COMPUTER NETWORKs – II

Topic:

- DNS Server
- DHCP Server
- Private / Public IP
- NAT
- ARP
- Introduction to System Design

DNS Server (Domain Name Server):

Every website on the Internet has its own unique address. It's called an IP address. But unlike the physical street address for a house or building, an IP address consists of a set of numbers strung together and separated by periods. A typical IP address in the IPv4 address space looks like: **123.123.123.2**.

If customers had to memorize the IP addresses of every website they visited, they wouldn't spend much time on the Internet. Thankfully, we use URLs instead. And behind the scenes, there's an "address book" of sorts that helps convert these user-friendly URLs and web addresses into the IP addresses that computers understand. It's called a Domain Name System, or DNS.

In the simplest form, a DNS is a directory of domain names that align with IP addresses. They bridge the gap between computer language and human language – keeping both servers and people happy.

If you enter "**157.240.198.35**" IP address, in the windows account, you will get the Facebook page. Every Domain Name is its own IP address; it is mapped to the IP address in other words.

When we enter www.google.com in the web browser, it will send the request to DNS server and the DNS server will give the IP address (8.8.8.1) to our browser which will open the google.com

DHCP Server (Dynamic Host Configuration Protocol):

DHCP Definition

DHCP stands for dynamic host configuration protocol and is a network protocol used on IP networks where a DHCP server automatically assigns an IP address and other information to each host on the network so they can communicate efficiently with other endpoints.

In addition to the IP address, DHCP also assigns the subnet mask, default gateway address, domain name server (DNS) address and other pertinent configuration parameters. Request for comments (RFC) **2131** and **2132** define DHCP as an Internet Engineering Task Force (IETF)- defined standard based on the BOOTP protocol.

DHCP Simplifies IP Address Management

The primary reason DHCP is needed is to simplify the management of IP addresses on networks. No two hosts can have the same IP address, and configuring them manually will likely lead to errors. Even on small networks manually assigning IP addresses can be confusing, particularly with mobile devices that require IP addresses on a non-permanent basis.

Also, most users aren't technically proficient enough to locate the IP address information on a computer and assign it. Automating this process makes life easier for users and the network administrator.

Private | Public IP

IPV4 was about to end soon as the addresses were not sufficient enough. Therefore, people invented NAT, Network Address Translation.

All the devices in our home which are using internet via a router will have their own IP address. So, the NAT is introduced and present inside your router.

The private address are special addresses which start with 10 or 172 or 192 and the remaining are public addresses. The router will assign a private IP addresses to all the devices that are connected to it. The NAT present in the router does this, so that we do not exhaust IPV4 addresses.

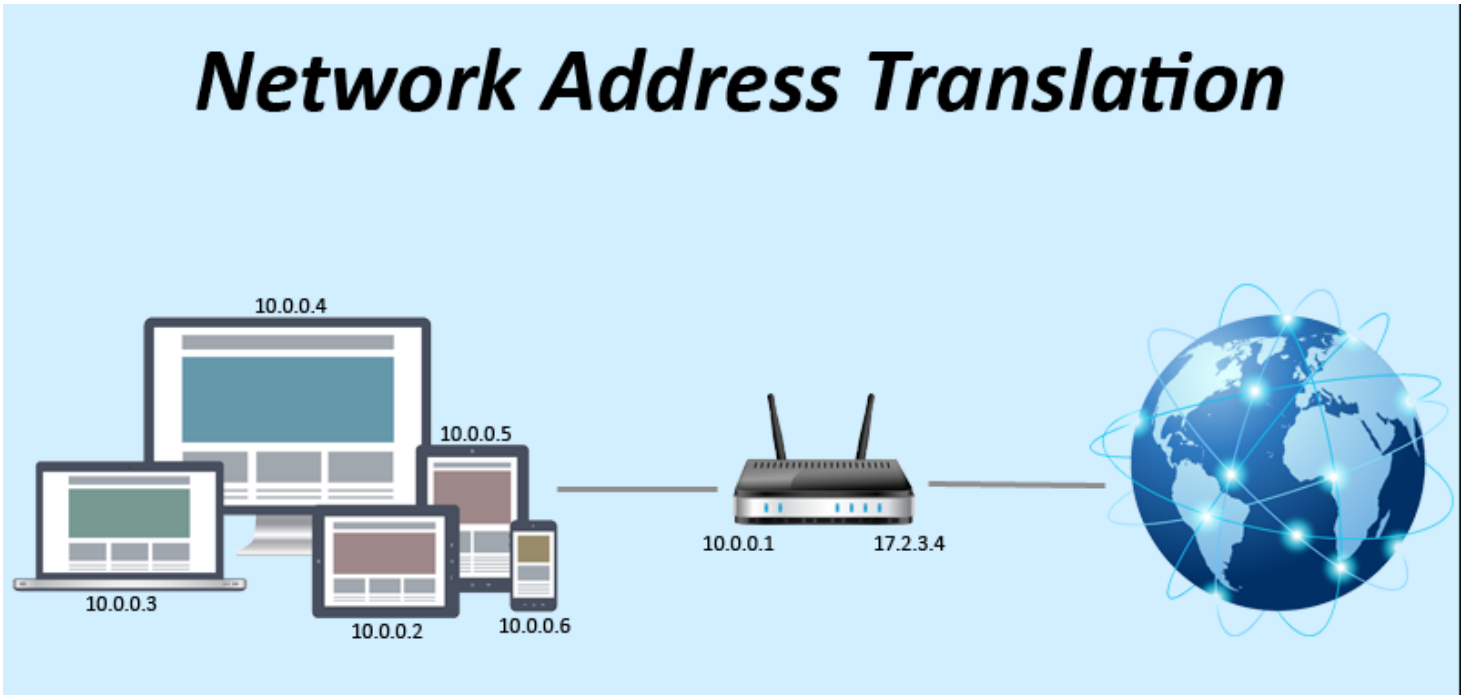
Private IP address of a system is the IP address which is used to communicate within the same network. Using private IP data or information can be sent or received within the same network.

