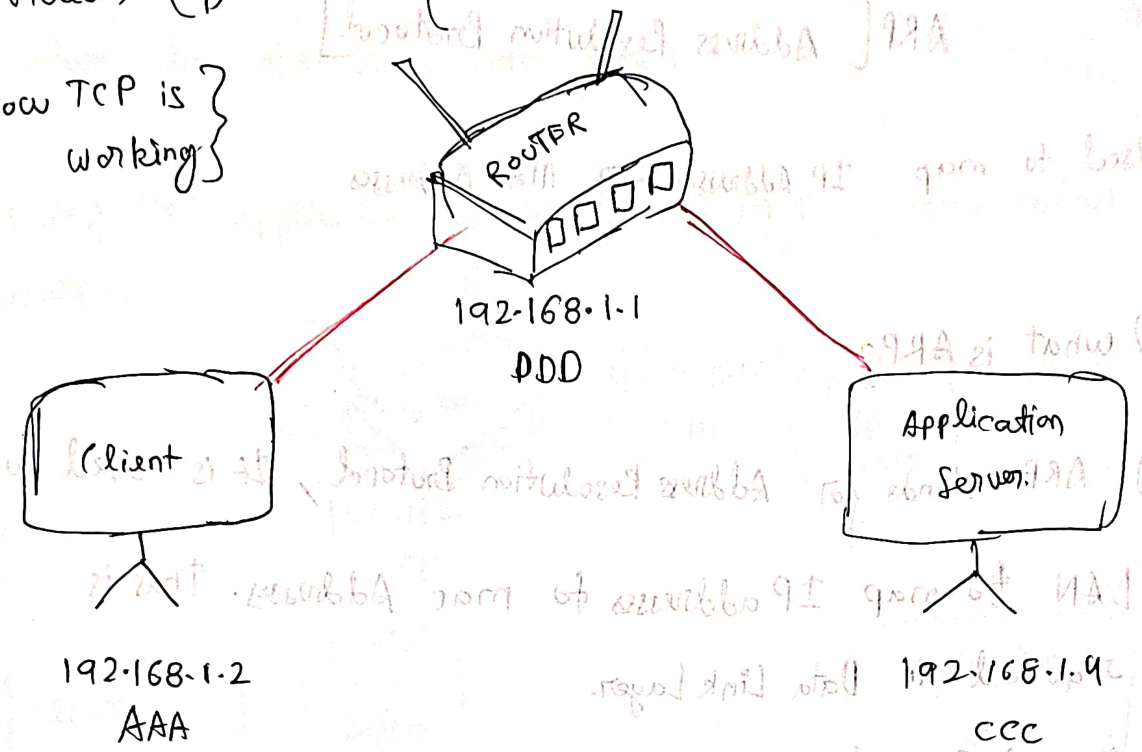
Video → (9) NAT (Network Address Translation)

{How TCP is working}



[Client and Application Server belong to the same subnet.]

Subnet: [192.168.1]

		src		dest		
AAA	8992	192.168.1.2	GET/	192.168.1.4	8080	CCC

It can directly send the ~~TCP~~ request, through router.

The router will Act as a dummy object and request will directly go to Application Server.

This MAC address of the destination ip is obtained using the ARP.

(p.T.o)

ARP[Address Resolution Protocol]

Used to map IP Address → MAC Address

Q) what is ARP?

A) ARP stands for Address Resolution Protocol, It is used with LAN to map IP addresses to mac Addresses. This is required in Data Link Layer.

Q) How ARP works?

ARP Request:-

- when a device wants to communicate with another device on the same local network. It needs to know the Mac address of that device
- The device broadcasts an ARP requests packet to all devices on the network. This request contains IP address for which the MAC Address is being sought.

