RGPVNOTES.IN

Please do not share these notes on apps like WhatsApp or Telegram.

The revenue we generate from the ads we show on our website and app funds our services. The generated revenue **helps us prepare new notes and improve the quality of existing study materials**, which are available on our website and mobile app.

If you don't use our website and app directly, it will hurt our revenue, and we might not be able to run the services and **have to close them**. So, it is a humble request for all to **stop sharing the study material** we provide on various apps. Please **share the website's URL instead.**

Syllabus: Review of Traditional Networks: Review of LAN, MAN, WAN, Intranet, Internet, and Interconnectivity devices: Bridges, Routers. Review of TCP/IP Protocol Architecture: ARP/RARP, IP Addressing, IP Datagram Format and Its Delivery, Routing Table Format, ICMP Messages, Sub Netting, Super Netting and CIDR, DNS. NAT: Private Addressing and NAT, SNAT, DNAT, NAT and Firewalls, VLANS: Concepts, Comparison with Real LANS, Type of VLAN, Tagging, IPV6: Address Structure, Address Space and Header.

TRADITIONAL NETWORKING

Traditional networking is rooted in fixed-function network devices, such as a switch or router. These devices each have certain functions that operate well together and support the network. If the network's functions are implemented as hardware constructs, then its speed is usually bolstered. Flexibility is a recurring hurdle for traditional networks. Few APIs are exposed for provisioning and most switching hardware and software is proprietary. Traditional networks often work well with proprietary provisioning software, but this software can't be quickly modified as needed. Traditional networking consists of the following traits:

- The functions of traditional networking are primarily implemented from dedicated devices, using one or more switches, as well as routers and application delivery controllers.
- The functionality of traditional networking is largely implemented in dedicated hardware, such as application-specific integrated circuits (ASIC). One of the negative aspects of this traditional hardware-centric networking is its limitations.

Figure 1.1 Traditional Network Device

SDN (SOFTWARE-DEFINED NETWORKING)

SDN is defined by "the decoupling of control and packet forwarding planes in the network". It enables networks to directly connect to applications through application programming interfaces (APIs), bolstering application performance and security, and creating a flexible, dynamic network architecture that can be changed as needed. A network paradigm that yields programmatic management and control, and network resource optimization, SDN applies open APIs to help maintain network control.

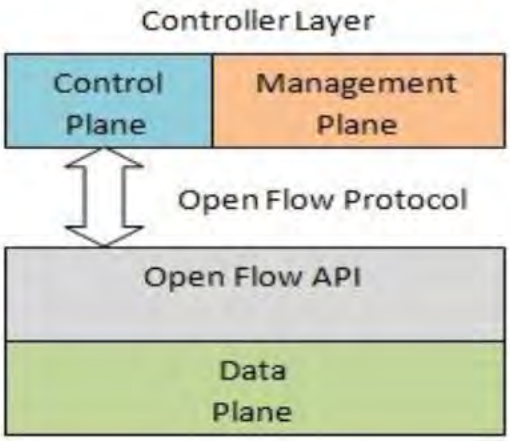

Figure 1.2 SDN Architecture

DIFFERENCES BETWEEN SDN AND TRADITIONAL NETWORKING

Table 1.1 Differences between SDN and traditional networking

Traditional Networking	Software Defined Networking
They are Static and inflexible networks. They are not useful for new business ventures. They possess little agility and flexibility	They are programmable networks during deployment time as well as at later stage based on change in the requirements. They help new business ventures through flexibility, agility and virtualization.
They are Hardware appliances.	They are configured using open software.
They have distributed control plane.	They have logically centralized control plane.
They use custom ASICs and FPGAs.	They use merchant silicon.

NETWORK ARCHITECTURE

Network architecture is the design of a communications network. It is a framework for the specification of a network's physical components and their functional organization and configuration. In telecommunication, the specification of a network architecture may also include a detailed description of products and services delivered via a communications network, as well as detailed rate and billing structures under which services are compensated. The network architecture of the Internet is predominantly expressed by its use of the Internet Protocol Suite, rather than a specific model for interconnecting networks or nodes in the network, or the usage of specific types of hardware link.

COMPUTER NETWORK'S CLASSIFICATIONS & TYPES

There are three types of network classification

- LAN (Local Area Network)
- MAN (Metropolitan Area Network)
- WAN (Wide Area Network)

Figure 1.3 Computer Network: Classifications

Local Area Network (LAN): LAN is a group of the computers placed in the same room, same floor, or the same building so they are connected to each other to form a single network to share their resources such as disk drives, data, CPU, modem etc. LAN is limited to some geographical area less than 2 km. Most of LAN is used widely is an Ethernet system of the bus topology.

Figure 1.4 Local Area Network

Metropolitan Area Network (MAN): The metropolitan area network is a large computer network that expands a Metropolitan area or campus. Its geographic area between a WAN and LAN. Its expand round 50km devices used are modem and wire/cable.

