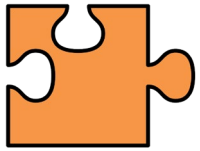
TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN ĐIỆN TỬ - VIỄN THÔNG

ET6540: Network Security

Domain Name Server (DNS)

VINH TRAN-QUANG (Ph.D., Assoc. Prof.)
Smart Applications & Network System Laboratory
Add : Room 618, Ta Quang Buu Library
No.1 Dai Co Viet Road, Hanoi, Vietnam
Email: vinhtq@hust.edu.vn
m706501@shibaura-it.ac.jp
Website: https://sanslab.vn

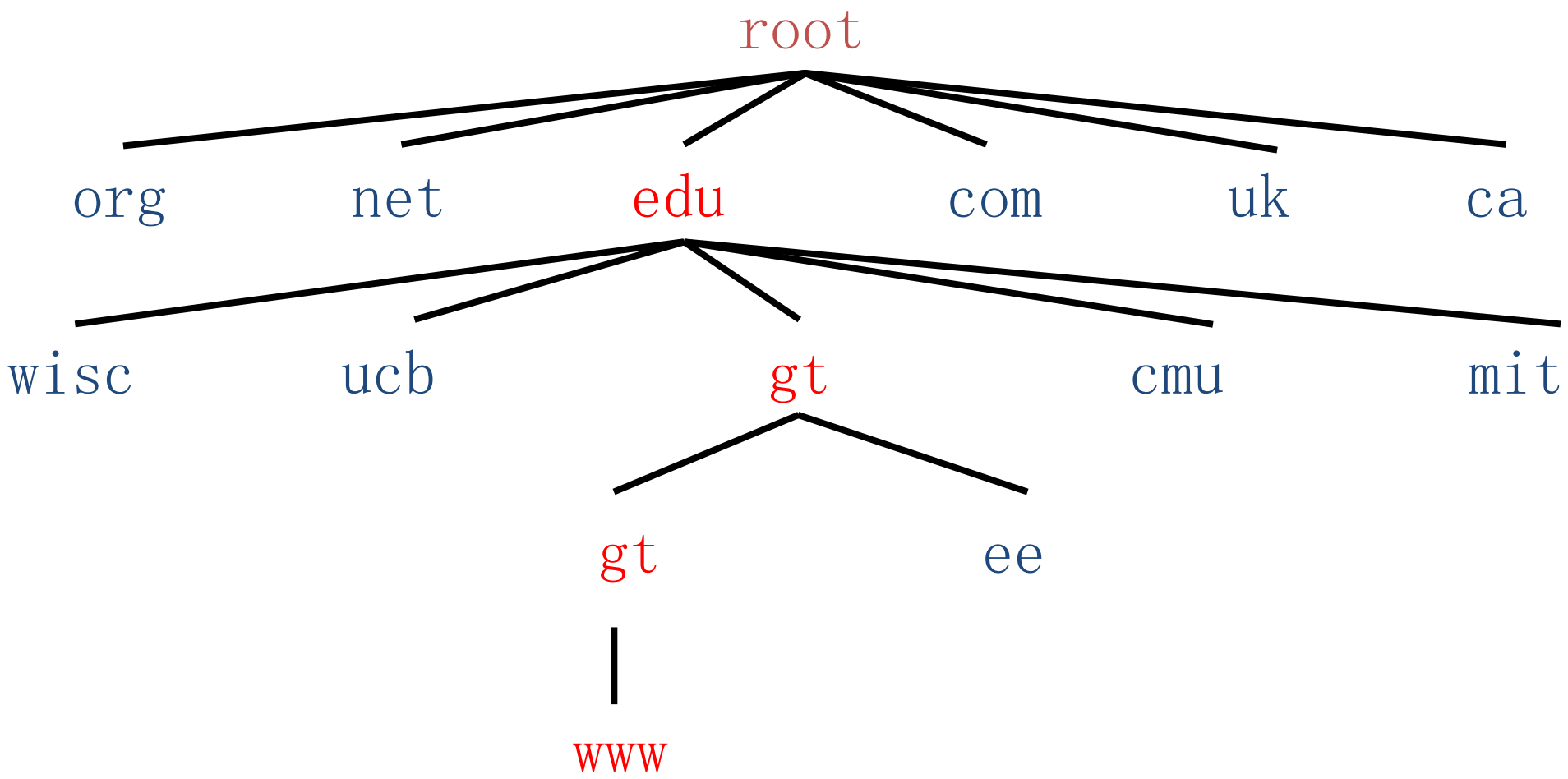


DNS Review Quiz

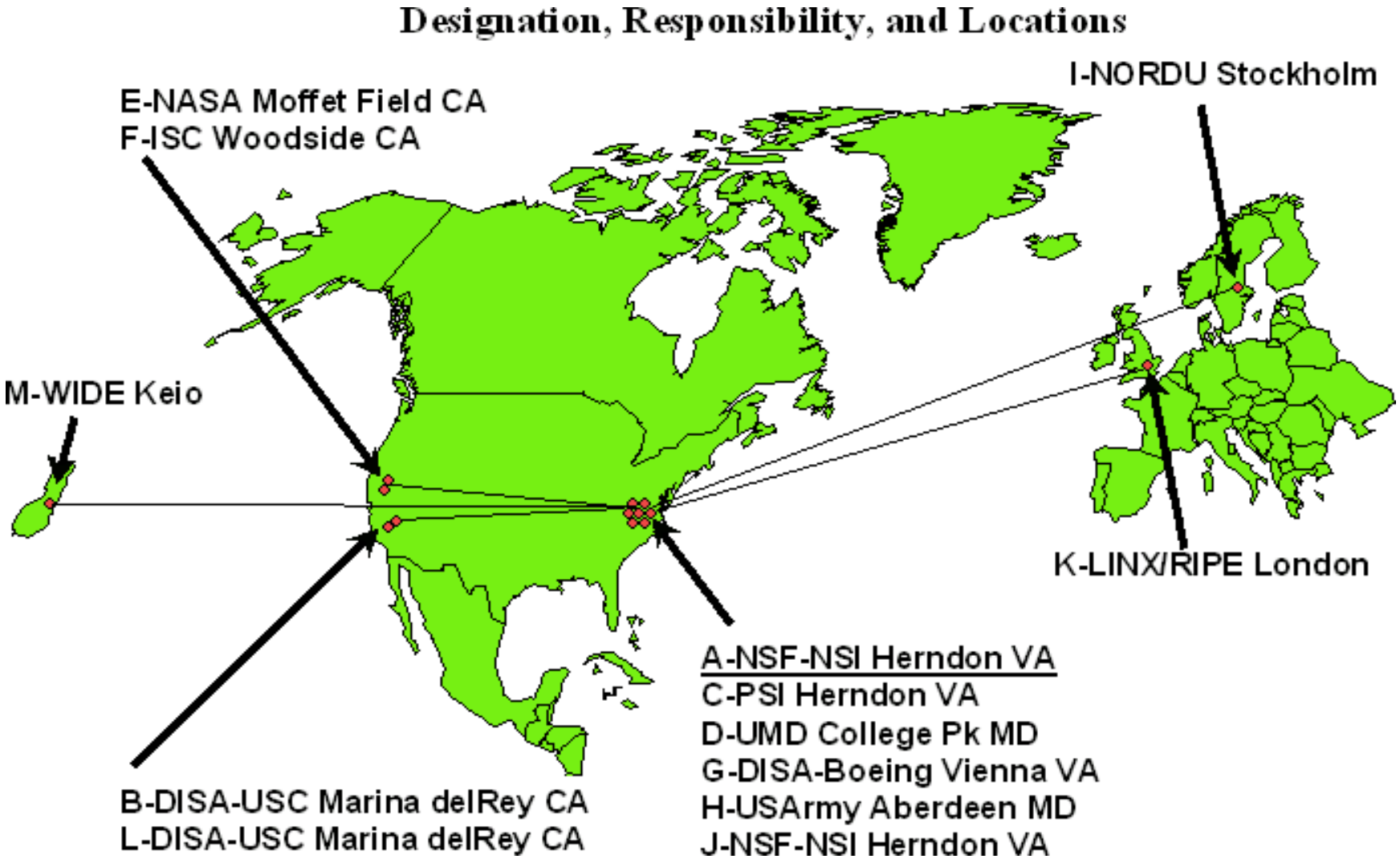
Match the term to the description:

Level:	Descriptions :
C Domain name	A. Transfer of authority for/to a sub- domain
