DNS: Records and Messages

Let's now get into what DNS records and messages look like.

WE'LL COVER THE FOLLOWING

- Resource Records
    - Format
    - Types of RRs
- DNS Messages

Resource Records

The DNS distributed database consists of entities called **RR**s, or **Resource Records**.

Format

RRs are 4-tuples with the following entries:

```
(name, value, type, ttl)
```

Every resource record has a `type` and a `TTL` along with a `name-value` pair. The TTL specifies **how long an RR entry can be cached by the client**. The remaining fields are described for each RR type below.

Types of RRs

- **Address**
    - Type `A` addresses are used to map IPv4 addresses to hostnames.
    - `name` is the hostname in question.
    - `value` is the IP address of the hostname.
    - **Example:** `educative.io. 299 IN A 104.20.7.183` where 299 is the TTL, educative.io is the name, `A` is the type, and `104.20.7.183` is the

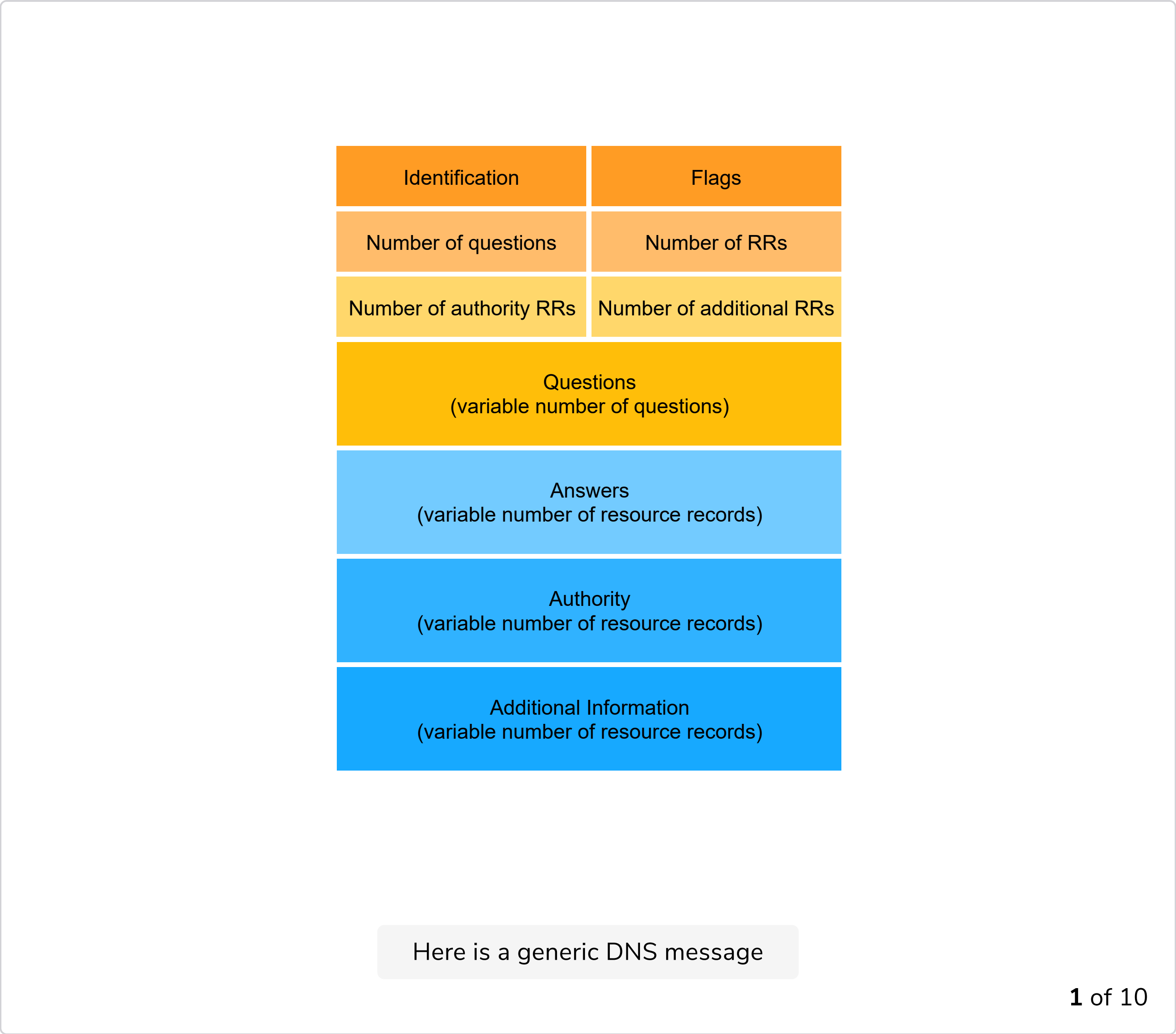
value.

