How the Domain Name System (DNS) works

The difference between Content and Resolving DNS services

From our experience, people expect DNS servers to provide a single service: to convert names such as `www.bytemark.co.uk` to IP addresses such as `80.68.80.52`. Although many DNS servers around the internet operate in this simplistic manner, this view is not a thorough understanding of the system, and may result in security issues if a systems administrator new to DNS tries to set up a server in this fashion. DNS servers should provide one of two services: *content* or *resolution* services.

Content servers

A *content server* is one which actually contains authoritative DNS records. These records are just single pieces of information such as:

- the name `www.bytemark.co.uk` refers to IP address `80.68.88.52`
- the domain `bytemark.co.uk` should have its mail delivered to address `80.68.80.228`
- the IP address `80.68.81.18` has the name `abc.bytemark.co.uk`

These records are “authoritative” because the person who owns the server claims that they are correct in the global naming system, and is asserting that a content DNS service provide these answers to anybody who asks for them. Content servers are usually authoritative for a fixed set of domains, owned or administered by the person who has set the server up.

If a content server does not itself know the answer to a particular DNS query, it may know that the domain has been delegated to another server, and so may answer with a referral instead. A referral is a hint to the client making the request that it will find the answer from another content server.

Resolving servers

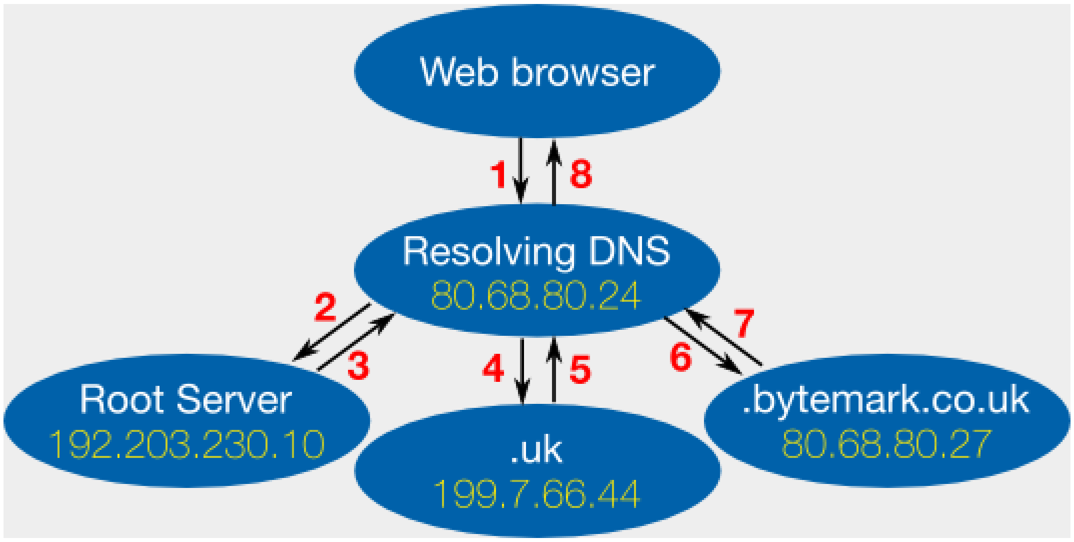
A resolving server’s job is not to return any authoritative information directly. Its job is to search for information on behalf of clients, and to return it. A resolving server usually remembers past queries so that if a lot of people ask for the same information, it can return it quickly without having to search for it twice. Hence a resolving server is sometimes known as a ‘DNS cache’ or ‘caching DNS resolver’. Most organisations providing internet access to a group of people maintain their own resolving server or servers. They are necessary part of the internet infrastructure because:

- Most DNS information does not change most of the time. Hence it makes sense for an organisation to set up their own server which will be able to more quickly return DNS information that is commonly requested by that particular organisation.

- Resolving a DNS query from scratch can be a complicated procedure, and most internet software (e.g., email clients, web browsers) does not need to know how to do it. A commonly-used server to do the job means internet applications need only have to deal with issuing a single question and receiving a single answer.

How a DNS query is resolved

Below we explain what happens when you type `www.bytemark.co.uk` into your computer's web browser.



1. Your web browser asks the resolving DNS server what the address of `www.bytemark.co.uk` is. Your computer already knows where the **local** resolving DNS server is through its network configuration. For customers on the Bytemark network, the resolving DNS servers are `80.68.80.24` and `80.68.80.25`. On a linux machine these addresses are listed in `/etc/resolv.conf`.
2. The Resolving DNS server does not know the address. So it asks a root server the same question. The 13 root servers have globally well-known IP addresses, and are run by a US-based company called ICANN
3. The root server replies that it does not know, but it gives the address of the server which knows about `.uk` domains. All UK domains are managed by a non-profit organisation called Nominet
4. The resolving DNS server asks the `.uk` server what the address of `www.bytemark.co.uk` is.
5. The `.uk` server replies that it does not know, but it gives the address of the server which knows about `.bytemark.co.uk` domain. This server is (finally!) at an IP address which we manage, on one of our servers. We pay Nominet an annual fee (via a domain registrar) to maintain this referral for our domain, and for them to maintain the address as belonging to us.
6. The resolving DNS server asks the `.bytemark.co.uk` server what the address of `www.bytemark.co.uk` is.

7. Our server answers the query with the IP address of `www.bytemark-hosting.co.uk`, and marks the response as “authoritative”. This is an assertion that the answer is correct and complete. It also adds to its reply that “this data is valid for 24 hours”, so that anyone who is asking can confidently re-use the information for that time without having to issue another query.
8. The resolving DNS server finally has its answer, and can reply back to the web browser with the IP address. Crucially it marks its answer as “non-authoritative”, so that the web browser knows it has the information indirectly.

Multiple answers to DNS queries

Our example above makes a simplification: it pretends that DNS queries only ever have one answer. In fact, certain queries usually return more than one answer. For instance if you ask what the address of `www.yahoo.com` is, you’ll (at the time of writing) get 13 different IPs supplied in the response. Each IP will still respond with Yahoo’s home page, so that if one of them falls over, the others will still keep Yahoo’s front page visible.

In the example, if you ask which server is responsible for the `.uk` domain, you will get five different IPs supplied in response. All of them should serve the same data; it is very important that machine which server content DNS data for “top-level” domains are always available.

While you can perform the same trick for your own web or mail services if you need resilience, you will be forced to supply more than one DNS server when you ask your registrar to re-delegate your domain. That is to say, it is a condition of owning a domain that you must have two separate IPs which will answer authoritatively for it.