architecture



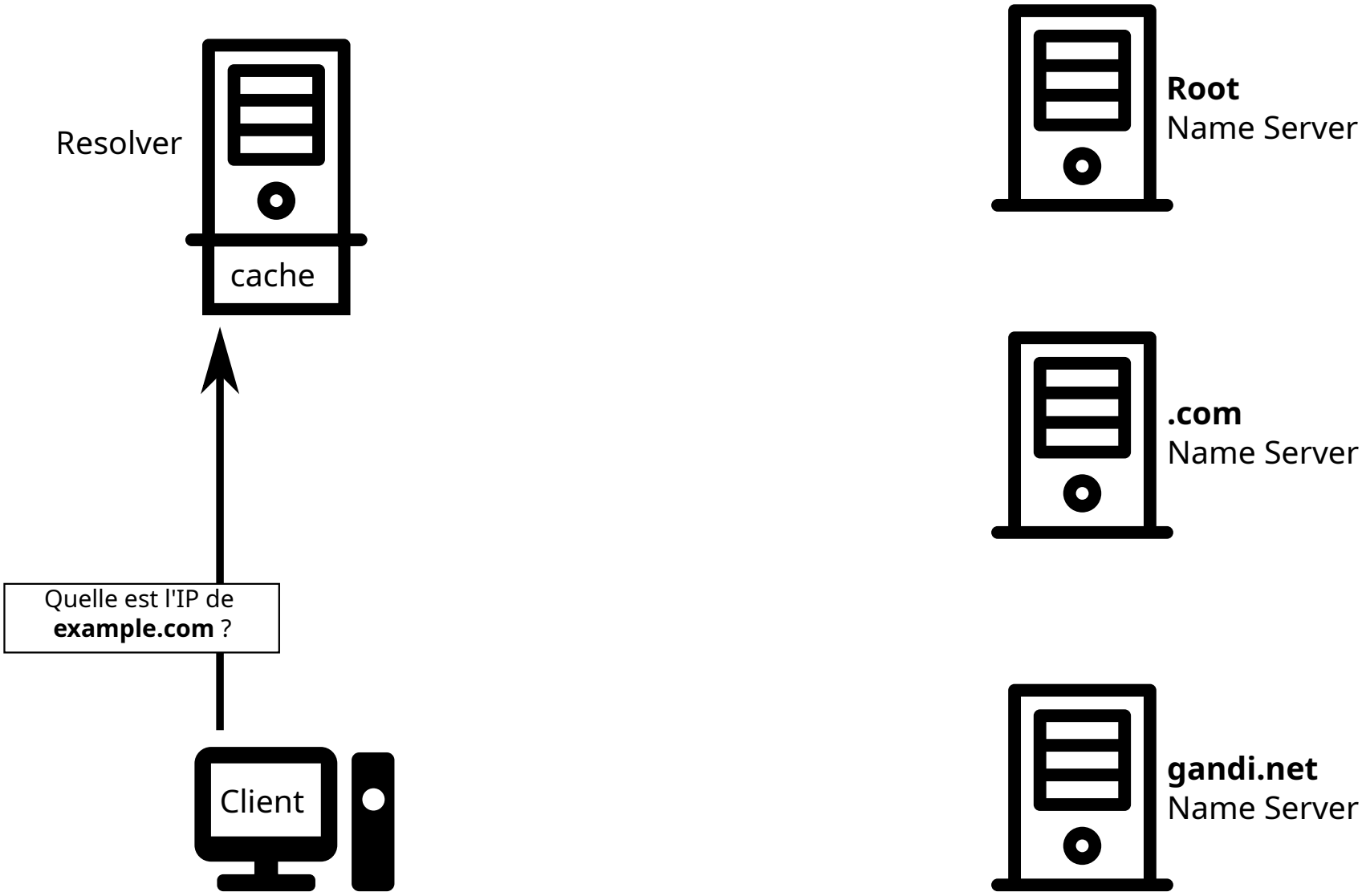
DNS - Architecture



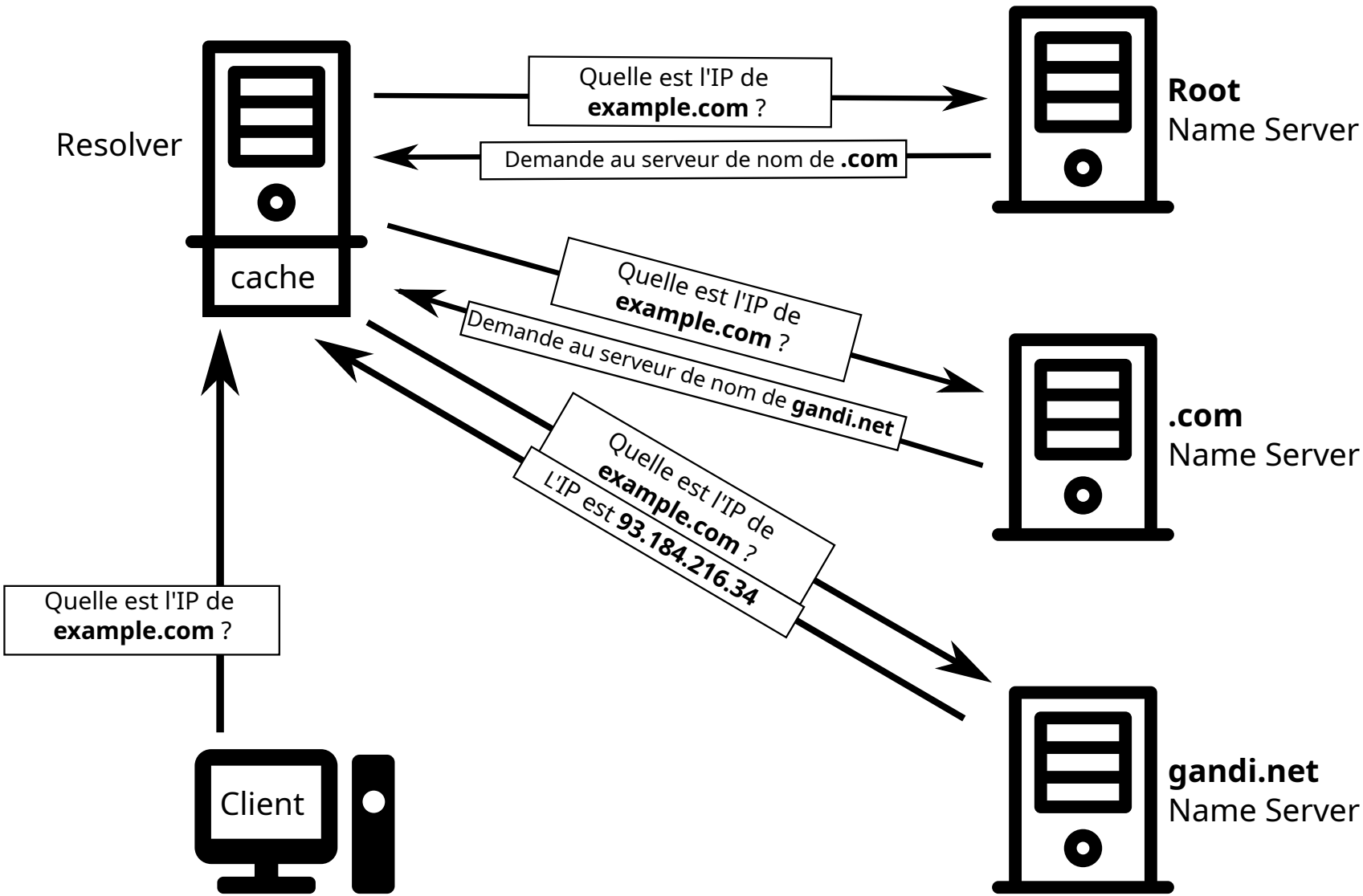
DNS - Architecture



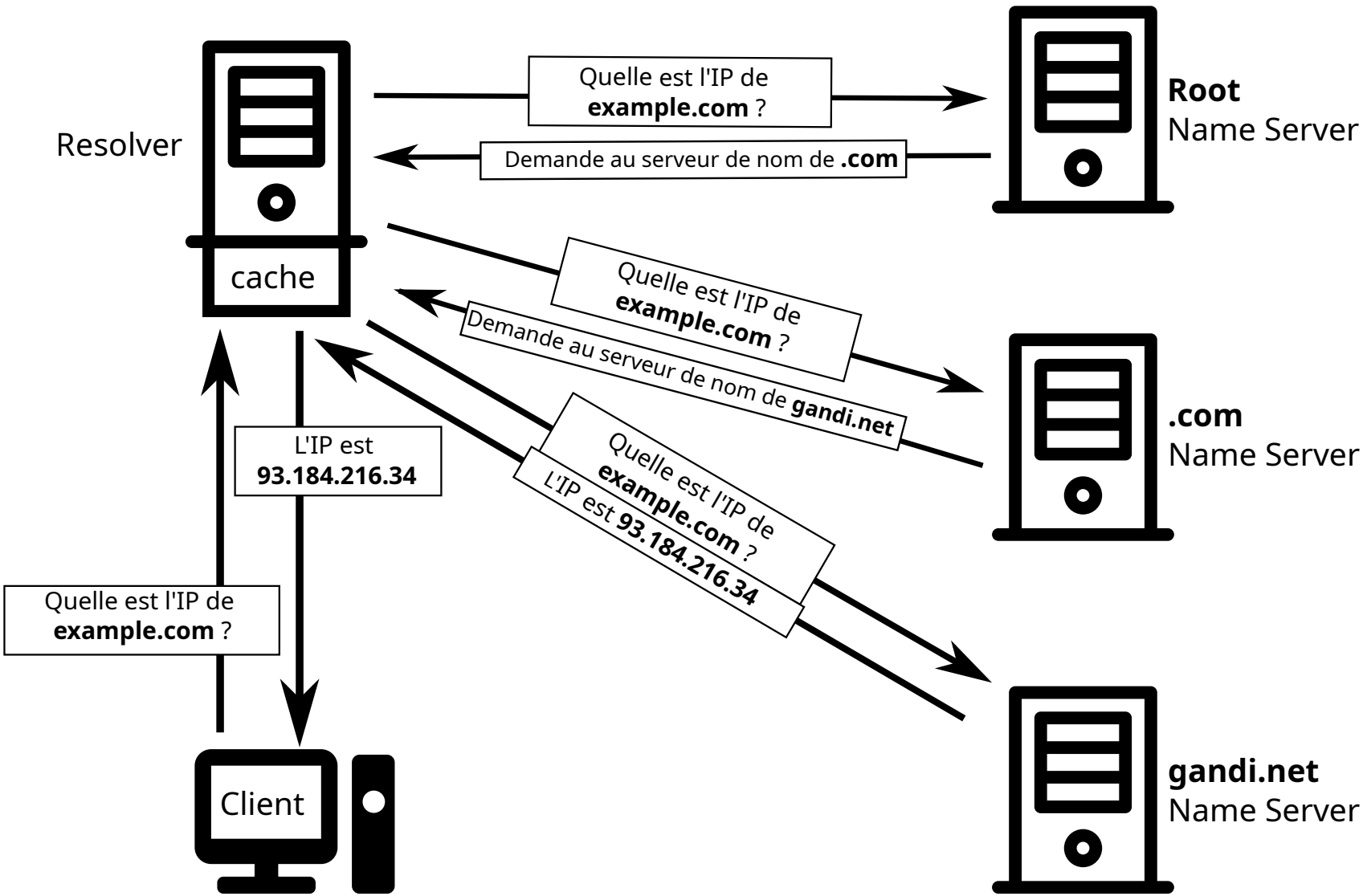
DNS - Architecture



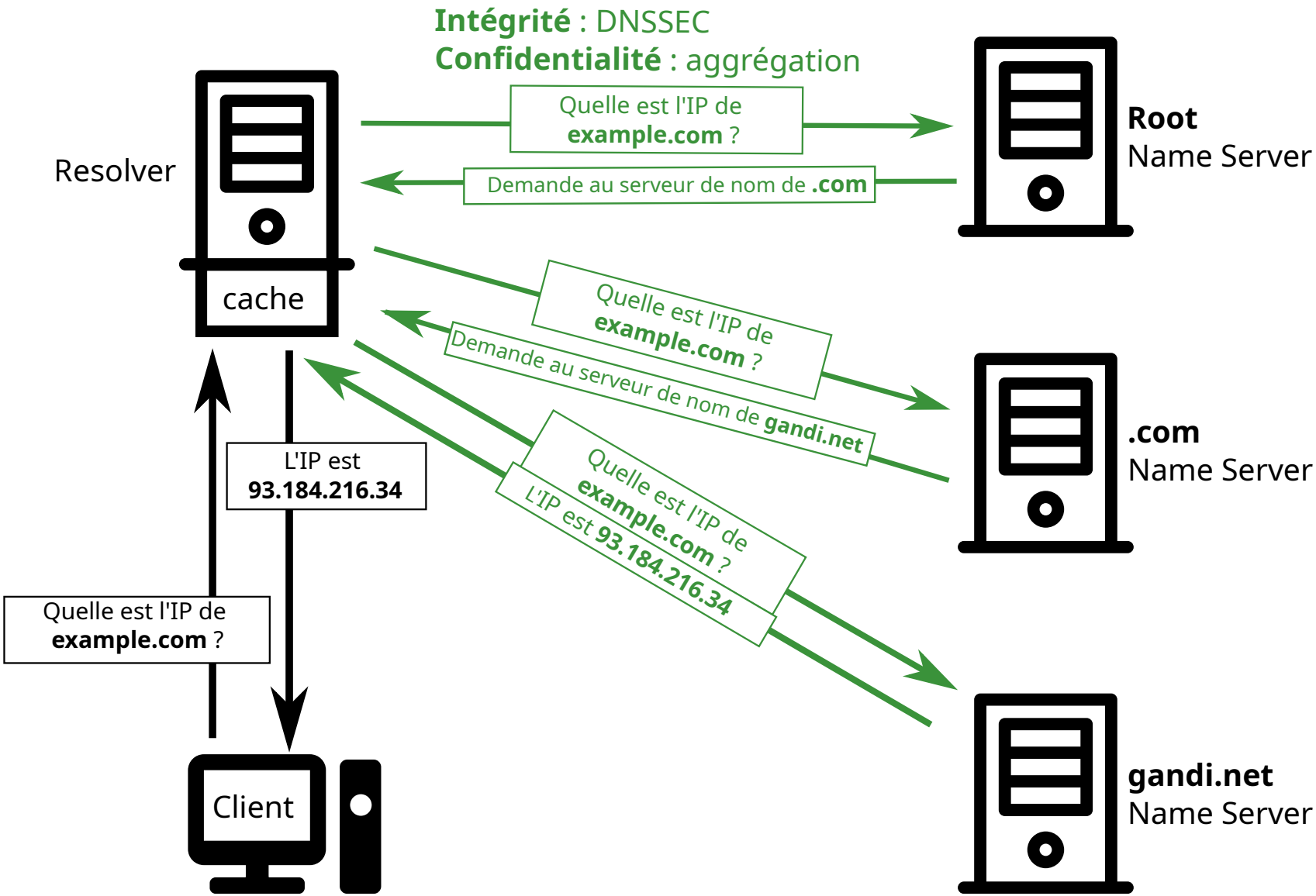
DNS - Architecture



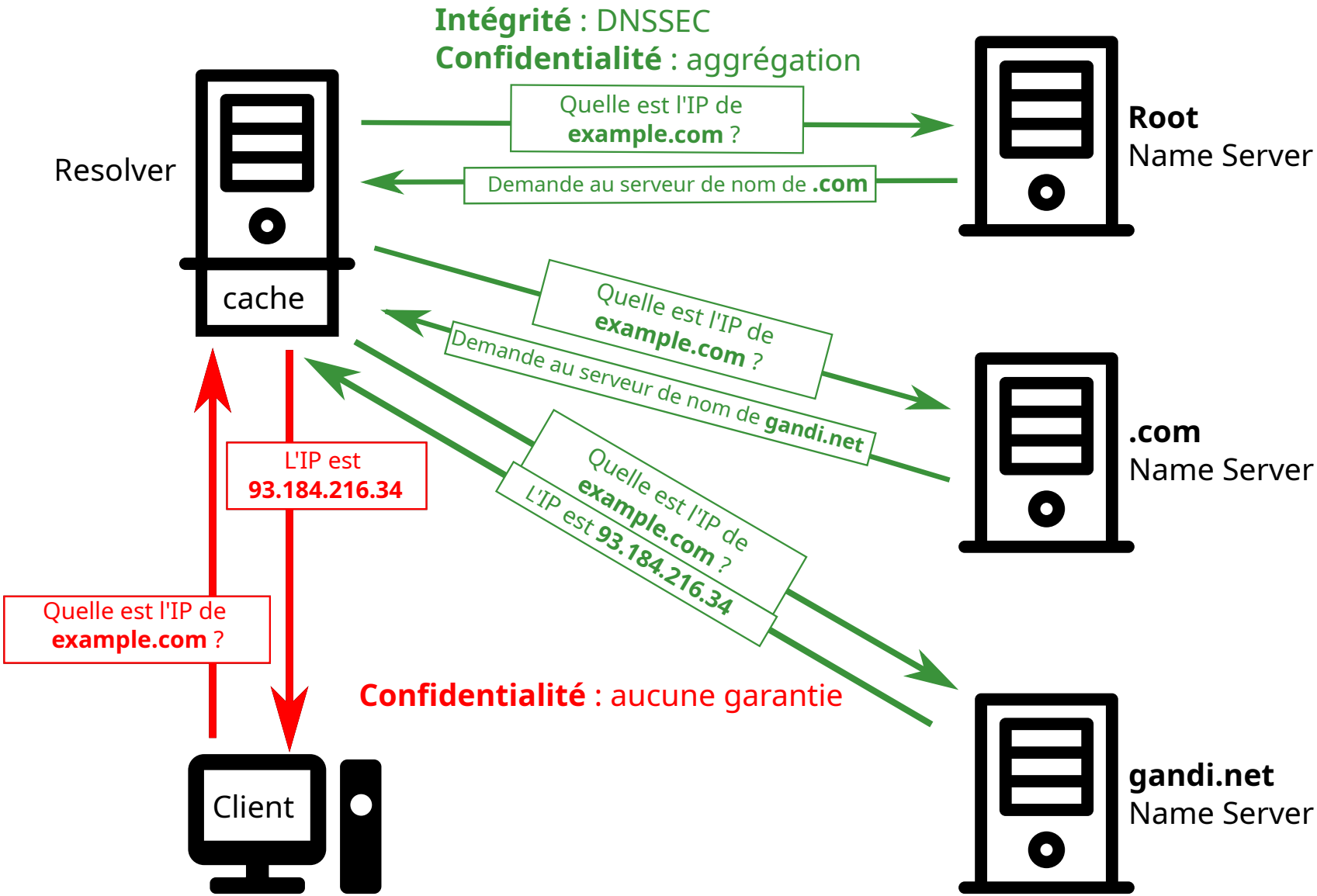
DNS - Architecture



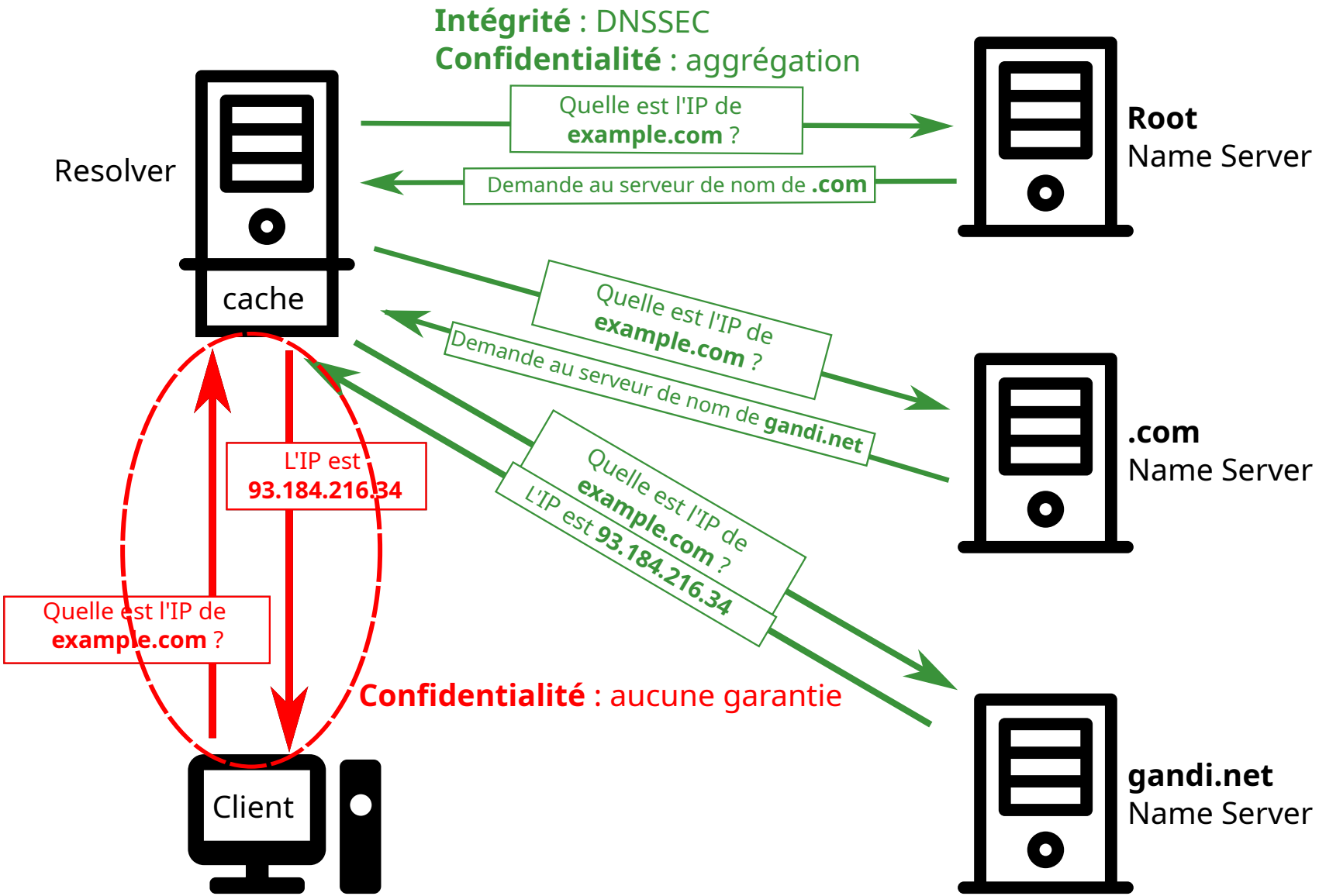
DNS - Architecture



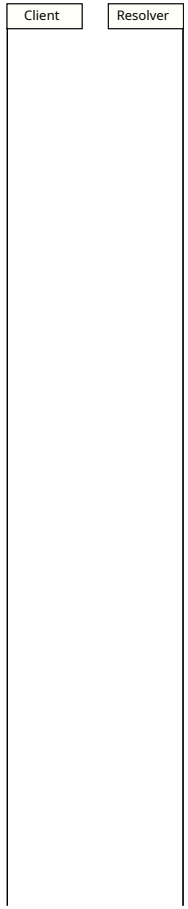
DNS - Architecture



DNS - Architecture

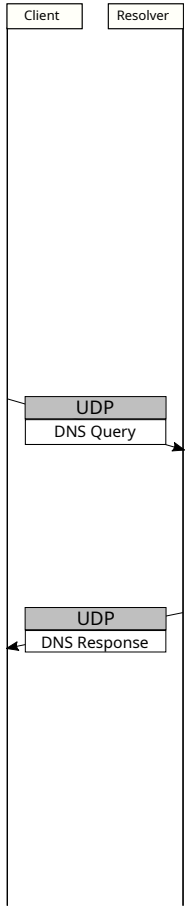


Protocoles



DNS over UDP
(DoUDP)

Protocoles

