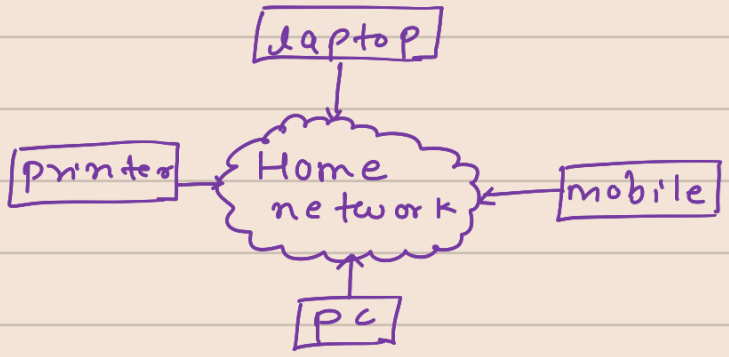
* Networking (lesson 19)

How does computer network work?
How does computer connect to internet?
what is ip address and port?
What is DNS?

* LAN, Switch, Router, WAN, Gateway



Devices are connected to that network
Such a network is called LAN

LAN = local area network.

→ Collection of devices connected together in one physical location
private home lan, school, big building.

– each device has a unique IP address

IP – Internet protocol.

laptop → 172.16.0.1
printer – 172.16.0.3

→ Devices can talk to each other on the network via these IP address

IP

172.16.0.0 → 32 bit value

10101100 . 00010000 . 00000000 . 00000000 → 1 bit = 1 or 0

octet → 172
octet → 16

11111111 – 255

IP address can range from
0.0.0.0 to 255.255.255.255

How do devices talk to each other? → special device, SWITCH

→ Switch sits within the LAN.
and knows IP address
of all devices
→ facilitates the connection betn
all the devices within LAN.

laptop can talk to phone or printer.

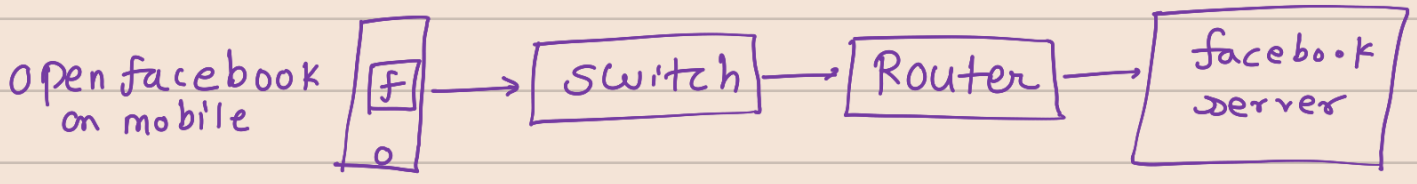
But what if we want to talk to server
or some other device not in LAN
eg - you want to open facebook website
on your laptop so you want to connect to and
talk to facebook server. (or any website hosted
on server outside your lan)

→ for connecting to outside devices there
is a device called 'Router'

Router.

→ Sits between LAN and outside
networks (WAN)
WAN = wide area network.
→ connects devices on LAN and WAN
→ allows networked devices to
access the internet.

eg.



phone will send the request to
router and router will send the
request to facebook server
over internet

IP address of Router = "Gateway"

* Subnet

How to know, wheather the other device is inside or outside the LAN?.

- It knows Ip of target device
- Ip are not random, devices in the lan belong to same ip address range to identify devices in same network

Subnet = logical subdivision of an ip network.

Subnetting = process of dividing a network into two or more networks.

eg of an ip address range.

192.168.0.0 — 1.) IP address. 255.255.255.0 — 2.) Subnet mask.

1.) Starting point of ar ip range, the first ip in the range

2.) Set the range

Starting - 192.168.0.x

Subnet mask 255.255.0.0 → ip address start : 192.168.x.x

255.255.0.0 → 16 bits are fixed.

255.255.255.0 → 24 bits are fixed

value 255 fixe the octet.

Value 0 means free range

198.192.0.0 to 198.192.0.255

198.192.0.0 to 198.192.255.255

CIDR Block.

Classless Inter-Domain Routing. → shorthand

192.168.0.0/16 or 192.168.0.0/24

16 bits fixed 24 bits fixed.

any device needs 3 pieces of data for communication:

1.) IP address
2.) Subnet
3.) Gateway.

