Empoisonnement DNS (Attaque de Dan Kaminski)

M1 - Outils de l'Internet 2008-2009

Victor Poupet (victor.poupet@lif.univ-mrs.fr)

Fonctionnement du DNS

Idée générale

- Client demande l'adresse IP correspondant à un nom de domaine à un serveur DNS (souvent celui de son FAI)
- Le serveur peut être récursif ou non (effectuer les requêtes successives jusqu'à avoir une réponse)
- Il existe un serveur qui fait autorité sur chaque domaine (exceptionnellement plusieurs)

Récursivité

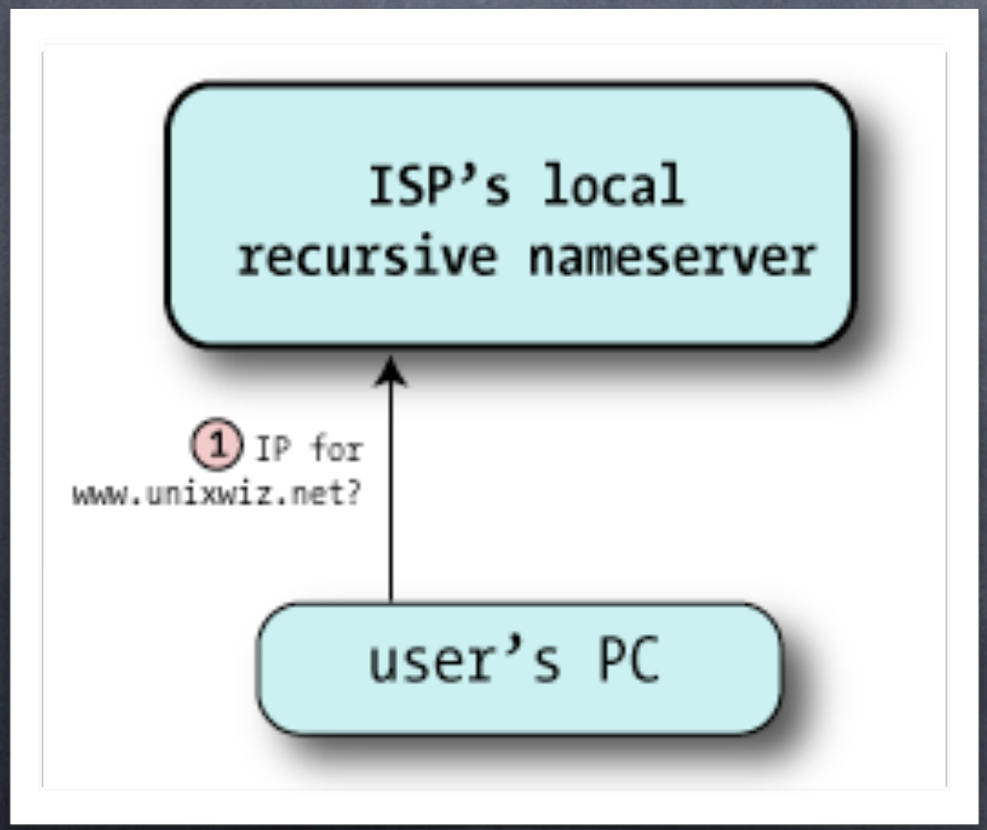
- En général les serveurs n'acceptent pas de faire des requêtes récursives
- Ce sont principalement les DNS des FAI qui le font
- Les autres serveurs se contentent de donner l'adresse du serveur suivant dans la hiérarchie
- Souvent les serveurs récursifs n'acceptent que des utilisateurs authentifiés

Remarque

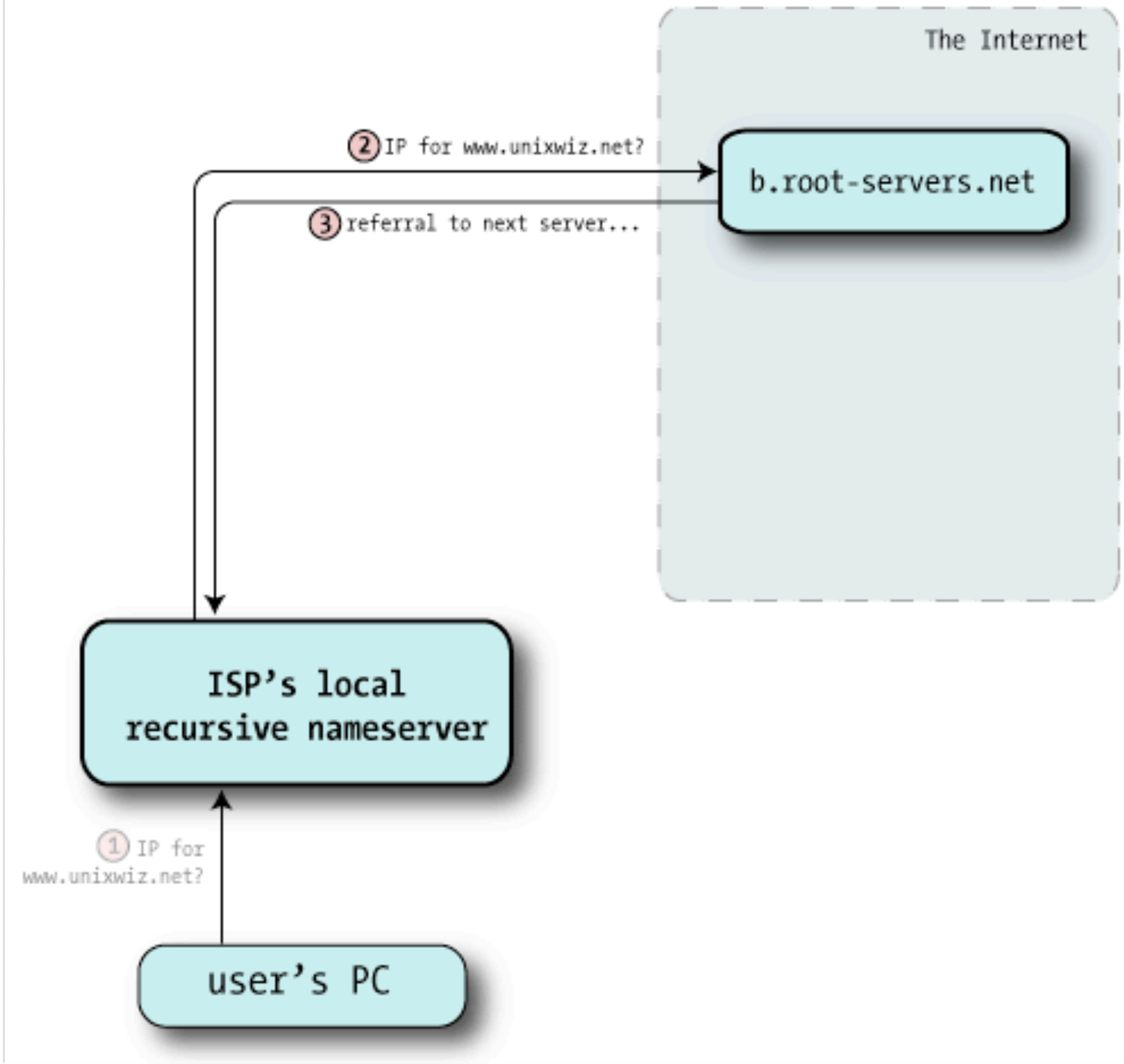
- Le DNS n'est pas que pour la correspondance nom - IP. Il existe plusieurs types de requêtes, entre autres :
  - A : Adresse IP
  - NS : NameServer (serveur responsable du domaine)
  - MX : Mail Exchanger
  - SOA : Start of Authorities (infos sur l'admin)
  - CNAME : Canonical Name
  - TXT : Texte, informations sur un domaine