B DNS zone	B. A set of names under the same authority (ie “.com”)
A Delegation	C. A name in the DNS format

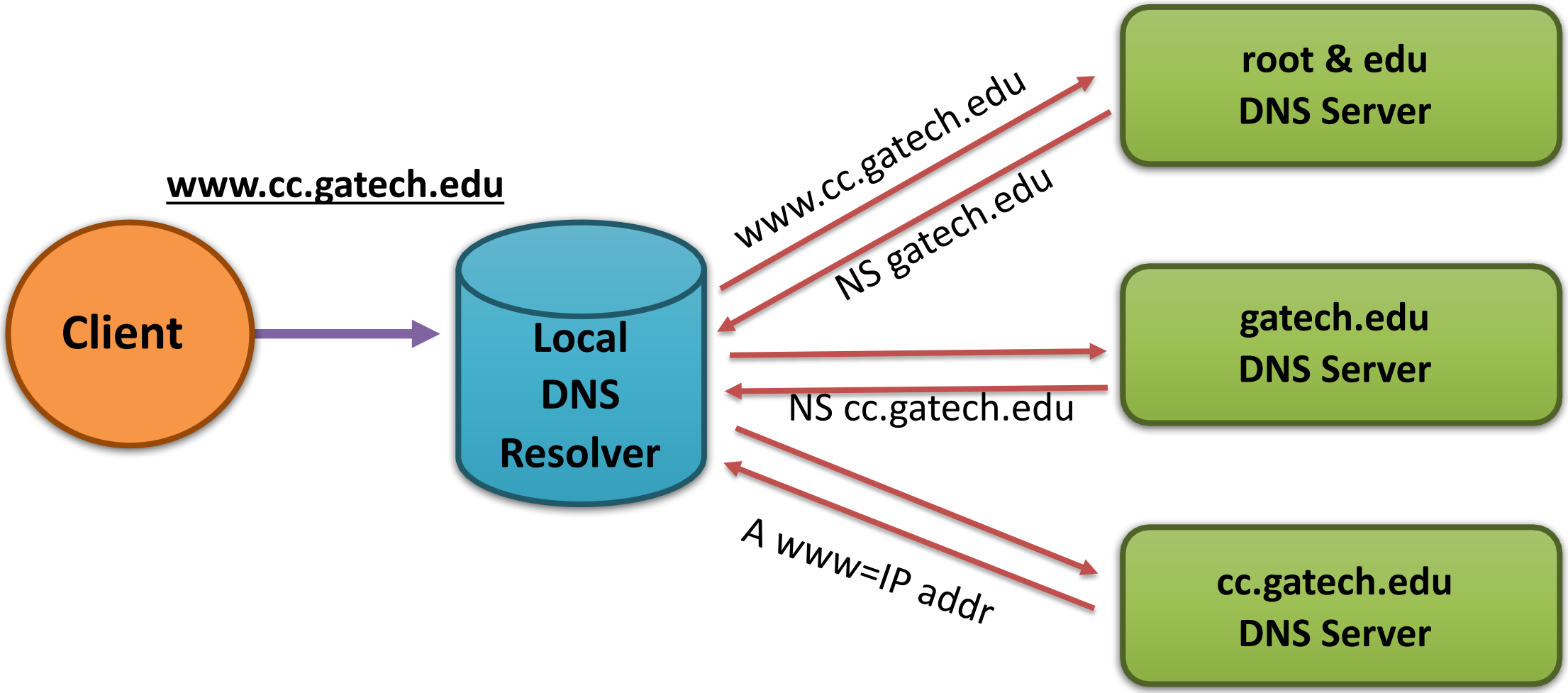
DNS: Hierarchical Name Space



DNS: DNS Root Name Servers



DNS: DNS Lookup Example



DNS: DNS Lookup Example

DNS record types (partial list):

- NS: name server (points to other server)
- A: address record (contains IP address)
- MX: address in charge of handling email
- TXT: generic text (e.g. used to distribute site public keys (DKIM)

DNS Caching Quiz

Fill in the blanks:

Changing a domain name into an IP address involves a large number of steps. To save time, the records are cached cached on a local server for reuse later.