Public IP address of a system is the IP address which is used to communicate outside the network. Public IP address is basically assigned by the ISP (Internet Service Provider).

Difference between Private and Public IP address:

PRIVATE IP ADDRESS	PUBLIC IP ADDRESS
Scope is local.	Scope is global.
It is used to communicate within the network.	It is used to communicate outside the network.
Private IP addresses of the systems connected in a network differ in a uniform manner.	Public IP may differ in uniform or non-uniform manner.
It works only in LAN.	It is used to get internet service.
It is used to load network operating system.	It is controlled by ISP.
It is available in free of cost.	It is not free of cost.
Private IP can be known by entering “ipconfig” on command prompt.	Public IP can be known by searching “what is my ip” on google.
Range: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255, 192.168.0.0 – 192.168.255.255	Range: Besides private IP addresses, rest are public.
Example: 192.168.1.10	Example: 17.5.7.8

NAT



To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of private IP address to a public IP address is required. Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on router or firewall.

Network Address Translation (NAT) working –

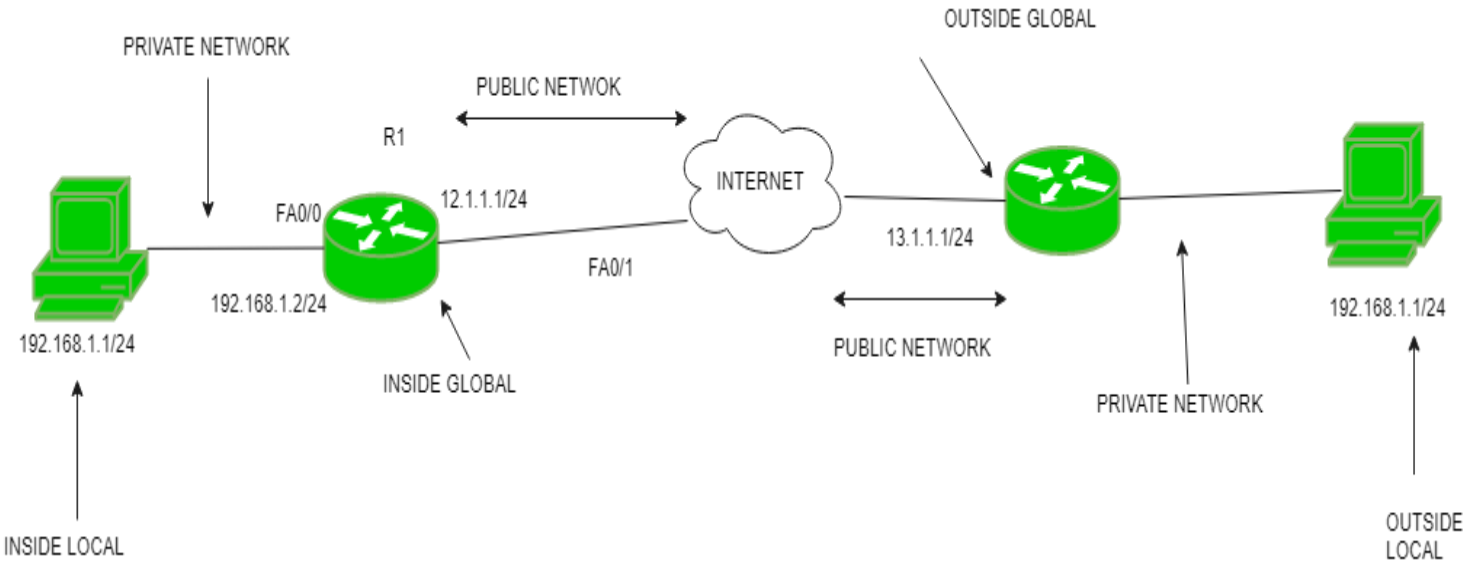
Generally, the border router is configured for NAT i.e the router which has one interface in local (inside) network and one interface in the global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address.

