IP Address Classes

IP addresses are generally classified by the ratio of network part to local part.

Class A

0	Network Part	Local Part
0	1	8 32

For Large Networks

126 networks (7 bits)
16, 777, 214 hosts for each network (24 bits)

IP addresses 1.n.n.n to 126.n.n.n

Class B

10	Network Part	Local Part
0	2	16 32

For Medium sized Networks

16,384 networks (14 bits)
65,532 hosts for each network (16 bits)

IP addresses 128.0.n.n to 191.255.n.n

Note: UCC falls into this category, e.g. the computer bureau Vax is 143.239.1.2

Class C

110	Network Part	Local Part
0	3	24 32

For Small Networks

2,097,152 Networks (21 bits)
254 hosts for each network (8 bits)

IP addresses 192.0.0.n to 223.255.255.n

Class D

1110	Multicast Address
0	4 32

Reserved for Multicasting (sending to several machines at the same time)

IP addresses 224.n.n.n to 239.n.n.n

Class E

11110	Reserved
0	5 32

Reserved for future use

IP addresses 240.0.0.0 to 247.255.255.255

Domain Name Service (DNS)

The Domain Name System is outlined in two RFC's (Numbers 1034 and 1035)

It is made up of 3 main components:

1) Resolvers

2) Name Servers

3) Resource Records

1) Resolvers

These are special programs or system calls which extract information from name servers in response to client requests. A Domain Name is usually sent to the resolver which returns the corresponding IP Address.

A resolver can be a system routine directly accessible to the user.

e.g. (in Unix)

```
nslookup pharos.ucc.ie
```

would return the IP address of pharos.ucc.ie (i.e. 143.239.1.159)

In order to return the IP address the resolver sends a request to a name server.

2) Name Servers

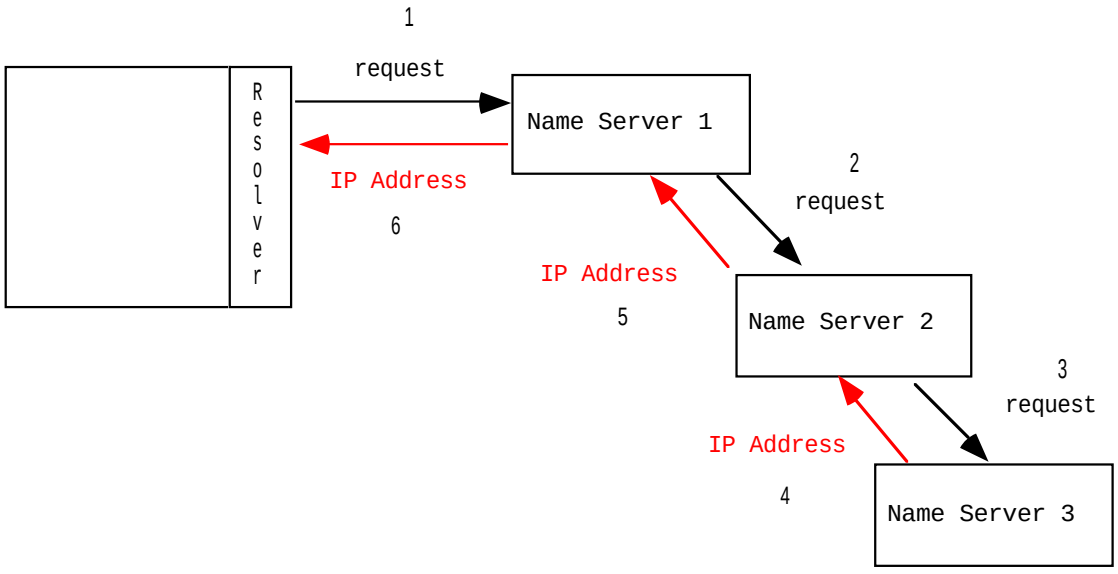
These are servers which store information about Domain Names. They contain lists of Domain Names along with information about them. This information includes the IP address of the Domain Name and is stored in *Resource Records*. Requests are made of name servers from either resolvers or other name servers.

On receiving a request about a particular Domain Name a server can return information about that Domain Name or, in cases where the server has no information about the Domain Name, arrange to get that information from another name server which is more likely to have it. A typical lookup will probably involve several servers in this way.

If a name server doesn't have the IP address of a Domain Name it will have the IP address of a server that will (or which will have the IP address of another server which is more likely to have it, and so on). A lookup request will then be sent to this server.

