DNS Zones and Zone Files Explained

steves-internet-guide.com/dns-zones-explained

DNS is comprised **logically of Domains** but **physically of zones.**

A domain is a logical division of the **DNS name space** whereas a **zone** is physical, as the information is stored in a file called a **zone file**.

In most cases you have a 1 to 1 relationship between a Domain and a DNS Zone i.e. the domain mydomain.com would be stored in a **zone file** called mydomain.com.txt.

This tutorial is for beginners and you will learn:

- What a DNS Zone Is.
- What a Zone File is
- How DNS Zones relate to Domains
- Different Zone Types
- How Zone transfer works

To Explain what zones and zone files and how they work are we are going to start with a simple analogy.

If you imagine that you (Bill) have organized a football league that has three teams.

Teams A,B,C and each team has 20 players in the squad.

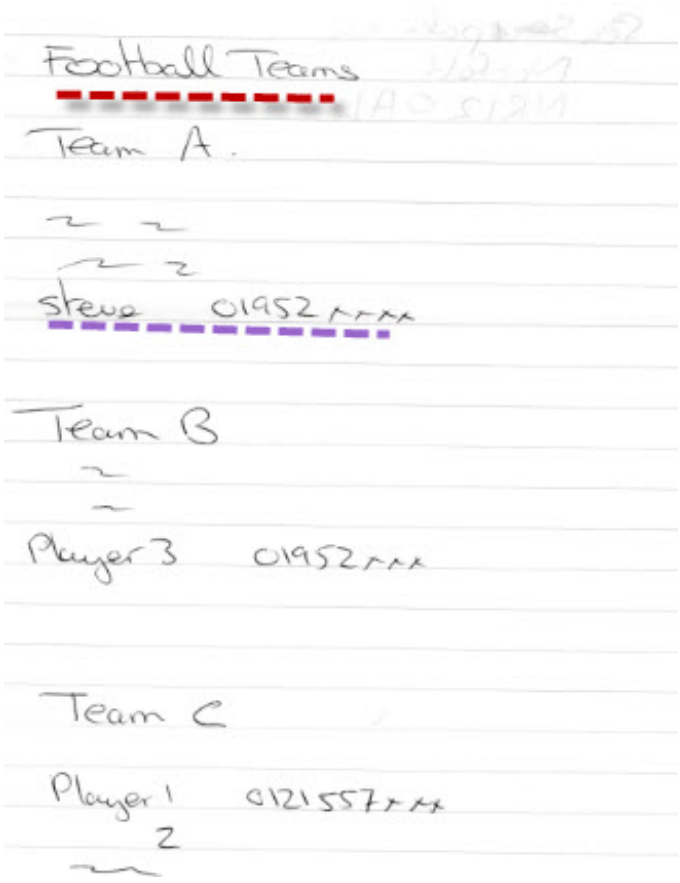
What you need is for anyone to be able to contact any player on any of the teams.

So you could create a paper list and write the names and phone numbers on it. (This was effectively the hosts file approach.

This works but gets to be a problem if the league expands and you get,for example, 10 teams.

So an alternative is to create **three lists** one for teamA , one for teamB and one for teamC.

If another team gets added then you create another paper list for teamD.



So now you have three lists but who manages the lists?
Well each team has a manager so you let the manager handle the list for the team. So

