CIS 457 - Data Communications

Nathan Bowman

Images taken from Kurose and Ross book

DNS Protocol

DNS is distributed database

We know how it is structured, but what do contents look like?

Entries in DNS are called Resource Records (RRs)

Resource records contain (among other things) mappings from hostnames to IP addresses

Each DNS response contains at least one resource record

RRs are 4-tuples

```
(Name, Value, Type, TTL)
```

TTL is time-to-live of record

Used to tell cache how long record should be maintained

Meanings of other entries depend on Type

Type A

Name: hostname

Value: IP address

Type A records are eventual goals of DNS queries

Type NS:

Name: domain

Value: hostname of authoritative DNS server for domain

```
(foo.com, dns.foo.com, NS)
```

Used for intermediate steps of DNS queries

Type CNAME:

Name: alias hostname

Value: canonical name

```
(www.enterprise.com, relay1.west-coast.enterprise.com, CNAME)
```

Allow aliasing of hostnames to make them more readable

Type MX:

Name: alias hostname *of mail server*

Value: canonical name

```
(foo.com, mail.bar.foo.com, MX)
```

Allows mail server to share name with one other server (e.g., web server) while keeping separate IP address

When web browser requests address of `yahoo.com`, it requests Type A record and finds IP address of web server

When sending email to `bob@yahoo.com`, client first requests MX record for `yahoo.com` to find canonical name of mail server

Client then requests Type A record for canonical name of mail server, which may be different than web server

Note difference between CNAME and MX

CNAME allows one host to have several names (same IP address)

MX allows same hostname to mean different things in different contexts (different IP addresses)

Normally one hostname with two IP addresses for different purposes would make no sense, but mail is such an important case that the exception is built directly into DNS

Authoratative server for particular hostname is server containing Type A record for that hostname

Non-authoratative server may also be able to return Type A record for hostname if it is cached from previous response

Otherwise, server contains

- NS record for domain responsible for hostname
- Type A record for that nameserver

In other words, nameserver either

- sends you requested address, or
- tells you who has address and where to find them

Example records returned from non-authoritative nameserver:

```
(umass.edu, dns.umass.edu, NS)
(dns.umass.edu, 128.119.40.111, A)
```