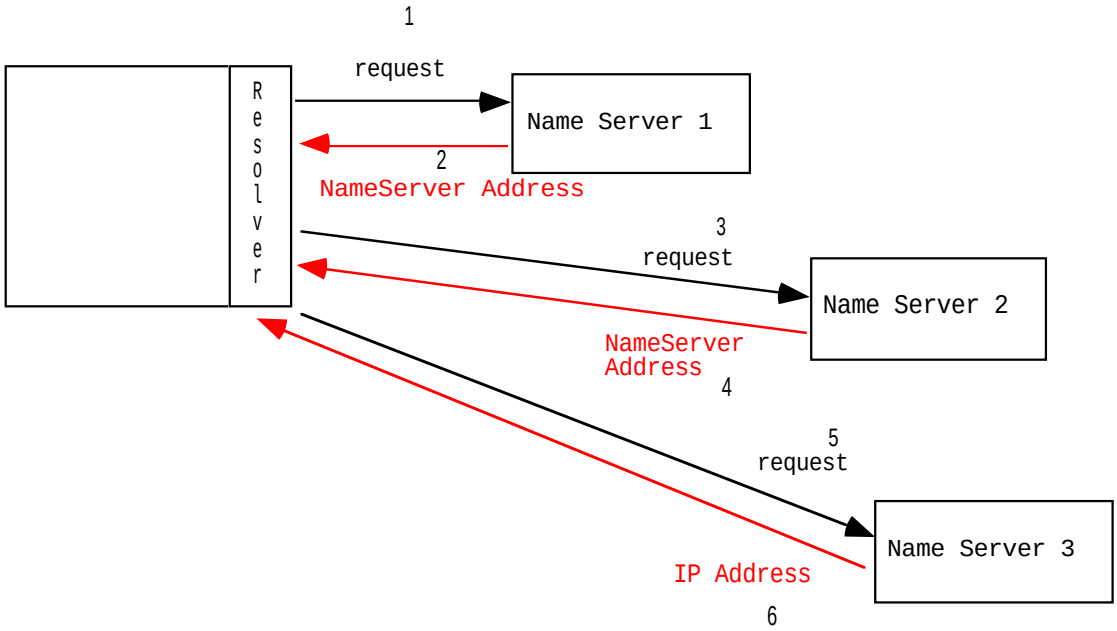
Domain Name lookups can be recursive or iterative.

Recursive



The resolver sends a request to a name server. If the name server does not have the IP address it finds the IP address of a Name server which is more likely to have it. The original name server then makes a Domain Name request of this new name server. The new name server either has the required IP address or the IP address of another name server which might. This process repeats until the IP address is found and it is returned to the name server which made the request of the name server containing the IP address, which in turn returns the IP address to the name server which made the request of it, and so on. This repeats until the IP address is returned to the resolver. This is the preferred scheme since the resolver and any of the name servers involved can keep local copies of commonly requested IP addresses (i.e. it can *cache* them).