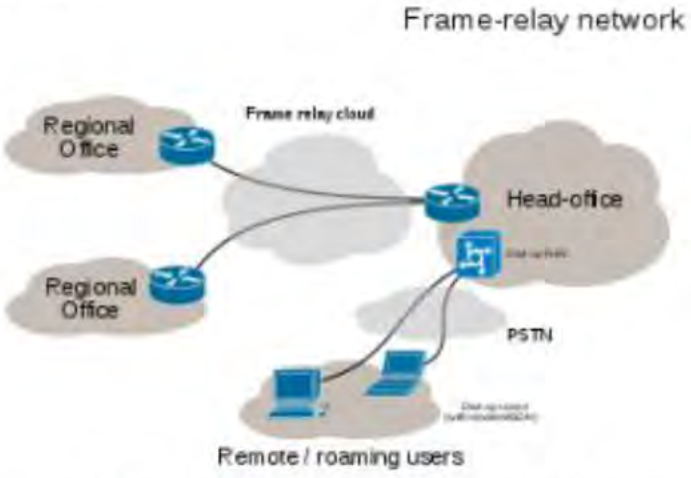

Figure 1.5 Metropolitan Area network

Wide area Network (WAN): The wide area network is a network which connects the countries, cities or the continents; it is a public communications links. The most popular example of a WAN is the internet. WAN is used to connect LAN so the users and the computer in the one location can communicate with each other.

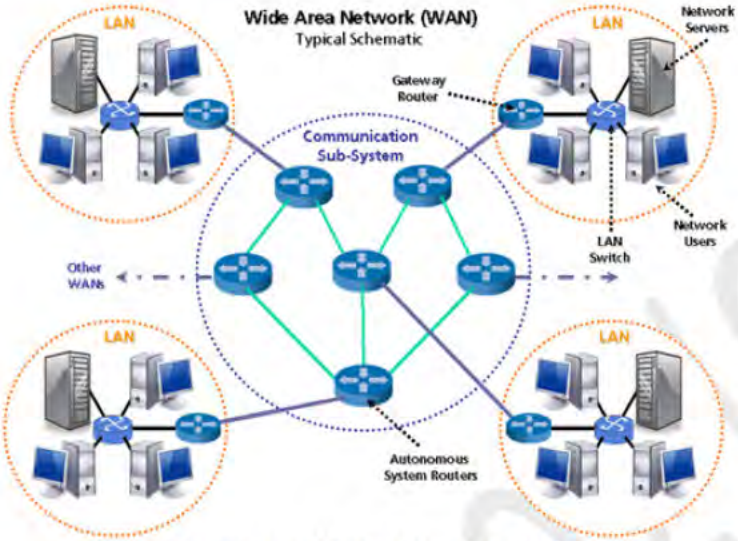

Figure 1.6 Wide Area Network

INTERNET

It is a worldwide/global system of interconnected computer networks. It uses the standard Internet Protocol (TCP/IP). Every computer in Internet is identified by a unique IP address. IP Address is a unique set of numbers (such as 110.22.33.114) which identifies a computer's location. A special computer DNS (Domain Name Server) is used to provide a name to the IP Address so that the user can locate a computer by a name

Figure 1.7 Internets

INTRANET

Intranet is the system in which multiple PCs are connected to each other. PCs in intranet are not available to the world outside the intranet. Usually each organization has its own Intranet network and members/employees of that organization can access the computers in their intranet.

Figure 1.8 Intranets

SIMILARITIES BETWEEN INTERNET AND INTRANET

- Intranet uses the internet protocols such as TCP/IP and FTP.
- Intranet sites are accessible via the web browser in a similar way as websites in the internet. However, only members of Intranet network can access intranet hosted sites.
- In Intranet, own instant messengers can be used as similar to yahoo messenger/gtalk over the internet.

DIFFERENCES BETWEEN INTERNET AND INTRANET

- Internet is general to PCs all over the world whereas Intranet is specific to few PCs.
- Internet provides a wider and better access to websites to a large population, whereas Intranet is restricted.
- Internet is not as safe as Intranet. Intranet can be safely privatized as per the need.

NETWORK DEVICES

- **Repeater** – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.
- **Hub** – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.
- **Bridge** – A bridge operates at data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.
- **Switch** – A switch is a multiport bridge with a buffer and a design that can boost its efficiency (a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only. In other words, switch divides collision domain of hosts, but broadcast domain remains same.
- **Routers** – A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

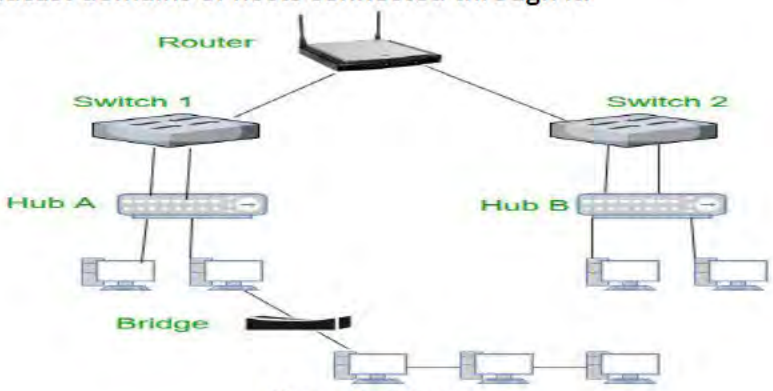

Figure 1.9 Routers

- **Gateway** – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.
- **Brouter** – It is also known as bridging router is a device which combines features of both bridge and router. It can work either at data link layer or at network layer. Working as router, it is capable of routing packets across networks and working as bridge, it is capable of filtering local area network traffic.