Format des requêtes

- N'importe quel accès à Internet peut provoquer une requête DNS
- Les requêtes ont toutes le même format indépendamment de ce qui les a provoquées


ISP's local
recursive nameserver
1 IP for
www.unixwiz.net?
user's PC

- L'utilisateur demande une adresse IP (A record)
- Le serveur ne fait pas autorité sur l'adresse demandée
- Le serveur n'a pas cette adresse dans son cache


The Internet
2 IP for www.unixwiz.net?
b.root-servers.net
3 referral to next server...
ISP's local
recursive nameserver
1 IP for
www.unixwiz.net?
user's PC

Liste de serveurs root (sur le serveur du FAI)

```
A.ROOT-SERVERS.NET.   IN   A   198.41.0.4
B.ROOT-SERVERS.NET.   IN   A   192.228.79.201
C.ROOT-SERVERS.NET.   IN   A   192.33.4.12
...
M.ROOT-SERVERS.NET.   IN   A   202.12.27.33
```

13 serveurs préconfigurés dans tout serveur DNS

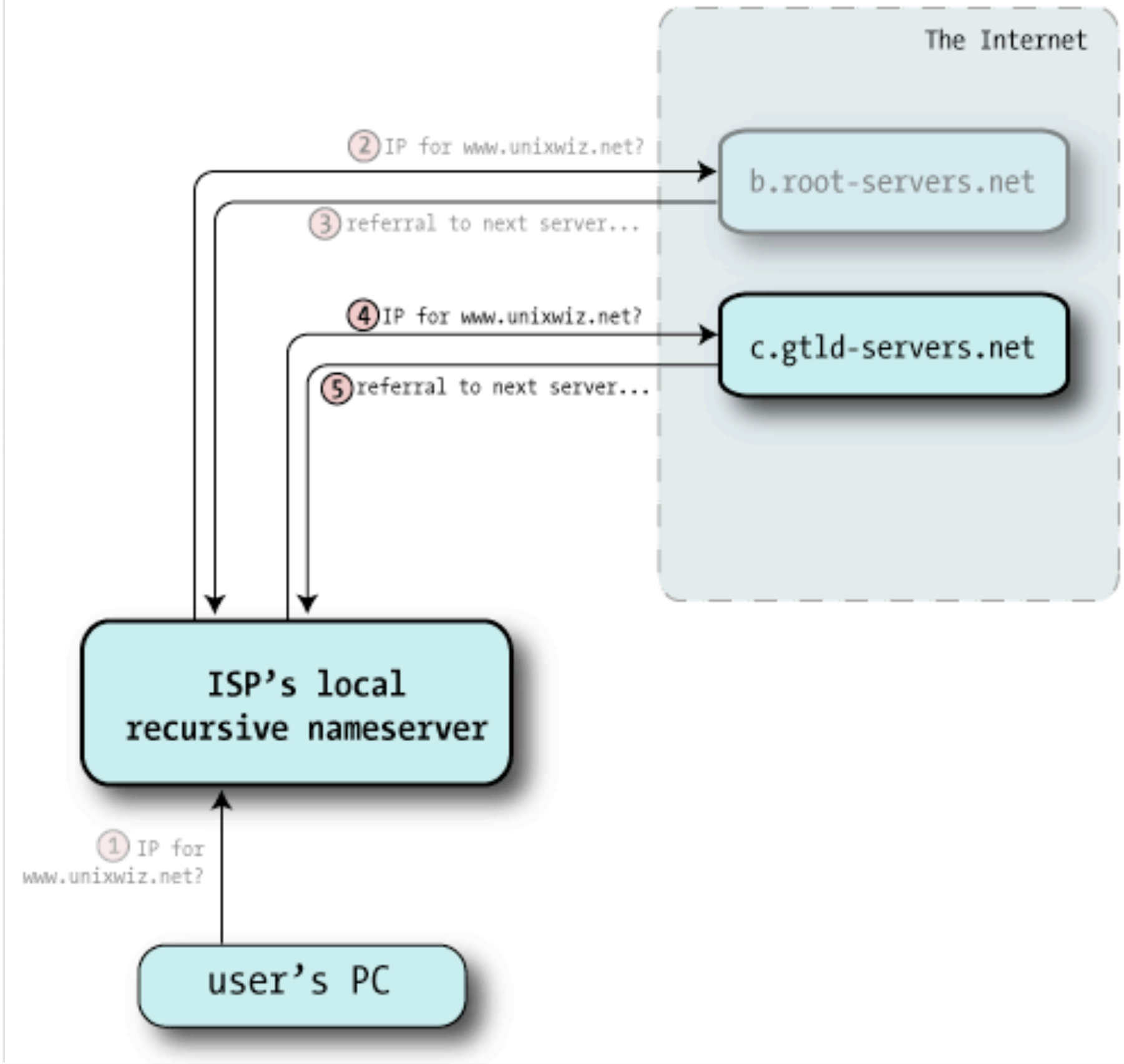
Réponse du serveur

```
/* Authority section */
NET.                        IN   NS A.GTLD-SERVERS.NET.
                            IN   NS B.GTLD-SERVERS.NET.
                            IN   NS C.GTLD-SERVERS.NET.
                            ...
                            IN   NS M.GTLD-SERVERS.NET.

/* Additional section - "glue" records */
A.GTLD-SERVERS.net.   IN   A   192.5.6.30
B.GTLD-SERVERS.net.   IN   A   192.33.14.30
C.GTLD-SERVERS.net.   IN   A   192.26.92.30
...
M.GTLD-SERVERS.net.   IN   A   192.55.83.30
```