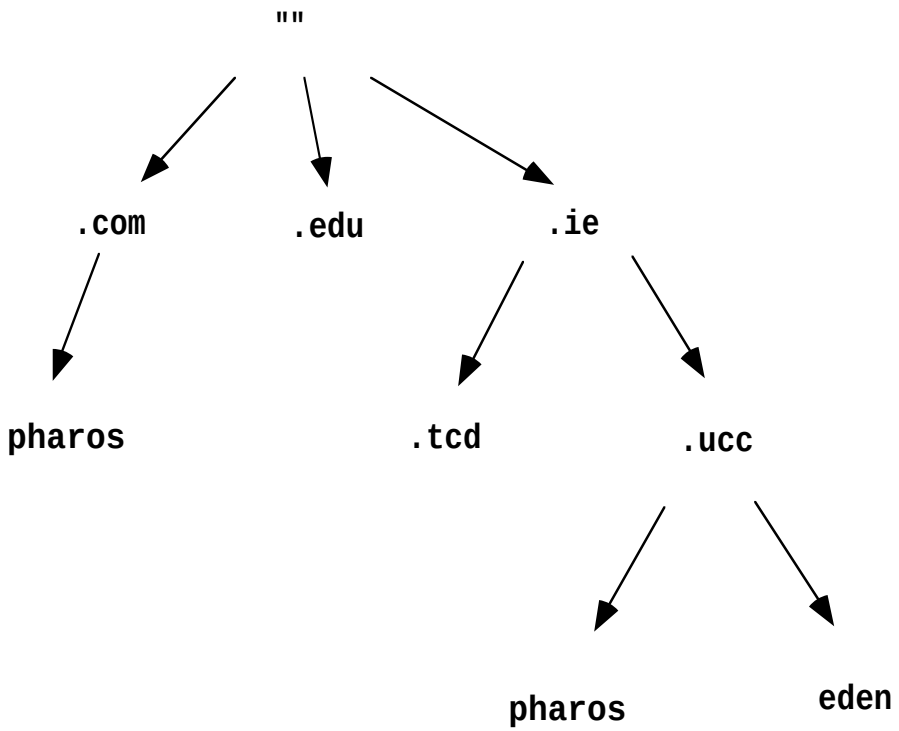
Iterative



In this case the resolver sends a request to a name server. If the name server does not have the IP address it finds the IP address of a Name server which is more likely to have it. This IP address (of the new name server) is returned to the resolver which uses it to do another Domain Name lookup. This process repeats until the IP address required is found.

3) Resource Records

Resource Records contain the data about domain names. Each record is a leaf or node on a tree representing the domain name space.



Resource Records are kept for each node and can contain

address of name server
Host Address
OS/CPU of host
Mail Exchange
Authoritative Name Server
Start of Zone of Authority (ZOA)
Time to Live (TTL)

Authoritative Data

Domain Names stored in the name server which serve their ZOA are considered Authoritative. Name servers see the Domain System in terms of zones (of authority) and each server supports part of the domain tree. Each zone is supported by at least two name servers (i.e. there would be a backup server). In some cases a server can keep local copies of the records of another zone. These records, being only copies and not necessarily up-to-date, are considered non-authoritative. These records may have a TTL (time to live) attribute which would indicate how long these records could be considered accurate.

Canonical Names

Some Domain Names are aliases for other Domain Names, the Domain Names which are mapped to an IP Address (and not another Domain
Name) are considered Canonical.

E.g., we wish to present a virtual machine called cs607.ucc.ie. There is no cs607 machine, instead we direct mail to one address, and every other type of request to another. We can also simulate a web server www.cs607.ucc.ie which would just point to whichever machine cs607 referred to.

A local name server could have the following resource records:

host name	**type of record**	**returned address**	**note**

www.cs607	CNAME	cs607	here we direct requests for www.cs607.ucc.ie to be redirected to cs607.ucc.ie. (its canonical name - CNAME)
cs607	A	143.239.1.159	requests for cs607 return this IP address
cs607	MX	43.239.1.145	Any mail requests for cs607 are sent to another IP address

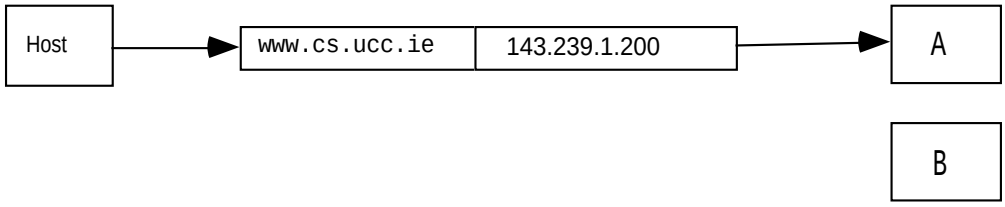
Advantages of Domain Names

1) They are easier to remember than IP addresses

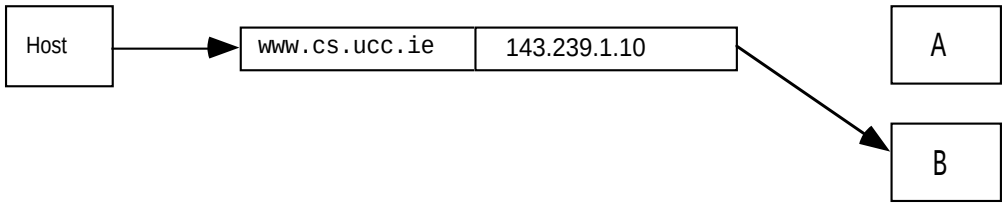
2) You can change the IP address without changing the Domain Name. This allows you to change the physical machine you use without having to alert everyone to the change since the Domain Name remains the same.

Consider the example below. The IP address in the Resource Record is changed to point to a new machine. However, the host is unaware since it only makes requests of the domain name.

Before the change:



After the change:



3) A domain can span many different physical networks.

e.g.
```
host1.exampledomain.ie A    143.239.1.2
host2.exampledomain.ie A    198.34.23.5
```

Both hosts in the example above are in the *exampledomain.ie* domain but are on entirely different physical networks.