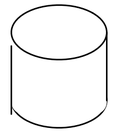
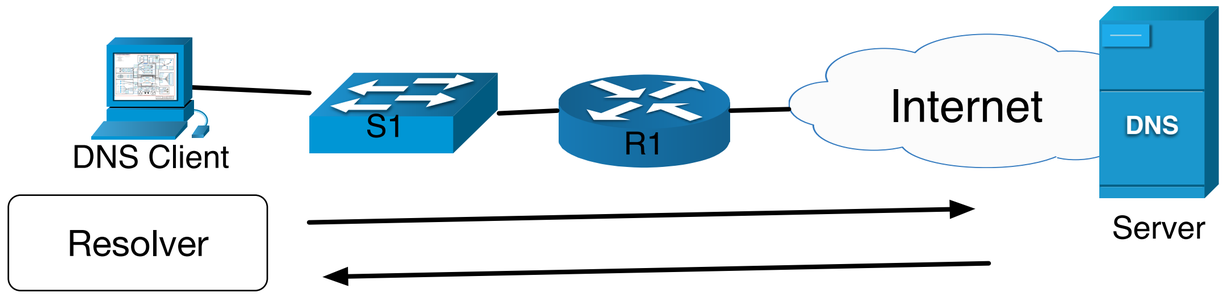
DNS (Domain Name System)

Translates computer names to IPs (resolution)
It is a distributed database



DNS clients run a resolver
(a resolver is an application built into the computers Operating System used to make DNS queries)



Forward lookup = hostname to IP

Reverse lookup = IP to hostname

Domain Name Space

The Naming Scheme is organised into a tree like hierarchy

FQDN (Fully Qualified Domain Name) will give the exact location within the tree structure

Each level is separated by a dot **.**

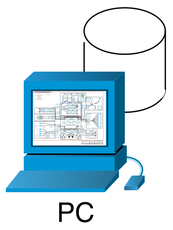
host1.test.mysite.com.

Name	Type
.	Root Domain - top of the tree (typing this is optional)
.com	Top Level - type of organisation or geographical location (.govt, .co.uk)
.mysite	Second Level Domains - usually registered to an organisation
test	Subdomains - areas within an organisation (e.g. north or south)
host1	Host

Domain Name Resolution

Let's say that this PC needs to access server1.mycompany.local

First the PC checks its ***hosts file*** (just a text file) - this is a manual specification of IP to Host mappings. This is read *before* DNS



Then it checks its ***Resolver Cache***. If it has been accessed recently it will be in here.

If it still cant find it, a Forward lookup is sent to the local DNS Server

If the required address is within the local network, the local DNS server will send the IP back (with a TTL telling host how long to cache the record before aging it out).

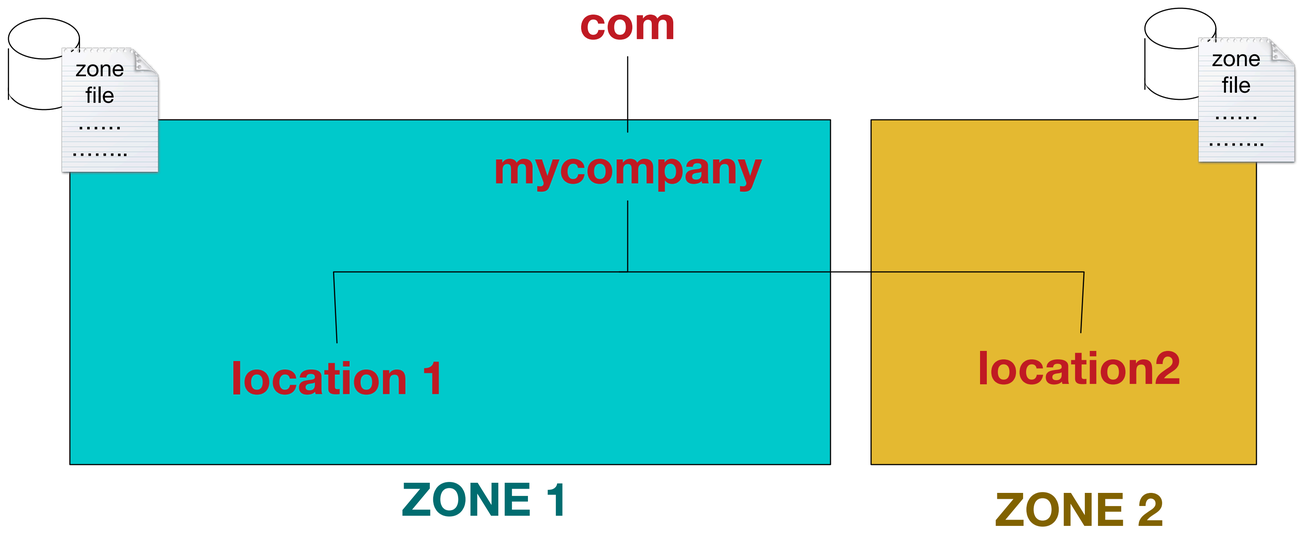
If however it is an external resource (e.g. www.theircompany.com) the following process is followed…

Zones

Zones divide a namespace into portions for easy management

You can have more than one DNS server per zone.They can back each other up.

One DNS server can look after more than one zone.



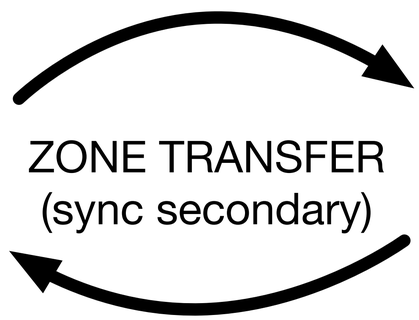
A DNS server holds the ZONE DATABASE FILE

And the ZONE DATABASE FILE holds the ZONE RECORDS (the actual mappings)

In the above diagram you can have a situation where one administrator manages zone 1 and another manages zone 2

Master copy (primary zone database file) stored on this server. Records are updated here (i.e. addition, removal and so on)

PRIMARY/MASTER DNS SERVER



SECONDARY/SLAVE DNS SERVER
(maintains copy of primary zone database file)

To prevent security problems you should control what secondary DNS servers can obtain zone file updates

Zones Records

(this list is by no means exhaustive but gives a good overview)

Record Type	Purpose
SOA (Start of Authority)	First record in DNS zone file. Specifics the authoritative server (the Master Nameserver for the domain)…. e.g. server1.mycompany.local
NS (Name Server)	Specifies the domains name server(s) - could be same as above
A (Host)	Map a hostname to IPv4 address.
CNAME (canonical name)	Create an alias, or an alternative name for an existing host (www is common). A web service mapping is usually found on an external server. When creating, specify CNAME and FQDN of A record.
MX (Mail Exchanger)	Specify which server mail is to be delivered to (again, normal found externally)
PTR (pointer)	This is an entry in the reverse lookup zone (IP to domain)

Useful tools

nslookup <IP/HOSTNAME> <DNS_SERVER>

When using nslookup, you can move into interactive made by leaving out all arguments

ifconfig /displaydns - show revolver cache

ifconfig /flushdns - clear resolver cache

ipconfig /registerdns - renews the clients registration to the DNS server.

The dig command can be used to find out DNS record types. For example use ***dig example.com MX @ns0.resolver1.com*** to find MX records.