Question

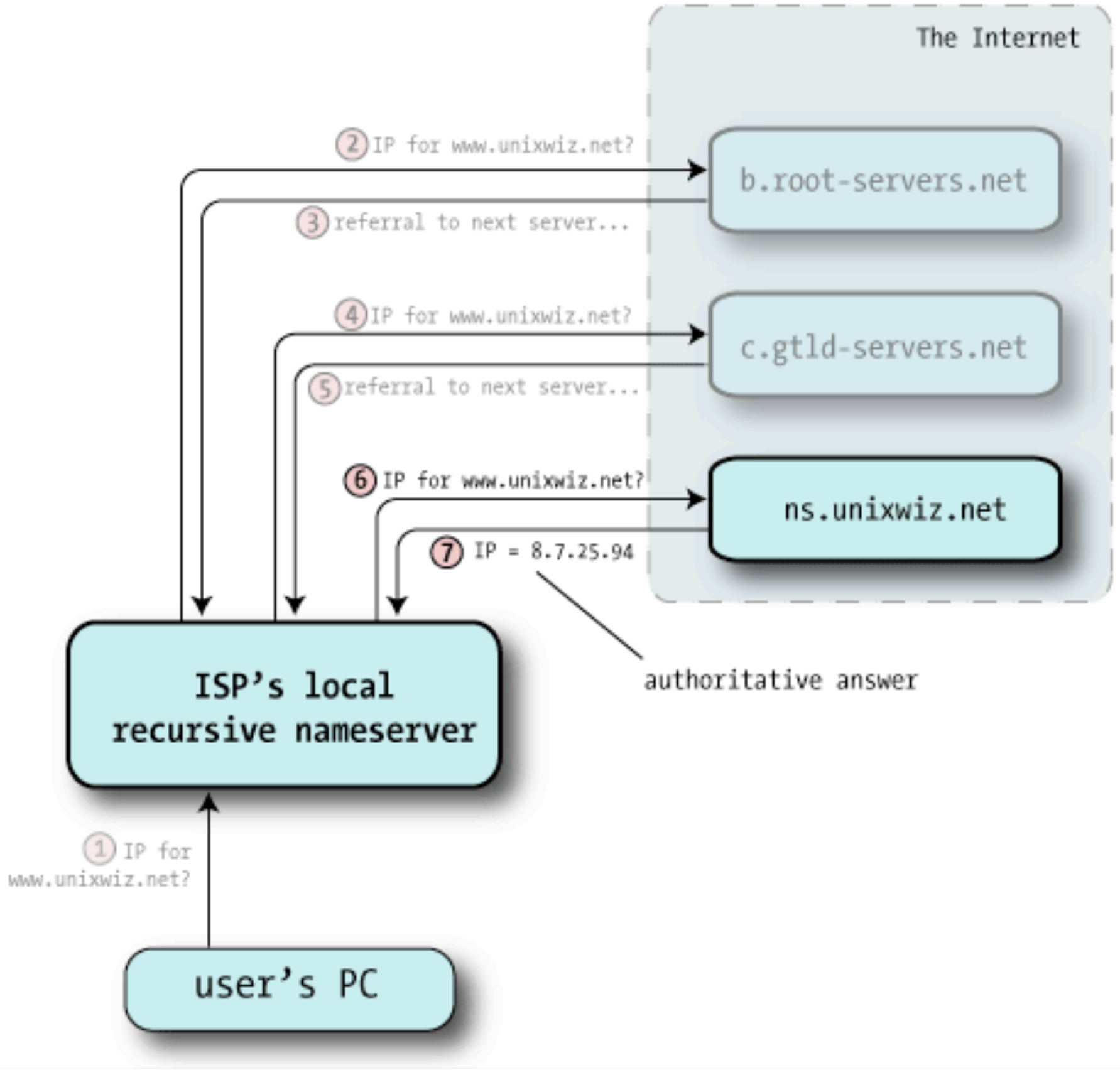
- À quoi servent les "glue records" ?

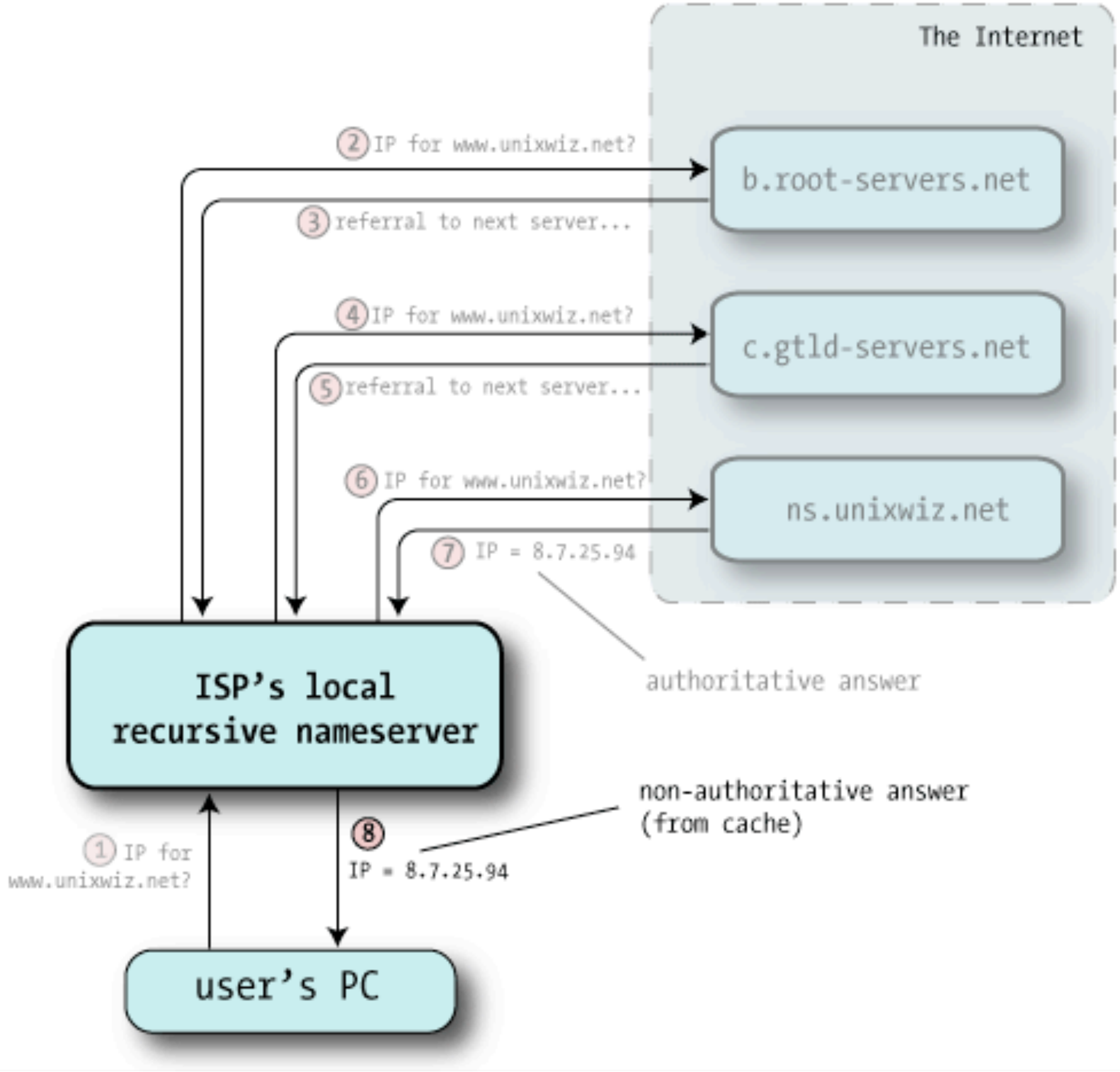

The Internet
2 IP for www.unixwiz.net?
b.root-servers.net
3 referral to next server...
4 IP for www.unixwiz.net?
c.gtld-servers.net
5 referral to next server...
ISP's local
recursive nameserver
1 IP for
www.unixwiz.net?
user's PC

Réponse du serveur

```
/* Authority section */
unixwiz.net.            IN  NS cs.unixwiz.net.
                        IN  NS linux.unixwiz.net.

/* Additional section - "glue" records */
cs.unixwiz.net.         IN  A  8.7.25.94
linux.unixwiz.net.      IN  A  64.170.162.98
```


The Internet
2 IP for www.unixwiz.net?
b.root-servers.net
3 referral to next server...
4 IP for www.unixwiz.net?
c.gtld-servers.net
5 referral to next server...
6 IP for www.unixwiz.net?
ns.unixwiz.net
7 IP = 8.7.25.94
authoritative answer
ISP's local
recursive nameserver
1 IP for
www.unixwiz.net?
user's PC