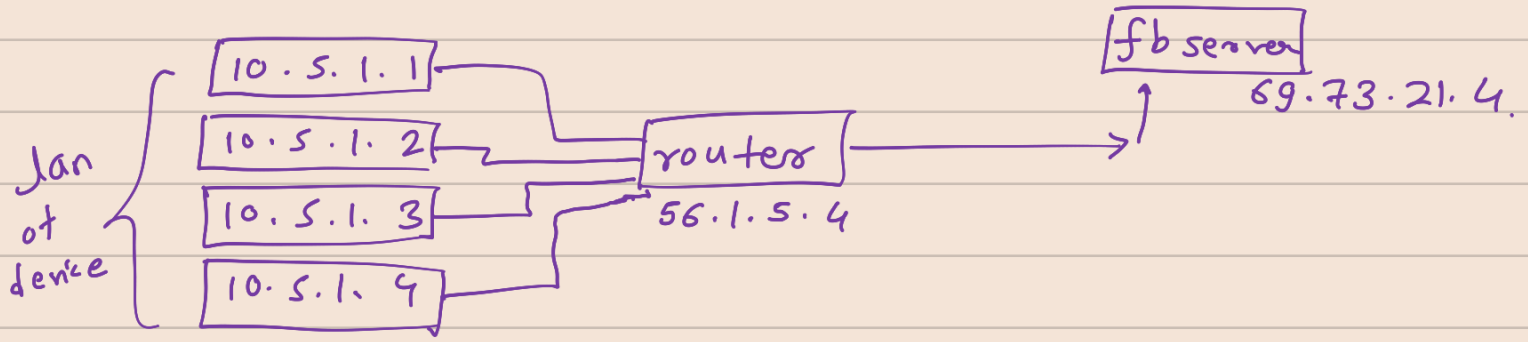
* network address translation (NAT)

1.) Ip address range choosen by administrator (ISP etc)
2.) each device get unique IP address from that range

How to make sure IP add in our lan does'nt overlap with IP address of other lan ?

→ Ip address within LAN are not visible to the outside network or internet.

→ Your laptop private ip address is replaced by the ip of router this is known as NAT.



when a device from lan request the facebook page suppose (10.5.1.2) want to access fb page. Then that request first reaches the router. The router changes the source of ip from 10.5.1.2 to its own ip (56.1.5.4) and sends that request to fb server. fb sends the response to

router (56.1.5.4) and then the router sends it to private lan (10.5.1.2)

Benefits

1.) Security and protection of devices within LAN

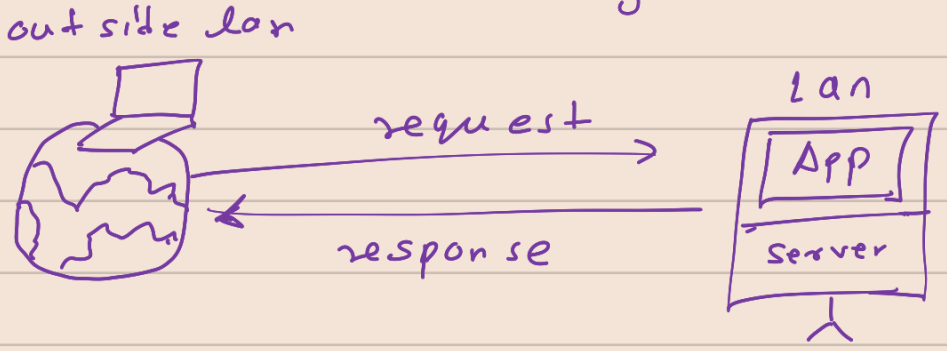
2.) Reuse ip address.

Two huge companies can have same ip range within their org LAN.

Limited no of IP (from IPV4)

* firewall.

outside device wants to talk to your lan directly



→ By default, the server is not accessible from outside the LAN.

firewall → a system that prevent unauthorized access from entering a private network

→ using firewall rules you can define, which request are allowed

firewall rules

→ which ip address in your network is accessible

→ which ip address can access your server.

→ eg - you can allow any device access your server.

eg. web application

→ also specify which ports are accessible on your server.

Type	Protocal	Port range	Sources
SSH	TCP	22	178.19.1.2
Custom	TCP	3000	All IPv4
Custom	TCP	8081	All Ipv4.

Port:

1.) every device has a set of ports
ports are like doors to the same building

2.) you can allow specific ports (doors) so that some request may enter and keep others locked

3.) you can allow specific ports to specific IP address.

4.) Diff application listen on specific ports.

5.) Standard ports many apps.
Port 80 – http (web)
Port 443 – https (web)
Port 21 – FTP.