REVIEW OF TCP/IP PROTOCOL ARCHITECTURE

The TCP/IP reference model was developed prior to OSI model. The major design goals of this model were,

- To connect multiple networks together so that they appear as a single network.
- To survive after partial subnet hardware failures.
- To provide a flexible architecture.

Unlike OSI reference model, TCP/IP reference model has only 4 layers. They are,

- Host-to-Network Layer
- Internet Layer
- Transport Layer
- Application Layer

Layer 1: Host-to-network Layer

- Lowest layer of the all.
- Protocol is used to connect to the host, so that the packets can be sent over it.
- Varies from host to host and network to network.

Layer 2: Internet layer

- Selection of a packet switching network which is based on a connectionless internetwork layer is called an internet layer.
- It is the layer which holds the whole architecture together.
- It helps the packet to travel independently to the destination.
- Order in which packets are received is different from the way they are sent.
- IP (Internet Protocol) is used in this layer.
- The various functions performed by the Internet Layer are:
    - Delivering IP packets
    - Performing routing
    - Avoiding congestion

Layer 3: Transport Layer

- It decides if data transmission should be on parallel path or single path.
- Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
- The applications can read and write to the transport layer.
- Transport layer adds header information to the data.
- Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
- Transport layer also arrange the packets to be sent, in sequence.

Layer 4: Application Layer

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

- TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
- FTP (File Transfer Protocol) is a protocol that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
- SMTP (Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
- DNS (Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.
- It allows peer entities to carry conversation.
- It defines two end-to-end protocols: TCP and UDP
    - **TCP (Transmission Control Protocol):** It is a reliable connection-oriented protocol which handles byte-stream from source to destination without error and flow control.
    - **UDP (User-Datagram Protocol):** It is an unreliable connection-less protocol that does not want TCPs, sequencing and flow control. Example: One-shot request-reply kind of service.

MERITS OF TCP/IP MODEL

- It operated independently.
- It is scalable.
- Client/server architecture.
- Supports number of routing protocols.
- Can be used to establish a connection between two computers.

DEMERITS OF TCP/IP

- In this, the transport layer does not guarantee delivery of packets.
- The model cannot be used in any other application.
- Replacing protocol is not easy.
- It has not clearly separated its services, interfaces and protocols.

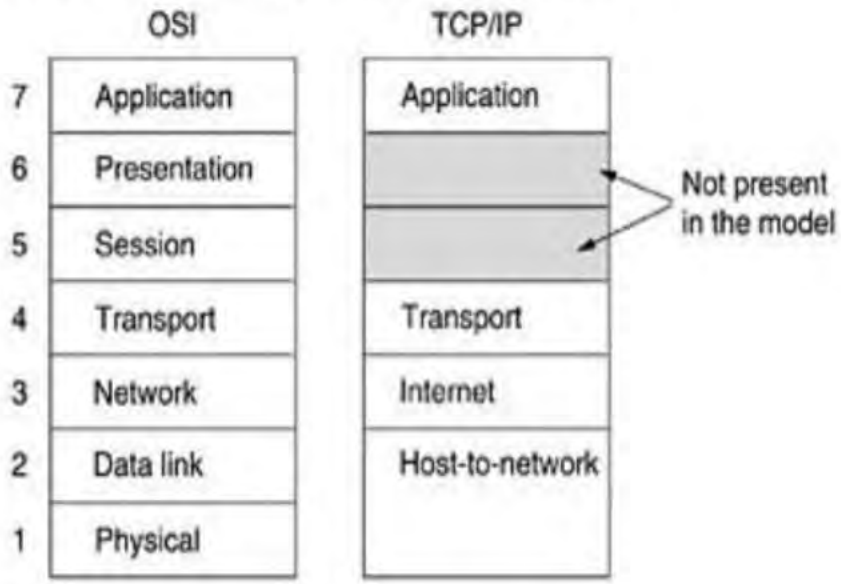

Figure 1.10 TCP/IP Model

Address Resolution Protocol (ARP): Receiver's MAC address is fetched. Through ARP, (32-bit) IP address mapped into (48-bit) MAC address.

Whereas, In Reverse Address Resolution Protocol (RARP), IP address is fetched through server. Through RARP, (48-bit) MAC address of 48 bits mapped into (32-bit) IP address.