- **Canonical name**
    - Type `CNAME` records are records of alias hostnames against actual hostnames. For example if, `ibm.com` is really `servereast.backup2.com`, then the latter is the canonical name of `ibm.com`.
    - `name` is the alias name for the real or ‘canonical’ name of the server.
    - `value` is the canonical name of the server.
    - **Example:** `bar.example.com. CNAME foo.example.com.`
- **Mail Exchanger**
    - We have seen this one before! Type `MX` records are records of the server that accepts email on behalf of a certain domain.
    - The `name` is the name of the host.
    - `value` is the name of the mail server associated with the host.
    - **Example:** `educative.io mail exchanger = 10 aspmx2.googlemail.com.`

These resource records are stored in text form in special files called **zone files**.

DNS Messages

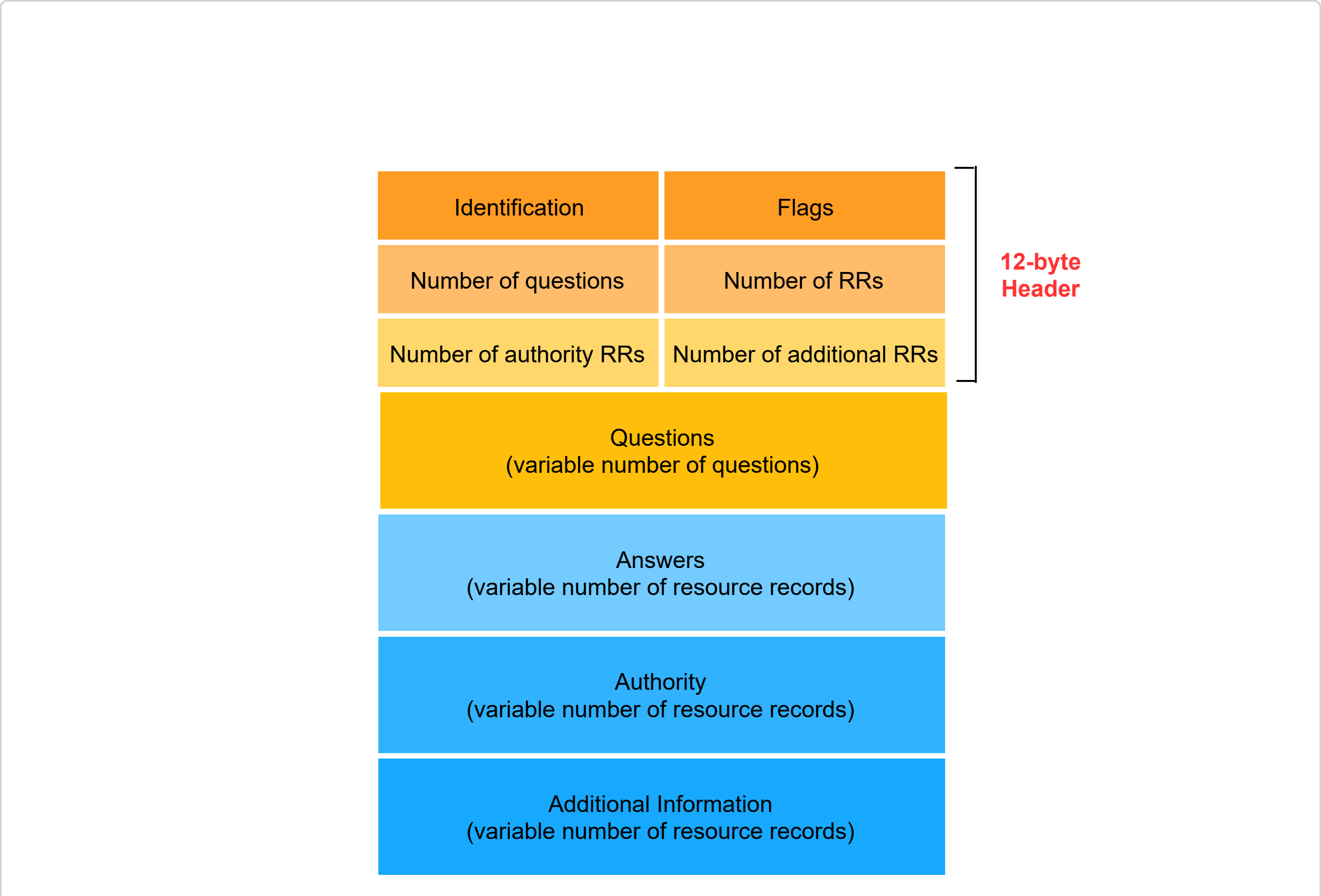
There are a few kinds of DNS messages, out of which the most common are **query** and **reply**, and both have the same format. Study the following slides for a detailed overview of a DNS message.