Type facebook.com → Request to fb server on port 80

which means that port 80 was unlocked to accept the browser request

Port 3306 – mysqldb
Port 5432 – PostgreSQL DB

Two app cannot listen on same port

∴ firewall configuration allows a specific combination of device ip add and port to be accessed.
– port forwarding.

* Domain name system (DNS).

every computer on network is identified by unique Ip address. And a device can talk to other device by using Ip add

When we want to visit a website we don't type ip add of it instead we type www.facebook.com or www.docker.com. and not https://69.63.1.5

Because fb runs on many servers which have their own ip address

Why do we use name instead of ip address?

→ 1.) Humans are better remembering words and names instead of nos. (ip)

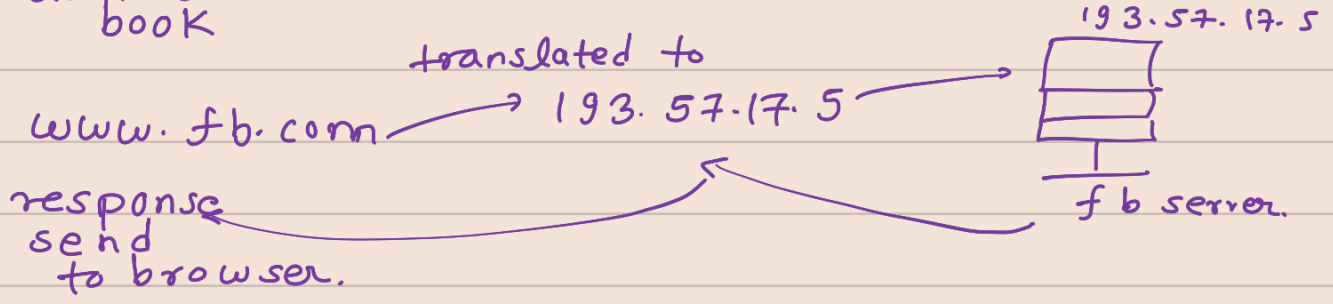
"Mapping Ip address to Names"

Names gets translated into ip where that app is running which then your computer can send request to

DNS = translates domain names to Ip address.

↓

address book



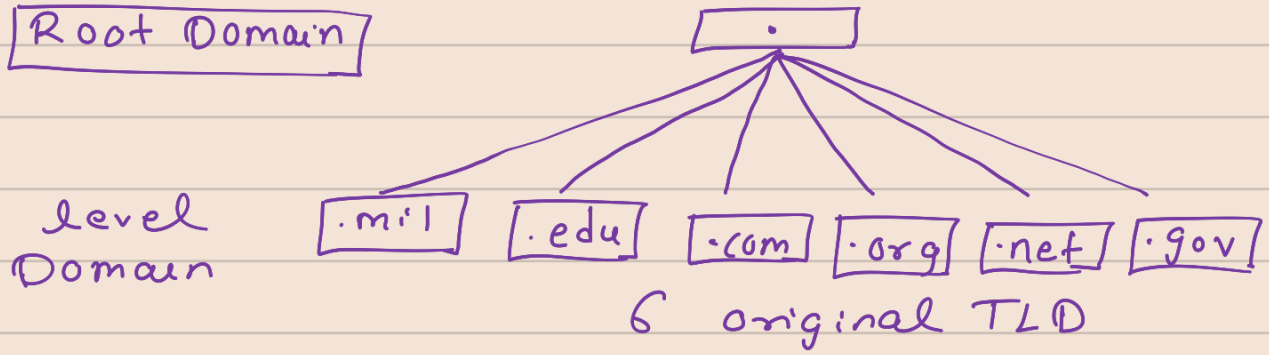
So many websites

google.com, mit.edu, marines.mil, nyc.gov.

How does DNS manage all these Ip address?

→ Domain name have hierarchical structure.

