ICS 451: Today's plan

- Application Layer
- Domain Name System:
  - Domain Name Hierarchy
  - DNS Server Hierarchy
  - DNS Protocol

Application Layer

- Reminder: the Application Layer takes care of all the functionality NOT provided by the lower layers
- Including security, sessions, login, multimedia...
- The application layer also resolves **domain names** to IP addresses

Domain Names

- www.hawaii.edu
- www2.hawaii.edu
- www.rcuh.com
- www.ietf.org
- www.wikipedia.org
- www.hawaii.gov
- portal.ehawaii.gov

Domain Name Hierarchy

- Domain names are arranged hierarchically:
  - there is a small number of top-level domains (TLDs)
    - .edu .gov .org .com .arpa .us .ca .it .ch .jp .fr .uk..
  - below each TLD can be any number of unique domain names
    - hawaii.edu hawaii.gov hawaii.org hawaii.com...
  - the hierarchy can extend almost arbitrarily
    - www.ics.hawaii.edu
- the root of the hierarchy is just '.'

Domain Name Management

- The domain name space is divided into contiguous *zones*
- Each zone is under a single management
  - But one administrator can manage many zones
- hawaii.edu, botany.hawaii.edu, and www.botany.hawaii.edu are in the same zone
  - but ics.hawaii.edu and www.ics.hawaii.edu are in a different zone

Domain Name Zones

- Each zone should have at least two servers
- Each server must keep the IP addresses of:
  - every domain name in the zone
  - the servers for every sub-zone
- This way, every server can be reachable by starting from a root server

Domain Name Resolution

- Domain Name resolution is the process of converting a domain name to an IP address
  - this can fail!
  - some domain names have no IP address
- Ask the root server
  - get the IP of the server on the next level down
- Ask the next level-down server
- until you get the translation if any

Types of DNS resolutions

- Alice asks Bob to tell her the IP for foo.org
- iterative: Bob tells Alice to ask Charlie
- recursive: Bob asks Charlie
  - and Donna and Eve, if necessary
  - then tells Alice whatever Charlie (Donna, or Eve) said
- It is up to each DNS server (that doesn't have the answer) to respond iteratively or recursively
  - the client can specify a preferred mode

DNS Resolvers

- A network may have a specialized server that handles DNS queries recursively
  - this is a *resolver*
- A resolver may also cache the results of popular queries, to decrease the number of queries that need to go out onto the Internet