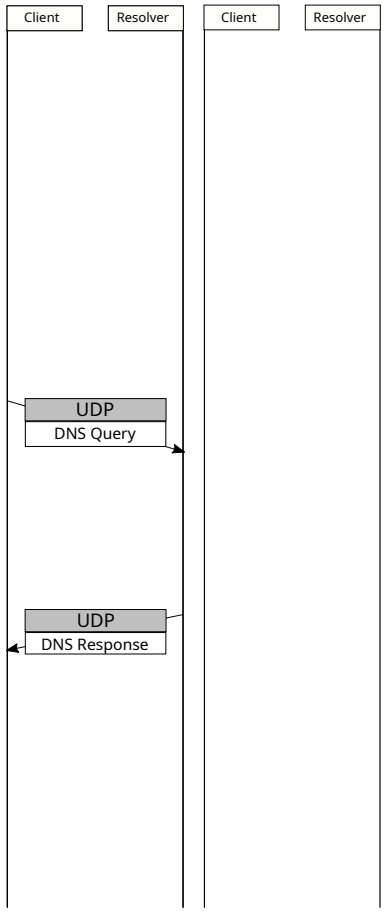


DNS over UDP (DoUDP)

Le plus simple

2 messages

Protocoles



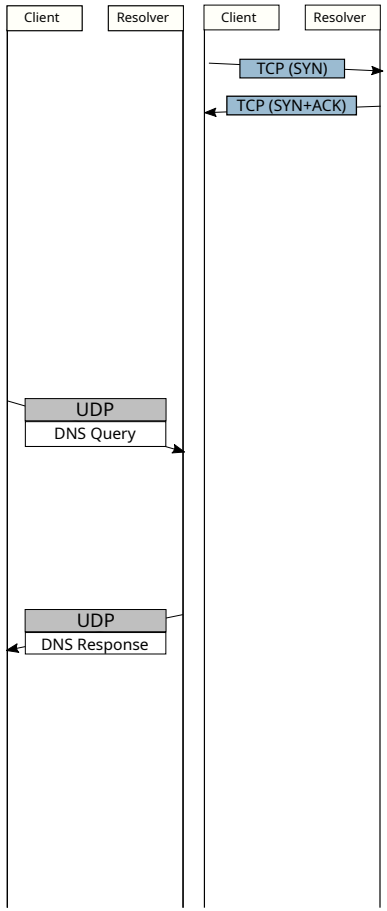
DNS over UDP (DoUDP)

Le plus simple

2 messages

DNS over TCP (DoTCP)

Protocoles



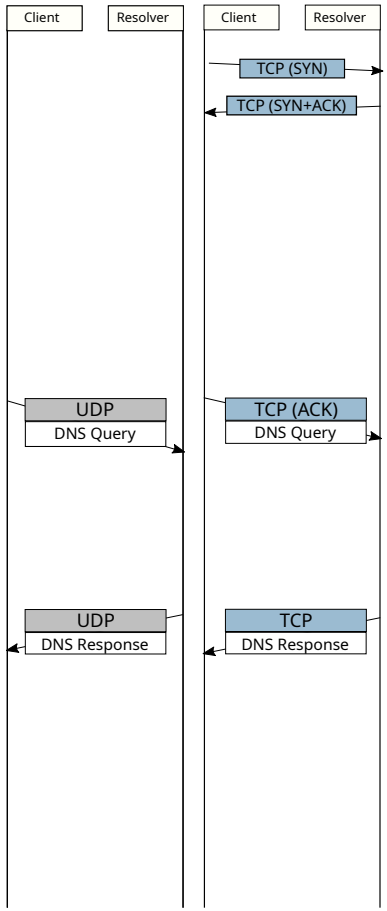
DNS over UDP (DoUDP)

Le plus simple

2 messages

DNS over TCP (DoTCP)

Protocoles



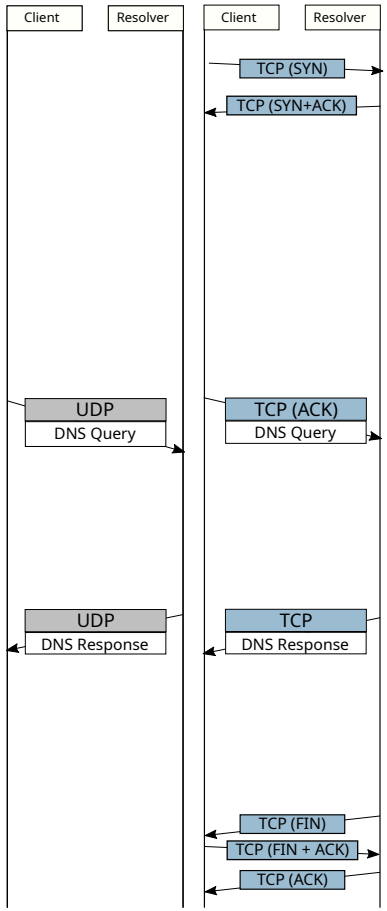
DNS over UDP (DoUDP)

Le plus simple

2 messages

DNS over TCP (DoTCP)

Protocoles



DNS over UDP (DoUDP)

Le plus simple

2 messages

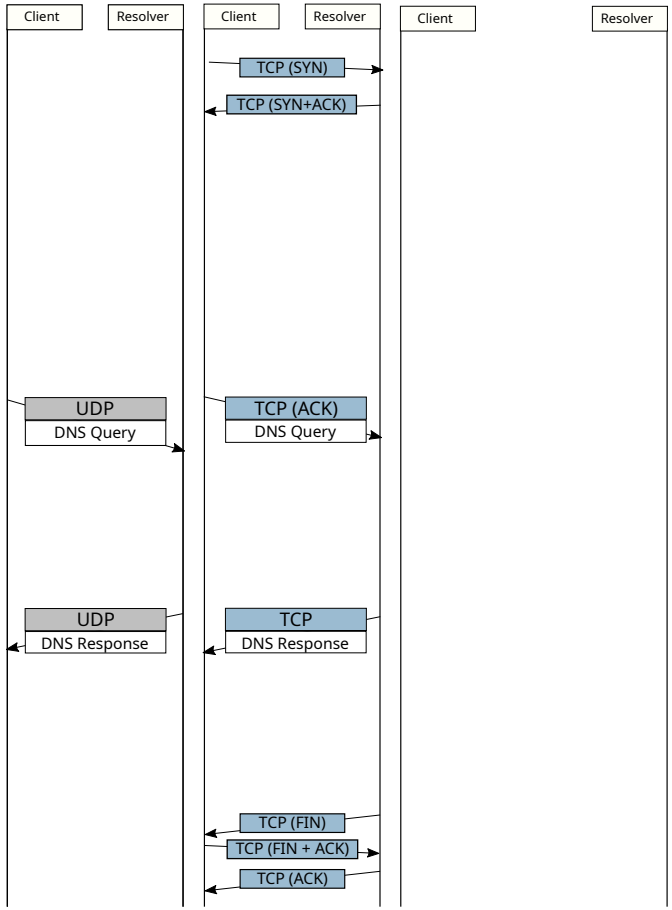
DNS over TCP (DoTCP)