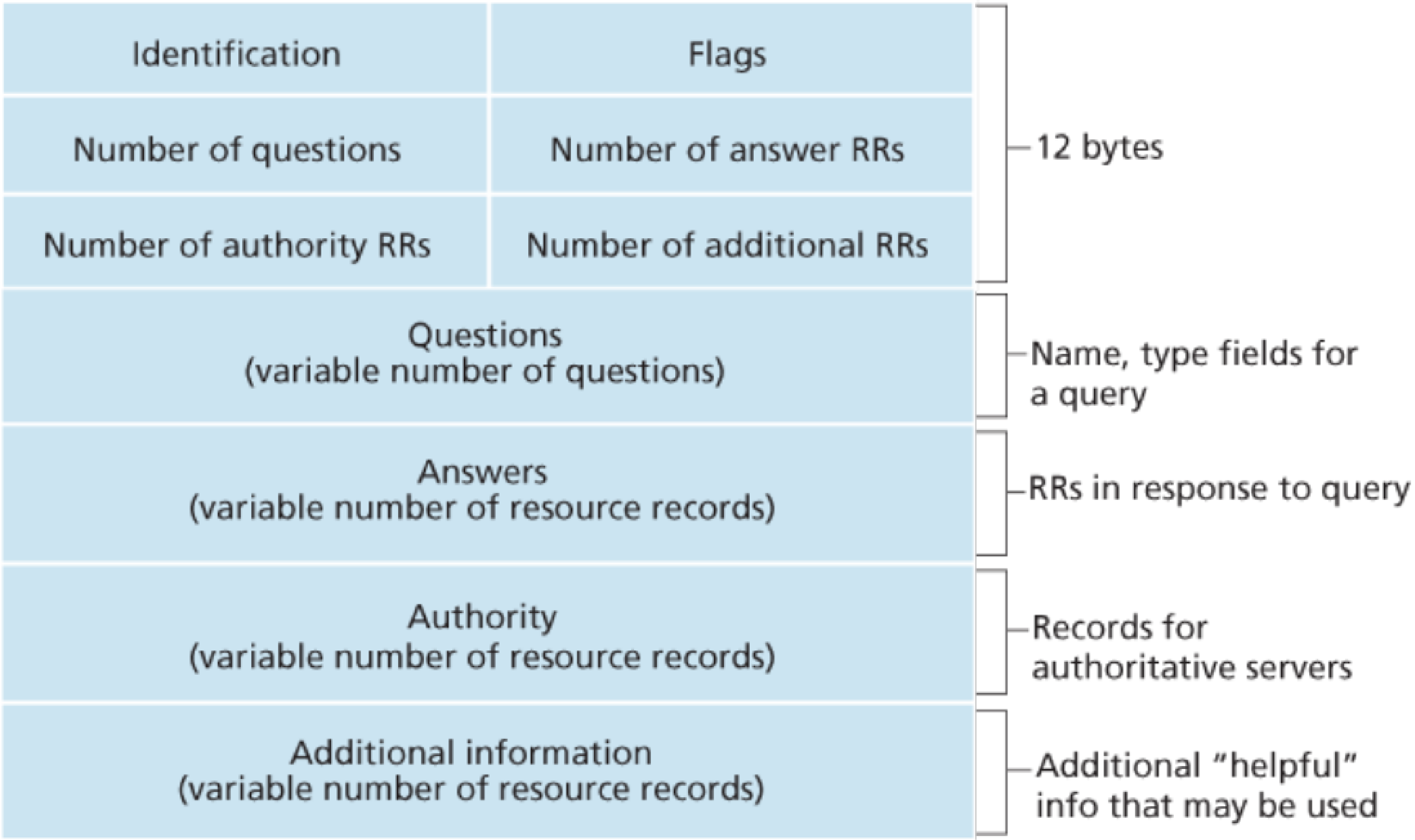
DNS messages

Using DNS protocol, like any protocol, requires knowing format of messages to send and receive

DNS query and reply both have same format

As mentioned previously, DNS responses contain RRs

Unlike HTTP and SMTP, protocol is not entirely text-based



Identification

Flags

Number of questions

Number of answer RRs

Number of authority RRs

Number of additional RRs

12 bytes

Questions
(variable number of questions)

Name, type fields for a query

Answers
(variable number of resource records)

RRs in response to query

Authority
(variable number of resource records)

Records for authoritative servers

Additional information
(variable number of resource records)

Additional “helpful” info that may be used

ID: copied from request to reply so client can keep track

Some of the flags:

- query (0)/reply (1)
- authoratative?
- recursion desired? (set by client)
- recursion available? (set by server)

Four numbers indicating how many records returned in each section

Question section: (Name, Type) pairs of requests

Answer section: RRs answering question

- (Name, Value, Type, TTL)

Authority section: RRs of other authorities

- nameserver can point to other nameservers that may be more suited to answer similar questions

Additional section: RRs that may be helpful

- RRs related to information from other sections -- for example, Type A record corresponding to canonical name returned by MX request
- server is trying to keep client from asking another question

Deciding who gets a hostname

For DNS to work, everyone on internet must agree which name maps to which IP address

Registrars are responsible for managing hostnames and updating TLD servers

Institution or company pays registrar a fee to ensure domain name is unique and to put information into DNS servers

Registrars are companies accredited by Internet Corporation for Assigned Names and Numbers (ICANN)

When registering a domain, also required to provide names and IP addresses of primary and secondary authoratative DNS servers

Recall that these servers manage hostname to IP address mapping for your domain

Part of job of registrars is entering those four records into DNS:

- NS records for primary and secondary servers
- Type A records for primary and secondary servers

Type A records within a domain do not need to be entered by registrar

These records are under control of institution's nameserver and can be changed at any time

Once an organization owns `gvsu.edu` domain, hostnames `www.gvsu.edu`, `cis.gvsu.edu`, etc. are all managed by their authoratative nameserver

Same is true for further levels of NS servers -- they can add a lower-level nameserver to manage hostnames in `cis.gvsu.edu` if desired