Figure 1.11 ARP and RARP

IPv4

IPv4 is a connectionless protocol used for packet-switched networks. Internet Protocol Version 4 (IPv4) is the fourth revision of the Internet Protocol and a widely used protocol in data communication over different kinds of networks. IPv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet. It provides a logical connection between network devices by providing identification for each device. There are many ways to configure IPv4 with all kinds of devices – including manual and automatic configurations – depending on the network type.

IPv4 uses 32-bit addresses for Ethernet communication in five classes: A, B, C, D and E. Classes A, B and C have a different bit length for addressing the network host. Class D addresses are reserved for military purposes, while class E addresses are reserved for future use.IPv4 uses 32-bit (4 byte) addressing, which gives 2^{32} addresses. IPv4 addresses are written in the dot-decimal notation, which comprises of four octets of the address expressed individually in decimal and separated by periods, for instance, 192.168.1.5.

IPv4 Datagram Header Size of the header is 20 to 60 bytes.

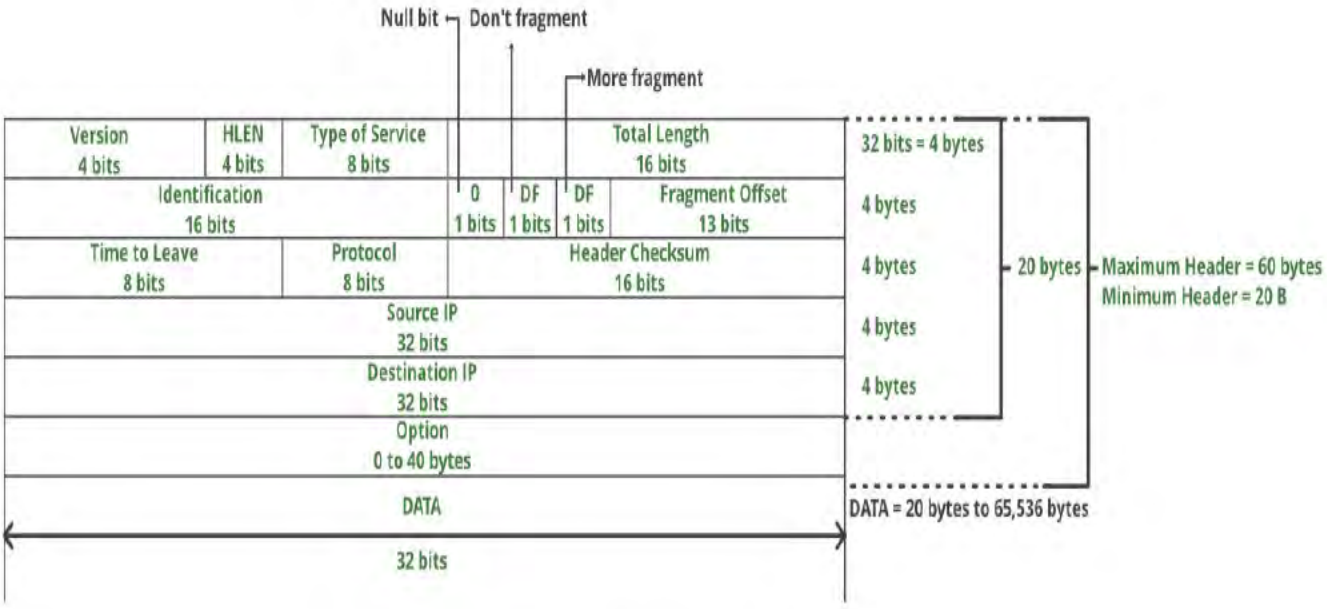

Figure 1.12 IP Header Format

Datagram Delivery Types

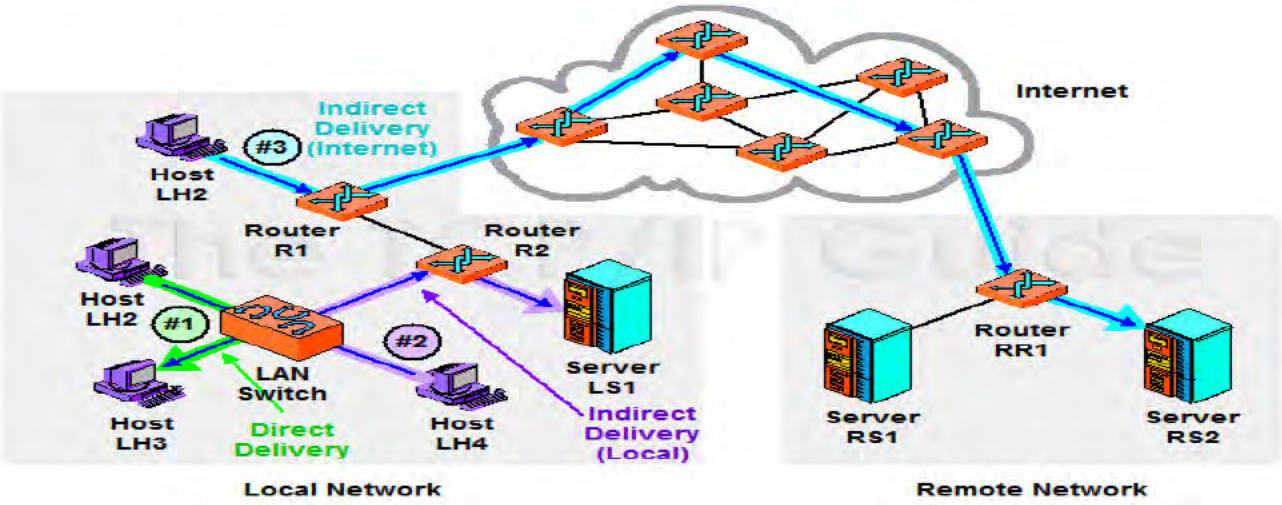

Figure 1.13 Datagram Deliveries

This diagram shows three examples of IP datagram delivery. The first transmission (highlighted in green) shows a direct delivery between two devices on the local network. The second (purple) shows indirect delivery within the local network, between a client and server separated by a router. The third shows a more distant indirect delivery, between a client on the local network and a server across the Internet.

- **Direct Datagram Deliveries:** When datagram's are sent between two devices on the same physical network, it is possible for datagram's to be delivered directly from the source to the destination. Imagine that you want to deliver a letter to a neighbor on your street. You probably wouldn't bother mailing it through the post office; you'd just put the neighbor's name on the envelope and stick it right into his or her mailbox.

- **Indirect Datagram Deliveries:** When two devices are not on the same physical network, the delivery of datagram's from one to the other is indirect. Since the source device can't see the destination on its local network, it must send the datagram through one or more intermediate devices to deliver it. Indirect delivery is analogous to mailing a letter to a friend in a different city.

ROUTERS

A Router is a networking device that forwards data packets between computer networks. This device is usually connected to two or more different networks. When a data packet comes to a router port, the router reads address information in packet to determine out which port the packet will be sent. For example, a router provides you with the internet access by connecting your LAN with the Internet.

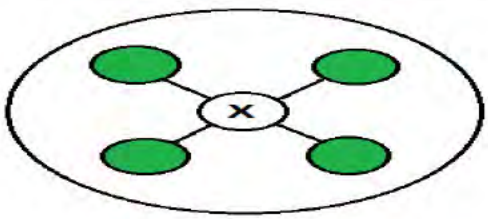

Figure 1.14 Router Network

When a packet arrives at a Router, it examines destination IP address of a received packet and makes routing decisions accordingly. Routers use Routing Tables to determine out which interface the packet will be sent. A routing table lists all networks for which routes are known. Each router's routing table is unique and stored in the RAM of the device.