Identification	Flags
Number of questions	Number of RRs
Number of authority RRs	Number of additional RRs
Questions (variable number of questions)	
Answers (variable number of resource records)	
Authority (variable number of resource records)	
Additional Information (variable number of resource records)	

Here is a generic DNS message

1 of 10

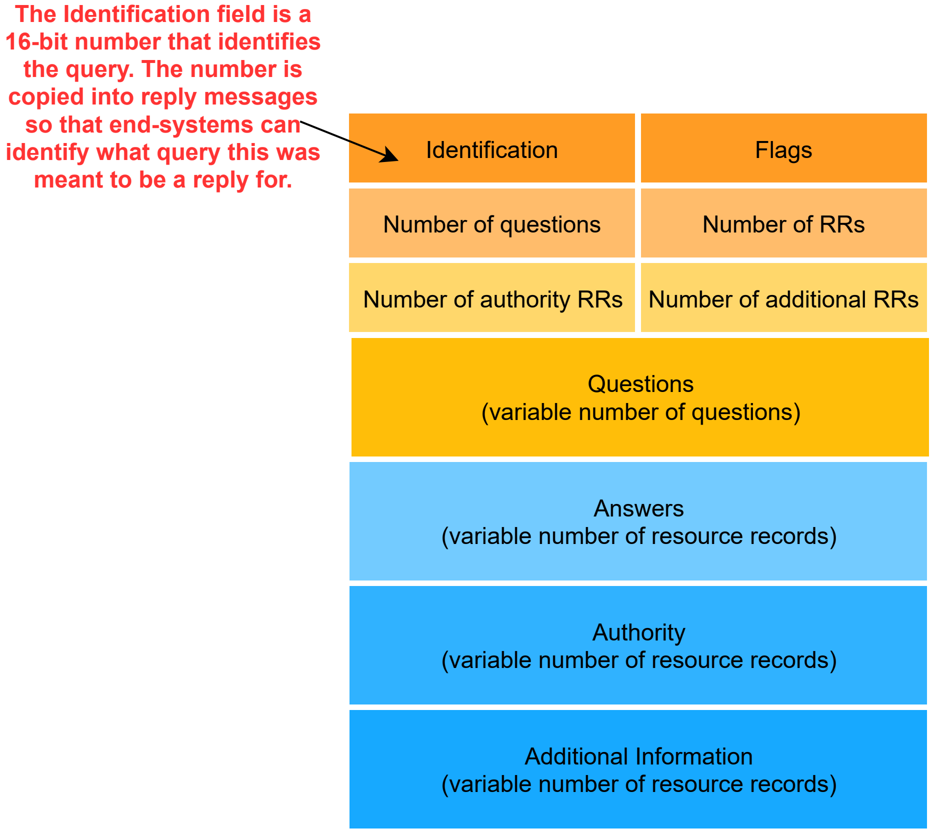


Identification	Flags
Number of questions	Number of RRs
Number of authority RRs	Number of additional RRs
Questions (variable number of questions)	
Answers (variable number of resource records)	
Authority (variable number of resource records)	
Additional Information (variable number of resource records)	

12-byte Header

Let's discuss the header first. It is 12-bytes long and contains a number of fields.

2 of 10



The Identification field is a 16-bit number that identifies the query. The number is copied into reply messages so that end-systems can identify what query this was meant to be a reply for.

Identification	Flags
Number of questions	Number of RRs
Number of authority RRs	Number of additional RRs

Questions
(variable number of questions)

Answers
(variable number of resource records)

Authority
(variable number of resource records)

Additional Information
(variable number of resource records)

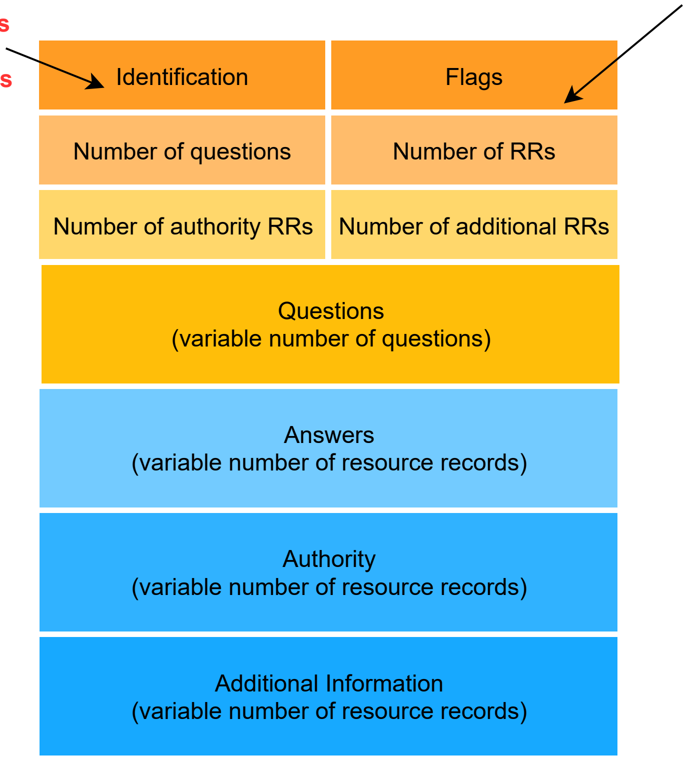
The identification field.