- John manages teamA
- Fred manages teamB
- Jane manages teamC

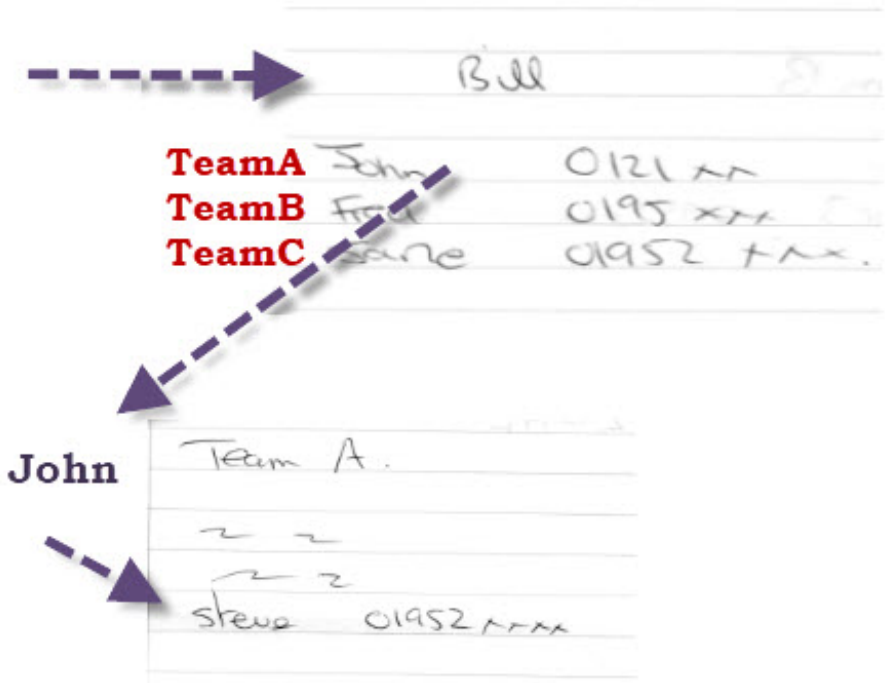
Now the league organiser Bill wants the phone number of Steve who plays for TeamA. How does he get it?

Well he first needs to know who has the player list for TeamA.

So **Bill** needs a list with the **name and phone numbers** of all the managers..

The manager's name isn't really important just the phone number.

So if someone wants to find the phone number of Steve on team A they contact Bill who contacts the manager of Team A (John) using the phone number returned by Bill and John tells them. As shown in the diagram below:



DNS Lookup Illustration

If you compare this to IP addresses and Domain names

- Steve = A web server, for example
- Phone number = the IP address
- TeamA = a Domain Name
- Bill,John,Fred,Jane are **name servers**.
- The lists are **zones or zone files**

Notice Bill doesn't have a list of players but managers i.e it doesn't contain host names (A records) but Manager names (name server records **NS records**).

Also Bill needs to know who has the team list for all of the teams below him, but John only needs to know the phone number for the Top of the Tree, which in this case is Bill as we have only two levels, but it doesn't have to be.

i.e you traverse the tree from top to bottom and not from bottom to top. See Understanding DNS lookups

Primary and Secondary Zones and **Zone Transfer**

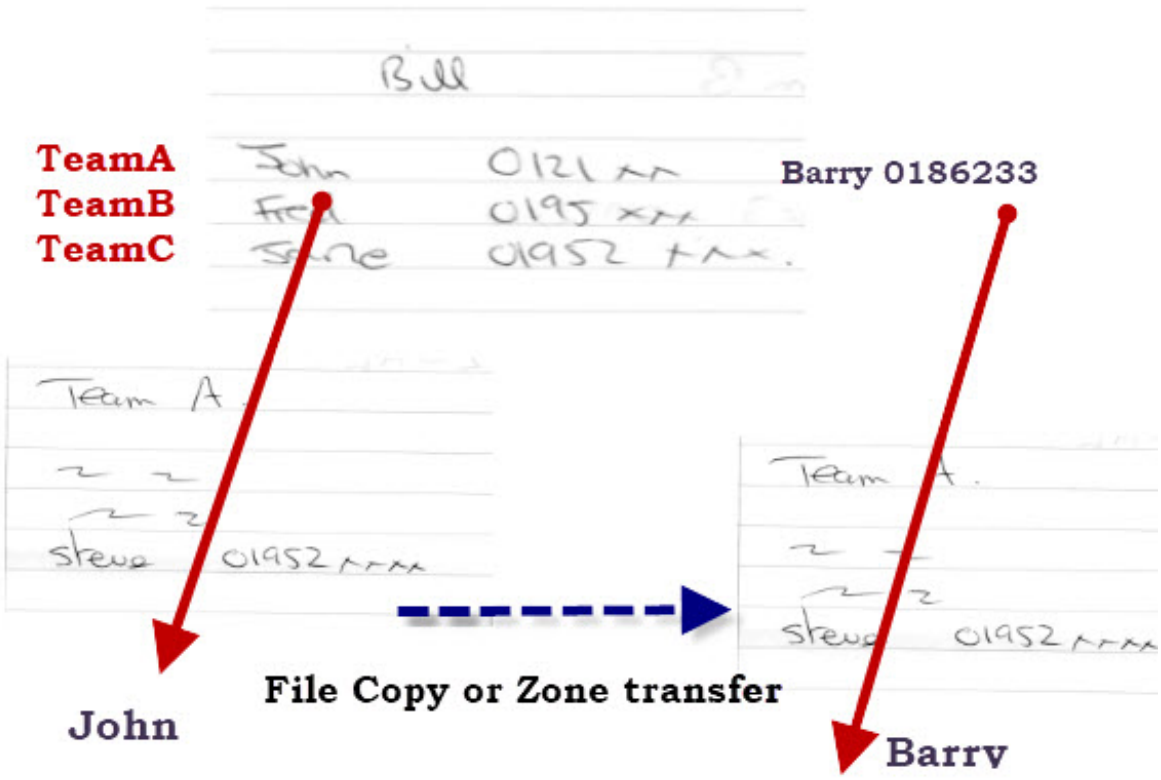
What happens when a Manager goes on holiday?