Routing Table

A routing table is a set of rules, often viewed in table format, that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. All IP-enabled devices, including routers and switches, use routing tables. See below a Routing Table:

Destination	Subnet mask	Interface
128.75.43.0	255.255.255.0	Eth0

The entry corresponding to the default gateway configuration is a network destination of 0.0.0.0 with a network mask (net mask) of 0.0.0.0. The Subnet Mask of default route is always 255.255.255.255.

Entries of an IP Routing Table

A routing table contains the information necessary to forward a packet along the best path toward its destination. Each packet contains information about its origin and destination. Routing Table provides the device with instructions for sending the packet to the next hop on its route across the network. Each entry in the routing table consists of the following entries:

- **Network ID:** The network ID or destination corresponding to the route.
- **Subnet Mask:** The mask that is used to match a destination IP address to the network ID.
- **Next Hop:** The IP address to which the packet is forwarded
- **Outgoing Interface:** Outgoing interface the packet should go out to reach the destination network.
- **Metric:** A common use of the metric is to indicate the minimum number of hops (routers crossed) to the network ID.

ICMP (INTERNET CONTROL MESSAGE PROTOCOL)

ICMP (Internet Control Message Protocol) is an error-reporting protocol network devices like routers use to generate error messages to the source IP address when network problems prevent delivery of IP packets. ICMP creates and sends messages to the source IP address indicating that a gateway to the Internet that a router, service or host cannot be reached for packet delivery. Any IP network device has the capability to send, receive or process ICMP messages.

	Bit 0–7	Bit 8–15	Bit 16–23	Bit 24–31
0	Type	Code	Checksum	
32	Header Information			

Figure 1.15 ICMP Header Format

Although ICMP header is different for each message type, 3 fields of the beginning are similar in all messages. The total size of these 3 fields is 4 byte. These fields are being given in detail.

- **Type:** This defines the type of field message. For example, when doing any type of error report, the code related to that error is defined in this field. Similarly if there is a query message then this field will come in that query's code.
- **Code:** For error messages, this defines the sub type of field error. For example, if the destination unreachable error has occurred, then the code field will indicate what type of destination is unreachable error such as network unreachable (code 0), host unreachable (code 1) or protocol unreachable (code 2) error etc. These sub types of Errors are also defined by codes.
- **Checksum:** The checksum is calculated by the header and the data that is used to detect the errors.
- **Rest of the Header:** As you know the ICMP message is encapsulated in the IP datagram. Rest of the header section in the ICMP message shows the remaining IP header.
- **Data:** In the context of error messages, the packet in this section contains the complete information of the packet.