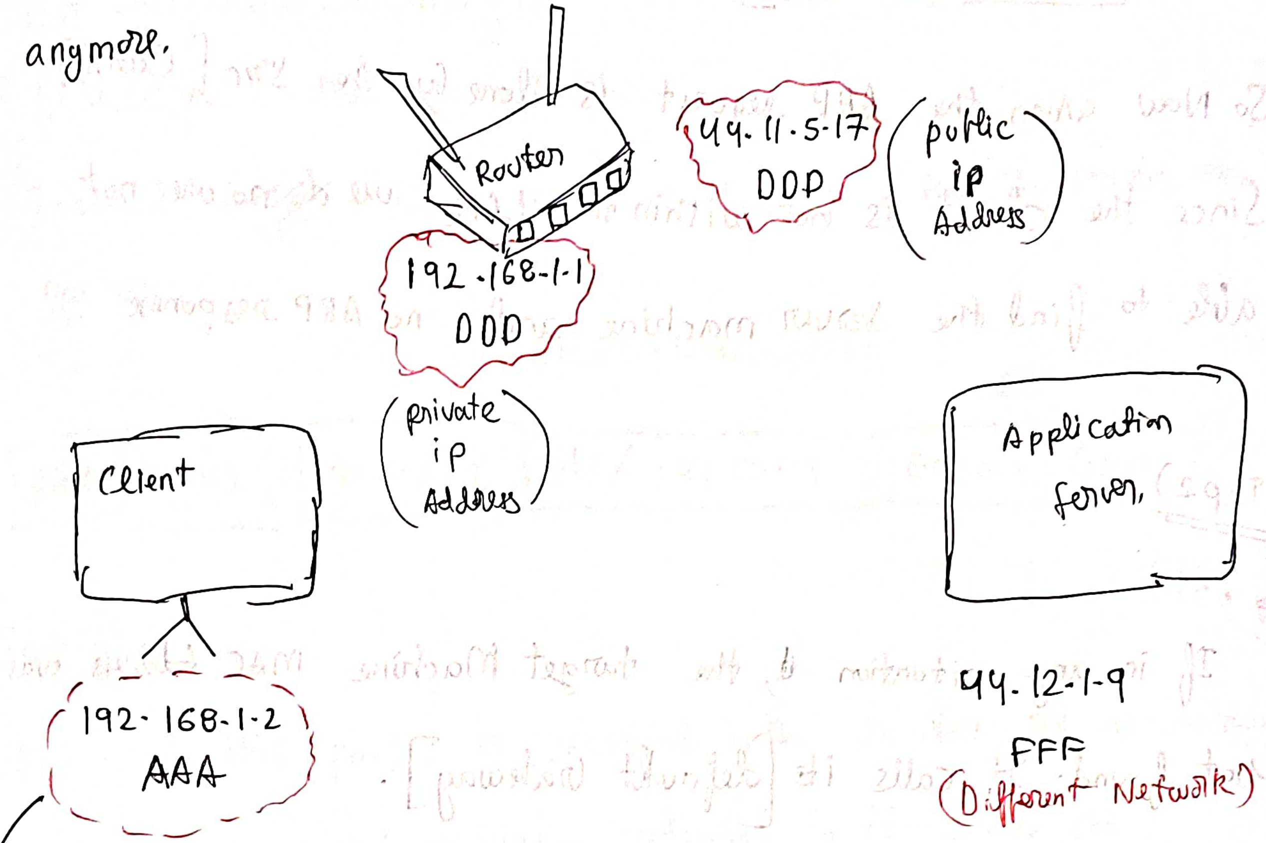
ARP Reply:-

- The device with the requested ip responds back to the client with the MAC Address.

[ARP cache] → Cache can be maintained for a Short time to ~~Mat~~ keep [ip Address → mac Address] map.

Q) Where does NAT come into play?

Lets say the application server is not in the same subnet anymore.



Now this is a private ip address, we cannot directly send GET request to server.

(**) We need some public representation.

So the router comes into play here.

It has both a public and a private ip address

The router is our gateway to connect to the application,

Lets see how its done

(Step1)

(src)			(destination)	
8992	192.168.1.2	GET/	44.12.1.9	8080

So Now when the ARP request is done by the src [Client]

Since the client is not within the LAN, we ~~depro~~ are not able to find the server machine and no ARP respones

(STep2)

(****)

If in any situation ~~A~~, the target Machine MAC Address was not found. It calls its [default Gateway].

In the [network Connection]

Network Interface{

ip Address,

SubNetmask,

default Gateway → (This is basically, if you are not sure, you send requests Here, That is basically our Router.)

⋮

}.

{Sometimes we can change It even, to do fancy things with Load Balancing}

So in STEP 2 basically the clients sends the packet ~~#~~ to the router.

But the important thing is, It does not change the destination ip address in the packet.