3 of 10

The Identification field is a 16-bit number that identifies the query. The number is copied into reply messages so that end-systems can identify what query this was meant to be a reply for.

The flag field contains a number of 1-bit flags:

- query or reply
- recursion desired
- recursion available
- reply is authoritative



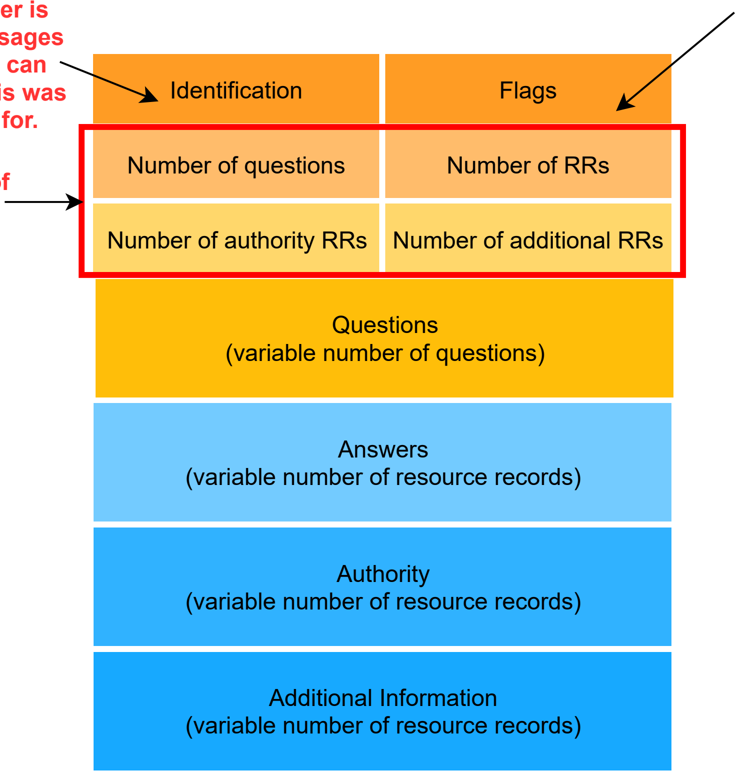
The flags field.

The Identification field is a 16-bit number that identifies the query. The number is copied into reply messages so that end-systems can identify what query this was meant to be a reply for.

The flag field contains a number of 1-bit flags:

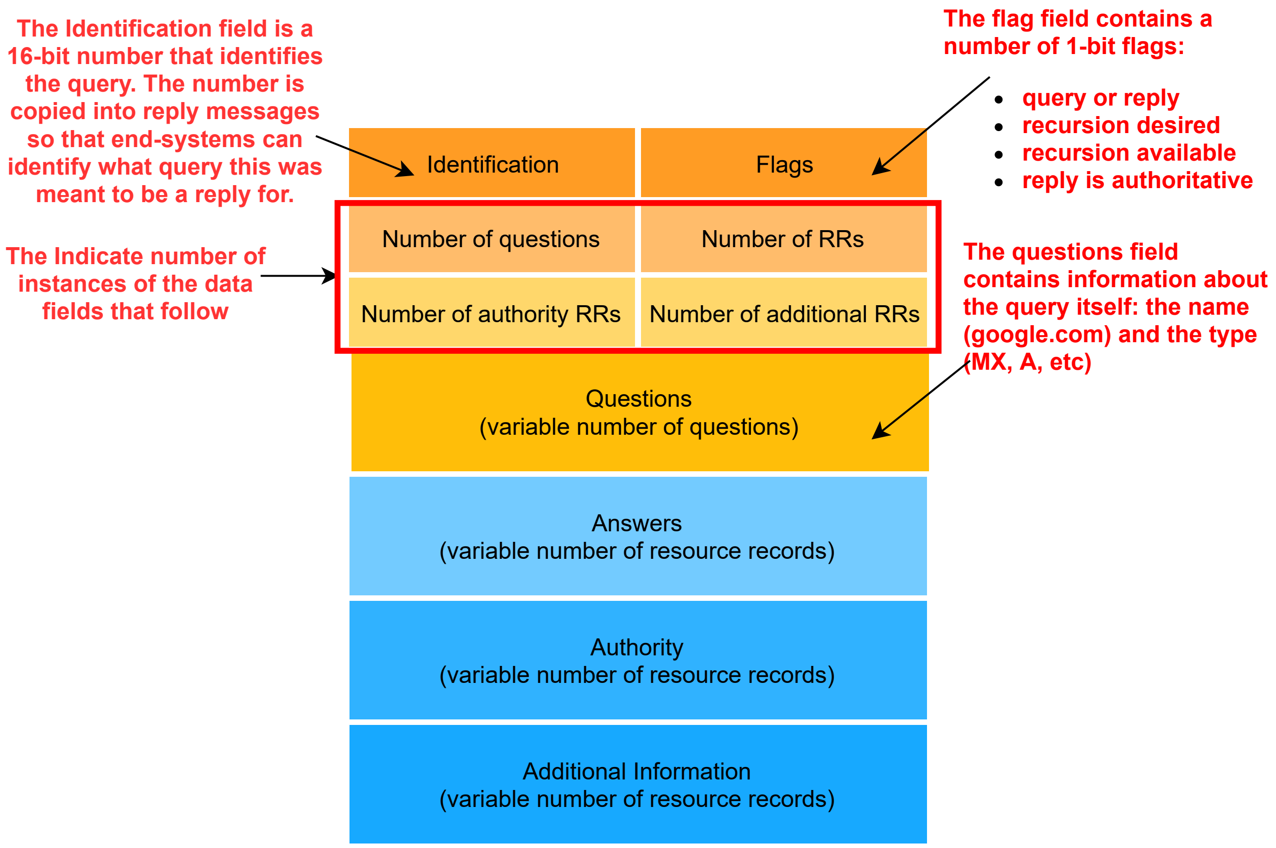
- query or reply
- recursion desired
- recursion available
- reply is authoritative