Well all they need to do is to **photocopy their list** and give it to someone else (Barry for example), and tell Bill the Contact number of the person so Bill can update his list.

Notice: In DNS there are always two name servers for resilience.

In the Diagram below I have modified Bills list to include Barry.

We also need to add a note in Johns list to include Barry as he needs to send him the list and list updates.



Secondary Zones Illustration

A zone can be either a **primary** or **secondary zone**.

Note: Primary zones are now called **master zones** and **secondary zones** are now called **slave zones**.

The primary zone is the master record, and it is the one that gets changed by the administrator.

To keep things simple only john can update the list. He has the **master copy (primary zone).**

When he changes the list he neds to send a copy to Barry who has a copy (**secondary zones** or **slave zones**).

On DNS these changes are copied to the **secondary zones** in a process called **zone transfer**.

Zone transfer is normally from **primary to secondary,** but it is requested by the DNS server responsible for the **secondary zone**.

In our illustration Barry would request an updates list from John.

However the primary servers can be configured to **notify** secondary servers of changes.

At it's most basic a **zone transfer** is simply a file copy.

A DNS server hosting a primary zone is normally called a **primary name server**(master) ,and one hosting a secondary zone is a **secondary name server** (slave).

A **DNS server** can store and manage **multiple zone files**, and they can be a mixture of primary and secondary zones.

In out analogy John could have a copy of TeamB list in case Fred goes on holiday.

Therefore a DNS server can be both a primary and secondary name server.

Primary and secondary name servers are both considered as **authoritative** for a domain.