The Internet
2 IP for www.unixwiz.net?
b.root-servers.net
3 referral to next server...
4 IP for www.unixwiz.net?
c.gtld-servers.net
5 referral to next server...
6 IP for www.unixwiz.net?
ns.unixwiz.net
7 IP = 8.7.25.94
authoritative answer
ISP's local
recursive nameserver
non-authoritative answer
(from cache)
8
IP = 8.7.25.94
1 IP for
www.unixwiz.net?
user's PC

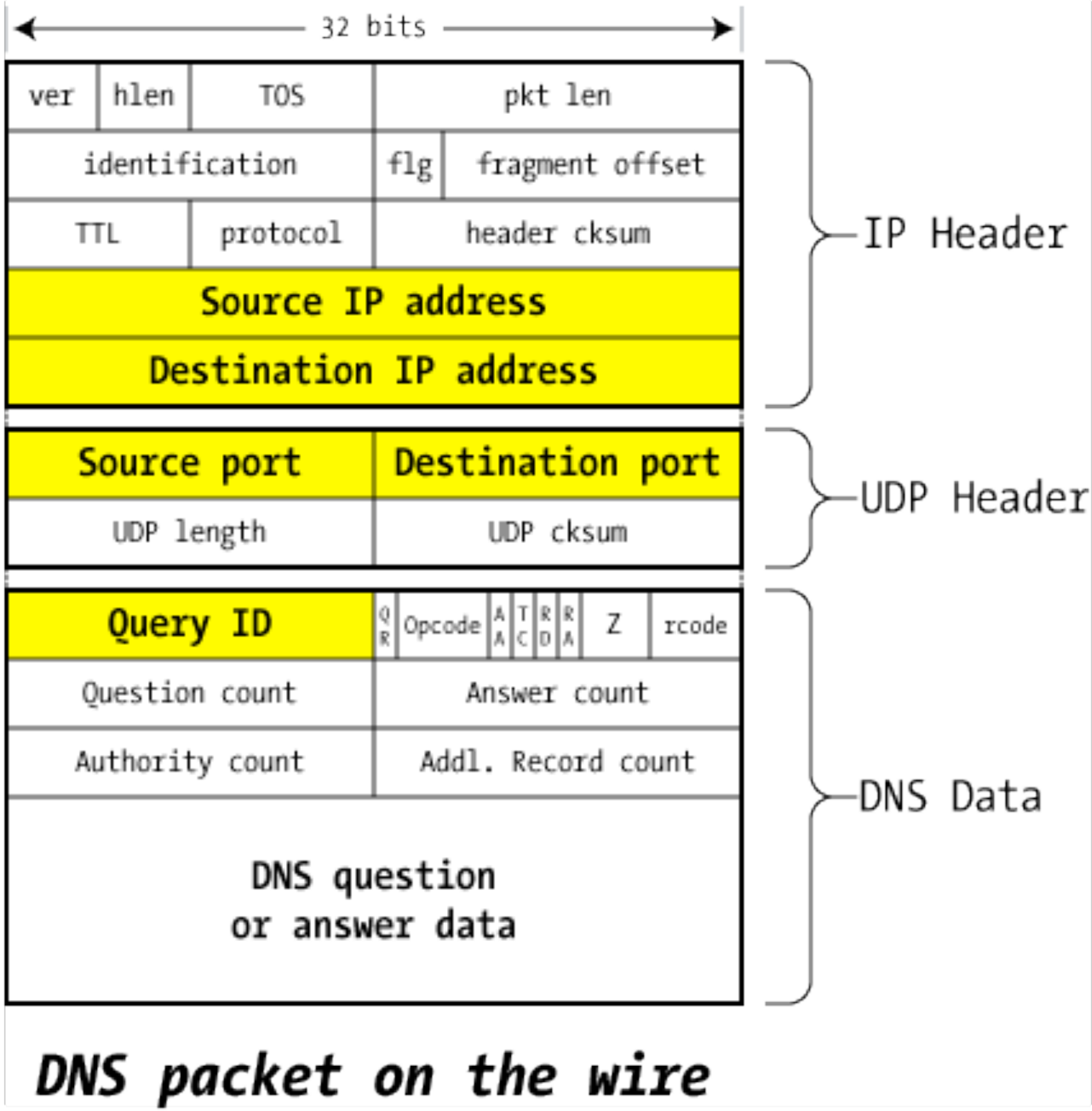
En un clin d'oeil

- Ces échanges ont lieu à chaque fois qu'on essaie de contacter une machine sur un réseau
- Heureusement l'ensemble des échanges se fait en une fraction de seconde (UDP plus rapide que TCP)

Question

- N'importe qui peut créer un serveur DNS qui se prétend être autorité sur un domaine quelconque... Pourquoi n'est-ce pas un problème ?

Détail des paquets DNS



DNS packet on the wire

Remarques

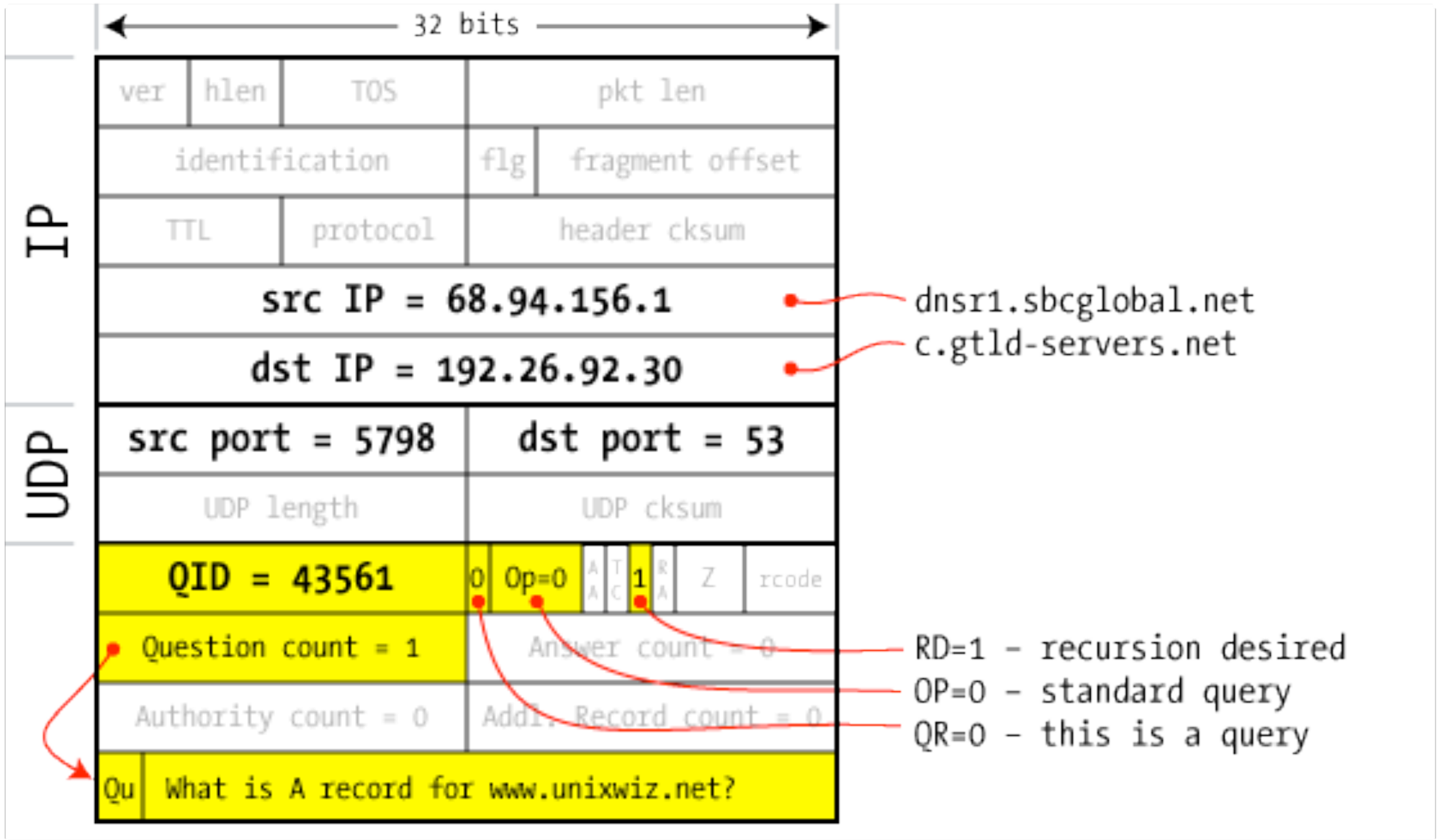
- On peut falsifier l'IP de la source, mais pas celle de la destination (pourquoi ?)
- Les serveurs DNS écoutent sur le port 53
- Souvent le port d'émission est tiré au hasard au démarrage de la machine, parfois changé à chaque requête