Each record has a TTL that states how long a record can be kept for future use.

Caching

DNS responses are cached

- Quick response for repeated translations
- Note: NS records for domains also cached

DNS negative queries are cached

- Save time for nonexistent sites, e.g. misspelling

Cached data periodically times out

- Lifetime (TTL) of data controlled by owner of data
- TTL passed with every record

Basic DNS Vulnerabilities

Users/hosts trust the host-address mapping provided by DNS:

- Used as basis for many security policies:
  - Browser same origin policy, URL address

Obvious problems

- Interception of requests or compromise of DNS servers can result in incorrect or malicious responses
  - e.g: malicious access point in a cafe

Solution

- authenticated requests/responses
  - Provided by DNSsec … but few use DNSsec (yet)

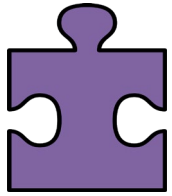
Basic DNS Vulnerabilities: Cache Poisoning

Basic idea: give DNS servers false records and get it cached

DNS uses a 16-bit request identifier to pair queries with answers

Cache may be poisoned when a name server:

- Disregards identifiers
- Has predictable ids
- Accepts unsolicited DNS records

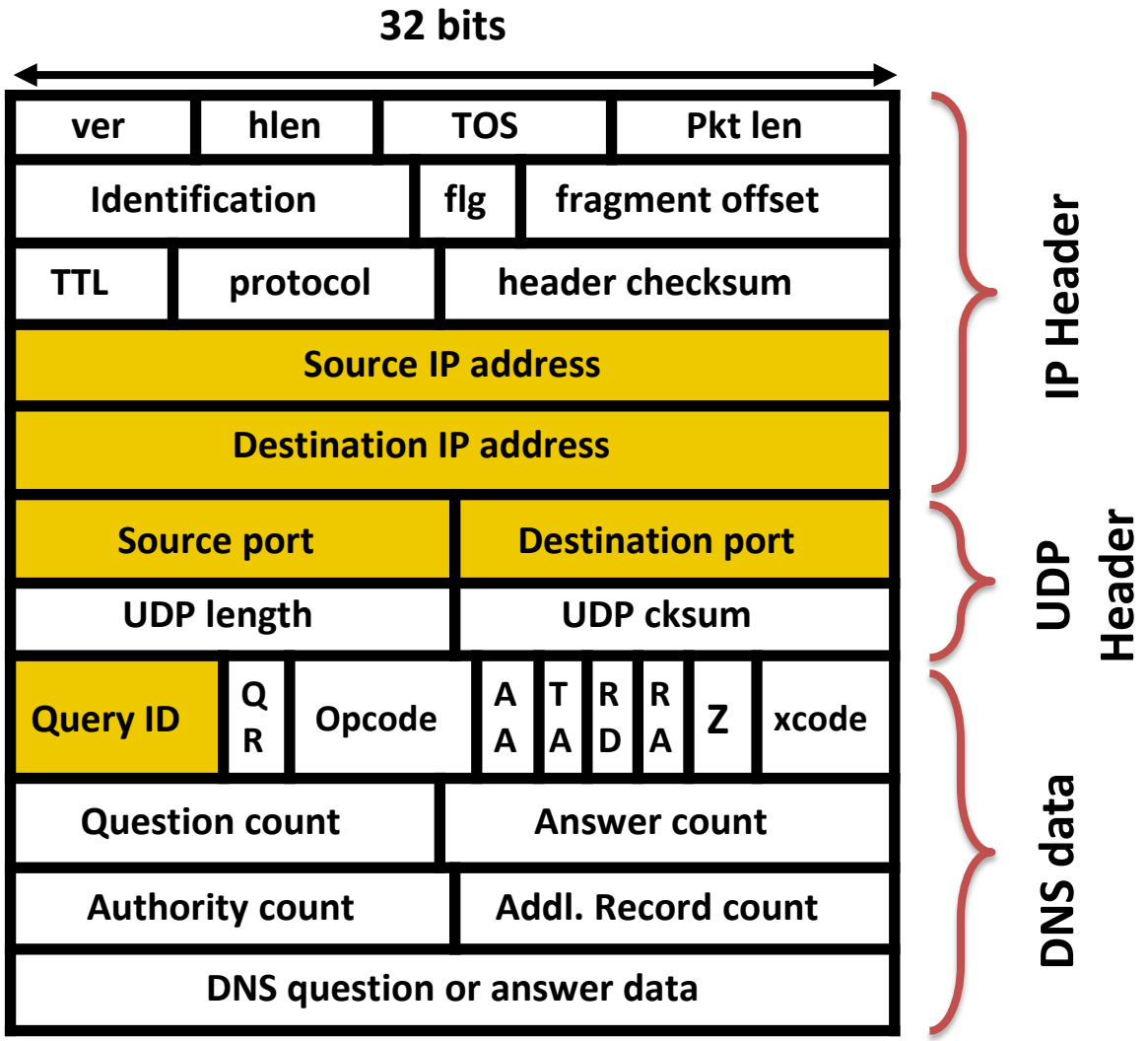


DNS Quiz

Select the true statements about DNS:

- [ ] DNS stores the IP address. For security reasons the domain name is stored somewhere else.
- [x] All domain names and IP addresses are stored at the Central Registry.
- [x] It can take several days for information to propagate to all DNS servers.