DNS Zones and Domains

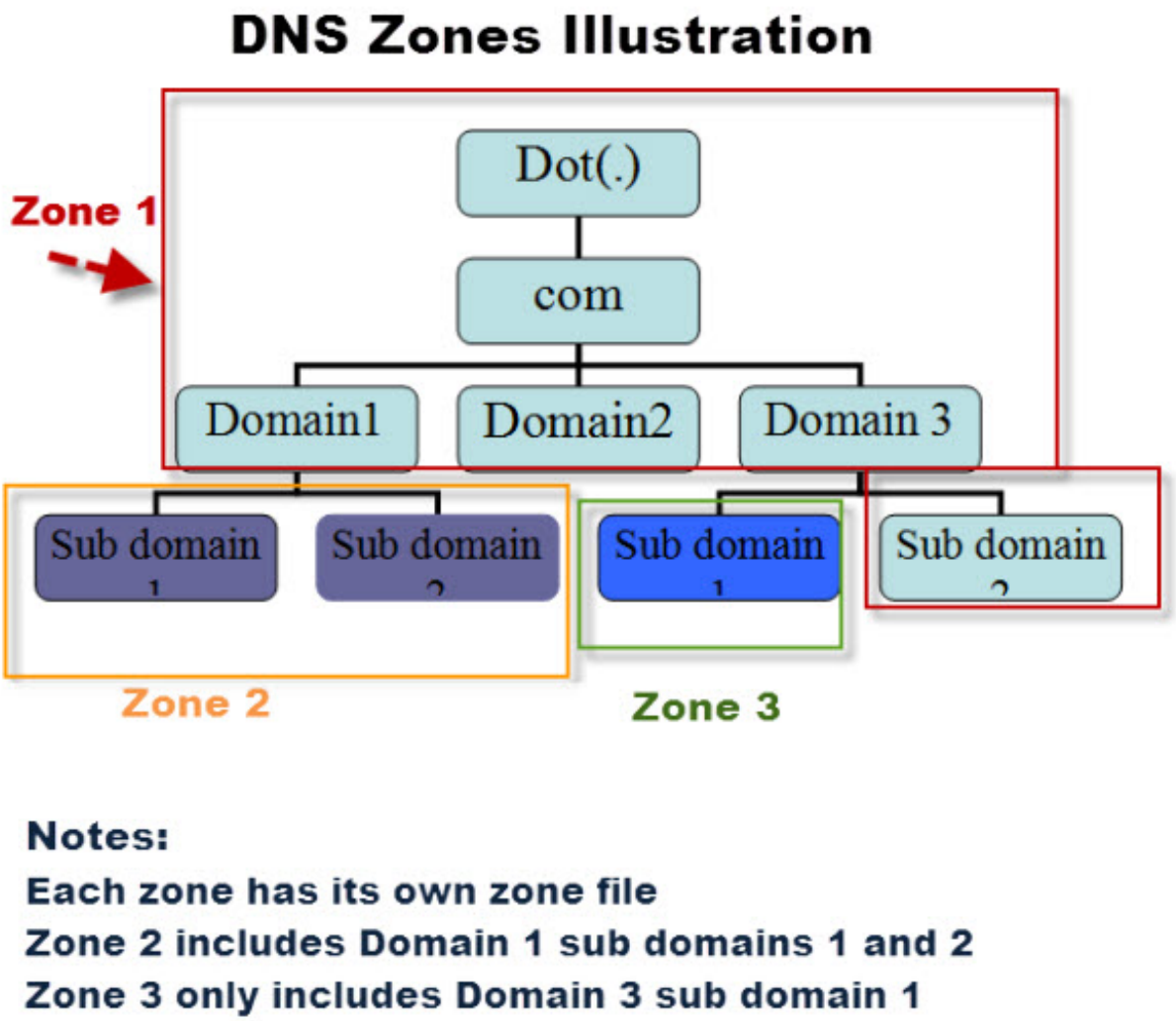
The use of zones and zone files is what allows DNS to be a distributed and resilient system.

DNS Zones provide a very easy and simple method of grouping domain data from multiple domains together for storage.

For domains to share a zone and hence a **zone file** the domains **must be contiguous.**

A **domain administrator** would be responsible for creating zones, and delegating responsibility for these zones to an administrator and DNS server.

To illustrate we will refer to the diagram below which shows a section of the domain name system which has been divided into **3 zones.**



You should note that you cannot create a zone that includes **Domain1 sub domain 1** and **Domain 3** because they are not contiguous.

Zone File Storage

In our analogy the data is stored on a paper list and kept by the team manager.

A **zone file** is a **text based file** with a format defined in RFC 1035 and 1034 and is stored on a **DNS server** (name server).

Zone files contain the IP and name data, MX records and other service records.

They also contain **glue data** that connects them to the other DNS servers.

Referring to the diagram above the DNS server responsible for **zone 1** will contain records that tell it:

- Which DNS servers have data for Domain2.
- Which DNS servers have data for Domain3 sub domain1 (i..e. zone3).
- List of Root servers (**root hints**)
- List of forwarding servers (if using forwarding)

The **DNS server** responsible for **Domain 1 -sub domain 1 and 2 – i.e. Zone 2** has **no knowledge** of who has data for **domain3 sub domain1 – i.e. Zone 3** and doesn't need any.

Zone File Structure and Record Contents

The DNS zone file consists of directives and resource records.