Ajout connexion

8 messages

790 octets

Protocoles

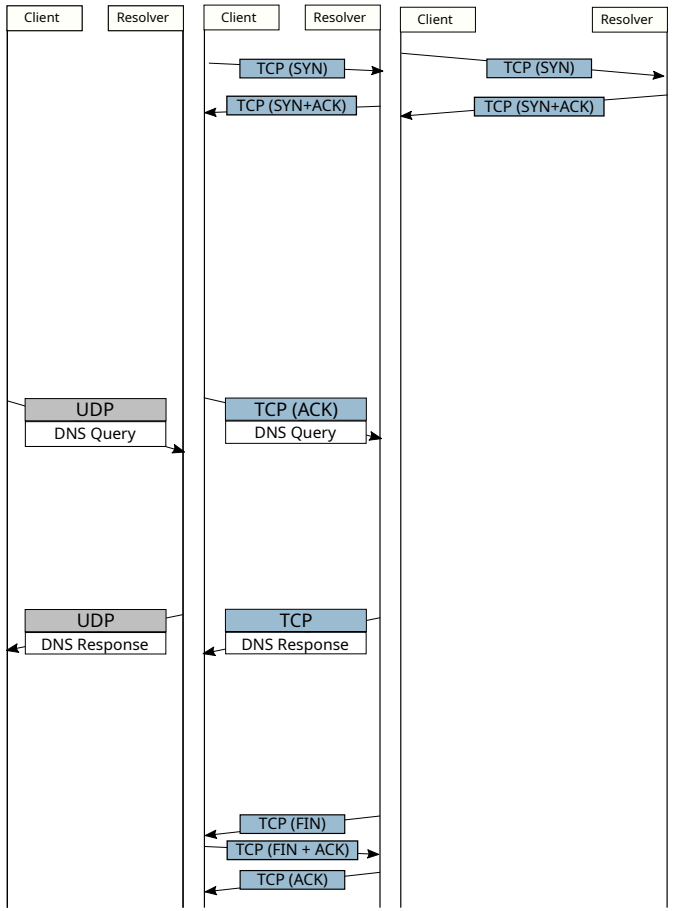


DNS over UDP (DoUDP)
Le plus simple
2 messages

DNS over TCP (DoTCP)
Ajout connexion
8 messages
790 octets

DNS over TLS (DoT)

Protocoles

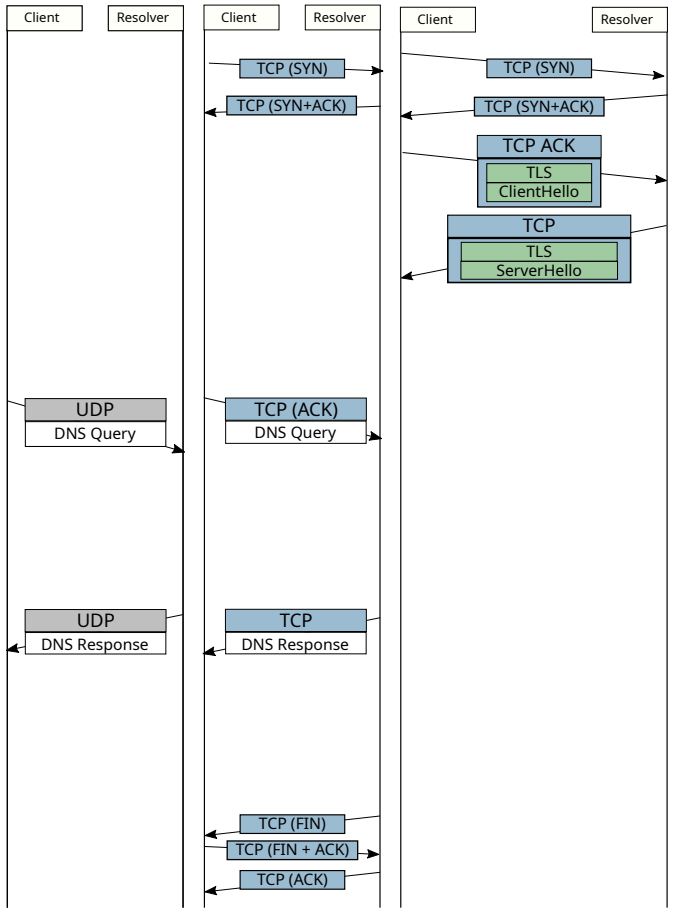


DNS over UDP (DoUDP)
Le plus simple
2 messages

DNS over TCP (DoTCP)
Ajout connexion
8 messages
790 octets

DNS over TLS (DoT)

Protocoles

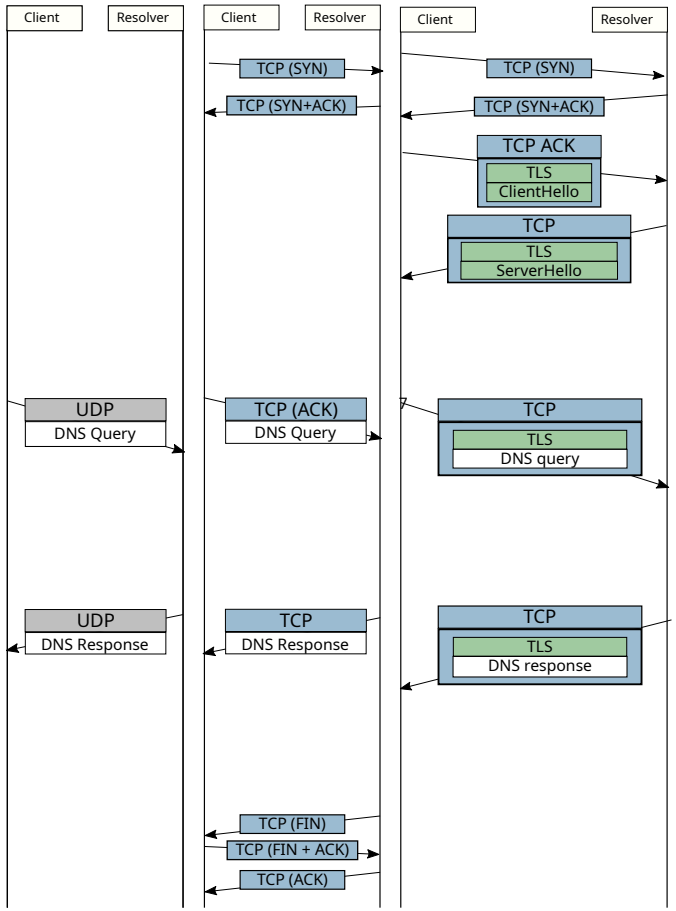


DNS over UDP (DoUDP)
Le plus simple
2 messages

DNS over TCP (DoTCP)
Ajout connexion
8 messages
790 octets

DNS over TLS (DoT)

Protocoles

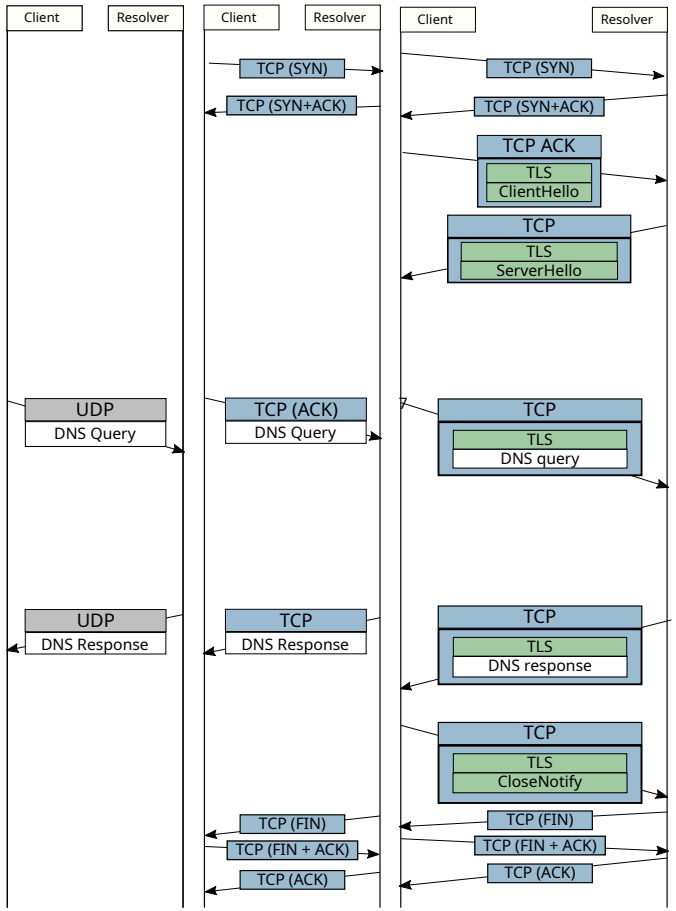


DNS over UDP (DoUDP)
Le plus simple
2 messages

DNS over TCP (DoTCP)
Ajout connexion
8 messages
790 octets

DNS over TLS (DoT)

Protocoles

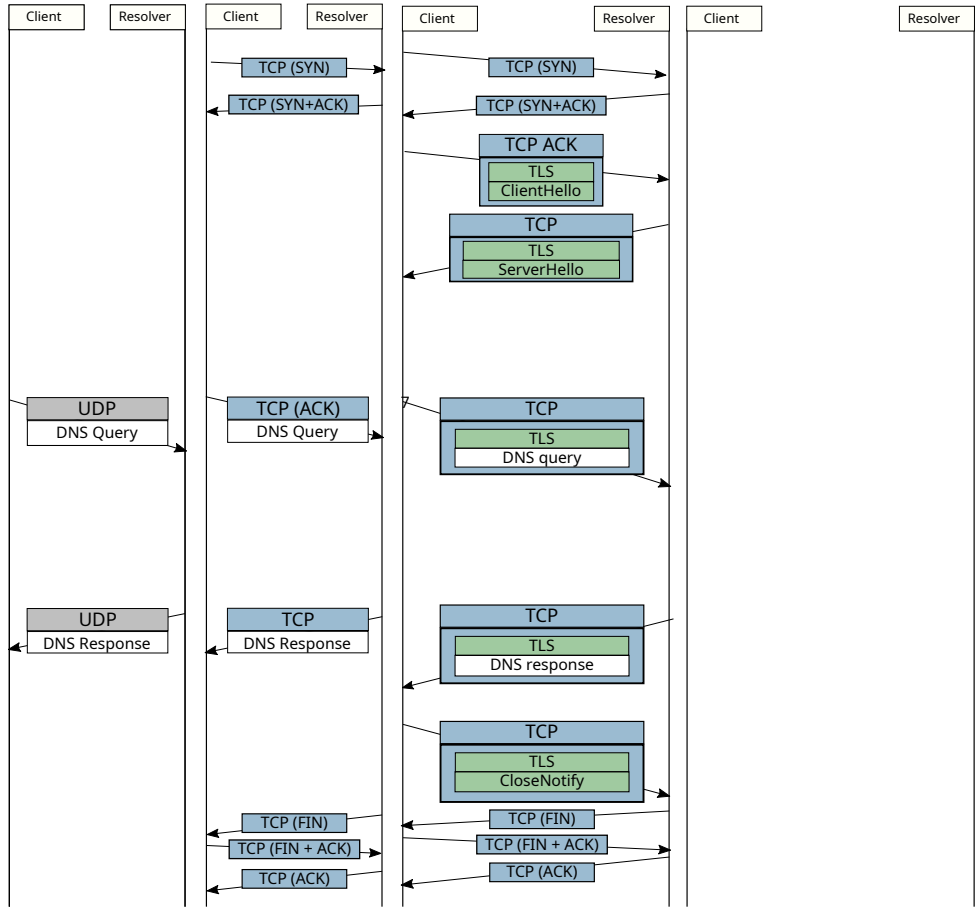


DNS over UDP (DoUDP)
Le plus simple
2 messages

DNS over TCP (DoTCP)
Ajout connexion
8 messages
790 octets

DNS over TLS (DoT)
Ajout chiffrement
10 messages
5589 octets
119 octets chiffrés

Protocoles



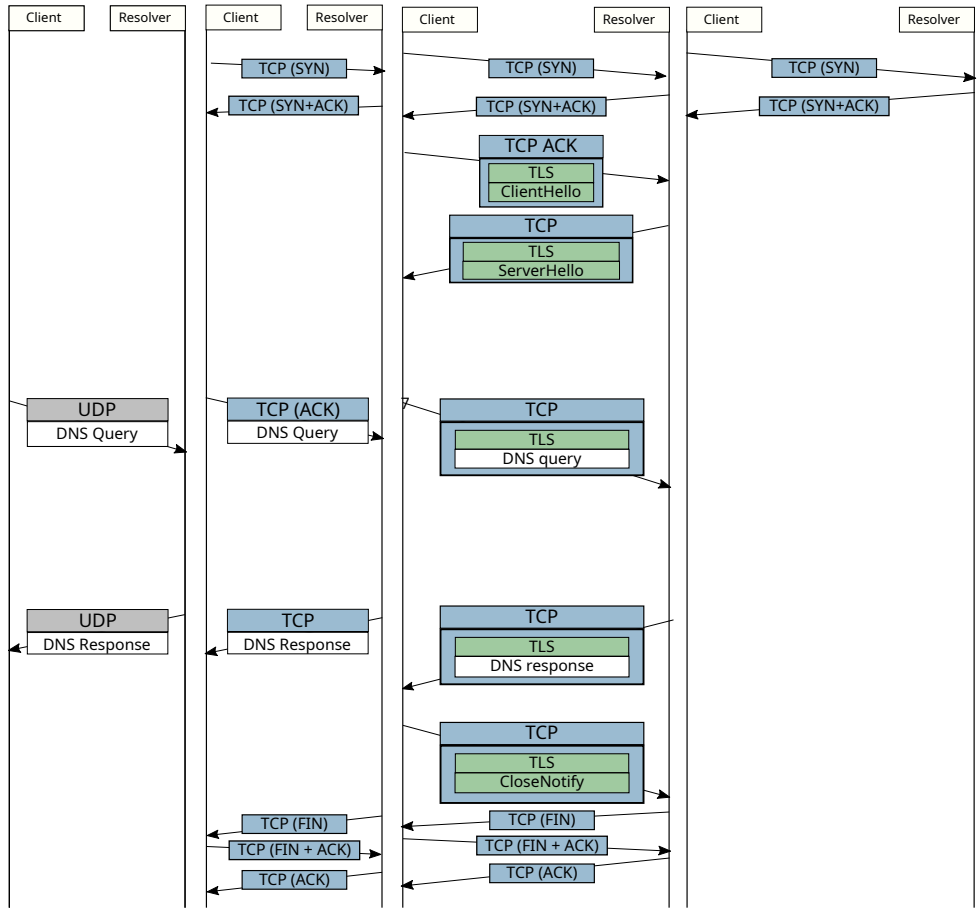
DNS over UDP (DoUDP)
Le plus simple
2 messages

DNS over TCP (DoTCP)
Ajout connexion
8 messages
790 octets

DNS over TLS (DoT)
Ajout chiffrement
10 messages
5589 octets
119 octets chiffrés

DNS over HTTPS (DoH)