The Indicate number of instances of the data fields that follow



Number-of fields. These indicate the number of instances of the 4 data sections that follow.

5 of 10



The Identification field is a 16-bit number that identifies the query. The number is copied into reply messages so that end-systems can identify what query this was meant to be a reply for.

The flag field contains a number of 1-bit flags:

- query or reply
- recursion desired
- recursion available
- reply is authoritative

The Indicate number of instances of the data fields that follow

The questions field contains information about the query itself: the name (google.com) and the type (MX, A, etc)

Identification	Flags
Number of questions	Number of RRs
Number of authority RRs	Number of additional RRs

Questions
(variable number of questions)

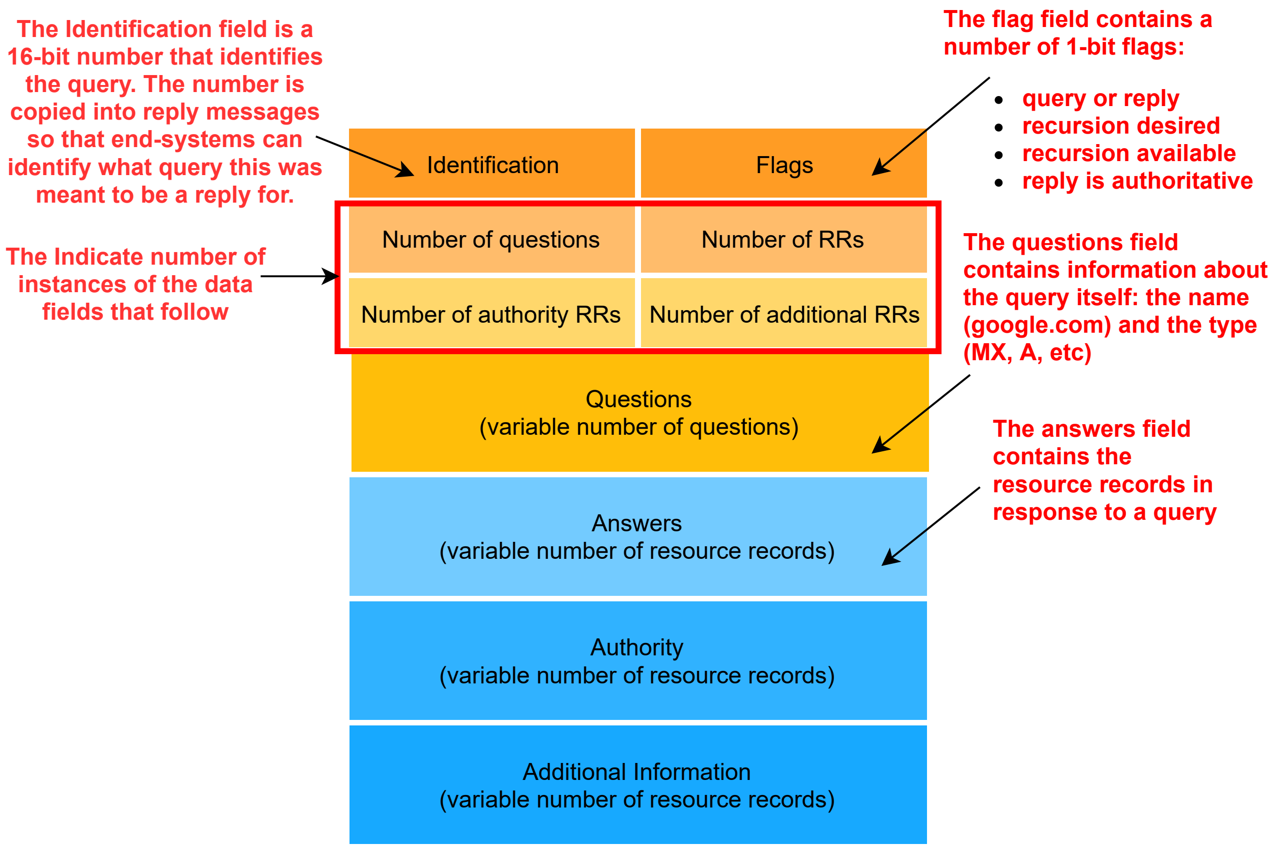
Answers
(variable number of resource records)

