How to get IP address from Domain Name Server (DNS)

Domain name Servers (DNS) are an important but invisible part of the internet, and form one of the largest databases on it. Each machine on an internet is assigned a unique address, called an IP address, which is 32 bit number and is expressed as 4 octets. The method user to represent these IP addresses is known as dotted decimal notation. A typical address looks like this: 199.249.150.4

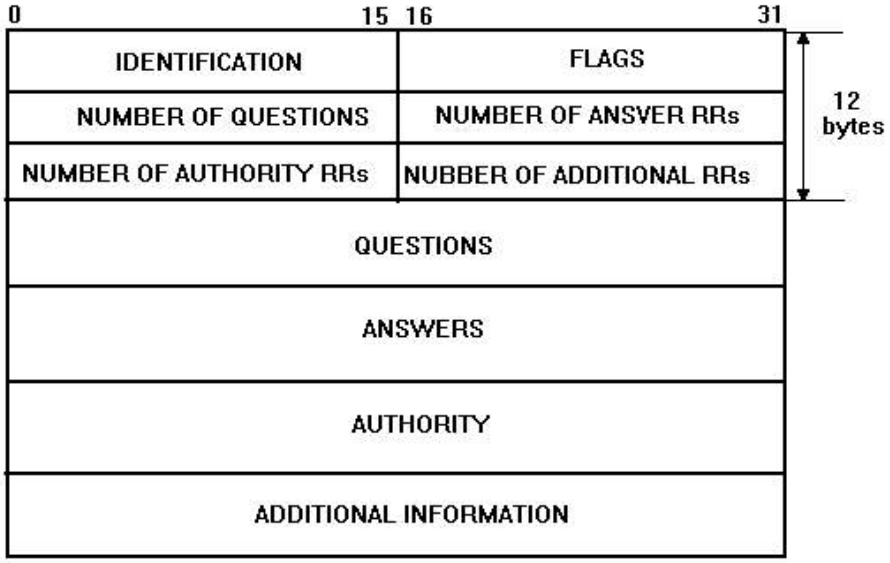
It is very difficult to keep in mind the IP addresses of all the websites we visit daily, because it's not easy to remember strings of numbers. However, we do remember words. This is where domain names come into the picture. If you want to connect to a particular site, you need to know its IP address but do need to know its URL. The DNS gets the mappings of the IP addresses and the corresponding names.

DNS converts the machine names (such as www.xyz.com) to IP addresses (such as 199.249.150.9). Basically, it translates from a name to an address and from an address to a name.

The mapping from the IP address to the machine name is called reverse mapping. When you type http://www.xyz.com into your browser, the browser first needs to get the IP address of www.xyz.com. The machine uses a directory service to look up IP addresses and this service is called DNS. When you type www.xyz.com your machines firsts contacts a DNS server, asking it to find the IP address for www.xyz.com. This DNS server might then contact other DNS servers on the internet. DNS is therefore is considered as the global network of servers. The great advantage of DNS is that no organization is responsible for updating it. It is what is known as distributed database.

DNS message format

There is one DNS message defined for both queries and responses.



The message has a fixed 12-byte header followed by four variable-length fields.

The **IDENTIFICATION** is set by the client and returned by the server.

The 16-bit **FLAGS** consists of:

- 0-th bit field -QR: 0 means the message is a query,1 means it's a response.
- 1-4 bit fields - OPCODE:

  0 -is a normal value (Standard query).

  1 - an inverse query.

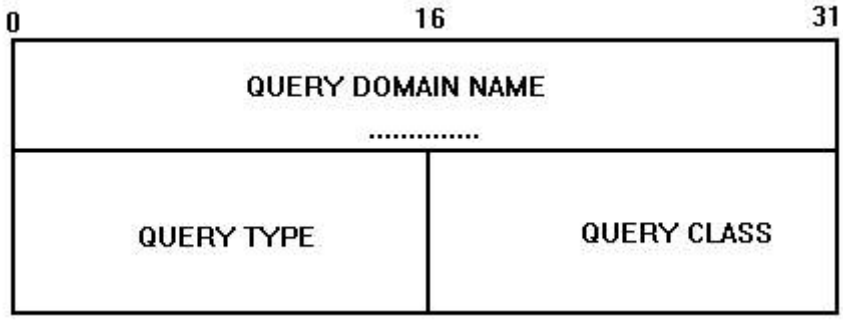
  2 - the server status request.
- 5-th bit field - Authoritative answer. The name server is authoritative for the domain in the question section.
- 6-th bit field is set if message truncated. With UDP this means that the total size of the reply exceeded 512 bytes, and only the first 512 bytes of the reply were returned.
- 7-th bit field - Recursion Desired. This bit can be set in a query and is then returned in the

response.

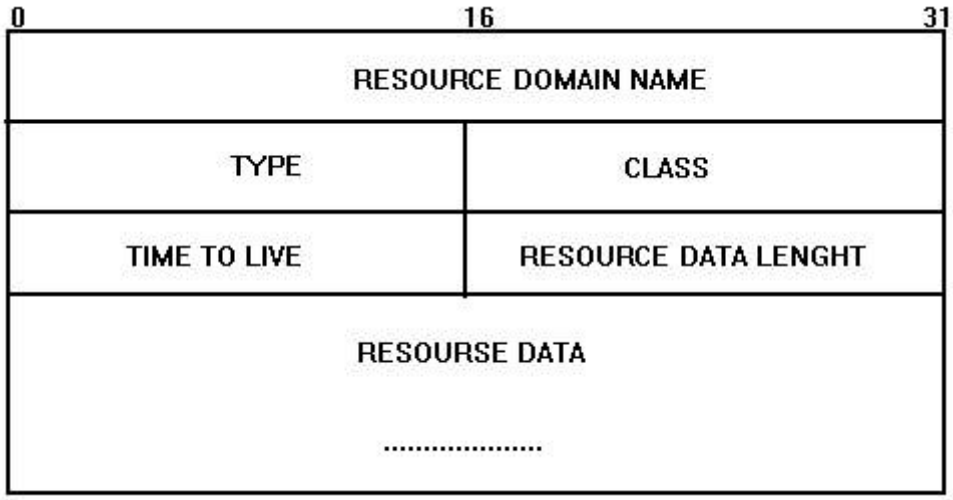
- 8-th bit field - Recursion Available.
- 9-11 -th bits field has to be 0.
- 12-15 -th bits field - Return Code. 0- no error, 3- name error.

The fields labeled **NUMBER OF** ... give each a count of entries in the corresponding sections in the message.

The **QUESTION SECTION** contains queries for which answers are desired. The client fills in only the question section; the server returns the question and answers with its response. Each question has **Query Domain Name** followed by **Query Type** and **Query Class** fields



ANSWER, AUTHORITY, ADDITIONAL INFORMATION sections consist of a set of resource records that describe domain names and mappings. Each resource record describes one name.



The **RESOURCE DOMAIN NAME** contains the destination name, and can be in an arbitrary length. The

TYPE field specifies the type of the data record. The **CLASS** field specifies its class. The **TIME TO LIVE** field contains an integer that specifies the number of seconds information in this resource record can be cached. It is used by clients who have requested a name binding and may want to cache the results. The **RESULTS DATA LENGTH** field specifies the count of octets in the **RESOURCE DATA** field.

Flow chart of sample DNS source