SACRAMENTO STATE

CSC/CPE 138 - Computer Network Fundamentals

Application Layer

The presentation was adapted from the textbook: *Computer Networking: A Top-Down Approach* 8th edition Jim Kurose, Keith Ross, Pearson, 2020

Redefine the Possible™

Caching DNS Information

- once (any) name server learns mapping, it *caches* mapping, and *immediately* returns a cached mapping in response to a query
  - caching improves response time
  - cache entries timeout (disappear) after time to live (TTL)
  - TLD servers typically cached in local name servers
- cached entries may be *out-of-date*
  - if named host changes IP address, may not be known Internet-wide until all TTLs expire!
  - *best-effort name-to-address translation!*

DNS records

DNS: distributed database storing resource records (RR)

RR format: (`name, value, type, ttl`)

type=A **(Address Record)**

Maps a domain name to an address.

- `name` is hostname
- `value` is IP address
- Example: example.com -> 192.0.2.1

DNS records

type=NS

- **Name Server Record**
- Points to the authoritative name servers for the domain
- `name` is domain (e.g., foo.com)
- `value` is hostname of authoritative name server for this domain (dns.foo.com)

```
example.com.    NS    ns1.hostingprovider.net.
example.com.    NS    ns2.hostingprovider.net.
```

DNS records

type=CNAME

- **Canonical Name Record**
- Maps one domain name to another.
- `Name` is alias name for some “canonical” (the real) name
- `value` is canonical name
- www.ibm.com is really servereast.backup2.ibm.com

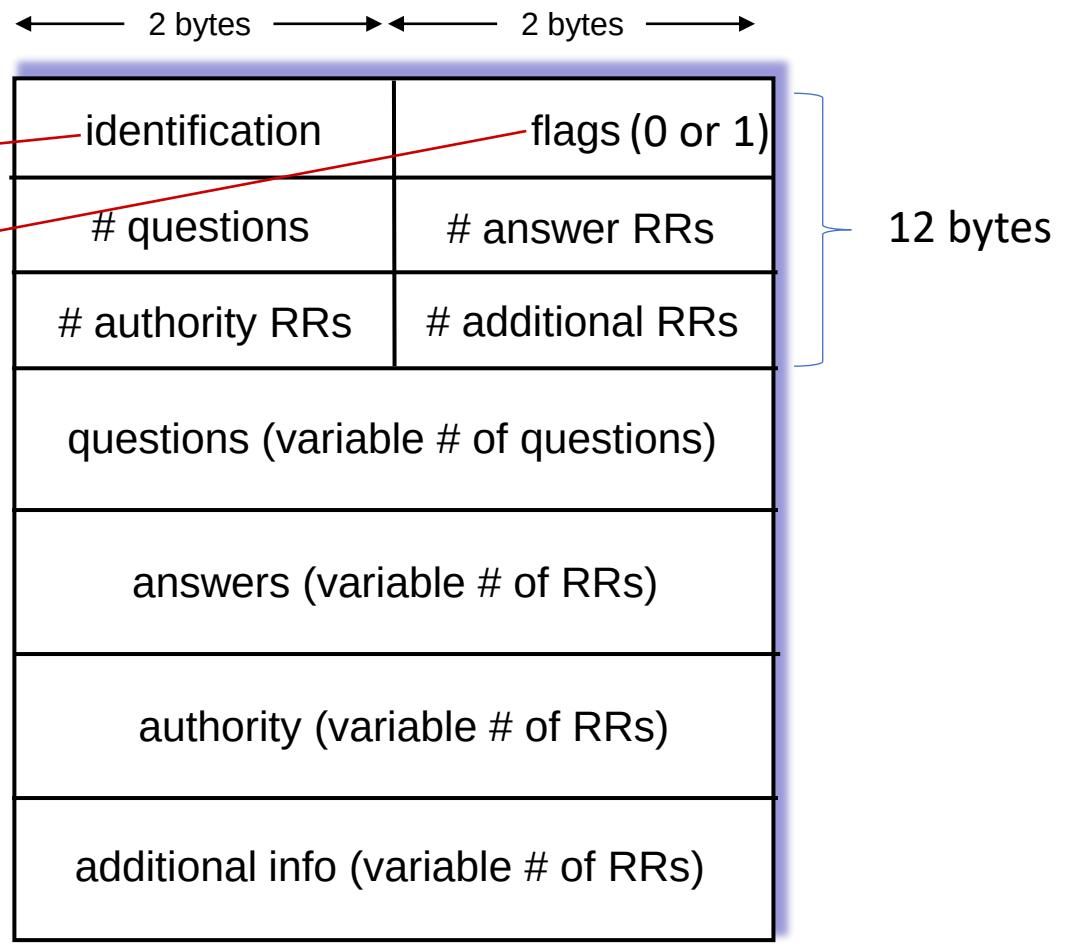
mywebsite.com. A 192.0.2.123
www.mywebsite.com. CNAME mywebsite.com.
info.mywebsite.com. CNAME mywebsite.com.