Authority
(variable number of resource records)

Additional Information
(variable number of resource records)

The questions field.

6 of 10



The Identification field is a 16-bit number that identifies the query. The number is copied into reply messages so that end-systems can identify what query this was meant to be a reply for.

The Indicate number of instances of the data fields that follow

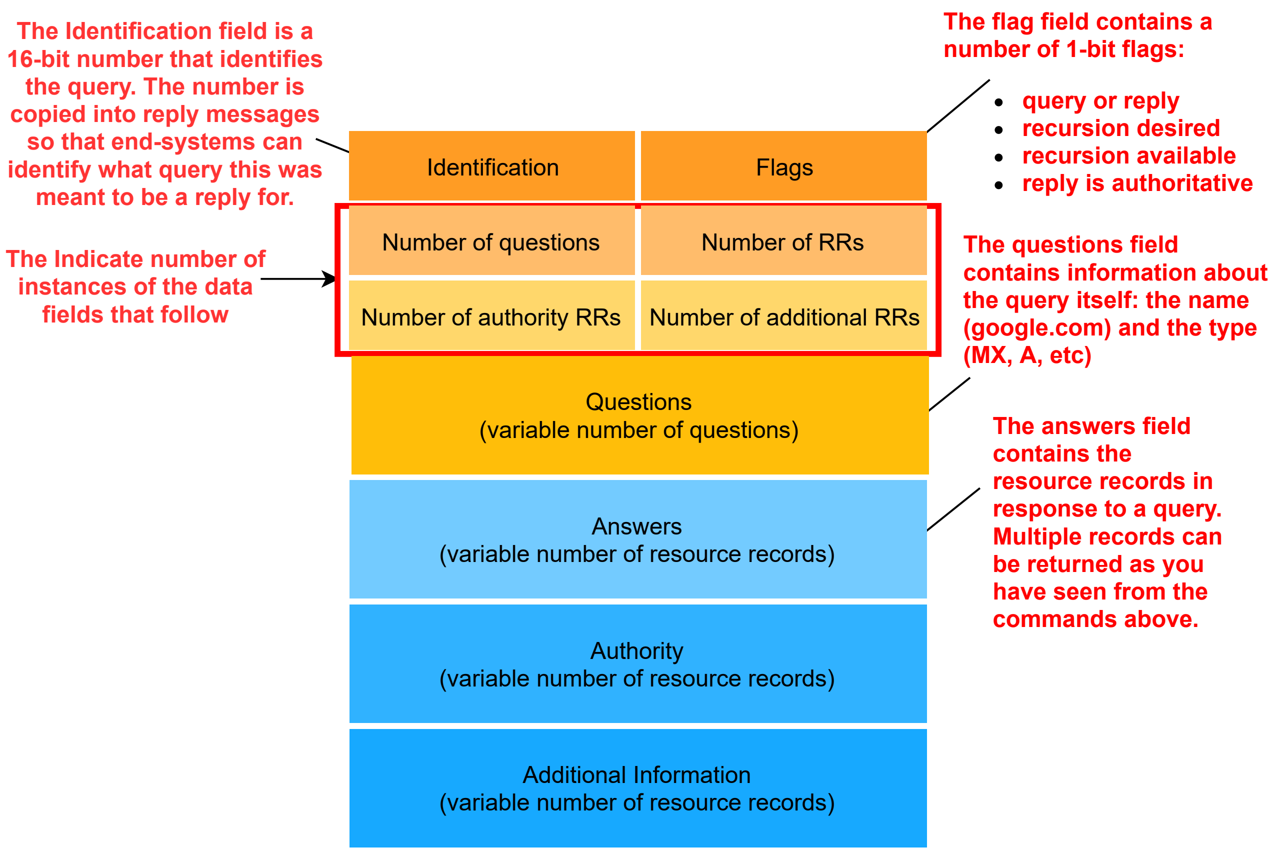
The flag field contains a number of 1-bit flags:

- query or reply
- recursion desired
- recursion available
- reply is authoritative

The questions field contains information about the query itself: the name (google.com) and the type (MX, A, etc)

The answers field contains the resource records in response to a query

The Answers field.