Identifiant de requête

- À quoi sert-il ? (penser aux différences entre UDP et TCP)
- La plupart du temps les identifiants sont générés dans l'ordre (on incrémente d'un à chaque requête)

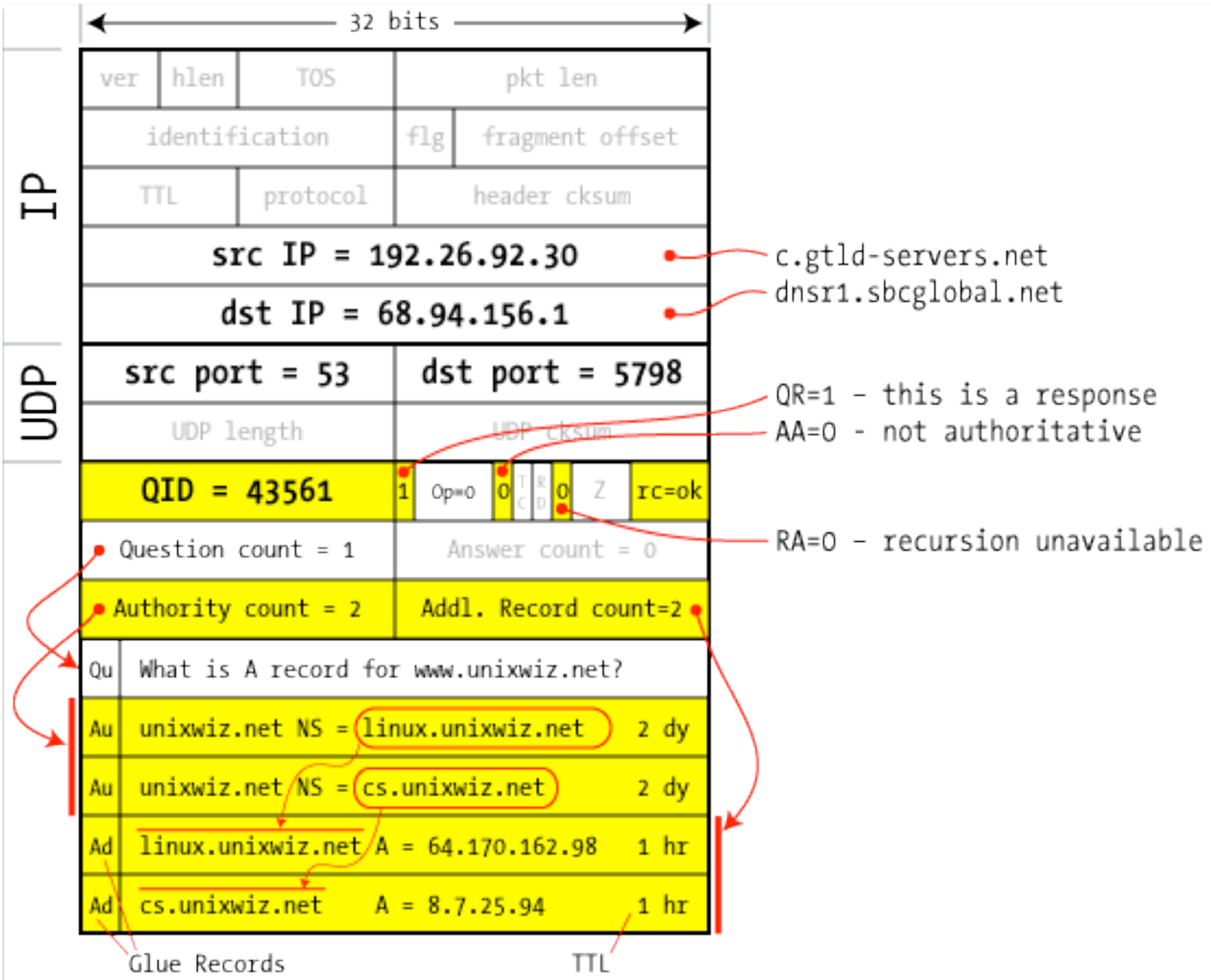
Requête

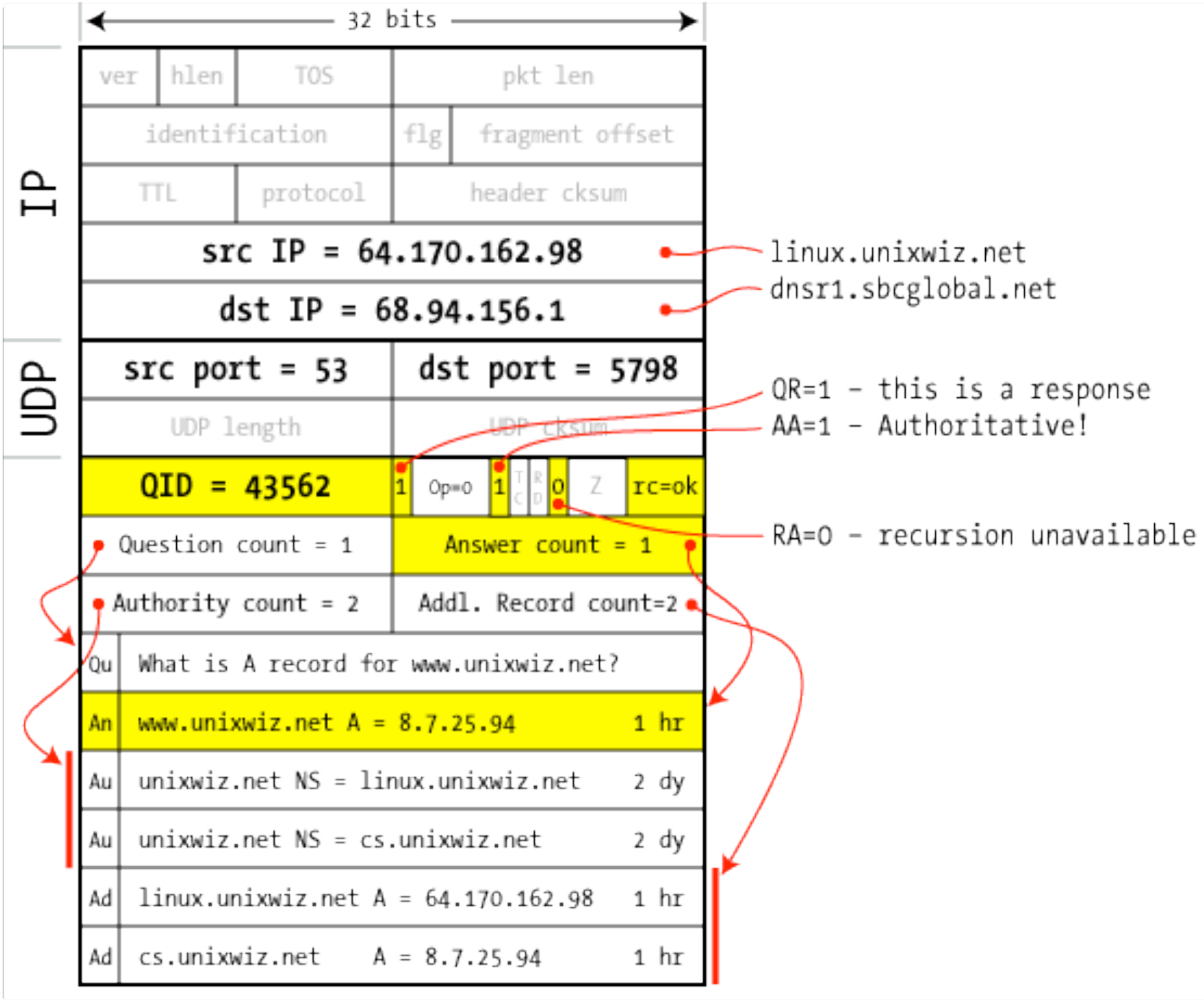
- Numéro de requête (quelconque)
- Question (en général une seule)
- Autres informations


32 bits
IP
ver
hlen
TOS
pkt len
identification
flg
fragment offset
TTL
protocol
header cksum
src IP = 68.94.156.1
dst IP = 192.26.92.30
dnsr1.sbcglobal.net
c.gtld-servers.net
UDP
src port = 5798
dst port = 53
UDP length
UDP cksum
QID = 43561
0
Op=0
1
Z
rcode
Question count = 1
Authority count = 0
Qu
What is A record for www.unixwiz.net?
RD=1 - recursion desired
OP=0 - standard query
QR=0 - this is a query

Réponse

- Numéro de requête (identique à celui de la requête)
- Question (identique)
- Réponses (souvent plusieurs)
- Glue records
- Réponse peut être celle demandée ou partielle (demander à un autre serveur)


32 bits
IP
UDP
ver
hlen
TOS
pkt len
identification
flg
fragment offset
TTL
protocol
header cksum
src IP = 192.26.92.30
dst IP = 68.94.156.1
src port = 53
dst port = 5798
UDP length
UDP cksum
QID = 43561
1
Op=0
0
T C
R D
0
Z
rc=ok
Question count = 1
Answer count = 0
Authority count = 2
Addl. Record count=2
Qu
What is A record for www.unixwiz.net?
Au
unixwiz.net NS = linux.unixwiz.net
2 dy
Au
unixwiz.net NS = cs.unixwiz.net
2 dy
Ad
linux.unixwiz.net A = 64.170.162.98
1 hr
Ad
cs.unixwiz.net A = 8.7.25.94
1 hr
c.gtld-servers.net
dnsr1.sbcglobal.net
QR=1 - this is a response