DNS protocol messages

DNS *query* and *reply* messages, both have same *format:*

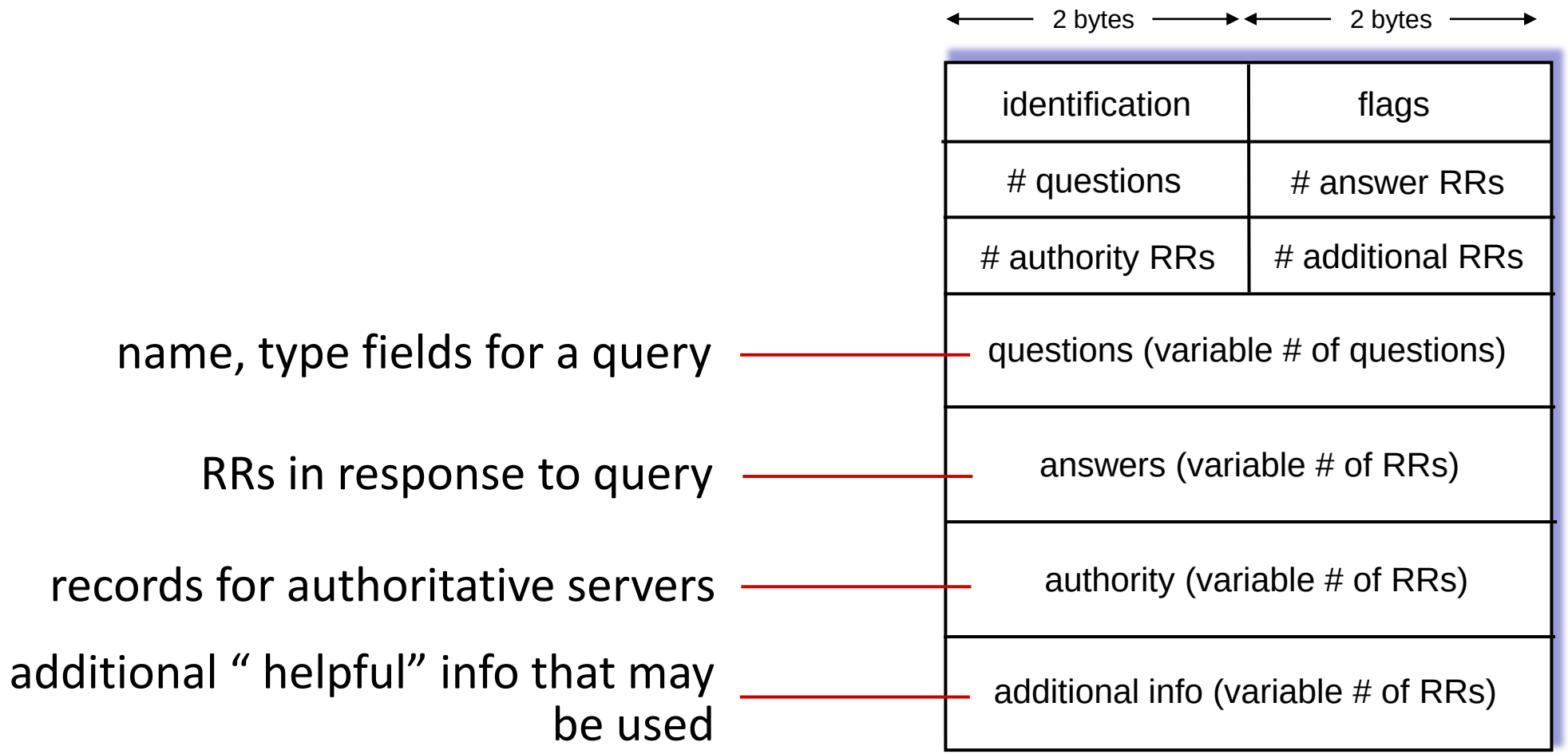
message header:

- identification: 16 bit # for query, reply to query uses same #
- flags:
  - query or reply
  - recursion desired
  - recursion available
  - reply is authoritative



DNS protocol messages

DNS *query* and *reply* messages, both have same *format:*



Getting your info into the DNS

example: new startup “Network Utopia”

- register name networkuptopia.com at *DNS registrar* (e.g., Network Solutions)
  - provide names, IP addresses of authoritative name server (primary and secondary)
  - registrar inserts NS, A RRs into .com TLD server:

    `(networkutopia.com, dns1.networkutopia.com, NS)`

    `(dns1.networkutopia.com, 212.212.212.1, A)`
- create authoritative server locally with IP address `212.212.212.1`
  - type A record for www.networkuptopia.com
  - type MX record for networkutopia.com

DNS security

DDoS attacks

- bombard root servers with traffic
  - not successful to date
  - traffic filtering
  - local DNS servers cache IPs of TLD servers, allowing root server bypass
- bombard TLD servers
  - potentially more dangerous

Spoofing attacks

- intercept DNS queries, returning bogus replies
  - DNS cache poisoning
  - RFC 4033: DNSSEC authentication services