The Identification field is a 16-bit number that identifies the query. The number is copied into reply messages so that end-systems can identify what query this was meant to be a reply for.

The Indicate number of instances of the data fields that follow

The flag field contains a number of 1-bit flags:

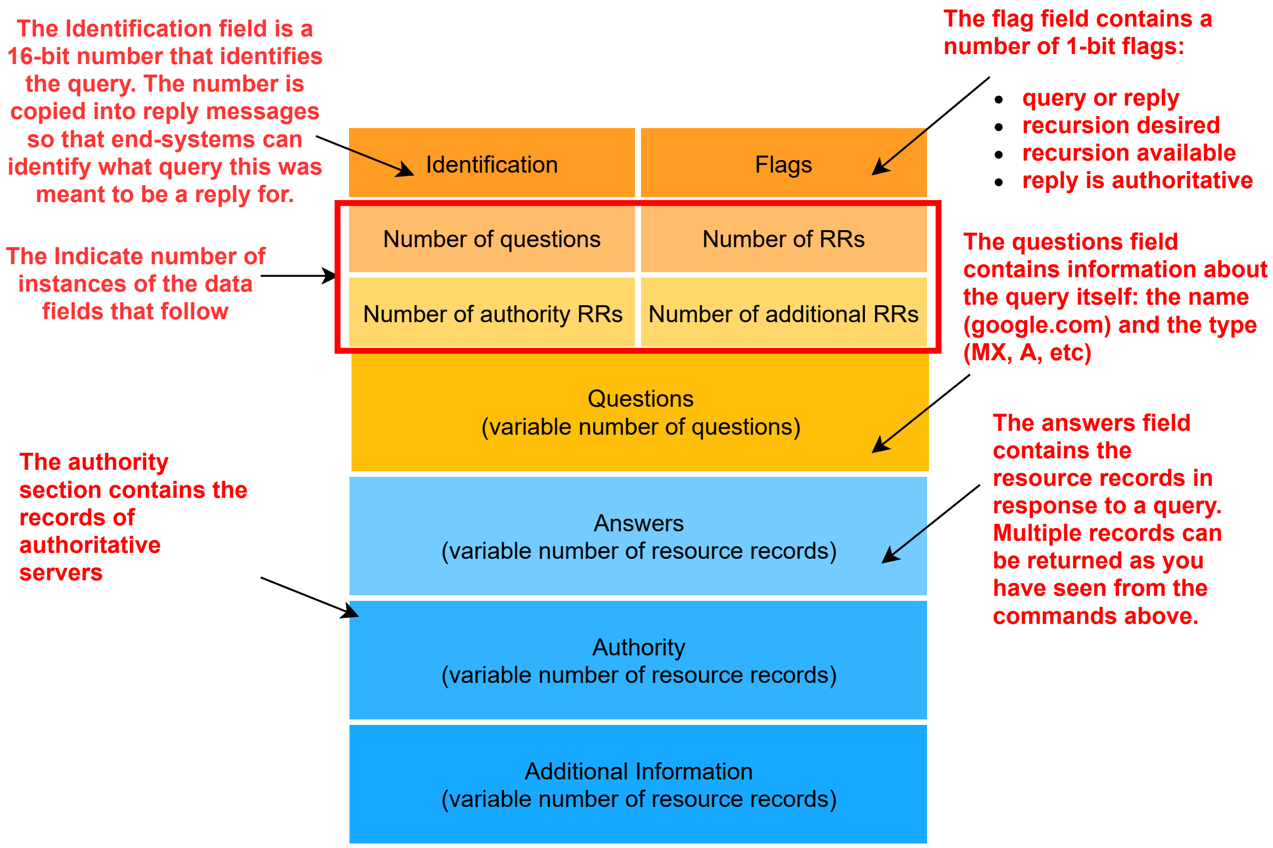
- query or reply
- recursion desired
- recursion available
- reply is authoritative

The questions field contains information about the query itself: the name (google.com) and the type (MX, A, etc)

The answers field contains the resource records in response to a query. Multiple records can be returned as you have seen from the commands above.

The Answers field.

8 of 10



The Identification field is a 16-bit number that identifies the query. The number is copied into reply messages so that end-systems can identify what query this was meant to be a reply for.