Protocoles



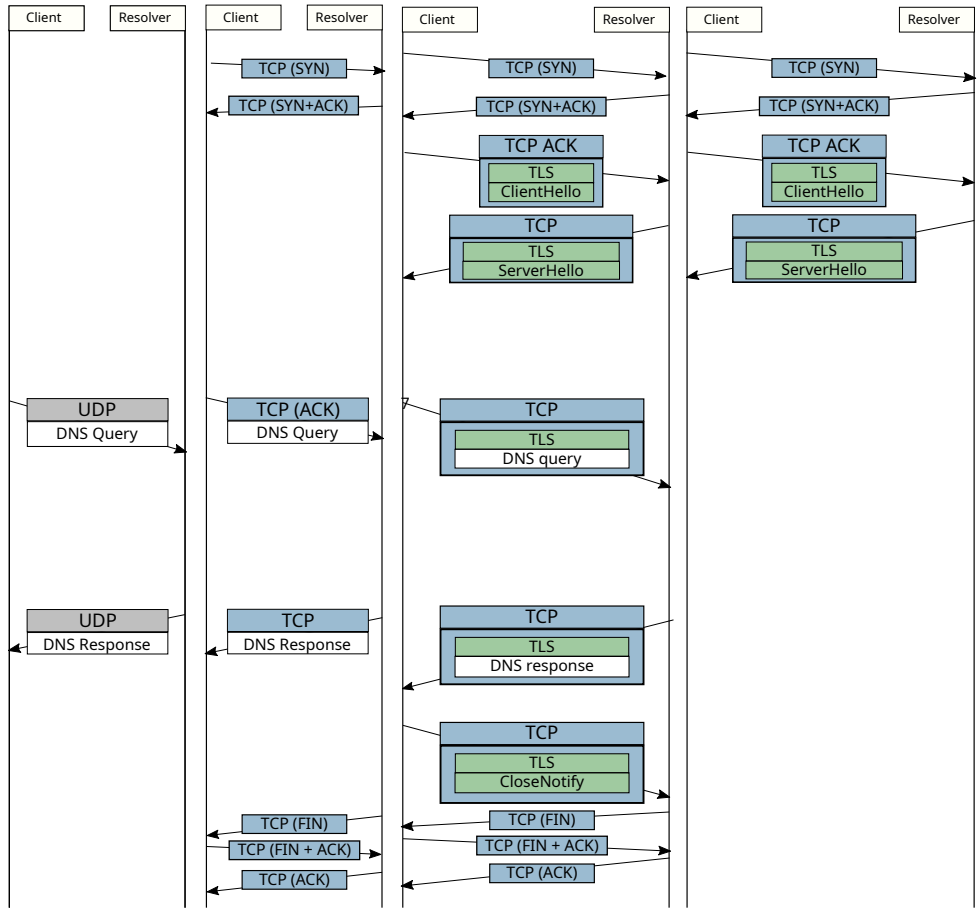
DNS over UDP (DoUDP)
Le plus simple
2 messages

DNS over TCP (DoTCP)
Ajout connexion
8 messages
790 octets

DNS over TLS (DoT)
Ajout chiffrement
10 messages
5589 octets
119 octets chiffrés

DNS over HTTPS (DoH)

Protocoles



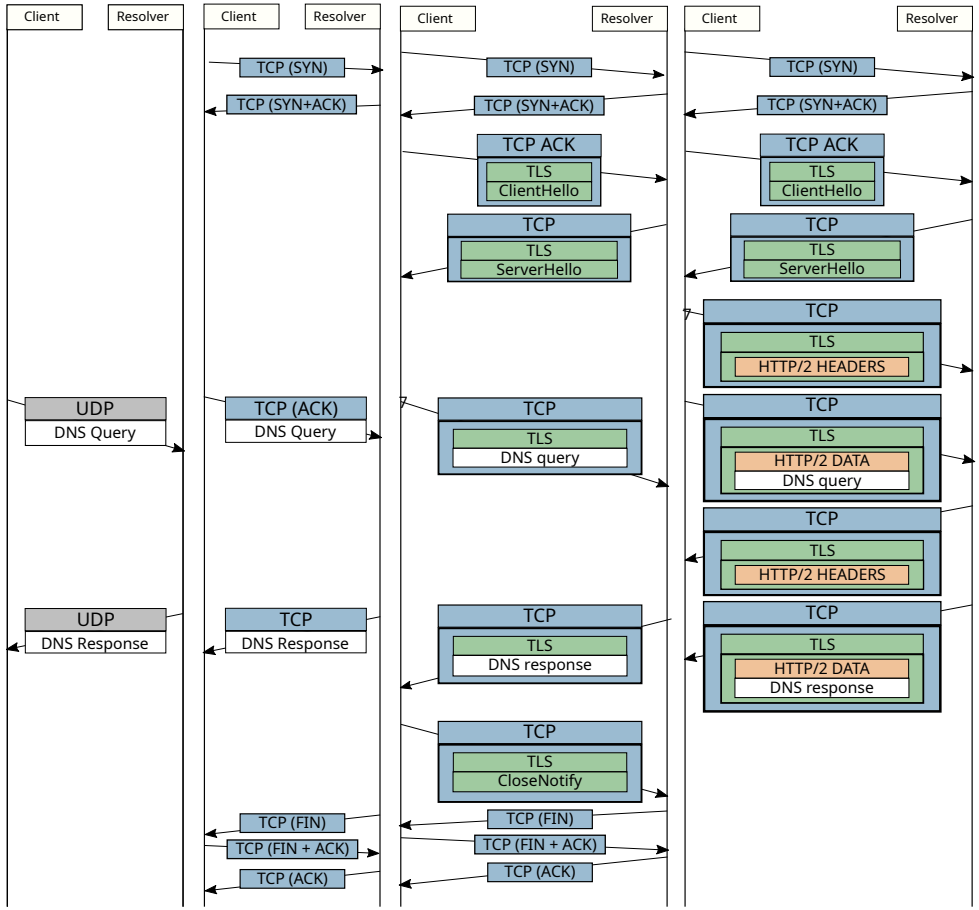
DNS over UDP (DoUDP)
Le plus simple
2 messages

DNS over TCP (DoTCP)
Ajout connexion
8 messages
790 octets

DNS over TLS (DoT)
Ajout chiffrement
10 messages
5589 octets
119 octets chiffrés

DNS over HTTPS (DoH)

Protocoles



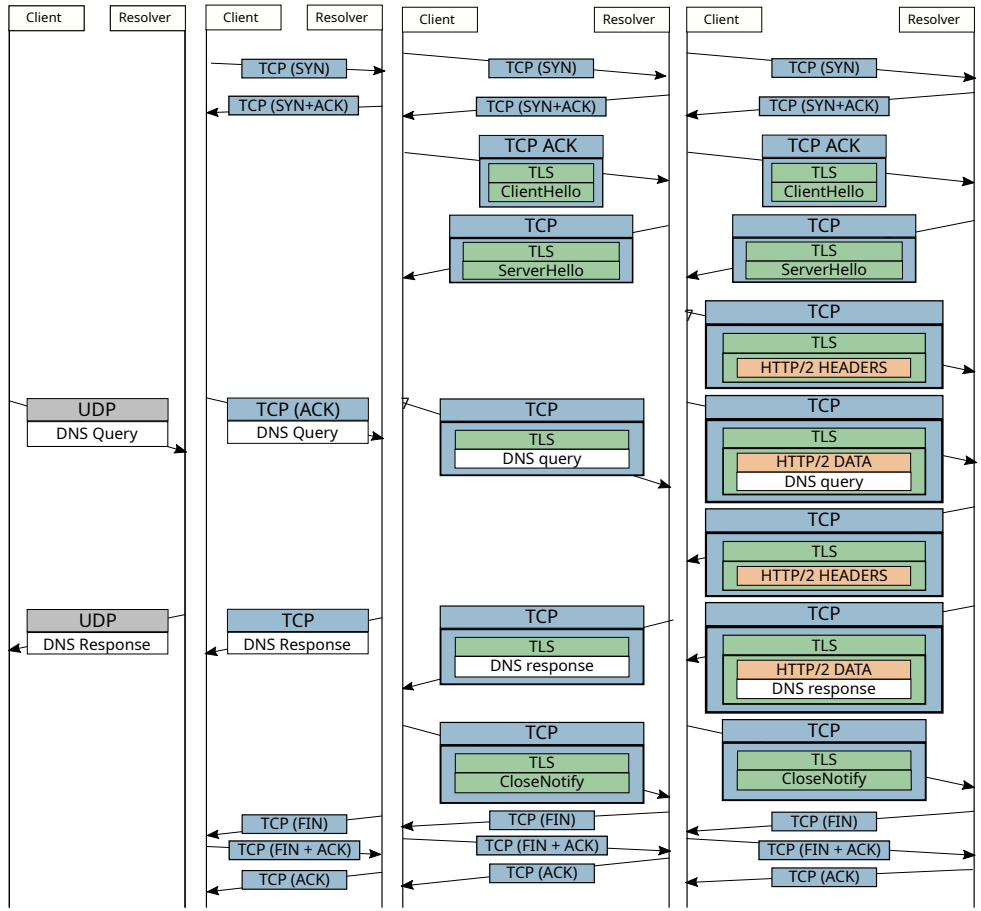
DNS over UDP (DoUDP)
Le plus simple
2 messages

DNS over TCP (DoTCP)
Ajout connexion
8 messages
790 octets

DNS over TLS (DoT)
Ajout chiffrement
10 messages
5589 octets
119 octets chiffrés

DNS over HTTPS (DoH)

Protocoles



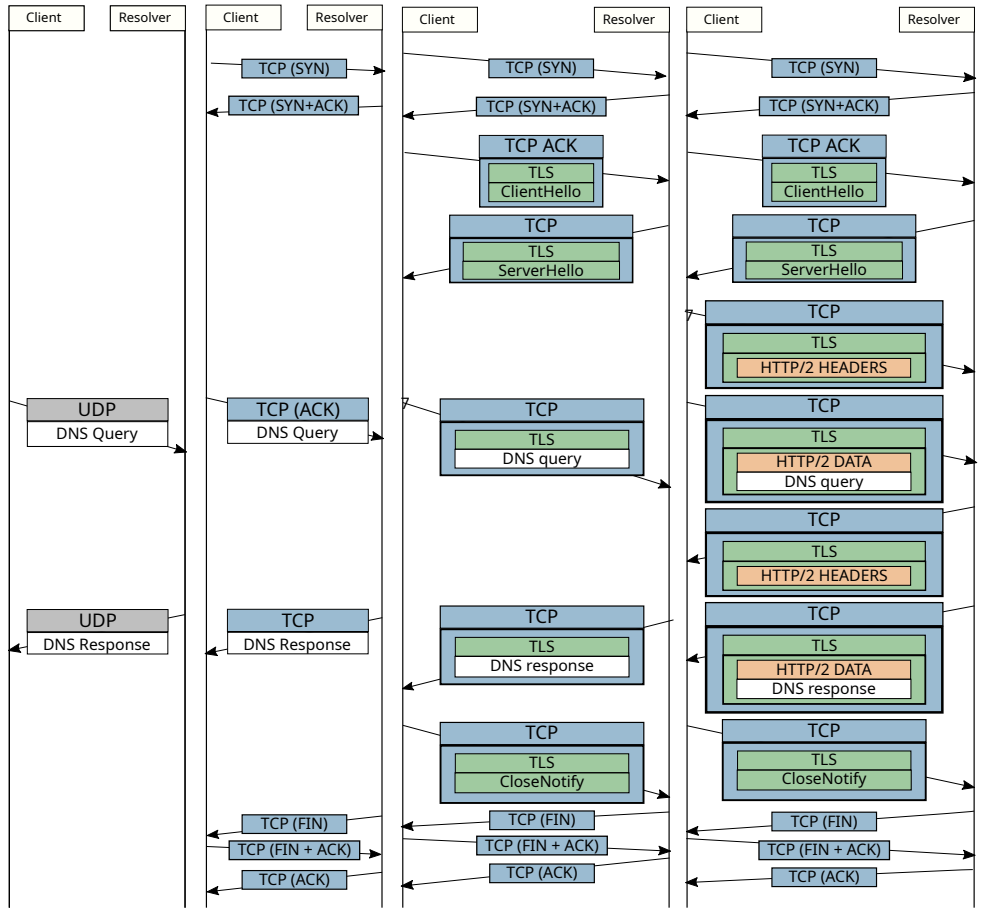
DNS over UDP (DoUDP)
Le plus simple
2 messages

DNS over TCP (DoTCP)
Ajout connexion
8 messages
790 octets

DNS over TLS (DoT)
Ajout chiffrement
10 messages
5589 octets
119 octets chiffrés

DNS over HTTPS (DoH)
Passage firewall
12 messages
6350 octets
515 octets chiffrés

Protocoles



DNS over UDP (DoUDP)
Le plus simple
2 messages

DNS over TCP (DoTCP)
Ajout connexion
8 messages
790 octets

DNS over TLS (DoT)
Ajout chiffrement
10 messages
5589 octets
119 octets chiffrés

DNS over HTTPS (DoH)
Passage firewall
12 messages
6350 octets
515 octets chiffrés

DoH représente aujourd'hui 1% du trafic DNS. Quel est le coût, en ressources serveur, d'y passer entièrement ?

Problématique

Comment les clients et serveurs déjà déployés utilisent DoH ?

Problématique

Comment les clients et serveurs déjà déployés utilisent DoH ?

Comment l'ajout de couche protocolaires affecte-t-il les performances du resolver ?

Problématique

Comment les clients et serveurs déjà déployés utilisent DoH ?

Comment l'ajout de couche protocolaires affecte-t-il les performances du resolver ?

- Quel est le surcoût lié au traitement des requêtes ?

Problématique

Comment les clients et serveurs déjà déployés utilisent DoH ?

Comment l'ajout de couche protocolaires affecte-t-il les performances du resolver ?

- Quel est le surcoût lié au traitement des requêtes ?
- Quel est le surcoût lié à l'ouverture et la gestion des connexions ?

Comportement des clients - Protocole

Comportement des clients - Protocole

Logiciels x resolvers testés :

Firefox	X	Cloudflare
Chromium		Google
dnscrypt-proxy		Quad9

Comportement des clients - Protocole

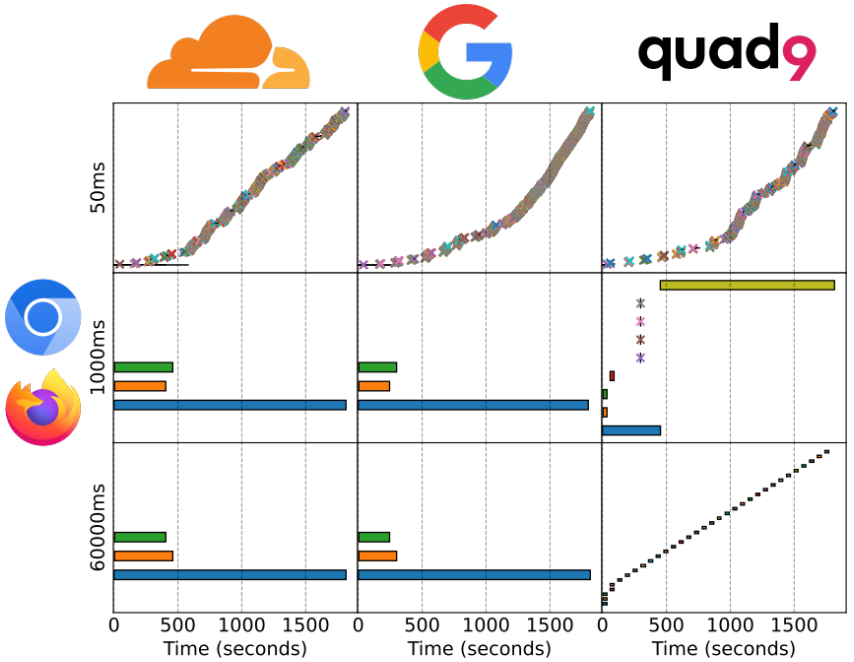
Logiciels x resolvers testés :

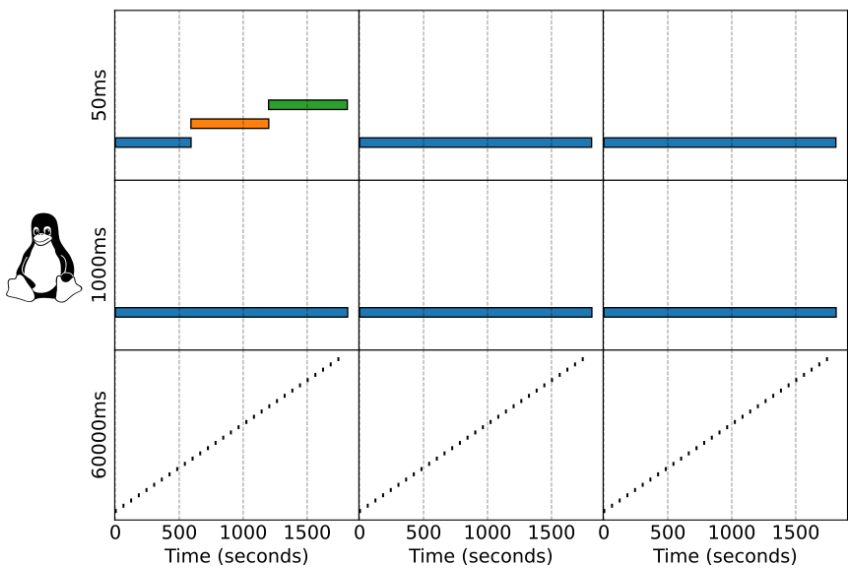
Firefox	X	Cloudflare
Chromium		Google
dnscrypt-proxy		Quad9