SUB NETTING

Computer networks can be broken into many networks or small networks can be combined to form large networks depending upon our needs. This is done by IP sub netting and Super netting. Suppose we have a class C network having network ID as 201.10.1.0(range of class C 192–223). So the total number of hosts is 256(for class C host is defined by last octet i.e. 2^8). But, the total usable host is 254. This is because the first IP address is for the network ID and the last IP address is Direct Broadcast Address (for sending any packet from one network to all other hosts of another network). So, in subnetting we will divide these 254 hosts logically into two networks. In the above class C network, we have 24 bits for Network ID and the last 8 bits for the Host ID. We are going to borrow the left-most bit of the host address and declare for identifying the subnet. If the leftmost bit of the host address is 0 then it is the 1st subnet network and if the leftmost bit is 1 then it would be 2nd subnet network. Using 1 bit we can divide it into 2 networks i.e. 2^1. If we want to divide it into four networks then we need 2 bits(2^2=4 networks). The range of IP address which is in 1st subnet network is from 201.10.1.0 to 201.10.1.127. The range of IP address that lies in the 2nd subnet network is from 201.10.1.128 to 201.10.1.255.

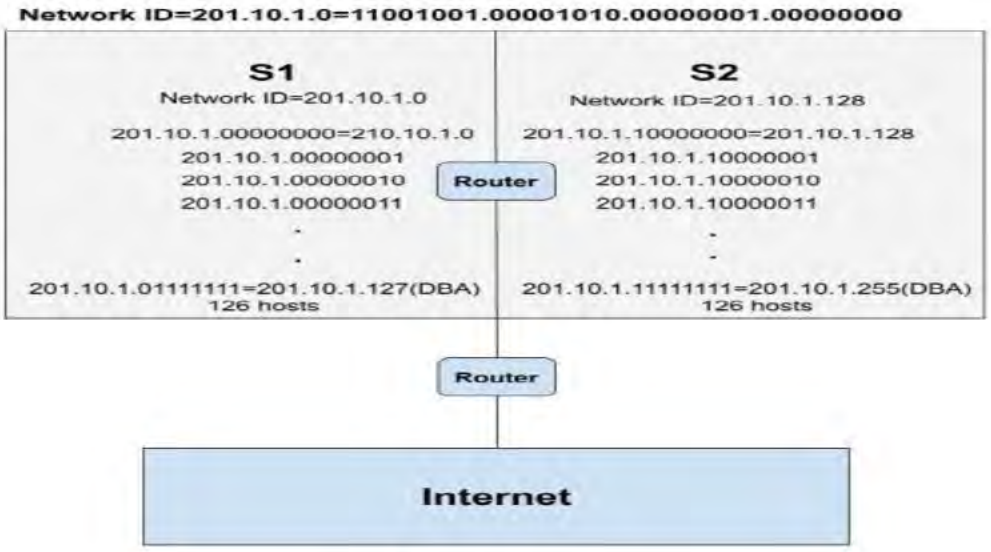

Figure 1.16 Sub-Netting

In the 1st subnet network (S1), we have a total of 126 hosts only because the first and last IP address is reserved for the network ID and the Direct Broadcast Address respectively. Similarly, in the 2nd subnet network, we have 126 hosts.

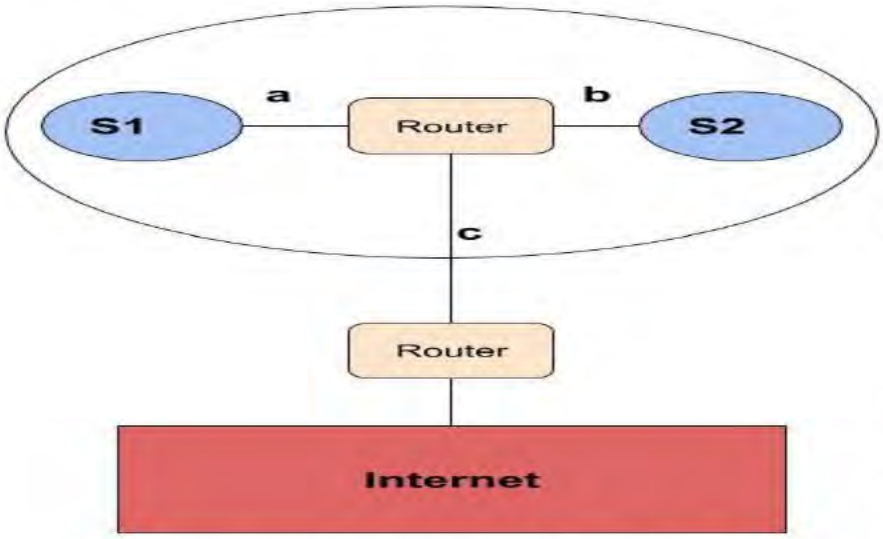

Figure 1.17 Sub-netting Network

The subnet mask is represented as 11111111.11111111.11111111.10000000 i.e. 255.255.255.128 for the above network. The router inside the network will have the routing table which will be as follows:

Network ID	Subnet Mask	Interface
201.10.1.0	255.255.255.128	a
201.10.1.128	255.255.255.128	b

Routing Table

Figure 1.18 Sub netting Routing Table

SUPER NETTING

Super Netting is the opposite of Sub netting. In sub netting, a single big network is divided into multiple smaller sub networks. In Super netting, multiple networks are combined into a bigger network termed as a Super network or Super net. Super netting is mainly used in Route Summarization, where routes to multiple networks with similar network prefixes are combined into a single routing entry, with the routing entry pointing to a Super network, encompassing all the networks. This in turn significantly reduces the size of routing tables and also the size of routing updates exchanged by routing protocols. More specifically,

- When multiple networks are combined to form a bigger network, it is termed as super-netting
- Super netting is used in route aggregation to reduce the size of routing tables and routing table updates

There are some points which should be kept in mind while Super netting:

- All the IP address should be contiguous.
- Size of all the small networks should be equal and must be in form of 2^n.
- First IP address should be exactly divisible by whole size of super net.

Example – Suppose 4 small networks of class C:

200.1.0.0, 200.1.1.0, 200.1.2.0, 200.1.3.0

Build a bigger network which has a single Network Id.

Explanation – Before Super netting routing table will be look like as:

Network Id	Subnet Mask	Interface
200.1.0.0	255.255.255.0	A
200.1.1.0	255.255.255.0	B
200.1.2.0	255.255.255.0	C

First, lets check whether three condition are satisfied or not:

- **Contiguous:** You can easily see that all network are contiguous all having size 256 hosts. Range of first Network from 200.1.0.0 to 200.1.0.255. If you add 1 in last IP address of first network that is 200.1.0.255 + 0.0.0.1, you will get the next network id that is 200.1.1.0. Similarly, check that all network are contiguous.
- **Equal size of all networks:** As all networks are of class C, so all of the have a size of 256 which in turn equal to 2^8.
- **First IP address exactly divisible by total size:** When a binary number is divided by 2^n then last n bits are the remainder. Hence in order to prove that first IP address is exactly divisible by while size of Super net Network. You can check that if last n v=bits are 0 or not.

In given example first IP is 200.1.0.0 and whole size of super net is $4*2^8 = 2^{10}$. If last 10 bits of first IP address are zero then IP will be divisible.

11001000	00000001	00000000	00000000
200 .	1 .	0 .	0

Figure 1.19 Subnet Mask

Last 10 bits of first IP address are zero (highlighted by green color). So 3rd condition is also satisfied.

Therefore, you can join all these 4 networks and can make a Super net. New Super net Id will be 200.1.0.0.

Advantages of Super Netting –

- Control and reduce network traffic
- Helpful to solve the problem of lacking IP addresses
- Minimizes the routing table

Disadvantages of Super netting –

- It cannot cover different area of network when combined
- All the networks should be in same class and all IP should be contiguous

CIDR NOTATION

A system called Classless Inter-Domain Routing, or CIDR, was developed as an alternative to traditional sub netting. The idea is that you can add a specification in the IP address itself as to the number of significant bits that make up the routing or networking portion. For example, we could express the idea that the IP address 192.168.0.15 is associated with the net mask 255.255.255.0 by using the CIDR notation of 192.168.0.15/24. This means that the first 24 bits of the IP address given are considered significant for the network routing.

CIDR is based on variable-length subnet masking (VLSM). This allows it to define prefixes of arbitrary lengths making it much more efficient than the old system. CIDR IP addresses are composed of two sets of numbers. The network address is written as a prefix, like you would see a normal IP address (e.g. 192.255.255.255). The second part is the suffix which indicates how many bits are in the entire address (e.g. /12). Putting it together, a CIDR IP address would look like the following:

192.255.255.255/12

The network prefix is also specified as part of the IP address. This varies depending upon the number of bits required. Therefore, taking the example above, we can say that the first 12 bits are the network part of the address while the last 20 bits are for host addresses.

DNS

An application layer protocol defines how the application processes running on different systems, pass the messages to each other.

- DNS stands for Domain Name System.
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
- For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain name is more reliable than IP address.

DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.