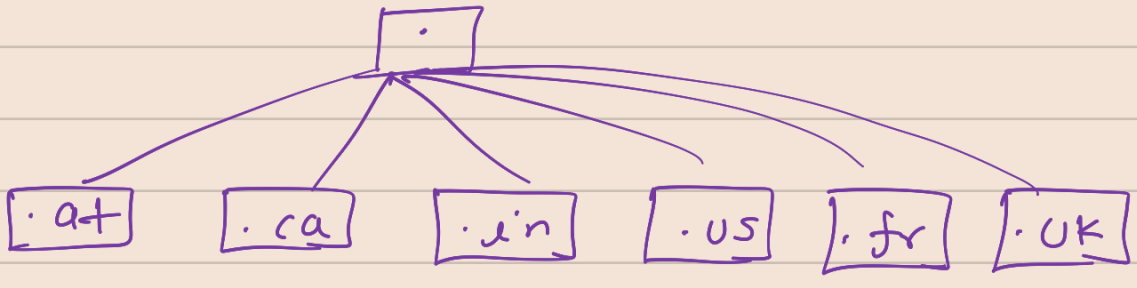
Root Domain → 13 (.a - .m)



6 original TLD

- .mil → military application
- .edu → educational institutes.
- .com → general purpose and business
- .org → ngo
- .net → networking technologies (can be general purpose)
- .gov → government.

There are also georgraphical top level domain.



austria india usa france

if your website is in local language and your visitors are local

you can buy domain name - mywebsite.com

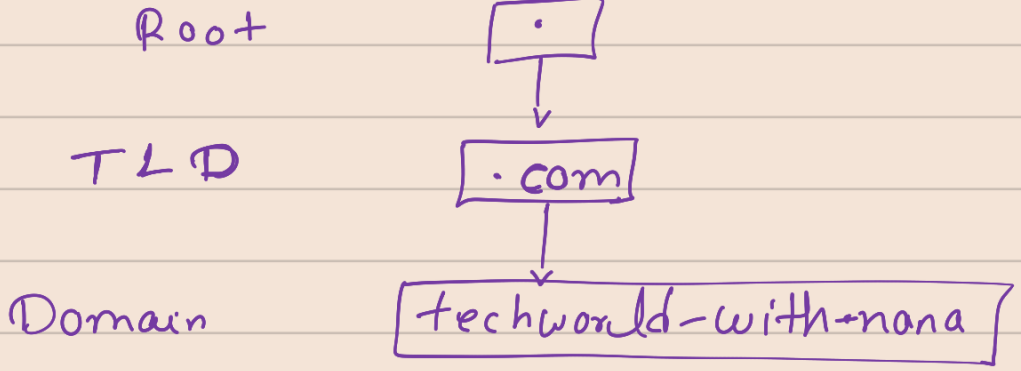
Who can manage these names?

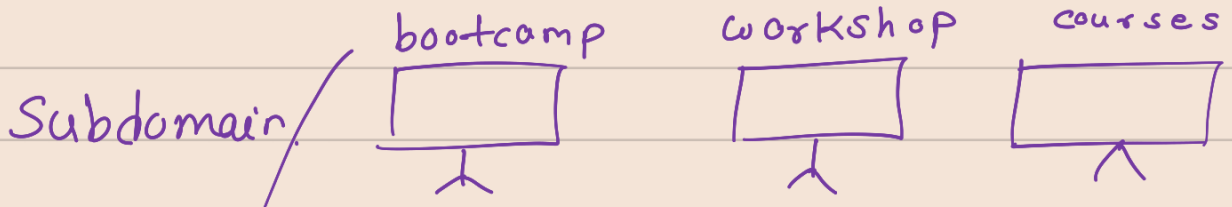
Who can see these domain names?

Who keeps track of availability of names?

Dedicated org → Internet corporation for assigned names and nos. (ICANN)

Subdomain.





3 server - with 3 apps all belong to my company

www.bootcamp.tech-world-nana.com

each app runs on its own dedicated server.

How does the DNS resolution work ?

① every comp has DNS client preinstalled. when you open browser and type facebook.com. Your OS makes a Dns query asking DNS to resolve that address or find ip address that match to facebook.com

② The DNS request first goes to recursive name server. (usually operated by ISP)

Recursive name server might have stored the Ip address (cache?)

③ But if doesn't it goes to one of 13 root server which manage request for TLD

Root server available all over the world

Root server will look at the address and .com and it sends the request back to resolver (ask(.com) server)

④ The resolver then ask .com server the ip address of fb.com. The .com server sends the response → (list of auth. name server) for .com domain.

auth name server → Responsible for knowing everything about the domain, including Ip address

⑤. finally resolver chooses the ip of one of the auth. name server from the list asking ip of facebook.com and this time name server response with ip address of fb.com.

⑥. now our comp sends the request to facebook ip address

→ Dns entries are cached for efficiency

* networking commands.

ifconfig → ip add, subnet mask, gateway add, etc

netstat → active connection

ps aux → current running processes.

nslookup → get ip add of any domain name.

nslookup google.com

ping → wheather a service is accessible.

ping google.com