The flag field contains a number of 1-bit flags:

- query or reply
- recursion desired
- recursion available
- reply is authoritative

Identification	Flags
Number of questions	Number of RRs
Number of authority RRs	Number of additional RRs

Questions
(variable number of questions)

Answers
(variable number of resource records)

Authority
(variable number of resource records)

Additional Information
(variable number of resource records)

The Indicate number of instances of the data fields that follow

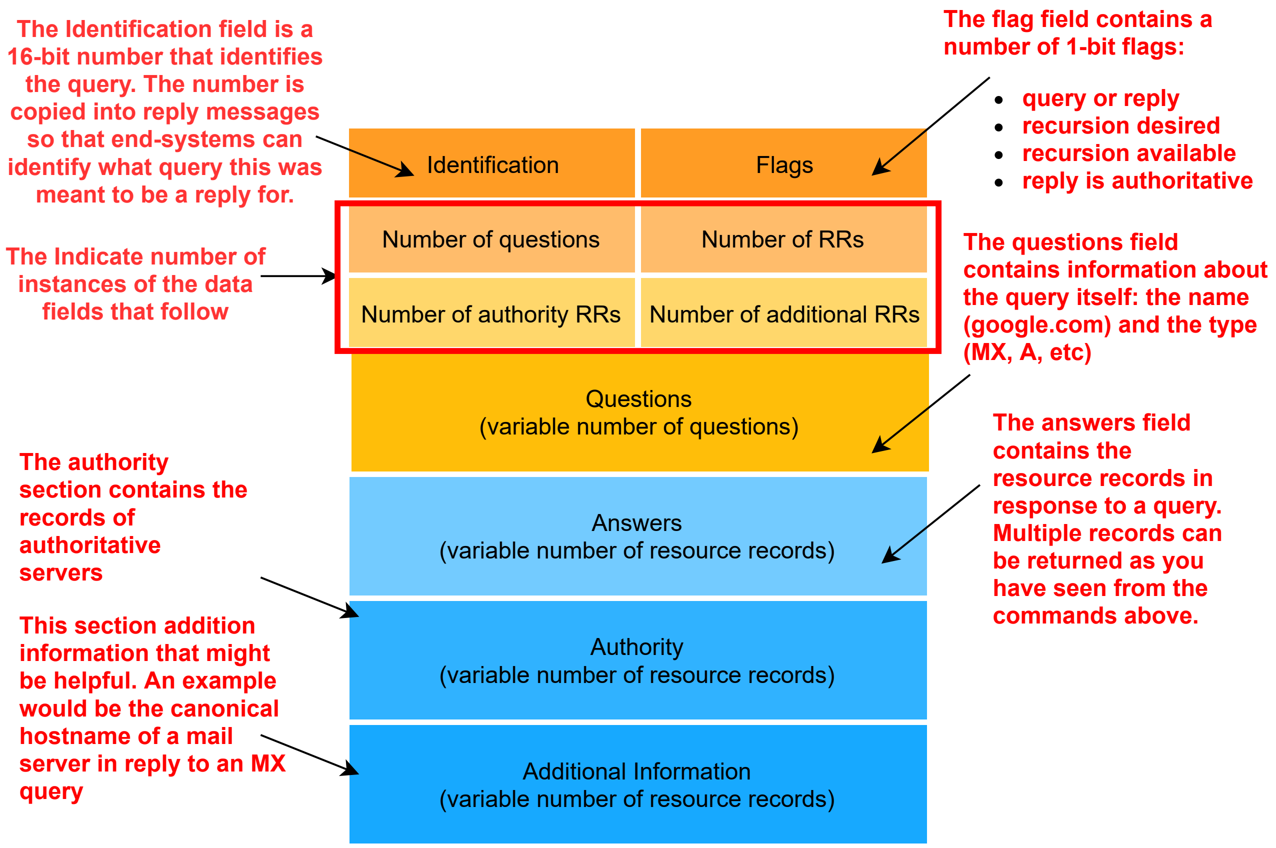
The questions field contains information about the query itself: the name (google.com) and the type (MX, A, etc)

The answers field contains the resource records in response to a query. Multiple records can be returned as you have seen from the commands above.

The authority section contains the records of authoritative servers

The Authority field.

9 of 10



Identification

Flags

Number of questions

Number of RRs

Number of authority RRs

Number of additional RRs

Questions
(variable number of questions)

Answers
(variable number of resource records)

Authority
(variable number of resource records)

Additional Information
(variable number of resource records)

The Identification field is a 16-bit number that identifies the query. The number is copied into reply messages so that end-systems can identify what query this was meant to be a reply for.

The flag field contains a number of 1-bit flags:

- query or reply
- recursion desired
- recursion available
- reply is authoritative

The Indicate number of instances of the data fields that follow

The questions field contains information about the query itself: the name (google.com) and the type (MX, A, etc)

The answers field contains the resource records in response to a query. Multiple records can be returned as you have seen from the commands above.

The authority section contains the records of authoritative servers

This section addition information that might be helpful. An example would be the canonical hostname of a mail server in reply to an MX query

The Additional Information field.

10 of 10

There are also **zone transfer request and response**. But, those are not used by common clients. Backup or secondary DNS servers use them for **zone transfers**, which are when zone files are copied from one server to another. This takes place over TCP.

1

Which of the following are valid DNS record entry types?

In the next lesson, we’ll use command-line tools to look at DNS response messages and resource records!