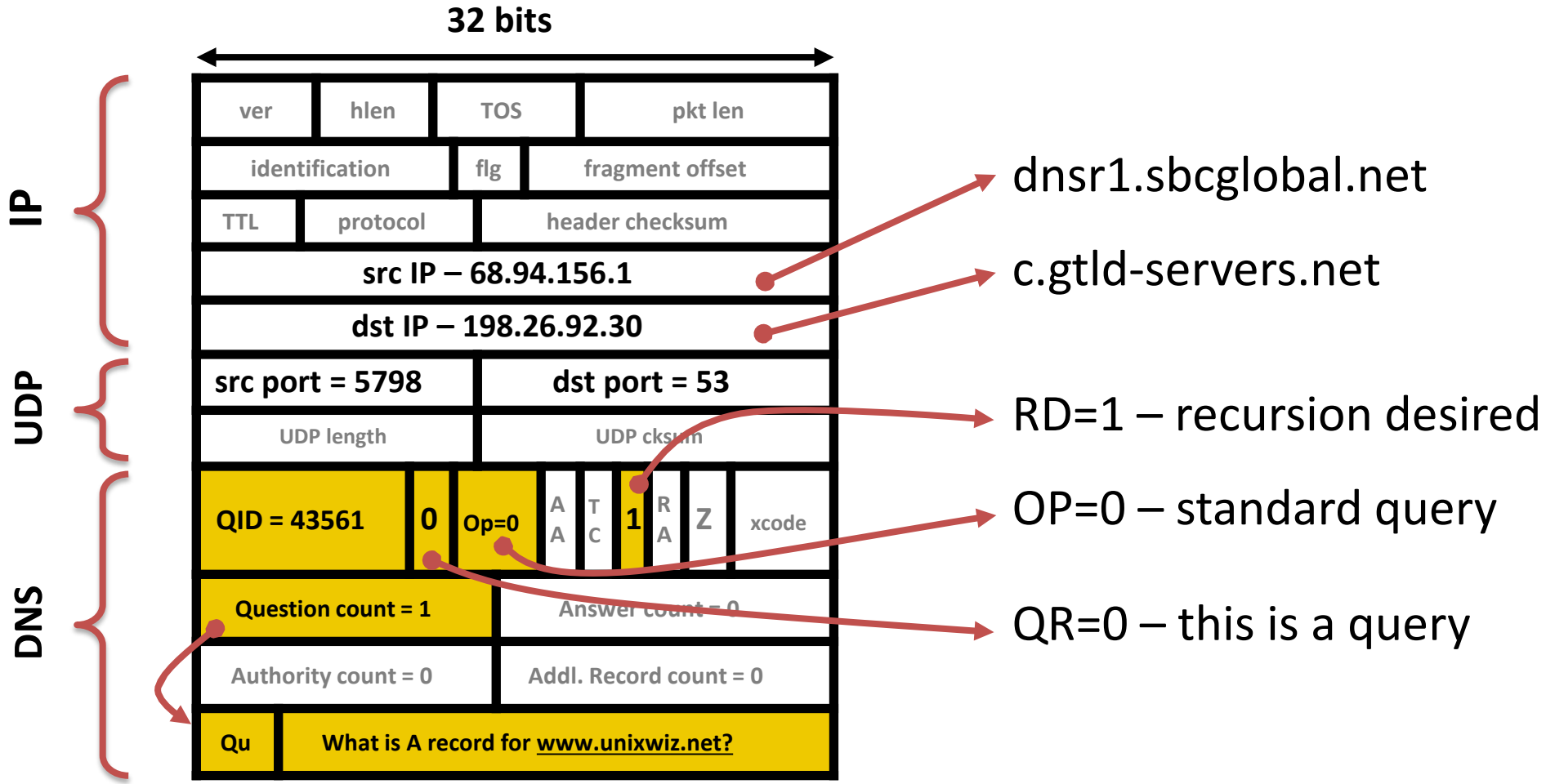
DNS Packet



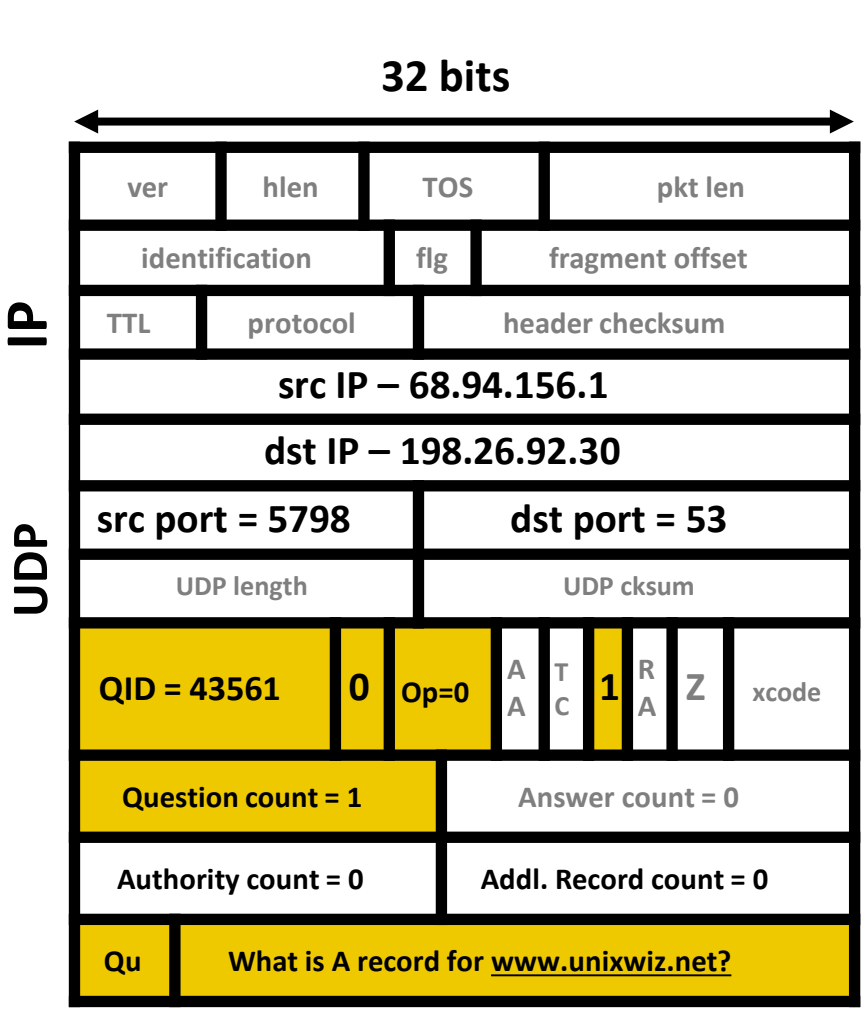
Query ID:

- 16 bit random value
- Links response to query

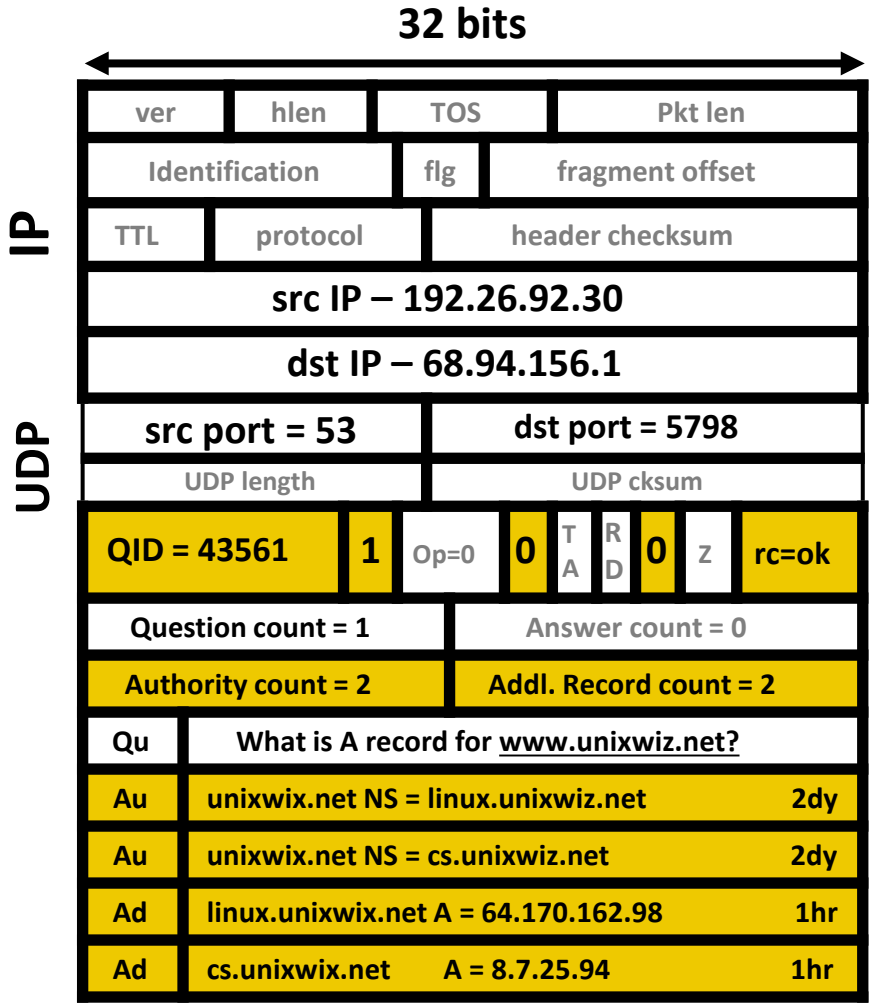
DNS Packet: Resolver to NS request



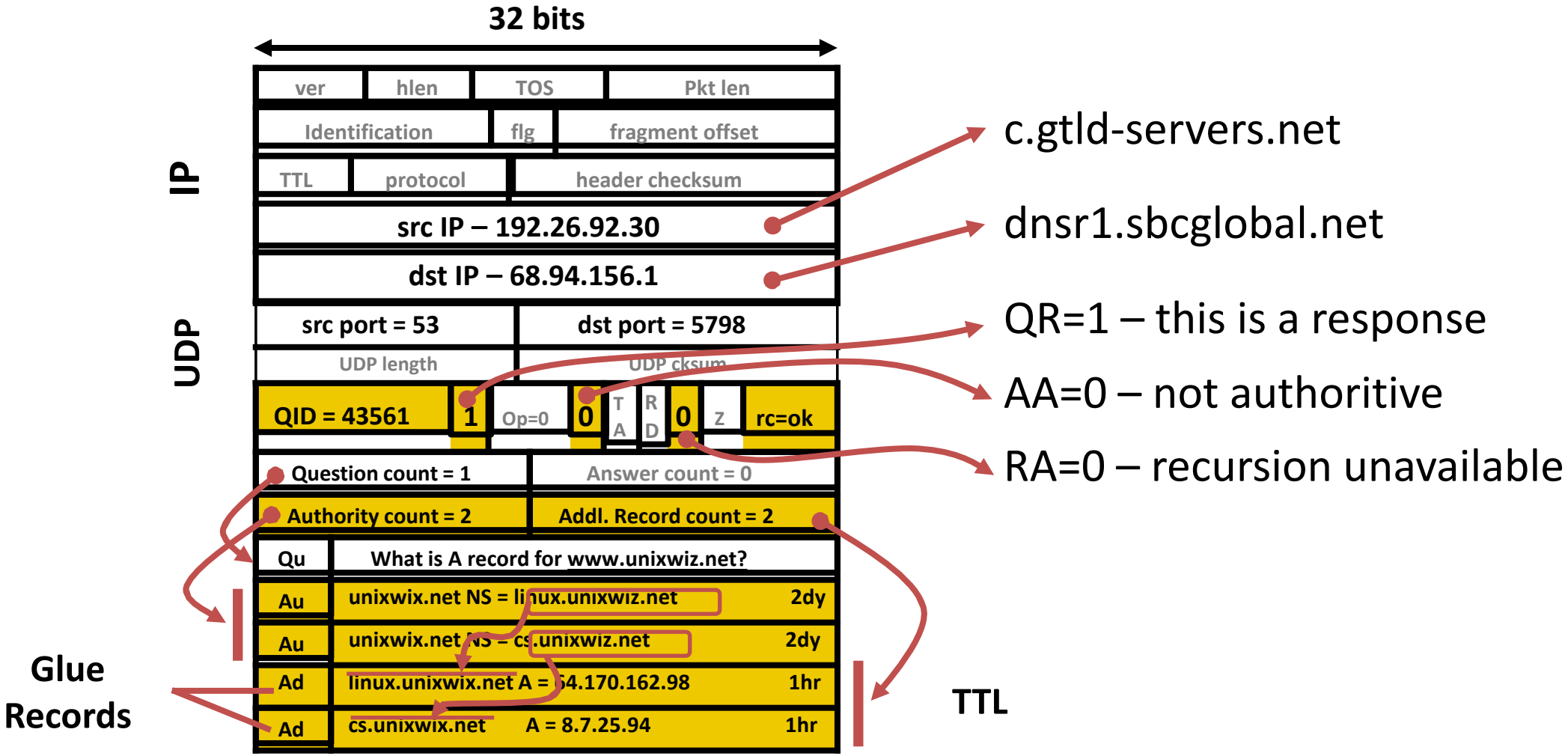
DNS Packet: Response to Resolver



Response contains IP addr of next NS server (called "glue")