Directives begin with a **$.** There are three Directives

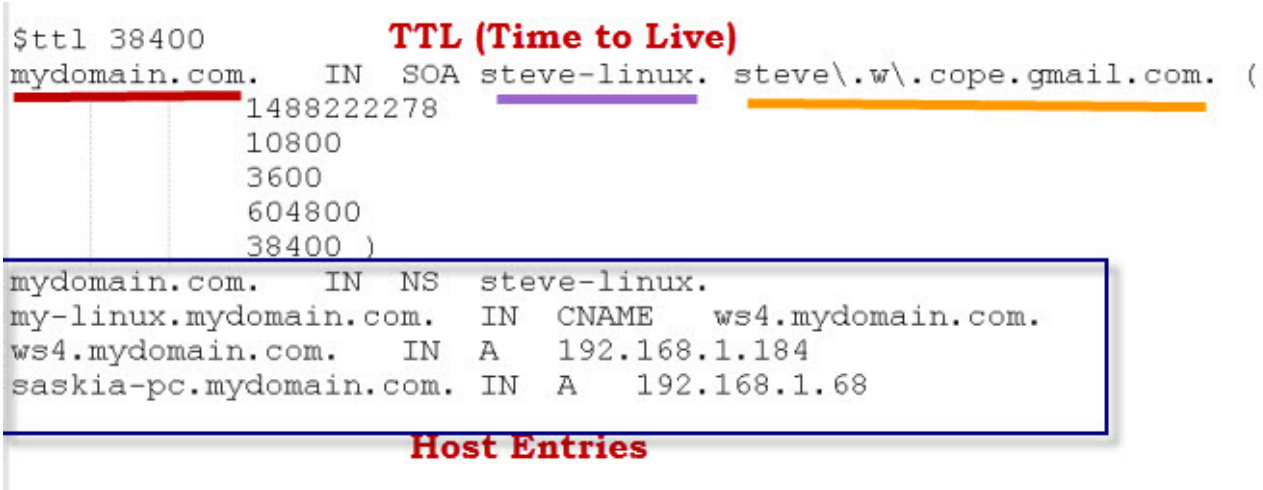
- **$TTL** – Time to Live value for the zone.
- **$ORIGIN** – Defines base name -used in domain name substitution
- **$INCLUDE**– Include a file

The **$TTL** directive must appear at the top of the Zone File before the **SOA** record.

The SOA (start of authority) **must be present** in a zone file, and defines the domain global values mainly to do with zone transfer.

```
mydomain.com  IN  SOA  primary-name-server hostmaster-email (
        serial-number
        time-to-refresh
        time-to-retry
        time-to-expire
        minimum-TTL )
```

An example record is shown below .



For more detail see this chapter from the Pro Bind and DNS book.

Zone Delegation

When an administrator of a domain decides to allocate responsibility of a child domain to someone else e.g. sub domain 1 of domain 3. then they will delegate the zone.

This means that the zone file is stored on another DNS server than the parent domain. However the parent domain will **keep track on the location of the zone** by creating **glue records** to the name servers responsible for the zone data.

We saw this with Bill Needing to know who had the list for Teams A.B.C.

Caching and TTL

Caching is the process of temporarily storing data and is used frequently in networking, and on the Internet.

DNS server and hosts cache **DNS lookup data** which means that they may be able to quickly resolve a lookup if it is already stored in the cache.

In our example above when someone requested the phone number of Steve, Bill remembers that information for a short time in case someone else needs to know it. The problem with caching data is what happens if the data changes, but the cache is still holding the old data?

To ensure that clients and servers don't hold on to old data for too long DNS records have a **TTL** (time to live value) which tells the client/server how long it can store data in its cache.

Caching greatly reduces the load on the **root DNS servers**.

Reverse Mapping Zones

Reverse mapping zones provide the data for reverse lookups i.e IP address to name.

In our analogy we would use the phone number to find the name of the player.
Reverse mapping is **not mandatory** but is used frequently by applications like email to prevent spamming.

Therefore without it some applications may not work correctly.

Reverse mapping uses the domains **IN-ADDR.ARPA** for IPv4 addresses and **IP6.ARPA** for IPv6 addresses.

Most DNS admin tools will automatically create the reverse mapping entry when you create the host entry.
For more details see chapter 3 of the Pro DNS and Bind book.