Métriques considérées :

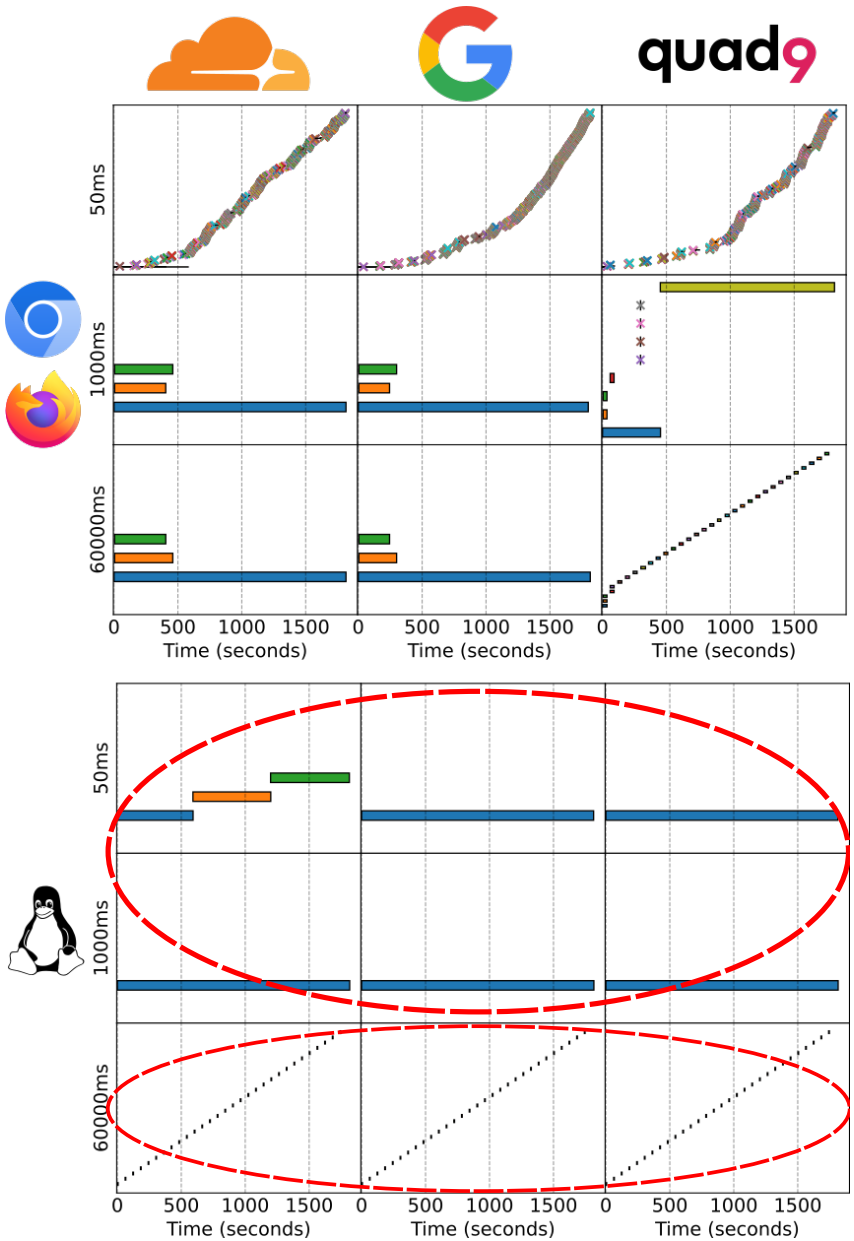
- Durées des connections
- Nombre de requêtes par connexion
- Origine de la fermeture

Comportement des clients - résultats



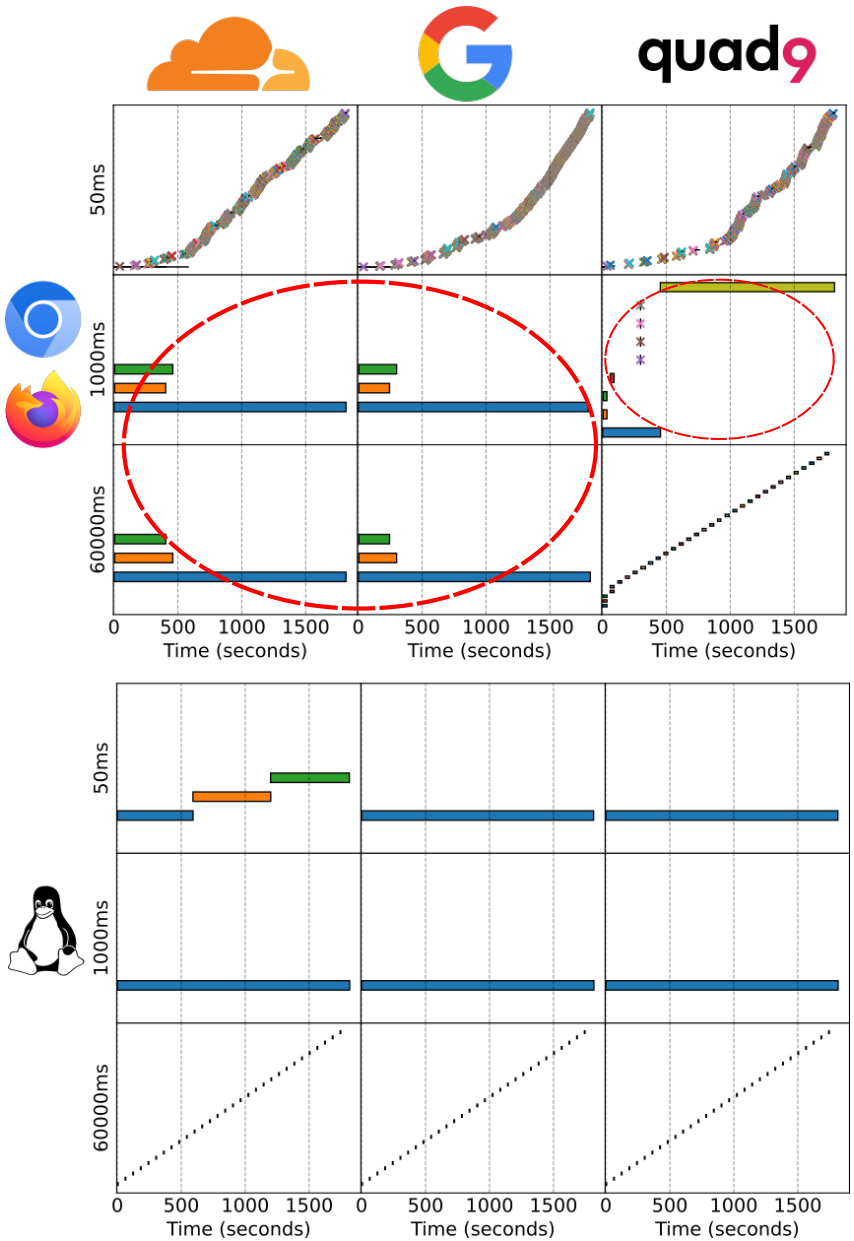


Comportement des clients - résultats



DNScrypt garde les connexions ouvertes, mais a un timeout de 5s

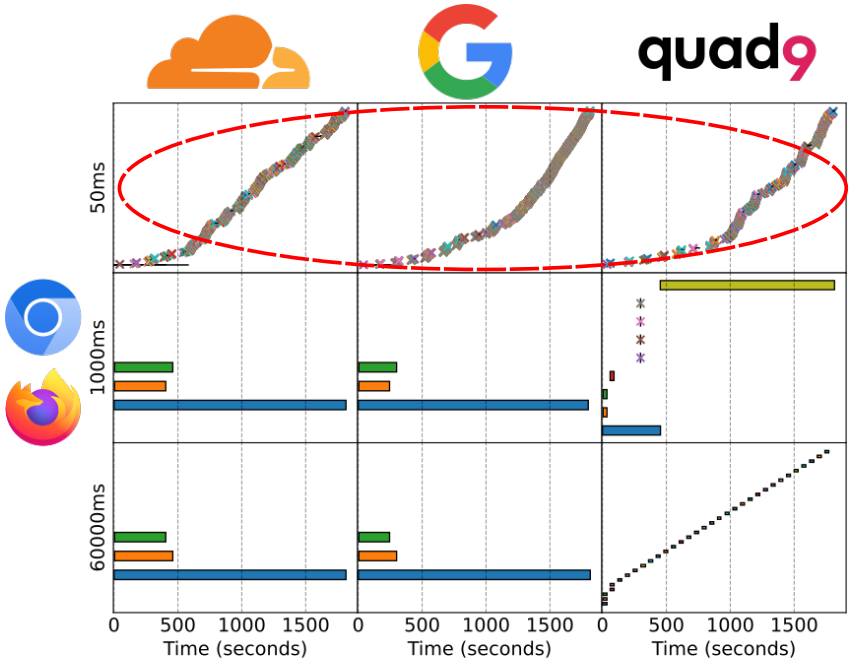
Comportement des clients - résultats

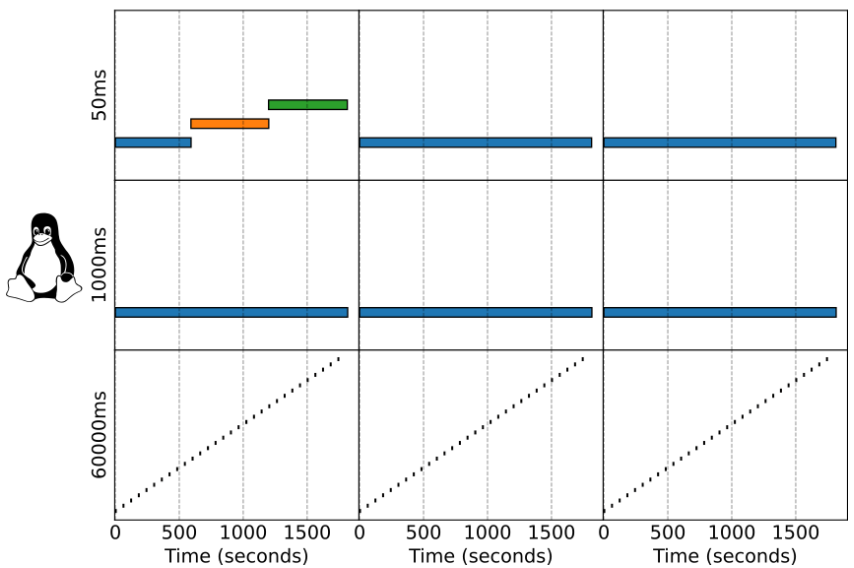


DNScrypt garde les connexions ouvertes, mais a un timeout de 5s

A traffic raisonnable, les navigateurs gardent les connexions ouvertes

Comportement des clients - résultats



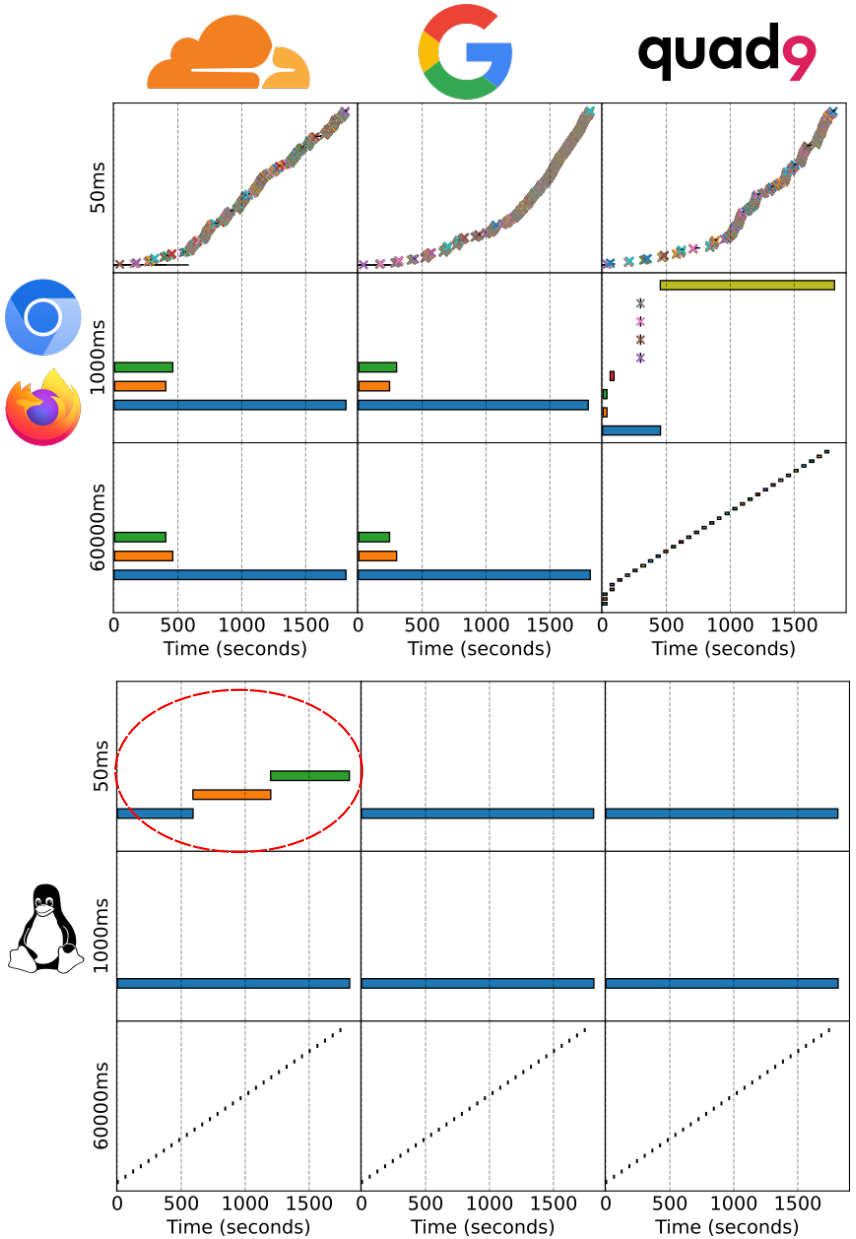


DNScrypt garde les connexions ouvertes, mais a un timeout de 5s

A traffic raisonnable, les navigateurs gardent les connexions ouvertes

Lorsque le traffic demandé est trop important, *undefined behaviour* pour les navigateurs

