**DNS (Domain Name System)**

* **Domain 🡪 IP (Forward Name Resolution)**
* **IP 🡪 Domain (Backward Name Resolution)**

**How a domain name is identified?**

1. Firstly, the Local DNS is checked i.e. if the data is cached in the history.
2. Then, the DNS is checked in ISP (Internet Service Provider)

Then, the DNS is check in root server (there are 13 root server which has got replicated data of all DNS) root server example 🡪 ʘ

**.**

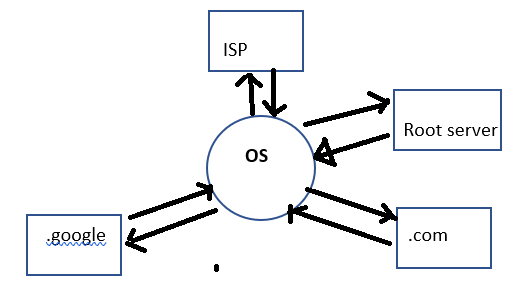
**com in org edu mil**

**UN SwissFed Harvard**

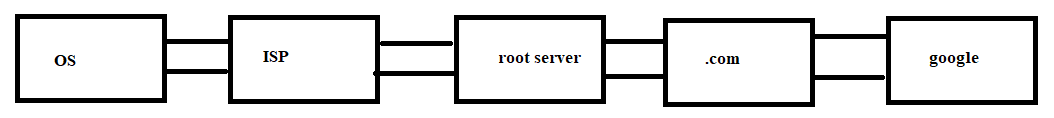
google amazon

* There are two methodologies of DNS identification

1. Iterative DNS identification : where the DNS request is first sent to the ISP by the OS then the result comes only of specific root server and then when contacted by root the root further acknowledges back with .com or .org i.e only the terminator and then the OS has to work on its own to identify further address by connecting links.



1. Recursive DNS identification is when the same functions works in the recursive way and it is the dominant identification technology today.



**Reverse Name resolution**

Reverse name resolution works identifying DNS from IP like say the ip is 172.24.0.10 now in this ip just leave the last 8 bits and make it as

**0.24.172.in-addr.arpa**

To identify the DNS from IP just move from backwards as

in-addr.arpa 🡪 172 🡪 24 🡪 0 🡪 now on the index of 0 search for 10 (the left bit) and on the index there would be the full fledged Domain Name.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

To check the domain name [ dnsdomainname ]

To check the host name [ hostname]

**To implement the DNS server originally ‘Berkeley internet named domain’ install bind\* and cach\***

[ yum install bind\* cach\* ]

1. Go to /etc/named.conf
2. Backup the file named.conf for security as named.conf.bak
3. In named.conf file serach for options and then edit at

listen-on port 53 { 127…..;<space> <your ip >; <space>};

1. Search for allow-query and edit

allow-query { localhost; <your server ip’s network id>/16; };

Note – 16 depicts no of systems allowed in the system i.e 2^16

1. Now remove the whole section from logging till end of file
2. After the recursion yes; }; edit as

|zone “ceact.com” IN {

| type master;

| file “forward”;

|};

|zone “0.24.172.in-addr.arpa” IN {

| type master;

| file “reverse”;

|};

Note 🡪 zone files are saved in /var/named/

In /var/named/ copy the file named.localhost as forward and edit it as

|$TTL 1D

|@ IN SOA root.ceact.com nsserver1.ceact.com. (

//something

| NS server1

|server1 A 172.24.0.10

|www CNAME server1

|download CNAME server1

Note 🡪 CNAME stands for allias

serial signifies if the data of the master is changed or not since in that case it changes its serial no

Refresh signifies the refreshment rate of data

Retry : when to retry to refresh the data if the master was busy

Expire

Minimum : minimum time to carry data

Note-> copy the forward file after configuration as ‘reverse’

$TTL 1D

@ <no change>

NS server10.ceact.com.

10 PTR server10.ceact.com.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Note 🡪 after saving the forward and reverse file change the owner and the group to ‘named’

Update the entry in client side at /etc/resolv.conf

Type in there anywhere

|**nameserver 172.24.0.10**

To check whether the dns is properly implemented or not

| nslookup www.ceact.com