

## HW3 – UDP DNS Client

RFC 1034  
RFC 1035

Netprog 2001 - Homework 3  
DNS client

1

---

---

---

---

---

---

---

---

## DNS Message Format

- There is a single message format used for both queries and responses.
  - some parts are empty in a query.
  - some parts are empty in a response.
- Each query has a 16 bit *identifier* established by the client – all responses include the matching identifier.

Netprog 2001 - Homework 3  
DNS client

2

---

---

---

---

---

---

---

---

## DNS Message Format and RFC 1035

- RFC 1035 describes the complete format for DNS messages – you need to look at the RFC!
- Network Byte Order!
- You'll need to do some *bit manipulations* in C: look at logical AND (&) and OR (|) operators.

Netprog 2001 - Homework 3  
DNS client

3

---

---

---

---

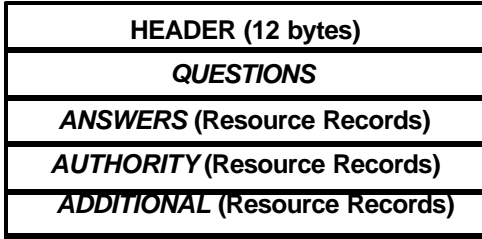
---

---

---

---

## DNS Message Format



Netprog 2001 - Homework 3  
DNS client

4

---

---

---

---

---

---

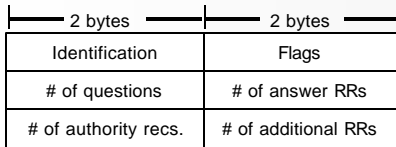
---

---

---

---

## DNS Message Header (12 bytes)



Identifier is set by the client (a query ID).

2 byte integers are in network byte order.

Netprog 2001 - Homework 3  
DNS client

5

---

---

---

---

---

---

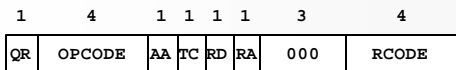
---

---

---

---

## DNS Header FLAGS field



QR: 0 means message is query, 1 means response.

OPCODE: 0 is *standard query* (use 0).

AA: 1 means authoritative answer (set by server).

TC: 1 means response was truncated (set by server).

RD: 1 means recursion desired (set by client).

RA: 1 means recursion available (set by server).

000: must be three zero bits.

RCODE: return code. 0 is no error, 3 is name error, etc.

Netprog 2001 - Homework 3  
DNS client

6

---

---

---

---

---

---

---

---

---

---

## Question Format

- Each *question* includes a variable length *query name* that specifies a hostname.
  - the format of this is not what you might expect!
- Each question also includes
  - *query type* (what kind of question is this)
  - *query class* is 1 for Internet Addresses

Netprog 2001 - Homework 3  
DNS client

7

---

---

---

---

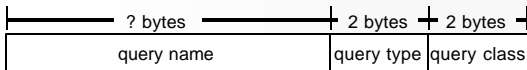
---

---

---

---

## Question Format



Query Name is a sequence of one or more *labels*.

Each *label* is a single byte count, followed by that many characters.

The last label must have a count of 0.

Netprog 2001 - Homework 3  
DNS client

8

---

---

---

---

---

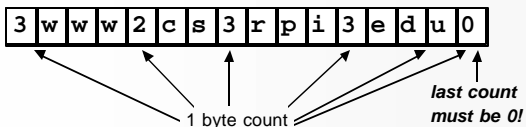
---

---

---

## Query Name Example

The name `www.cs.rpi.edu` would be sent like this:



Each count byte is a binary value in the range 0-63  
count bytes are not ASCII !

Netprog 2001 - Homework 3  
DNS client

9

---

---

---

---

---

---

---

---

## Query Type Field Values

A	1	IP Address
NS	2	Name Server
CNAME	5	Canonical Name
PTR	12	Pointer
HINFO	13	Host Info
MX	15	Mail Exchanger
ANY	255	<i>everything</i>

Netprog 2001 - Homework 3  
DNS client

10

---

---

---

---

---

---

---

---

---

---

## Answer Format Resource Records

The *answers*, *authority* and *additional information* parts of a response are all provided via the same format – called a Resource Record (RR).

Each Resource Record specifies the value of a single resource along with information about the resource (what kind it is, how long in the information is valid, etc.)

Netprog 2001 - Homework 3  
DNS client

11

---

---

---

---

---

---

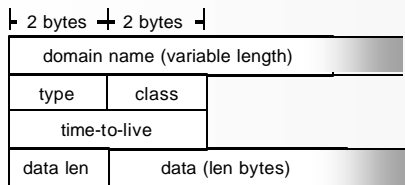
---

---

---

---

## Resource Record Format



Netprog 2001 - Homework 3  
DNS client

12

---

---

---

---

---

---

---

---

---

---

## RR Types

- There are many *types* of Resource Records – for HW3 you only need to handle a few:
  - A (address – the data is an IP address).
  - NS (name of the name server that can answer the original query).
- If you get an NS RR in a response, there will also be a matching A that indicates the address of the name server.

---

---

---

---

---

---

---

---

## High level look at HW3

- domain name to IP conversion:
  - build an **A** query, expect an **A** response.
    - RR contains an IP address.
  - If the server doesn't tell you the answer, you need to look for NS resource records.  
Resend the query to the new name server mentioned in the response.

---

---

---

---

---

---

---

---

## Issues

- Domain Name Compression
  - A response with multiple RRs can use internal pointers to reference previous copies of a domain name
    - Section 4.1.4 of RFC 1035
- Recursion
  - You can request recursion, but the server might not provide it. It will instead send back a list of name servers that you should contact (they can answer the original query).

---

---

---

---

---

---

---

---

## Bit Fiddling Required

*(another great name for a band)*

- Most of the fields in a DNS message are binary – not ASCII.
  - You need to understand the difference!
  - You need to be able to extract bit values and to set individual bit values.
- Debugging is tough!
  - It's worth writing subroutines that can print DNS messages.

Netprog 2001 - Homework 3  
DNS client

16

---

---

---

---

---

---

---

---

## UDP Only!

- You don't need to use TCP.
  - If a server sends a reply that has the TRUNC bit set – the answer couldn't fit in a 512 byte DNS message. That's fine – you can simply print this out (you don't need to retry using a TCP connection).

Netprog 2001 - Homework 3  
DNS client

17

---

---

---

---

---

---

---

---

## Important!

- For testing – use the name server running on 128.213.1.1.
- Do not use the rpi.edu name servers!

Netprog 2001 - Homework 3  
DNS client

18

---

---

---

---

---

---

---

---