Comportement des clients - résultats



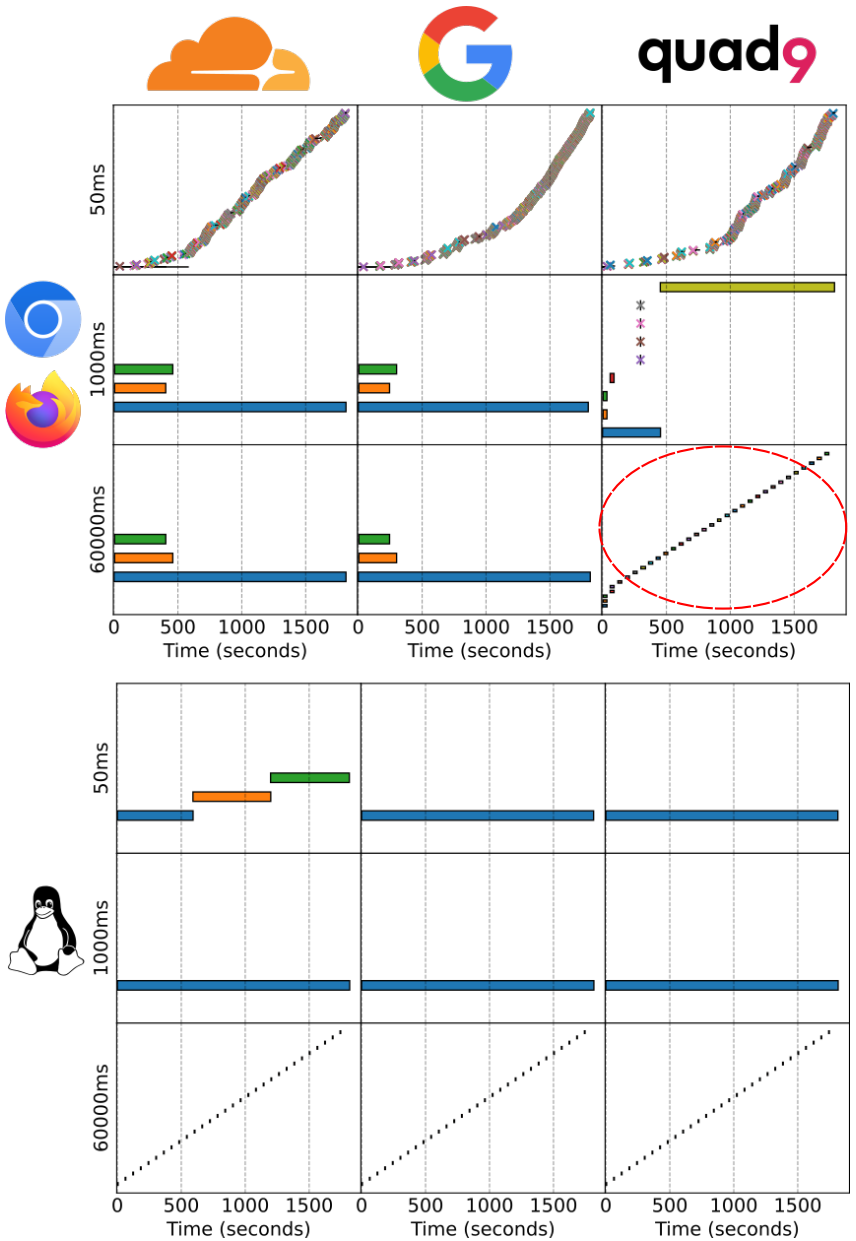
DNScrypt garde les connexions ouvertes, mais a un timeout de 5s

A traffic raisonnable, les navigateurs gardent les connexions ouvertes

Lorsque le traffic demandé est trop important, *undefined behaviour* pour les navigateurs

Cloudflare limite à 10 000 requêtes par connexion

Comportement des clients - résultats



DNScrypt garde les connexions ouvertes, mais a un timeout de 5s

A traffic raisonnable, les navigateurs gardent les connexions ouvertes

Lorsque le traffic demandé est trop important, *undefined behaviour* pour les navigateurs

Cloudflare limite à 10 000 requêtes par connexion

Quad9 ferme les connexions au bout de 15s

Ressources serveur - Protocole

On mesure chaque protocole afin de déterminer le sur-coût ajouté par chaque étape

Ressources serveur - Protocole

On mesure chaque protocole afin de déterminer le sur-coût ajouté par chaque étape

On mesure les performances de deux implémentations : knot-resolver et dnsdist

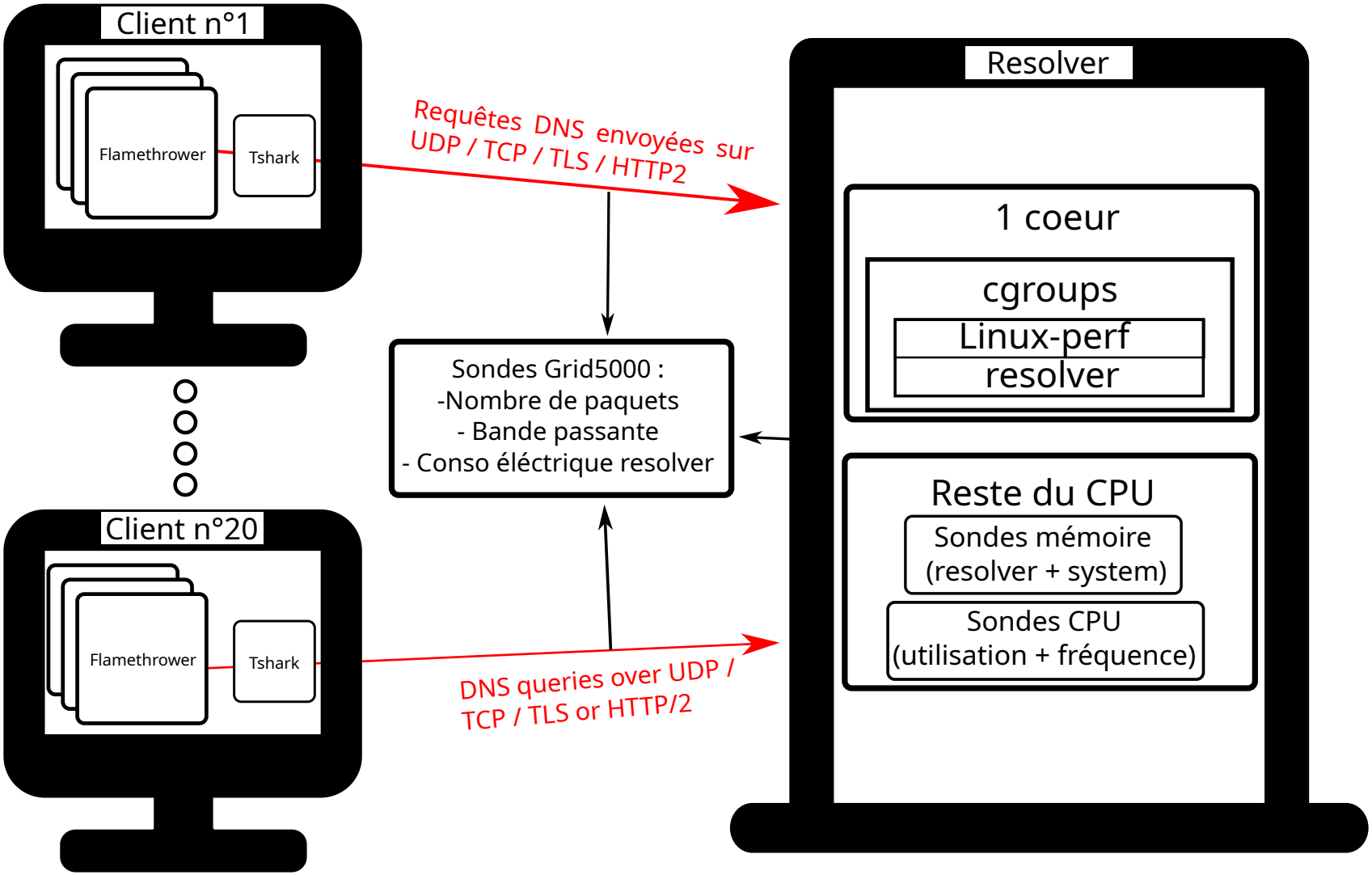
Ressources serveur - Protocole

On mesure chaque protocole afin de déterminer le sur-coût ajouté par chaque étape

On mesure les performances de deux implémentations : knot-resolver et dnsdist

Les mesures de performance sont prises à charge CPU maximale

Environnement experimental - Grid5000



Ressources serveur - Baseline

On compare le maximum de trafic que peut gérer chaque resolver over UDP

Ressources serveur - Baseline

On compare le maximum de trafic que peut gérer chaque resolver over UDP

115 000 QPS traitées pour knot-resolver

Ressources serveur - Baseline

On compare le maximum de trafic que peut gérer chaque resolver over UDP

115 000 QPS traitées pour knot-resolver

220 000 QPS traitées pour dnsdist

Ressources serveur - Baseline

On compare le maximum de trafic que peut gérer chaque resolver over UDP

115 000 QPS traitées pour knot-resolver

220 000 QPS traitées pour dnsdist

knot-resolver et dnsdist n'ont pas les mêmes responsabilités (resolver vs proxy)

Ressources serveur - Baseline

On compare le maximum de trafic que peut gérer chaque resolver over UDP

115 000 QPS traitées pour knot-resolver

220 000 QPS traitées pour dnsdist

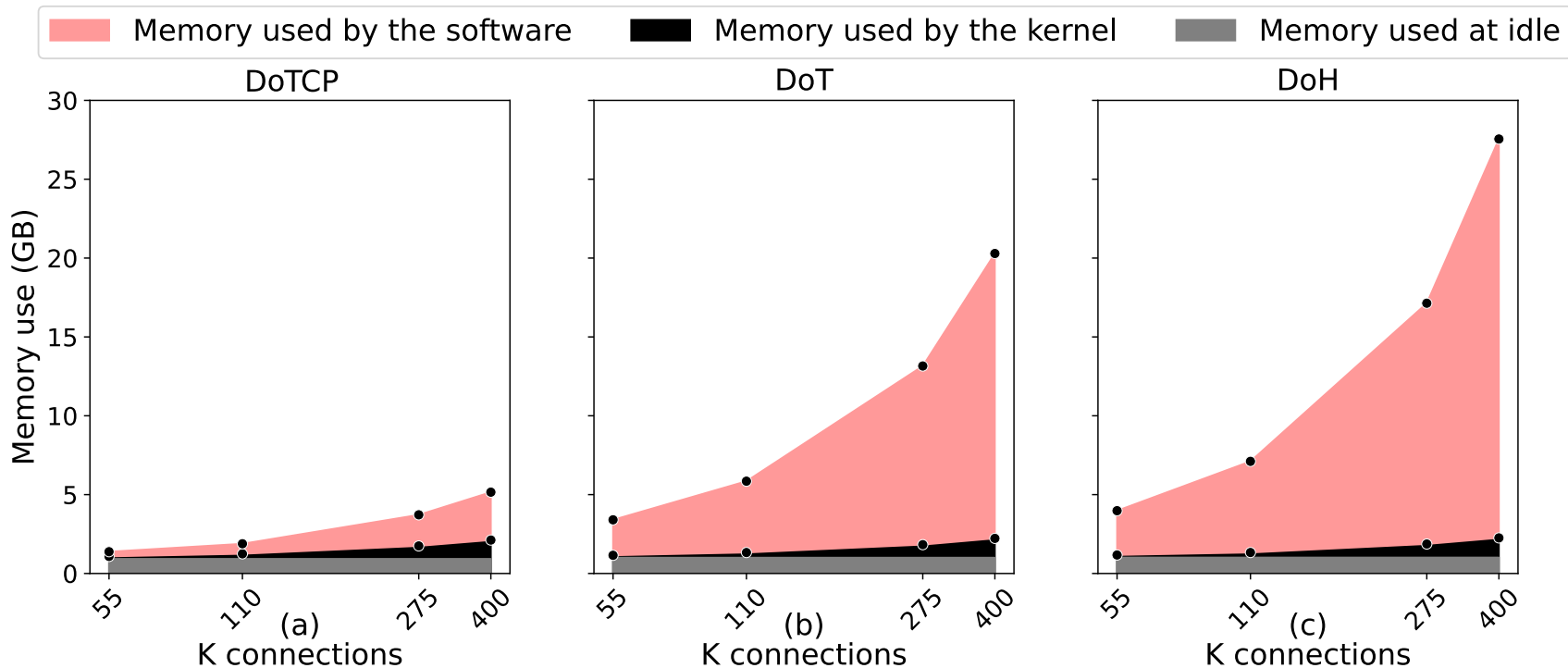
knot-resolver et dnsdist n'ont pas les mêmes responsabilités (resolver vs proxy)

Bottleneck = CPU, le lien réseau n'est pas un problème.

Ressources serveur - Utilisation mémoire TCP / TLS

On établit le plus de connexions possible pour mesurer la consommation mémoire associée.

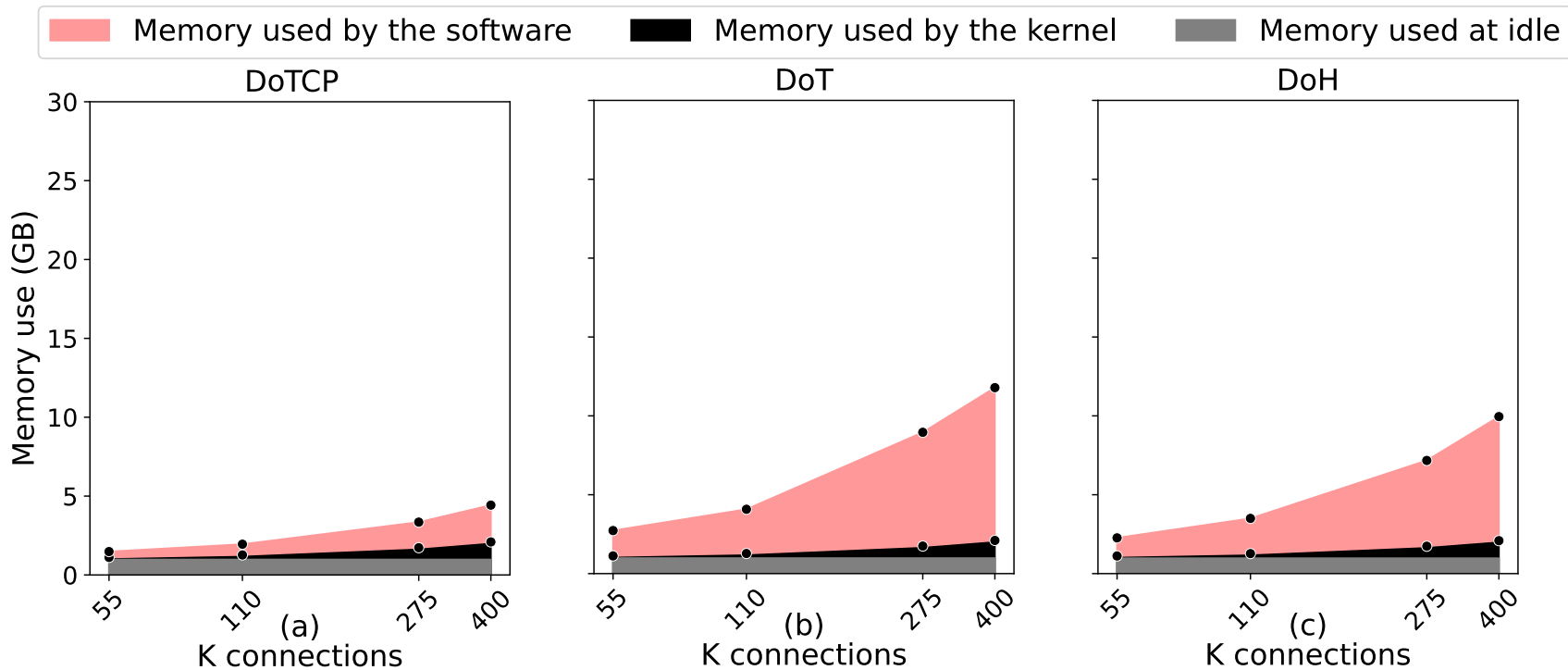
knot-resolver :



Ressources serveur - Utilisation mémoire TCP / TLS

On établit le plus de connexions possible pour mesurer la consommation mémoire associée.