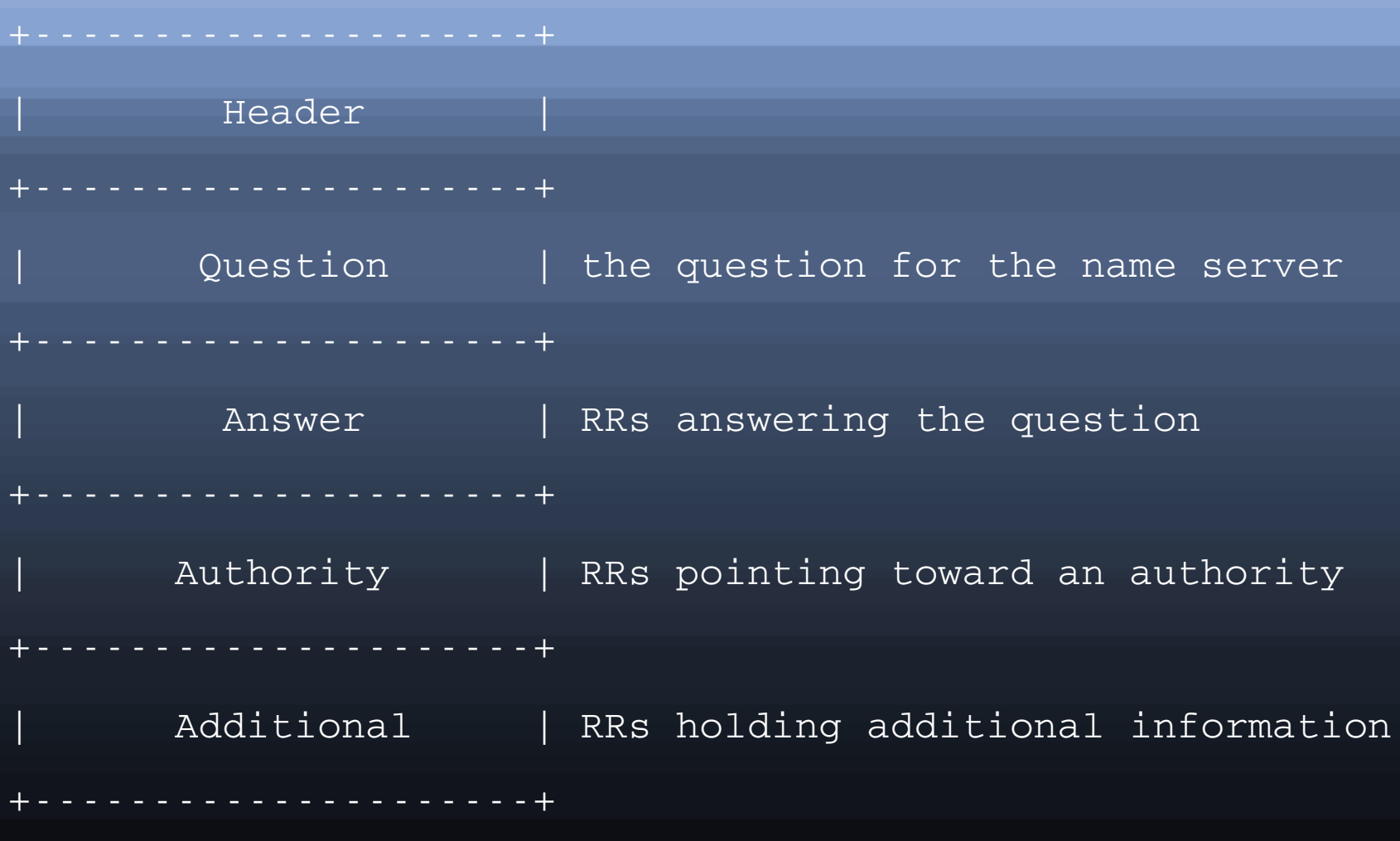
DNS Caching

- The DNS protocol allows read-only access to DNS data
- Therefore, there is no concern with concurrent access to this distributed database
- Each resolution returns a TTL (Time To Live) for the information
  - clients and resolvers may cache the information for up to the TTL
  - e.g. 86400s (1 day), 7200s, 600s

DNS Protocol

- DNS has requests and replies (*queries* and *answers*)
- Each query is for a Resource Record (RR)
  - each answer is a RR
- Each message has a header followed by one or more RRs
- The message can be sent over UDP
  - or, with a length header, over TCP