AA=0 - not authoritative
RA=0 - recursion unavailable
Glue Records
TTL


32 bits
IP
UDP
ver
hlen
TOS
pkt len
identification
flg
fragment offset
TTL
protocol
header cksum
src IP = 64.170.162.98
dst IP = 68.94.156.1
src port = 53
dst port = 5798
UDP length
UDP cksum
QID = 43562
1
Op=0
1
T C
R D
0
Z
rc=ok
Question count = 1
Answer count = 1
Authority count = 2
Addl. Record count=2
Qu What is A record for www.unixwiz.net?
An www.unixwiz.net A = 8.7.25.94 1 hr
Au unixwiz.net NS = linux.unixwiz.net 2 dy
Au unixwiz.net NS = cs.unixwiz.net 2 dy
Ad linux.unixwiz.net A = 64.170.162.98 1 hr
Ad cs.unixwiz.net A = 8.7.25.94 1 hr
linux.unixwiz.net
dnsr1.sbcglobal.net
QR=1 - this is a response
AA=1 - Authoritative!
RA=0 - recursion unavailable

Cache

Questions

- Qu'est-ce que le cache ?
- À quoi ça sert ?
- Comment ça marche ?

Time to Live (TTL)

An	www.unixwiz.net A = 8.7.25.94	1 hr

Au	unixwiz.net NS = linux.unixwiz.net	2 dy
Au	unixwiz.net NS = cs.unixwiz.net	2 dy
Ad	linux.unixwiz.net A = 64.170.162.98	1 hr
Ad	cs.unixwiz.net A = 8.7.25.94	1 hr

Time to Live (TTL)

- Le TTL est fixé par l'administrateur de la zone pour chaque entrée DNS
- Quel est l'intérêt du TTL ?
- Que faut-il faire lorsque des entrées DNS doivent être modifiées ?

L'attaque de base

Idée

- Envoyer des informations fausses au serveur DNS pour empoisonner le cache
- Il faut que les informations aient l'air de correspondre à une requête du serveur

Questions

- Quel est l'intérêt d'empoisonner le cache du serveur DNS ?
- Quelle est la différence avec le Phishing ?