If NAT run out of addresses, i.e., no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is sent.

Why mask port numbers?
Suppose, in a network, two hosts A and B are connected. Now, both of them request for the same destination, on the same port number, say 1000, on the host side, at the same time. If NAT does an only translation of IP addresses, then when their packets will arrive at the NAT, both of their IP addresses would be masked by the public IP address of the network and sent to the destination. Destination will send replies on the public IP address of the router. Thus, on receiving a reply, it will be unclear to NAT as to which reply belongs to which host (because source port numbers for both A and B are same). Hence, to avoid such a problem, NAT masks the source port number as well and makes an entry in the NAT table.

NAT inside and outside addresses –

Inside refers to the addresses which must be translated. Outside refers to the addresses which are not in control of an organisation. These are the network Addresses in which the translation of the addresses will be done.



- **Inside Local Address** – An IP address that is assigned to a host on the Inside (local) network. The address is probably not a IP address assigned by the service provider i.e., these are private IP address. This is the inside host seen from the inside network.

- **Inside Global Address** – IP address that represents one or more inside local IP addresses to the outside world. This is the inside host as seen from the outside network.
- **Outside Local Address** – This is the actual IP address of the destination host in the local network after translation.
- **Outside Global Address** – This is the outside host as seen from the outside network. It is the IP address of the outside destination host before translation.

Network Address Translation (NAT) Types –

There are 3 ways to configure NAT:

Static NAT – In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e one-to-one mapping between local and global address. This is generally used for Web hosting. These are not used in organisations as there are many devices who will need Internet access and to provide Internet access, the public IP address is needed.

Suppose, if there are 3000 devices who need access to the Internet, the organisation have to buy 3000 public addresses that will be very costly.

Dynamic NAT – In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP address. If the IP address of pool is not free, then the packet will be dropped as an only a fixed number of private IP address can be translated to public addresses.

Suppose, if there is a pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time. If 3rd private IP address wants to access Internet then the packet will be dropped therefore many private IP addresses are mapped to a pool of public IP addresses. NAT is used when the number of users who wants to access the Internet is fixed. This is also very costly as the organisation have to buy many global IP addresses to make a pool.

Port Address Translation (PAT) – This is also known as NAT overload. In this, many local (private) IP addresses can be translated to a single registered IP address. Port numbers are used to distinguish the traffic i.e., which traffic belongs to which IP address. This is most frequently used as it is cost-effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.

Advantages of NAT –

- NAT conserves legally registered IP addresses.
- It provides privacy as the device IP address, sending and receiving the traffic, will be hidden.
- Eliminates address renumbering when a network evolves.

Disadvantage of NAT –

- Translation results in switching path delays.
- Certain applications will not function while NAT is enabled.
- Complicates tunneling protocols such as IPsec.
- Also, router being a network layer device, should not tamper with port numbers (transport layer) but it has to do so because of NAT.

ARP (Address Resolution Protocol):

Address Resolution Protocol (ARP) is an important protocol of the network layer in the OSI model, which helps find the MAC (Media Access Control) address given the system's IP address. The ARP's main task is to convert the 32-bit IP address (for IPv4) to a 48-bit MAC address.

This protocol is mostly used to determine the hardware (MAC) address of a device from an IP address. It is also used when one device wants to communicate with some other device on a local network. The full form of ARP is Address Resolution Protocol.

If two computers want to communicate with each other, they need MAC address. Every computer will have an ARP table. If C1 wants to communicate with C2, it will check its ARP table for the C2’s ARP Table. If the address is not present, the C1 will broadcast, everyone in the network meaning, C1 will ask all the computers in the network. Once C2 confirms then C1 is connected with C2.

Address Resolution Protocol (ARP) is a procedure for mapping a dynamic Internet Protocol address (IP address) to a permanent physical machine address in a local area

network (LAN). The physical machine address is also known as a Media Access Control or MAC address.

The job of the ARP is essentially to translate 32-bit addresses to 48-bit addresses and vice-versa. This is necessary because in IP Version 4 (IPv4), the most common level of Internet Protocol (IP) in use today, an IP address is 32-bits long, but MAC addresses are 48-bits long.

ARP works between network layers 2 and 3 of the Open Systems Interconnection model (OSI model). The MAC address exists on layer 2 of the OSI model, the data link layer, while the IP address exists on layer 3, the network layer.

ARP can also be used for IP over other LAN technologies, such as token ring, fiber distributed data interface (FDDI) and IP over ATM.