DNS Message Structure

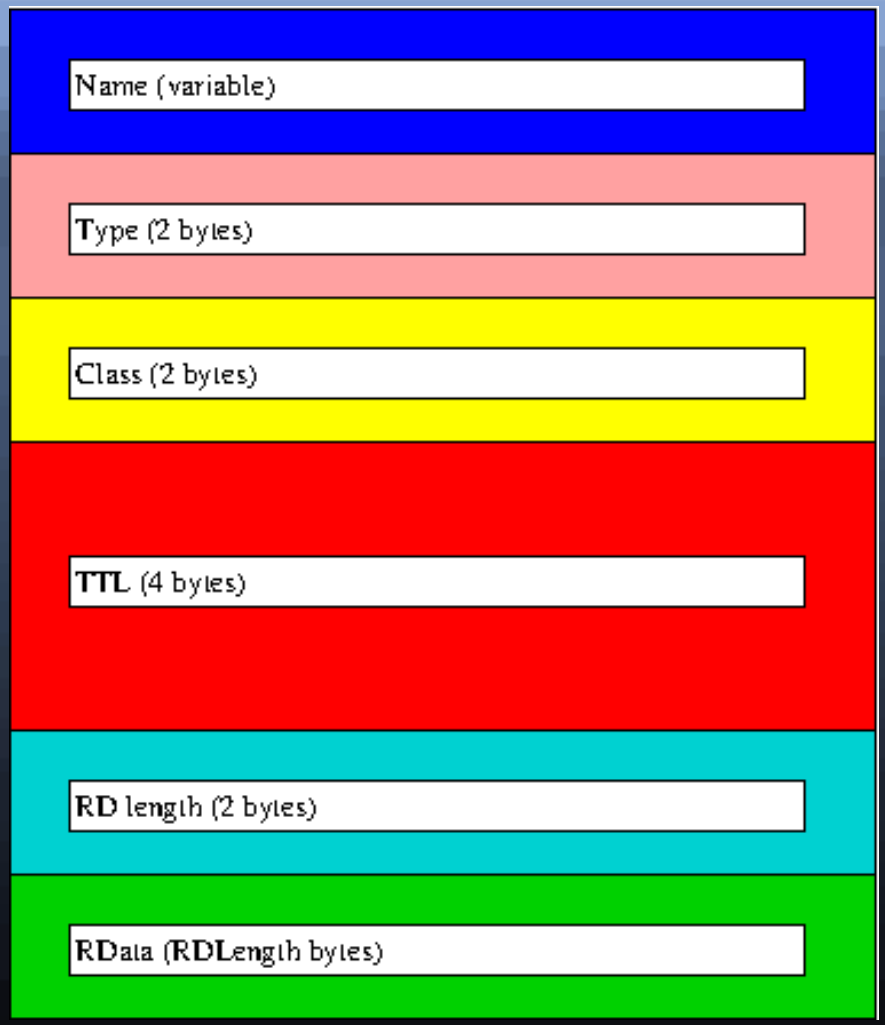


- from RFC 1035

DNS Header


ID
QR
Opcode
AA
TC
RD
RA
Z
RCODE
QDCOUNT
ANCOUNT
NSCOUNT
ARCOUNT

Resource Record Structure



Classes and Types

- Classes:
  - A (IPv4 address), AAAA (IPv6)
  - MX (mail server)
  - NS (name server)
  - CNAME (canonical name for an alias)
  - PTR (reverse lookup pointer)
- Only 1 Type: IN (1), the Internet
  - other types are obsolete

A DNS Lookup

- Query carries a Query Name, followed by a Type and a Class
  - e.g. www.hawaii.edu, A, IN
  - typically 1 query, and no other records
- Response has:
  - answers: CNAME web00.its.hawaii.edu

    web00.its.hawaii.edu A 128.171.224.100
  - authority: hawaii.edu NS dns1.hawaii.edu
  - additional: dns1.hawaii.edu A 128.171.213.116

Encoding Names

- Domain Names are encoded as sequences of labels, each label up to 63 bytes long
- Each label is 1 byte of length, then the name
  - The root is a single byte of 0
- Optimization: a label can be replaced by a 14-bit pointer preceded by two 1 bits
  - the remaining 14 bits are an index into the message
  - that is the beginning of another label

Encoding Names – example

- web00.its.hawaii.edu appears as:
  - **5**web00**3**its**6**hawaii**3**edu**0**
- if the index of the **5** in the message is 45, and the **6** is at index 55 in the message
- dns1.hawaii.edu can be encoded as
  - **4**dns1**xC0 x37** (55 is x37)
- any further web00.its.hawaii.edu can be
  - **xC0 x2D** (45 is x2D)
- www.hawaii.edu is **3**www**xC0 x37**

Request and Reply IDs

- The requester generates a different ID for each request
- The server copies the ID field into the reply
- The requester ignores replies with different Ids

- Security issue:
  - if I can guess what you are going to query
  - and I can guess your ID
  - I can send you a spoofed reply