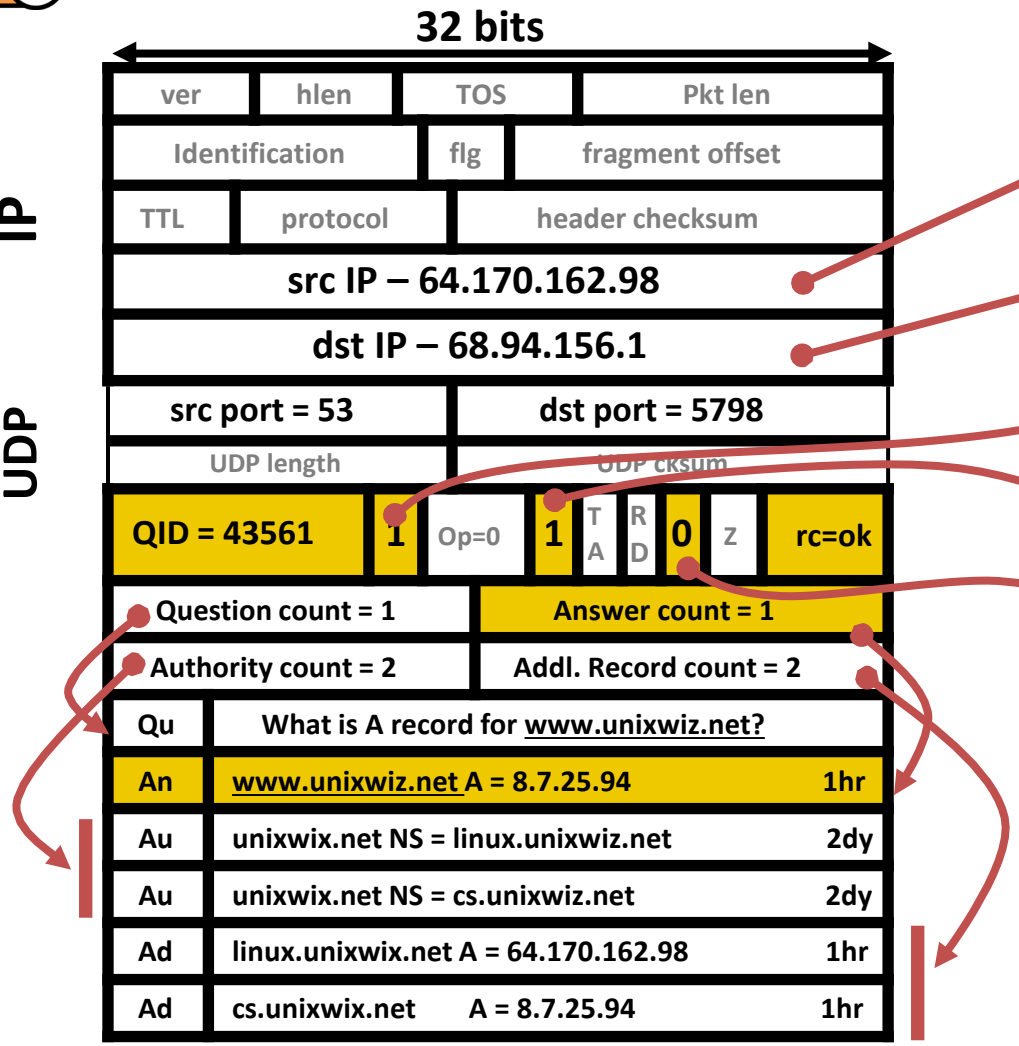


DNS Packet: Response to Resolver



DNS Packet: Authoritative Response

FINAL ANSWER



linux.unixwiz.net

dnsr1.sbcglobal.net

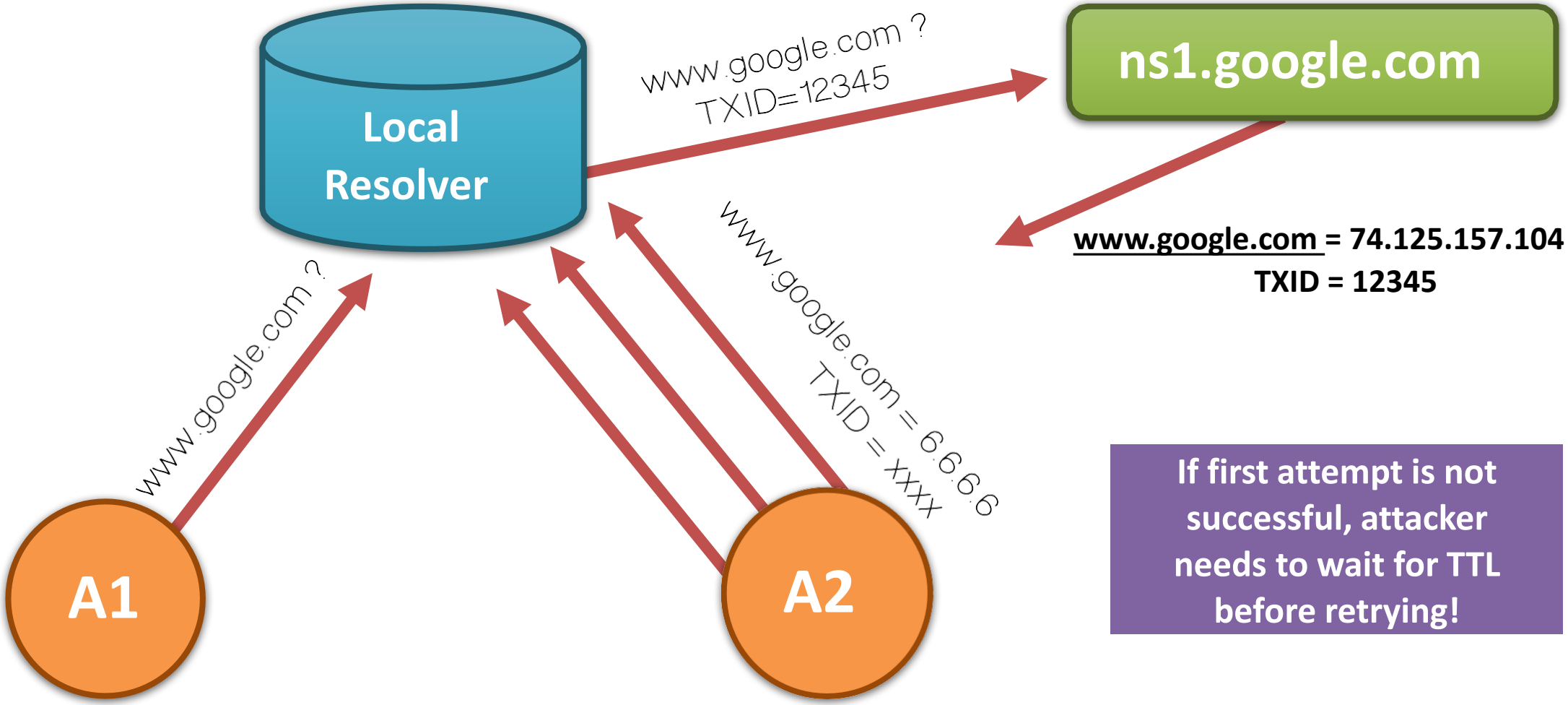
QR=1 – this is a response

AA=1 – Authoritative!

RA=0 – recursion unavailable