In IPv6, which uses 128-bit addresses, ARP has been replaced by the Neighbor Discovery protocol.

How ARP works

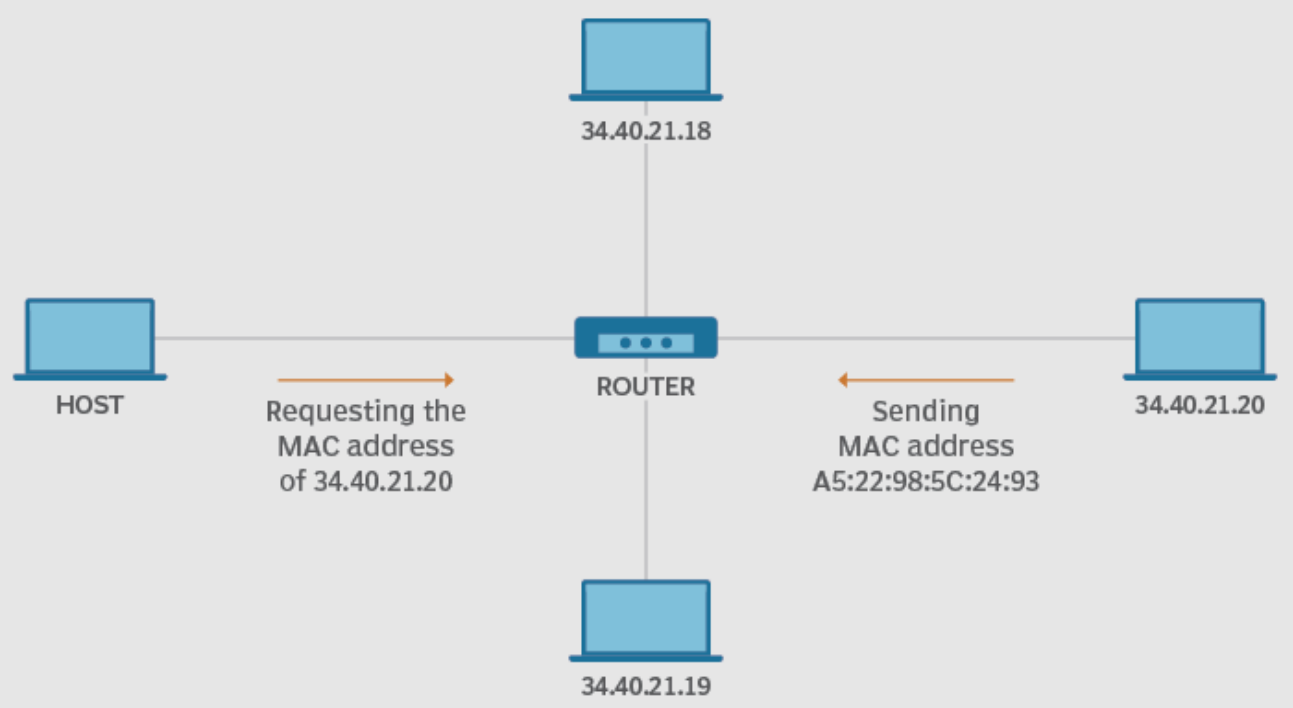
When a new computer joins a LAN, it is assigned a unique IP address to use for identification and communication. When an incoming packet destined for a host machine on a particular LAN arrives at a gateway, the gateway asks the ARP program to find a MAC address that matches the IP address. A table called the ARP cache maintains a record of each IP address and its corresponding MAC address.

All operating systems in an IPv4 Ethernet network keep an ARP cache. Every time a host requests a MAC address in order to send a packet to another host in the LAN, it checks its ARP cache to see if the IP to MAC address translation already exists. If it does, then a new ARP request is unnecessary. If the translation does not already exist, then the request for network addresses is sent and ARP is performed.

ARP broadcasts a request packet to all the machines on the LAN and asks if any of the machines know they are using that particular IP address. When a machine recognizes the IP address as its own, it sends a reply so ARP can update the cache for future reference and proceed with the communication.

Host machines that don't know their own IP address can use the Reverse ARP (RARP) protocol for discovery.

An ARP cache size is limited and is periodically cleansed of all entries to free up space; in fact, addresses tend to stay in the cache for only a few minutes. Frequent updates allow other devices in the network to see when a physical host changes their requested IP address. In the cleaning process, unused entries are deleted as well as any unsuccessful attempts to communicate with computers that are not currently powered on.



https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/configuration_examples/nat_1-to-1_config_example.html

https://www.geeksforgeeks.org/difference-between-private-and-public-ip-addresses/

https://www.coursera.org/learn/computer-networking

https://searchnetworking.techtarget.com/definition/Address-Resolution-Protocol-ARP

https://www.section.io/engineering-education/address-resolution-protocol/