Ce qui compte

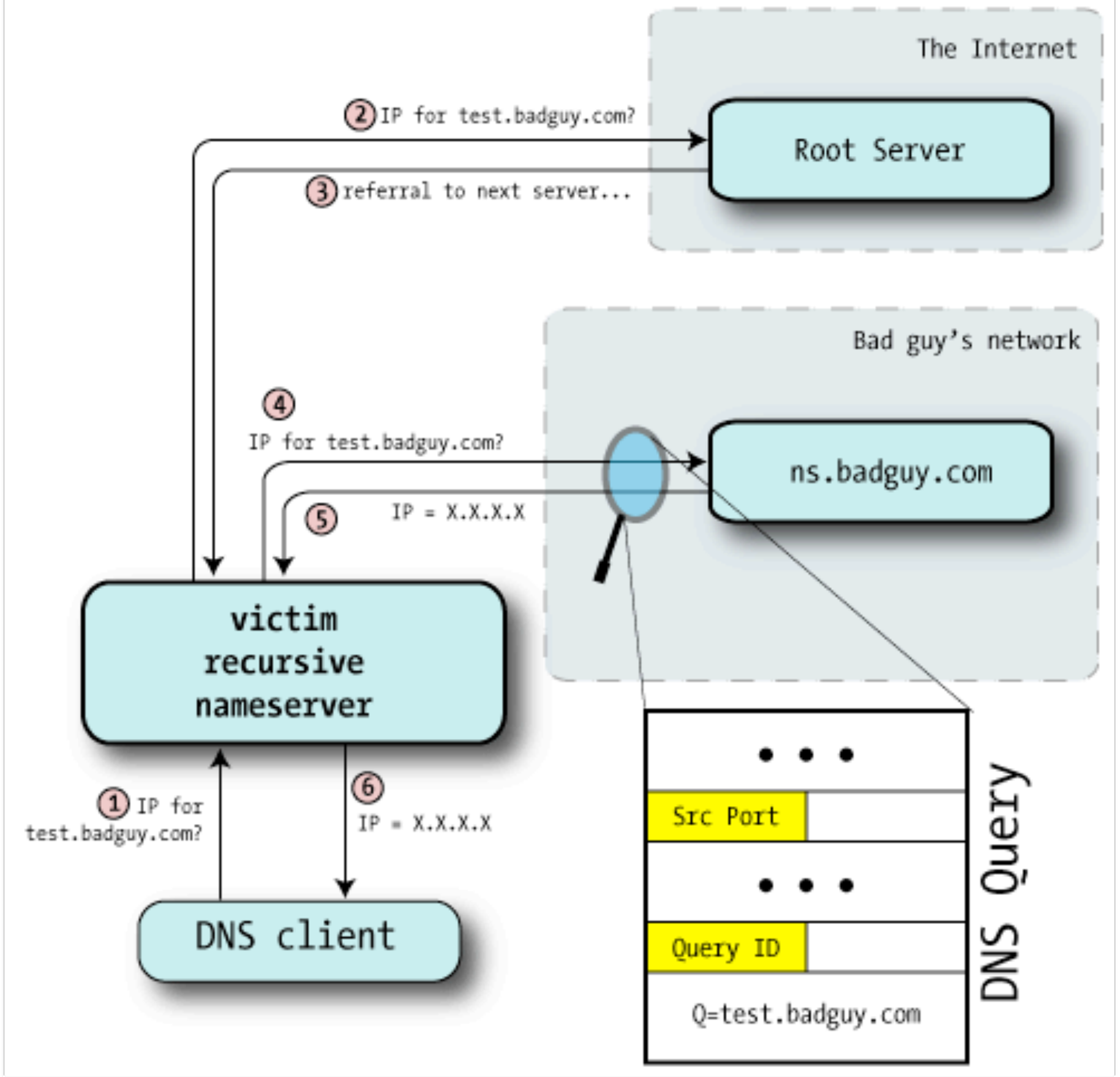
- La réponse arrive sur le bon port UDP
- La question doit être la même
  - le Query ID doit correspondre
  - Authority et Additional dans le même domaine que la question
  - Les paquets qui ne correspondent pas sont ignorés...

Question

- À quoi sert la dernière contrainte ?
- Il arrive qu'elle ne soit pas vérifiée par certains serveurs...

Query ID ?

- Sur certains serveurs, le Query ID est incrémenté d'un à chaque nouvelle requête
- Comment peut-on tirer parti de ce déterminisme ? (il faut réussir à trouver le query ID à un instant donné)

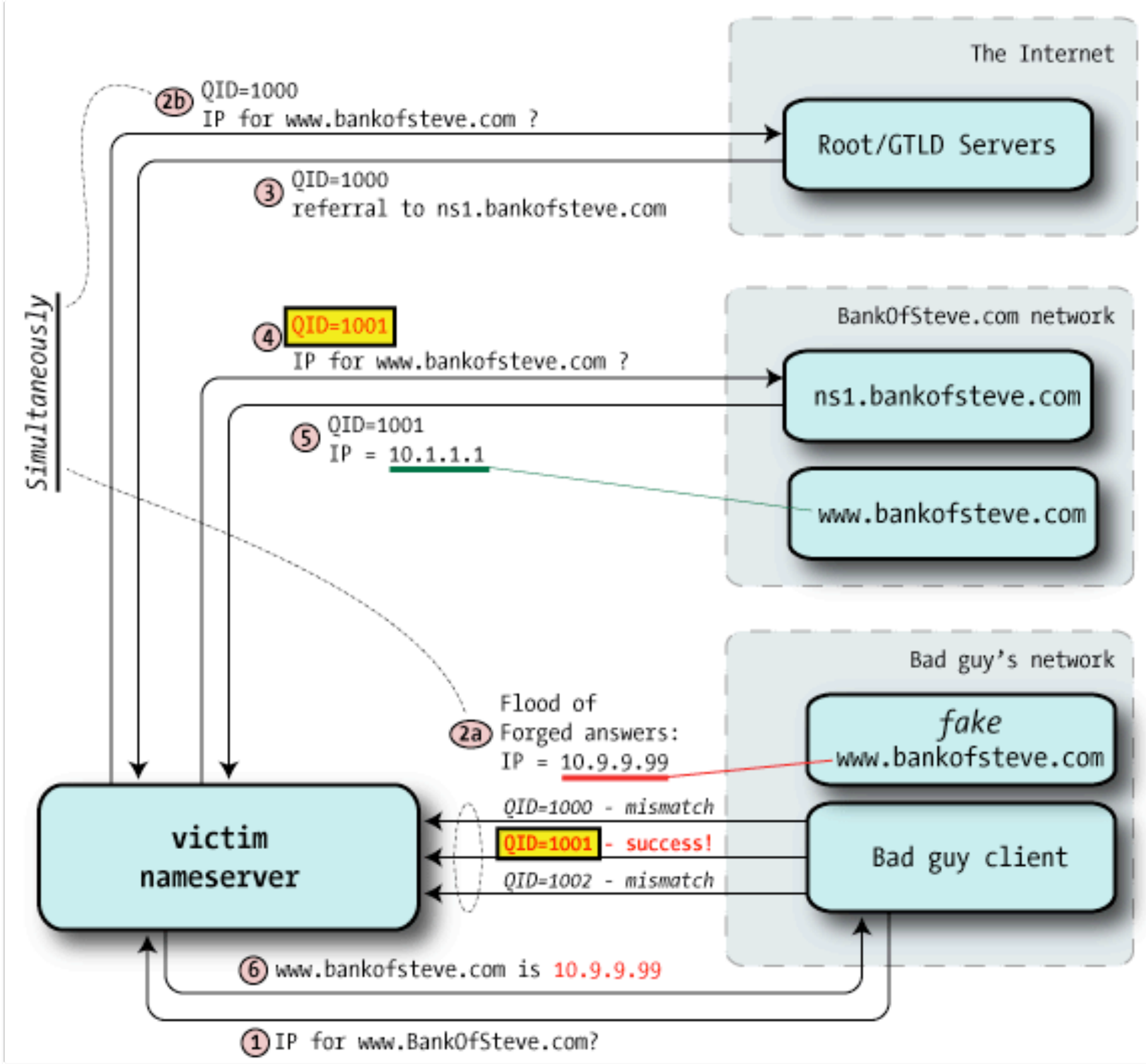

The Internet
2 IP for test.badguy.com?
Root Server
3 referral to next server...
Bad guy's network
4
IP for test.badguy.com?
ns.badguy.com
5
IP = X.X.X.X
victim
recursive
nameserver
1 IP for
test.badguy.com?
6
IP = X.X.X.X
DNS client
Src Port
Query ID
Q=test.badguy.com
DNS Query

Question

- Comment obtenir le Query ID si le serveur n'accepte pas les requêtes de l'attaquant ?

À l'attaque !