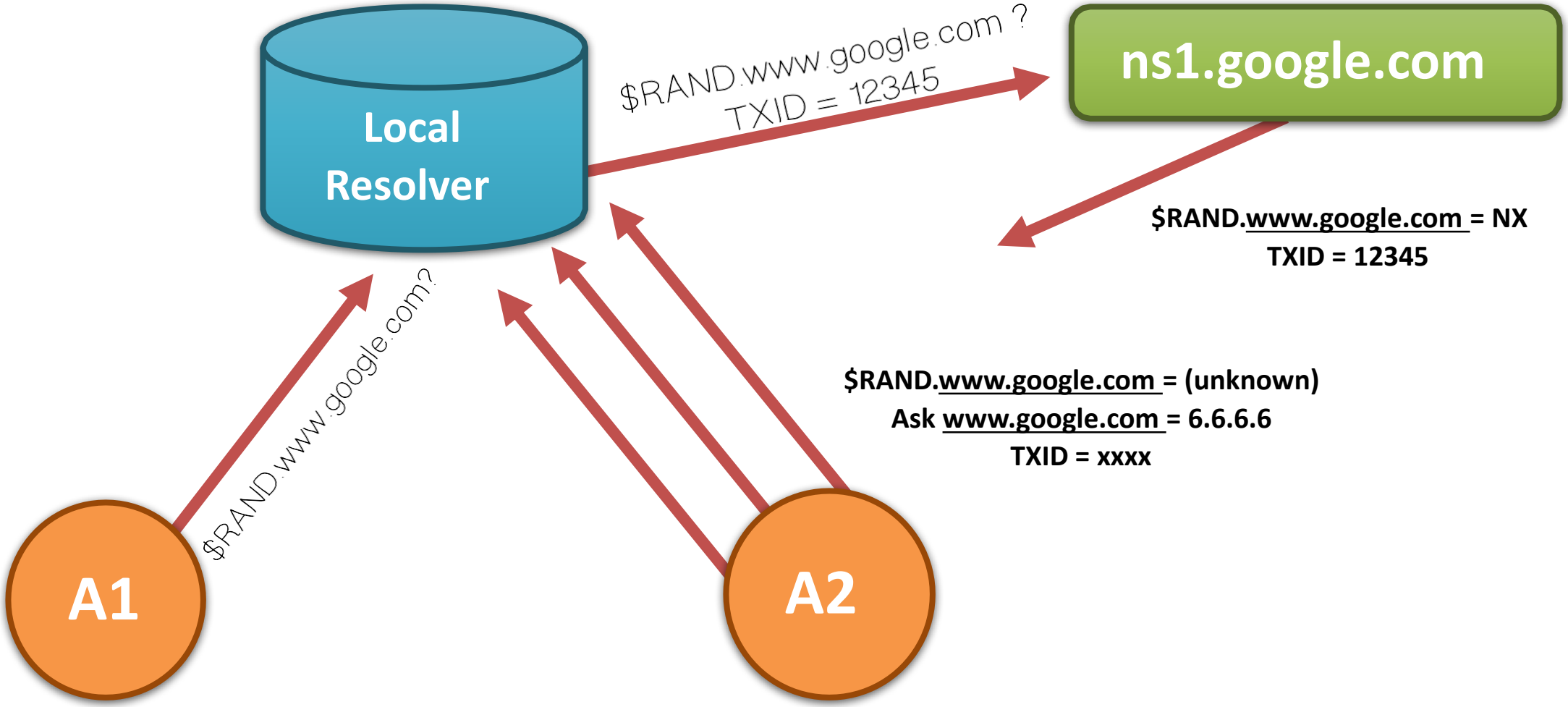
bailiwick checking: response is cached if it is within the same domain of query (i.e. a.com cannot set NS for b.com)

Traditional Poisoning Attack



If first attempt is not successful, attacker needs to wait for TTL before retrying!