Instead it just attaches the mac Address of the router to the packet.

{Router MAC Address}

AAA	8992	192.168.1.2	GET/	44.12.1.9	8080	DDD

(Step 3)

Now when this packet is received by the router, It understands the packet is not actually indended to it. Since the destination ip Address does not match.

(~~xxxx~~) {NAT Table is stored in-memory}

(Step 4) It removes the src ip Address and attaches its public ip Address to send it to the server.

Routers. ~~MACs~~ credentials.

Server Details.

DDD	8731	44.11.5.17	GET/	44.12.1.9	8080	FFF

These details are maintained in NAT so that when we get a response we can send it back to the original client

192.168.1.2:8892	44.11.5.17: 8731	44.12.1.9:8080
⇓ Client	⇓ Router	⇓ Server

[NAT Applications]

1) Private to public IP translation.

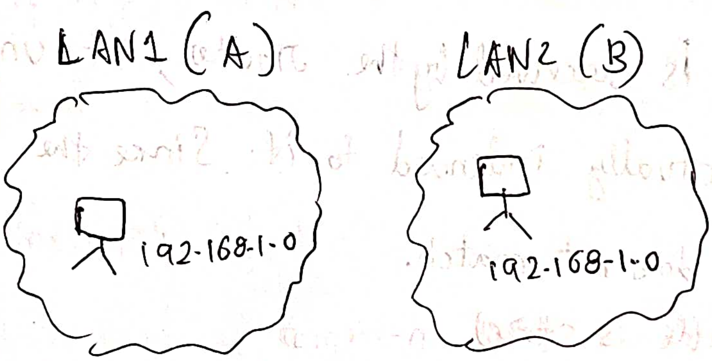
We cannot give every machine a public IP.

As per IP Address Standards (IPV4) 8bits . 8bits . 8bits . 8bits.

total 32 bits , 2^{32} unique IPs can be there.

Now public IPs need to be unique,

But private IPs need not be unique.



Machines inside LAN1 and LAN2 can have same ip address [private],

But Routers of LAN1, LAN2, which are public need to be unique

Using this NAT we can translate the private IP of the client to public IP of the router.

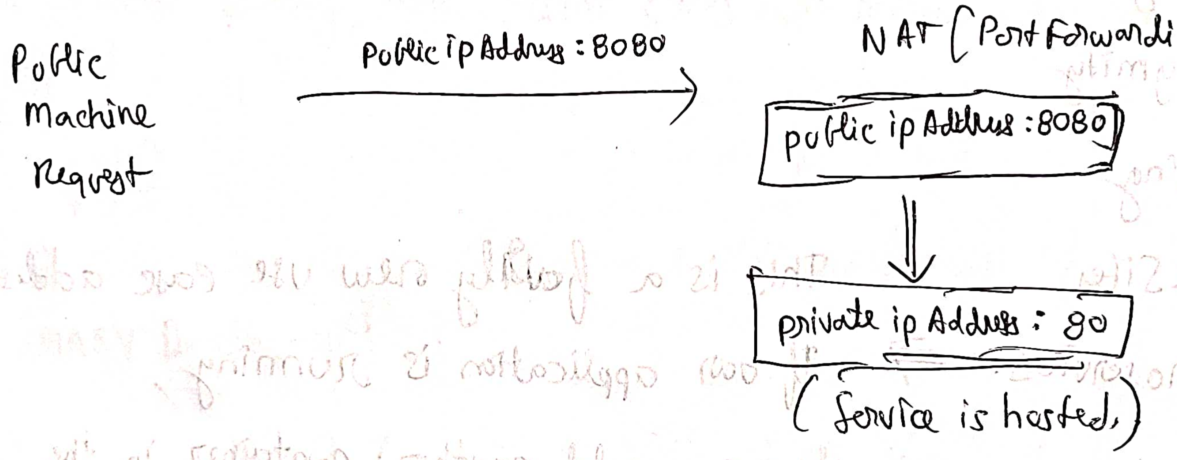
and expose it to public Network.

2) PortForwarding

So in any machine from [0 to 1023] ports are Restricted Access Ports and cannot be accessed directly.

Suppose any public machine wants to access this server, it is not possible,

But router can do it, NAT configuration can be made in this way



3) L4 LoadBalancer.