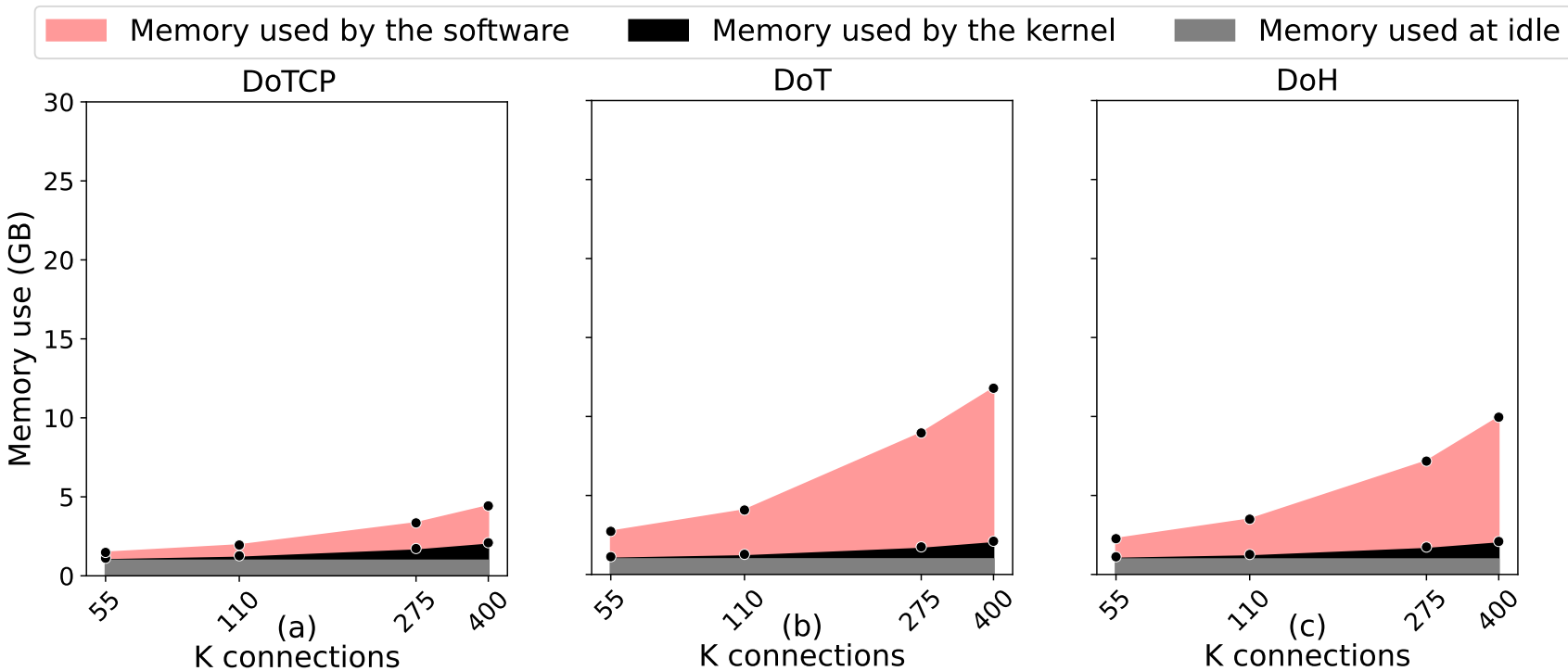
dnsdist :



Ressources serveur - Utilisation mémoire TCP / TLS

On établit le plus de connexions possible pour mesurer la consommation mémoire associée.

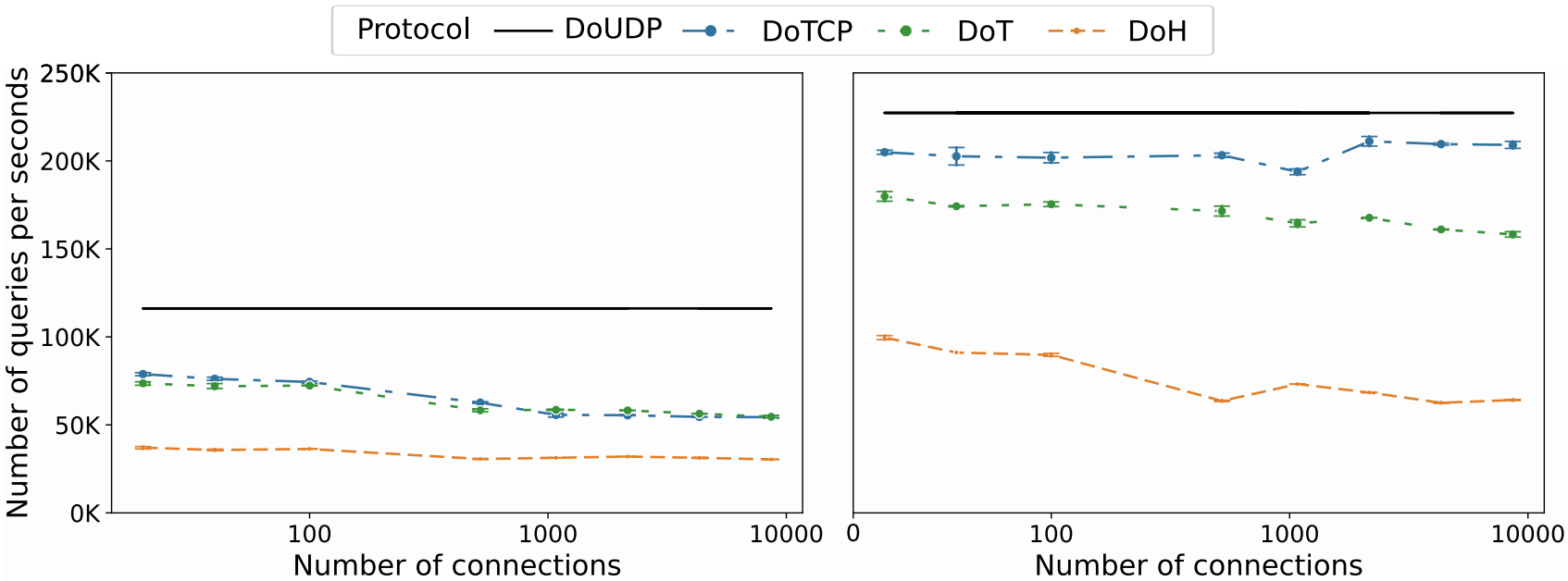
dnsdist :



La quantité de mémoire disponible n'est pas un bottleneck

Ressources serveur - Traitement des messages

On compare le maximum de trafic que peut gérer chaque protocole lorsque l'ouverture des connexions n'est pas prise en compte

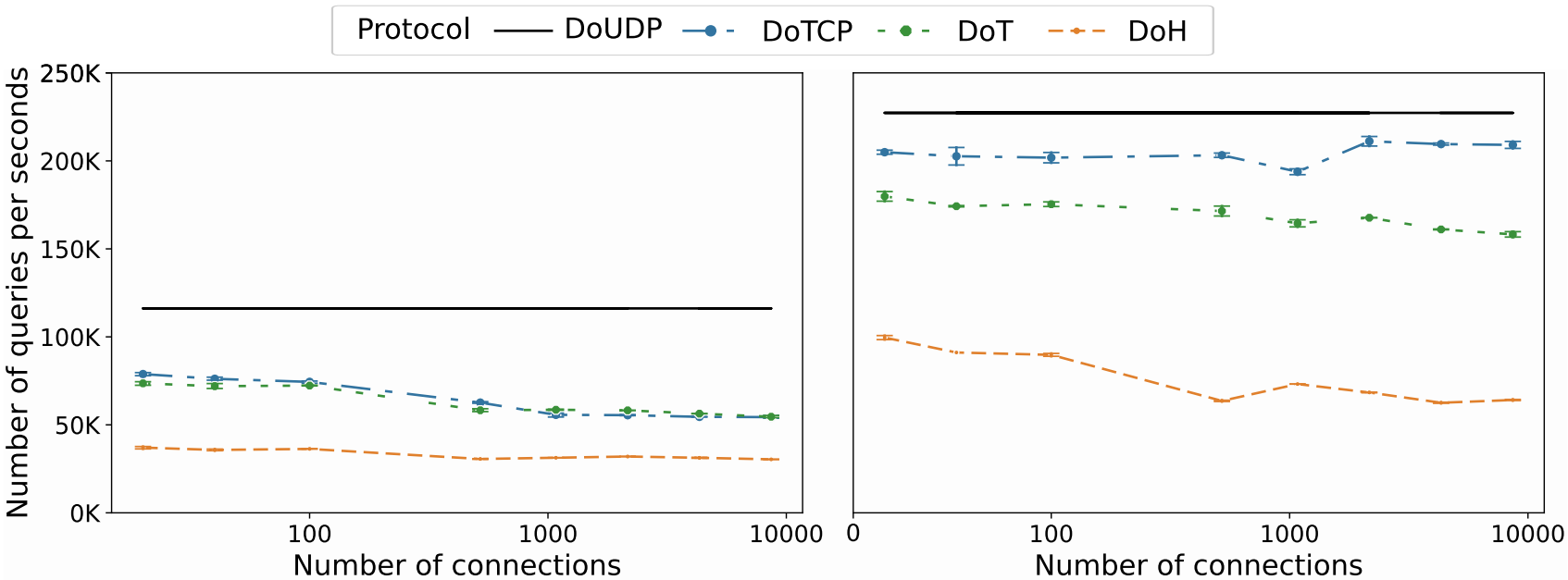


(a) knot

(b) dnsdist

Ressources serveur - Traitement des messages

On compare le maximum de trafic que peut gérer chaque protocole lorsque l'ouverture des connexions n'est pas prise en compte



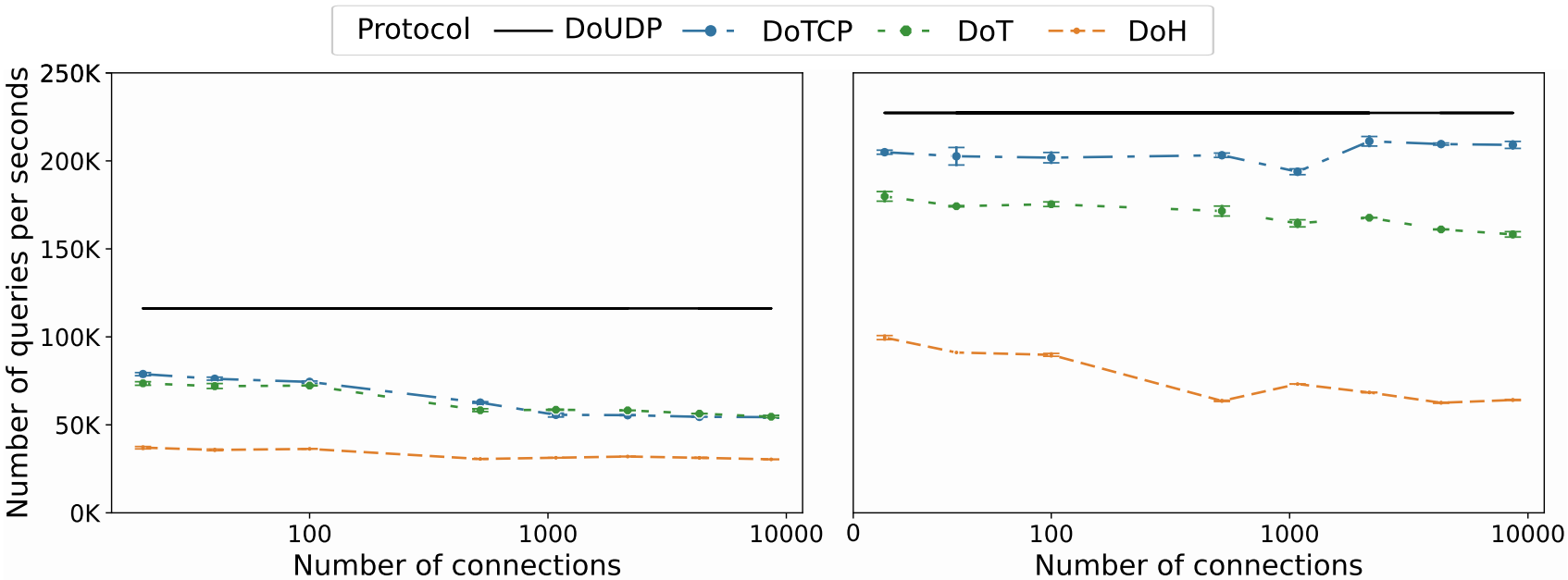
(a) knot

(b) dnsdist

Pour knot, le coût de traitement des messages absorbe celui du chiffrement.

Ressources serveur - Traitement des messages

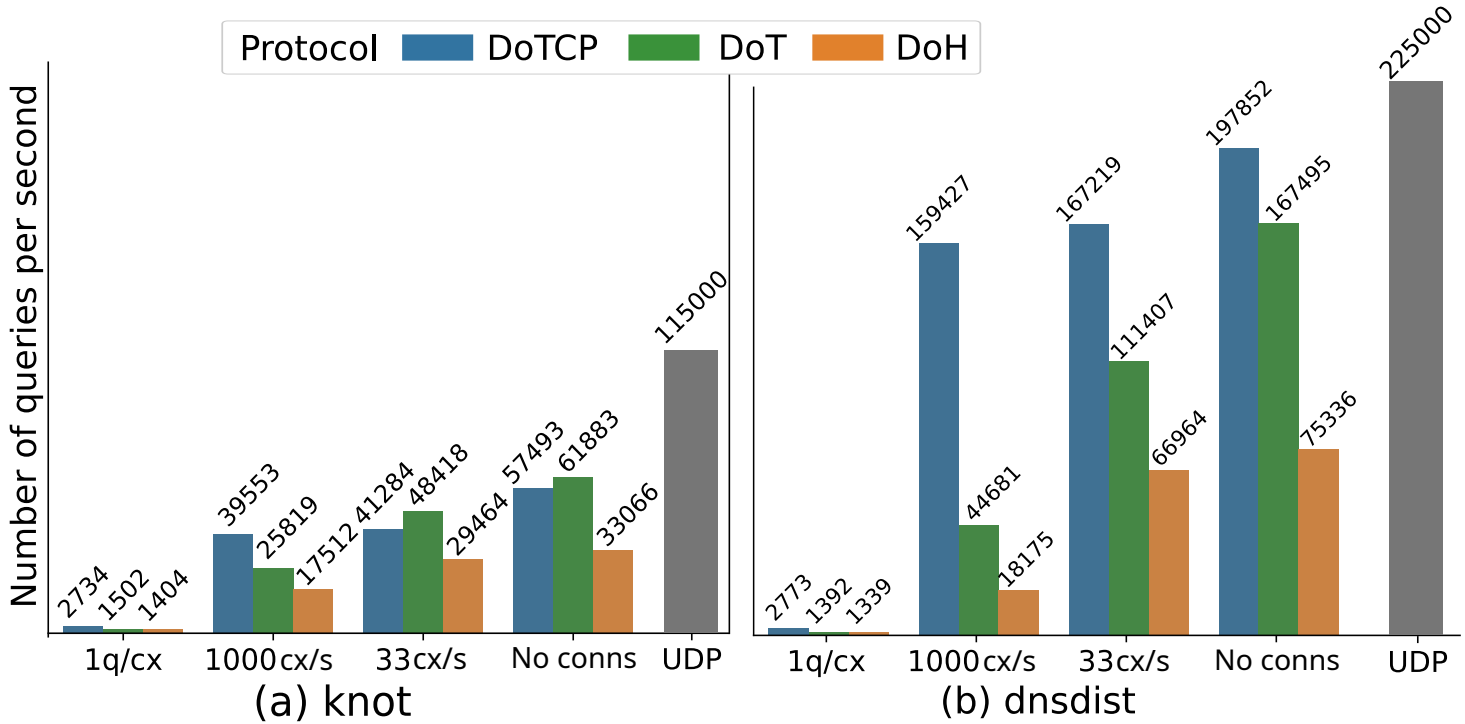
On compare le maximum de trafic que peut gérer chaque protocole lorsque l'ouverture des connexions n'est pas prise en compte



Pour knot, le coût de traitement des messages absorbe celui du chiffrement.
Gérer les messages HTTP représente un coût important.