Kaminsky's Poisoning Attack



DNS Defenses

Increase Query ID size

Randomize src port, additional 11 bits

- Now attack takes several hours

Ask every DNS query twice:

- Attacker has to guess QueryID correctly twice (32 bits) But DNS system cannot handle the load

Deploy DNSSEC (eventually)

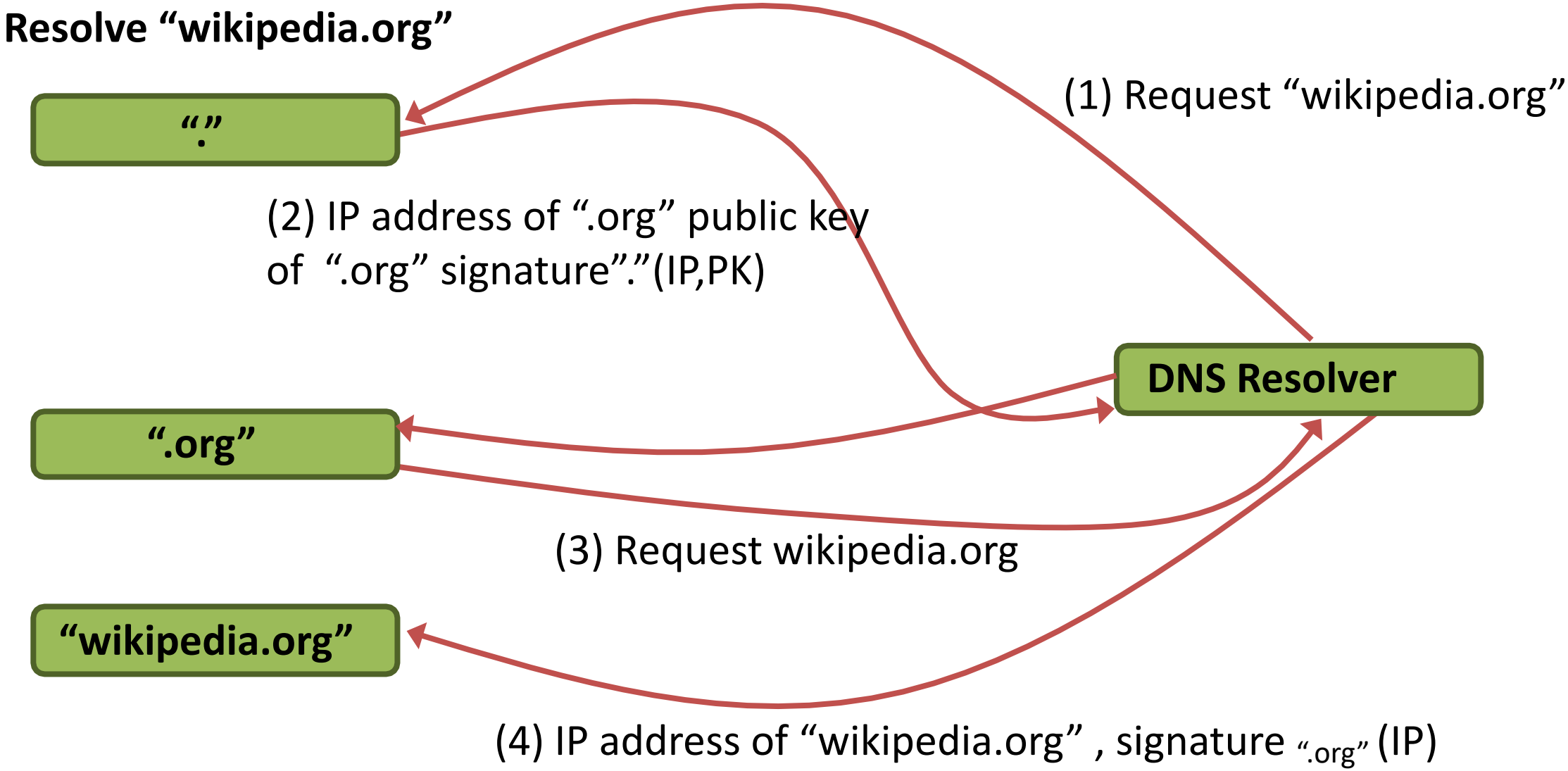
DNSSEC

Guarantees:

- Authenticity of DNS answer origin
- Integrity of reply
- Authenticity of denial of existence

- Accomplishes this guarantee by signing DNS replies at each step of the way
- Uses public-key cryptography to sign responses
- Typically use trust anchors, entries in the operating system to bootstrap the process

DNSSEC: DNS Signing



DNS Rebinding Attack

<iframe
src="Dhttp://www.evil.comD">

DNS-SEC cannot stop this attack

www.evil.com?

171.64.7.115 TTL = 0

192.168.0.100

ns.evil.com
DNS server

Firewall

corporate
web server

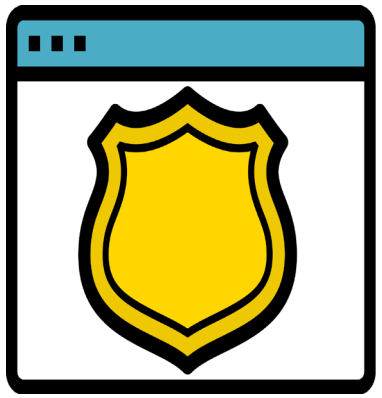
192.168.0.100

www.evil.com
web server

171.64.7.11
5

Read permitted: it's the "same origin"

DNS Rebinding Attack: Defenses



Browser mitigation: DNS Pinning

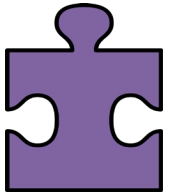
- Refuse to switch to a new IP
- Interacts poorly with proxies, VPN, dynamic DNS, …
- Not consistently implemented in any browser

Server-side defenses

- Check Host header for unrecognized domains
- Authenticate users with something other than IP

Firewall defenses

- External names can’t resolve to internal addresses
- Protects browsers inside the organization



DNS Rebinding Quiz

Select all the true statements about rebinding attacks:

- [x] The attacker needs to register a domain and delegate it to a server under his control.
- [x] The attacker's server responds with a short TTL record.
- [ ] A short TTL means the page will be quickly cached
- [x] The attacker exploits the same origin policy.