- Si on connaît le query ID, les autres informations sont faciles à trouver
- On peut fabriquer une fausse réponse à une question connue…


The Internet
Root/GTLD Servers
2b QID=1000
IP for www.bankofsteve.com ?
3 QID=1000
referral to ns1.bankofsteve.com
Simultaneously
4 QID=1001
IP for www.bankofsteve.com ?
BankOfSteve.com network
ns1.bankofsteve.com
5 QID=1001
IP = 10.1.1.1
www.bankofsteve.com
Bad guy's network
fake
www.bankofsteve.com
2a Flood of
Forged answers:
IP = 10.9.9.99
QID=1000 - mismatch
QID=1001 - success!
QID=1002 - mismatch
victim
nameserver
Bad guy client
6 www.bankofsteve.com is 10.9.9.99
1 IP for www.BankOfSteve.com?

Questions

- Que se passe-t-il si la réponse de l'attaquant arrive avant celle du serveur DNS de bankofsteve ?
- À combien de requêtes peut correspondre la réponse de l'attaquant ?

Questions

- Pourquoi est-ce que le système de cache est à la fois un avantage et un inconvénient pour l'attaquant ?
- Proposez une solution pour diminuer le risque d'une telle attaque.

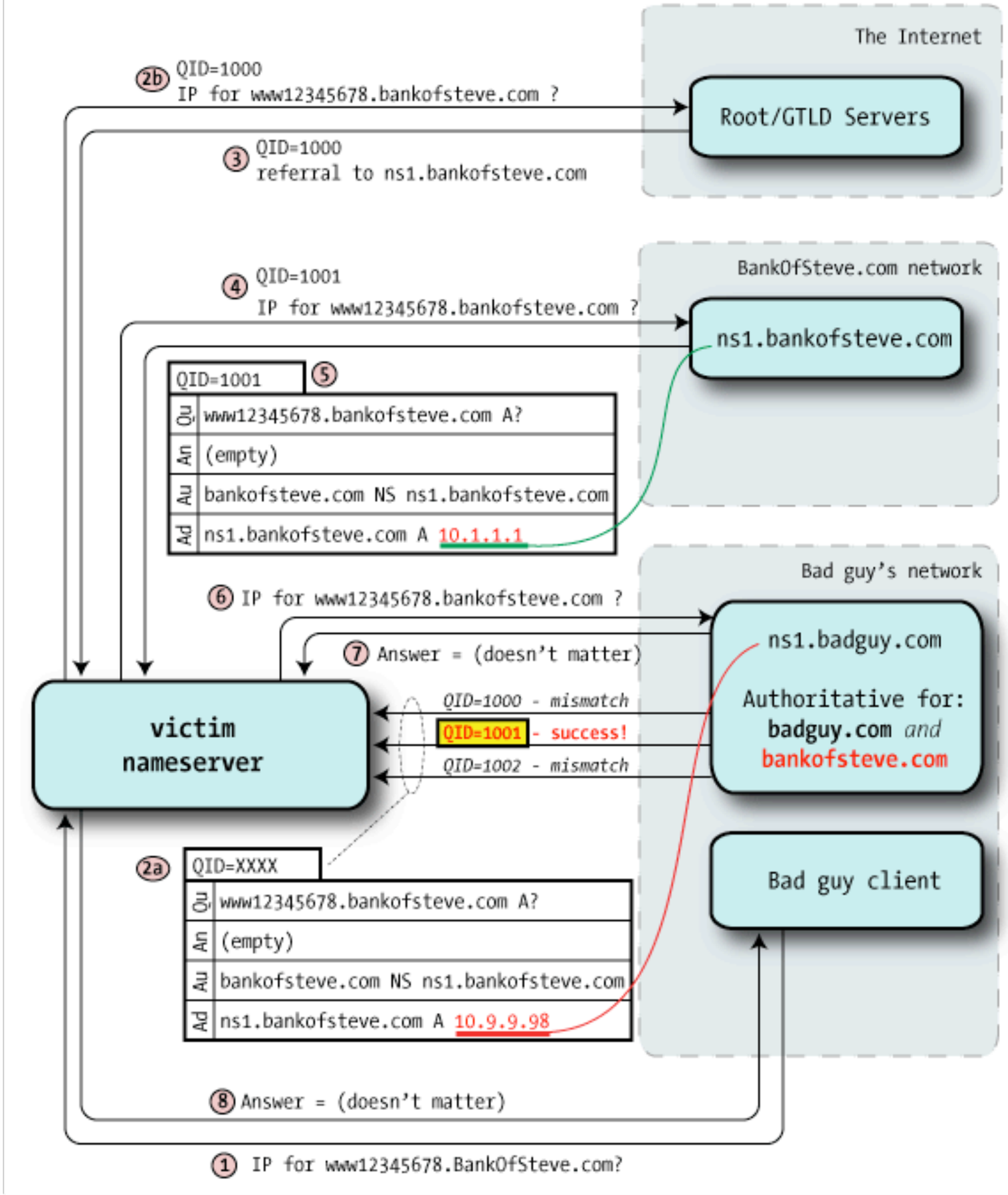
Amélioration de l'attaque

Idée

- Avec la méthode précédente, soit on contrôle une adresse peu utilisée, soit elle est probablement déjà dans le cache
- Au lieu de falsifier l'adresse IP d'une machine, on prend le contrôle d'un domaine
- On peut effectuer l'attaque même si des informations ont déjà été cachées

Glue records

- Quand un glue record arrive, le cache est mis à jour (si le glue record est sur le bon domaine)
- Comment pousser le serveur à faire beaucoup de requêtes sur un domaine donné, même s'il enregistre les réponses dans un cache ?


The Internet
2b QID=1000
IP for www12345678.bankofsteve.com ?
Root/GTLD Servers
3 QID=1000
referral to ns1.bankofsteve.com
BankOfSteve.com network
4 QID=1001
IP for www12345678.bankofsteve.com ?
ns1.bankofsteve.com
QID=1001
5
Qu www12345678.bankofsteve.com A?
An (empty)
Au bankofsteve.com NS ns1.bankofsteve.com
Ad ns1.bankofsteve.com A 10.1.1.1
Bad guy's network
6 IP for www12345678.bankofsteve.com ?
7 Answer = (doesn't matter)
ns1.badguy.com
Authoritative for:
badguy.com and
bankofsteve.com
QID=1000 - mismatch
QID=1001 - success!
QID=1002 - mismatch
victim
nameserver
Bad guy client
2a QID=XXXX
Qu www12345678.bankofsteve.com A?
An (empty)
Au bankofsteve.com NS ns1.bankofsteve.com
Ad ns1.bankofsteve.com A 10.9.9.98
8 Answer = (doesn't matter)
1 IP for www12345678.BankOfSteve.com?

Questions

- Que peut-on faire quand on contrôle le serveur qui fait autorité sur un domaine ?
- Quels domaines peut-on contrôler ?
- Quels sont les utilisateurs qui sont victimes de l'attaque ?
- Comment utiliser les TTL pour augmenter la portée de l'attaque ?

Questions

- Comment limiter cette attaque ?

Conclusion

- Il faut mettre à jour tous les serveurs (l'attaque est très simple)
- Serveurs sans cache ne sont pas affectés (authoritative only)
- Attention aux routeurs qui pourraient réduire le nombre de ports UDP utilisés
- En contrôlant le DNS on peut souvent tromper les certificats (on peut contrôler le domaine d'un CA)

- Source : An Illustrated Guide to the Kaminsky DNS Vulnerability

http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html