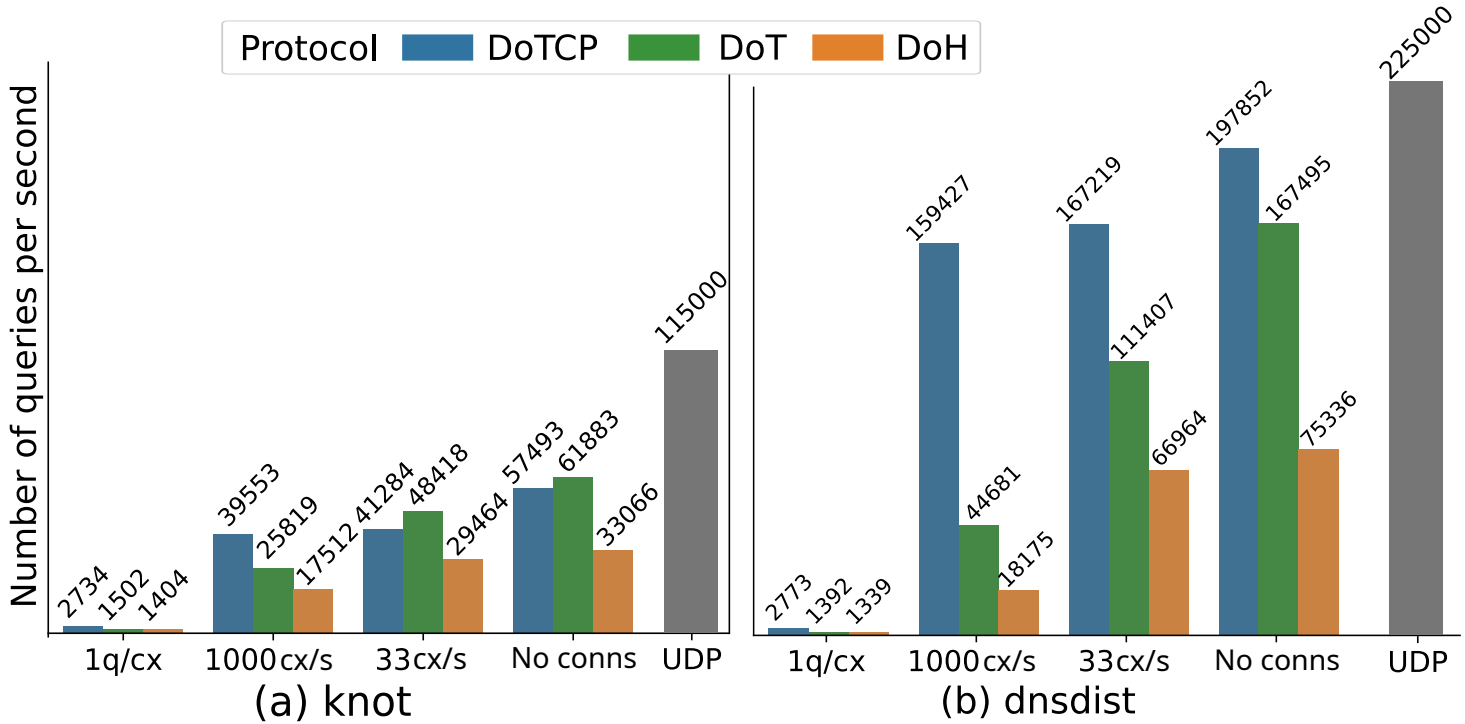
Ressources serveur - Établissement des connections

On introduit des ouvertures / fermetures de connections arbitraires au sein d'une expérience afin de mesurer leur impact



Ressources serveur - Établissement des connections

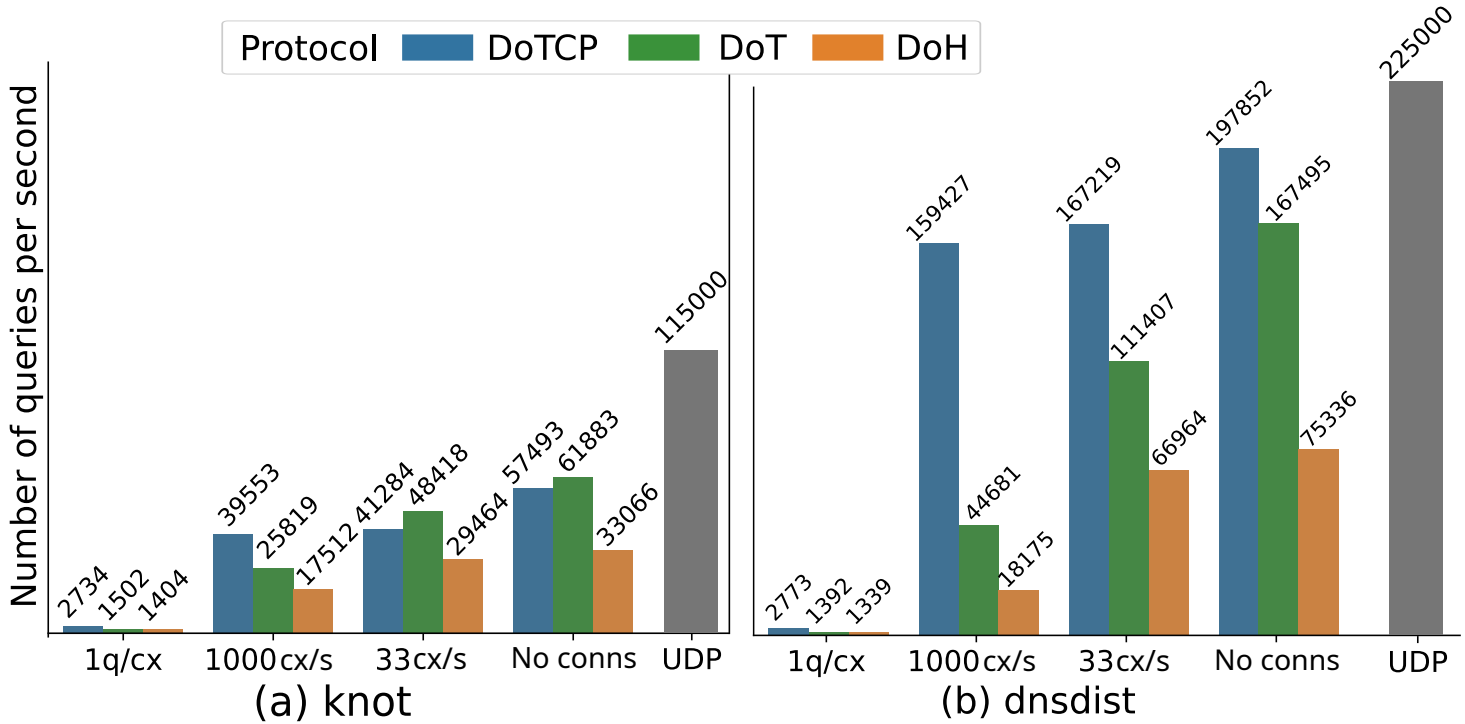
On introduit des ouvertures / fermetures de connections arbitraires au sein d'une expérience afin de mesurer leur impact



- TCP : coût d'établissement faible avec effet de seuil

Ressources serveur - Établissement des connections

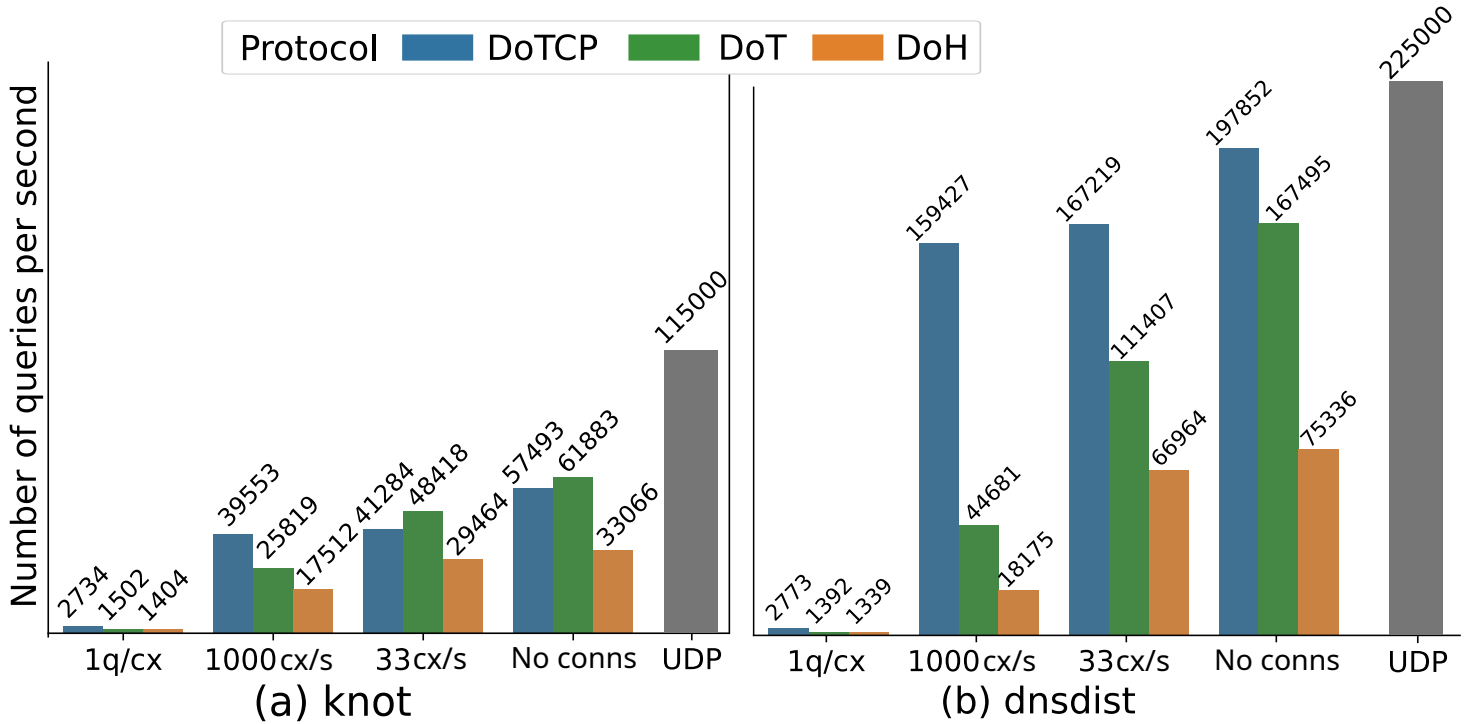
On introduit des ouvertures / fermetures de connections arbitraires au sein d'une expérience afin de mesurer leur impact



- TCP : coût d'établissement faible avec effet de seuil
- DoT : coût d'établissement proportionnel

Ressources serveur - Établissement des connections

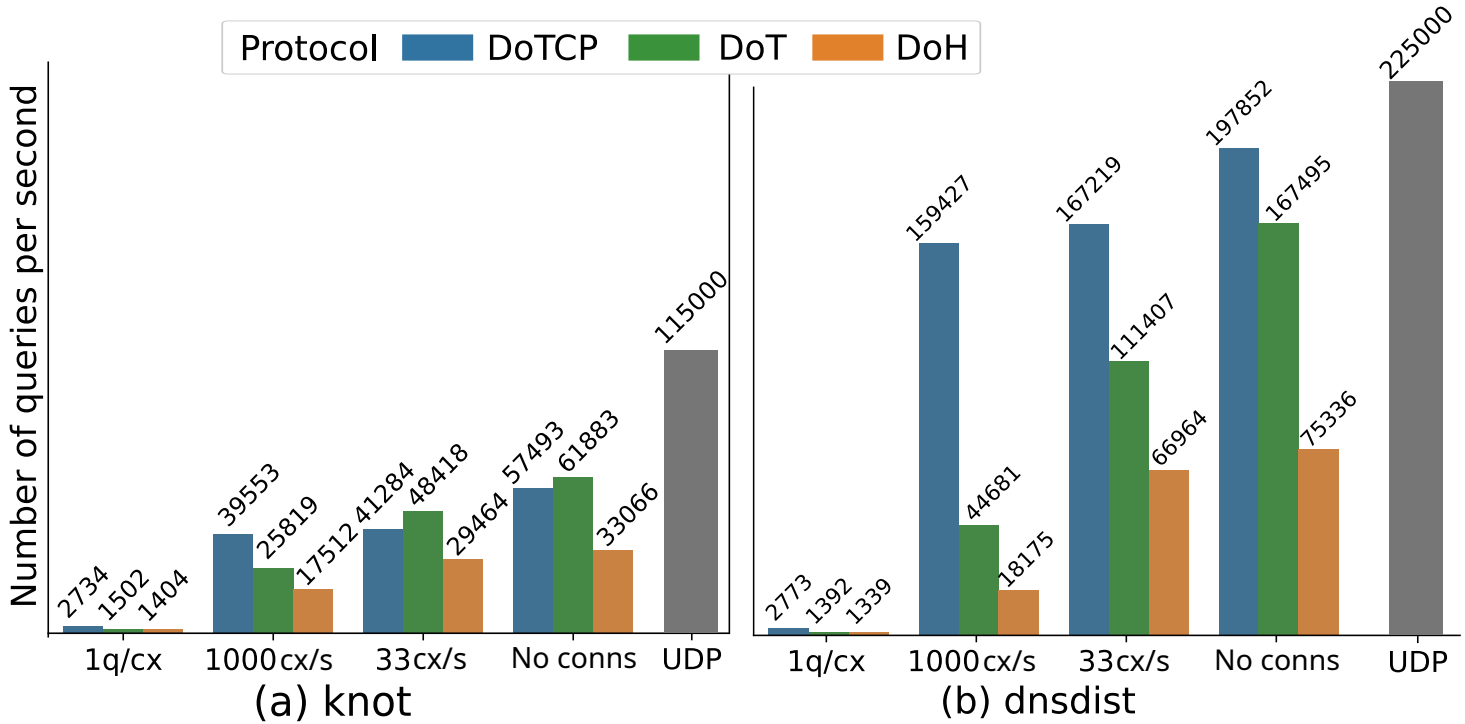
On introduit des ouvertures / fermetures de connections arbitraires au sein d'une expérience afin de mesurer leur impact



- TCP : coût d'établissement faible avec effet de seuil
- DoT : coût d'établissement proportionnel
- DoH : overhead protocole

Ressources serveur - Établissement des connections

On introduit des ouvertures / fermetures de connections arbitraires au sein d'une expérience afin de mesurer leur impact



- TCP : coût d'établissement faible avec effet de seuil
- DoT : coût d'établissement proportionnel
- DoH : overhead protocole
- *undefined behaviour* si ouverture de trop de connexions TCP.

Conclusion

Conclusion

Étude comportement clients et serveurs :

Conclusion

Étude comportement clients et serveurs :

- Proxy plus stables, mais usage pas poussé

Conclusion

Étude comportement clients et serveurs :

- Proxy plus stables, mais usage pas poussé

Analyse des performances :

Conclusion

Étude comportement clients et serveurs :

- Proxy plus stables, mais usage pas poussé

Analyse des performances :

- Hétérogénéité des perfs parmis les serveurs.

Conclusion

Étude comportement clients et serveurs :

- Proxy plus stables, mais usage pas poussé

Analyse des performances :

- Hétérogénéité des perfs parmis les serveurs.
- Ouverture connexions chiffrées à un coût.

Conclusion

Étude comportement clients et serveurs :

- Proxy plus stables, mais usage pas poussé

Analyse des performances :

- Hétérogénéité des perfs parmis les serveurs.
- Ouverture connexions chiffrées à un coût.
- Impact chiffrement symétrique relativement faible.

Conclusion

Étude comportement clients et serveurs :

- Proxy plus stables, mais usage pas poussé

Analyse des performances :

- Hétérogénéité des perfs parmis les serveurs.
- Ouverture connexions chiffrées à un coût.
- Impact chiffrement symétrique relativement faible.
- Utilisation HTTP/2 poussée par l'industrie, mais pertes de perfs les plus importantes (66%)