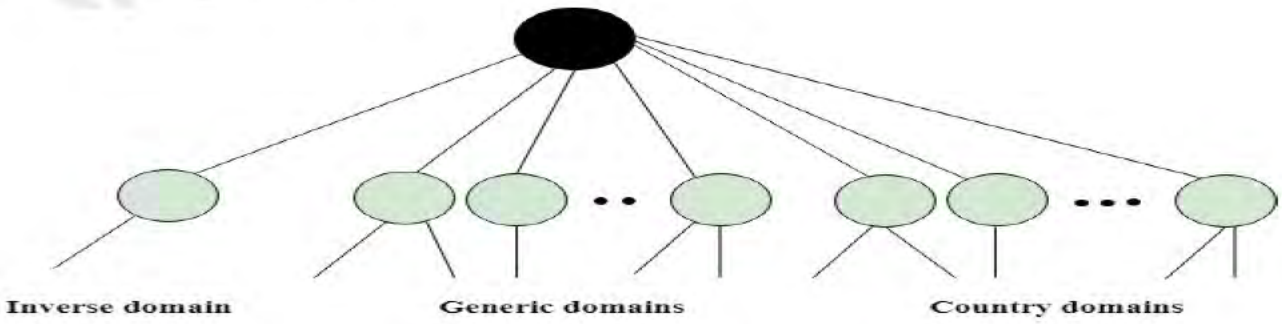

Figure 1.20 DNS

Generic Domains

- It defines the registered hosts according to their generic behavior.
- Each node in a tree defines the domain name, which is an index to the DNS database.
- It uses three-character labels, and these labels describe the organization type.

Table 1.3 Description

Label	Description
aero	Airlines and aerospace companies
biz	Businesses or firms
com	Commercial Organizations
coop	Cooperative Business Organizations

NAT, SNAT, DNAT, NAT

NAT is the magic that lets you share a single public IP address with a whole private subnet, and to run public servers with private no routable addresses. Suppose you have a typical low-cost DSL Internet account. You have only a single public IP address, and a LAN of 25 workstations, laptops, and servers, protected by a nice iptables NAT firewall. Your entire network will appear to the outside world as a single computer. Source NAT (SNAT) rewrites the source addresses of all outgoing packets to the firewall address. It works the other way as well. While having public routable IP addresses is desirable for public services, like web and mail servers, you can get by on the cheap without them and run public servers on private addresses. Destination NAT (DNAT) rewrites the destination address, which is the firewall address, to the real server addresses, then ip tables forwards incoming traffic to these servers.

PRIVATE IP ADDRESS

Home routers have their local address set to a default, private IP address number. It's usually the same address for the other models from that manufacturer, and it can be seen in the manufacturer's documentation. The concept of private IP addressing was developed to address the IP address exhaustion problem. The private IP addresses can be used on the private network of any organization in the world and are not globally unique. Internet routers are configured to discard any packets coming from the private IP address ranges, so these addresses are not routable on the Internet.

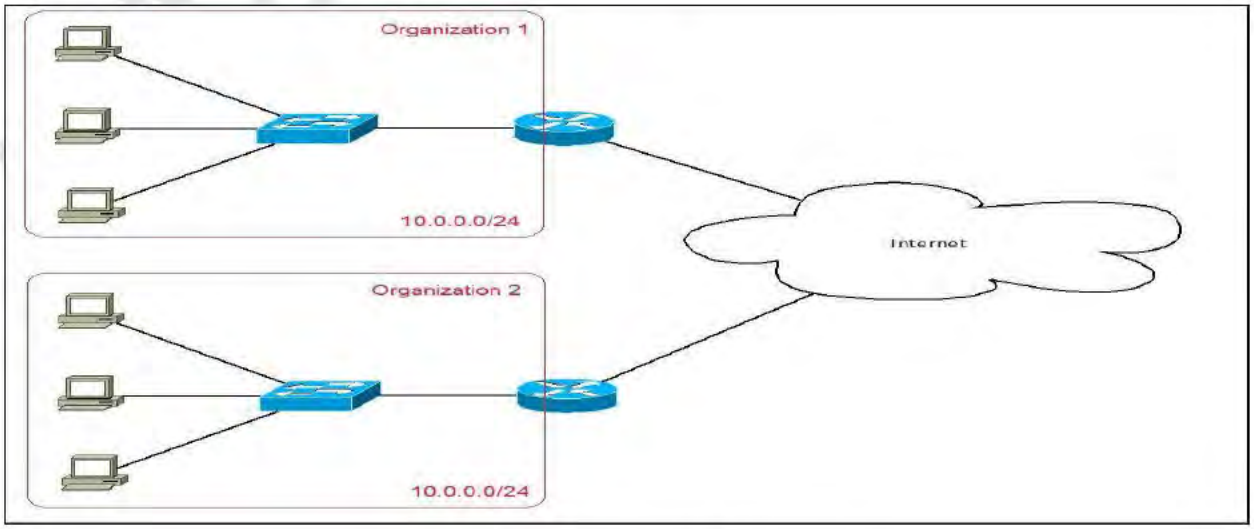

Figure 1.21 Private IP Addressing

In the above figure you can see that two organizations use the same private IP network (10.0.0.0/24) inside their respective internal networks. Because private IP addresses are not globally unique, both organizations can use private IP addresses from the same range. To access the Internet, the organizations can use a technology called Network Address Translation (NAT), which we will describe in the later lessons.

There are three ranges of addresses that can be used in a private network:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

FIREWALLS

A firewall is a type of cyber security tool that is used to filter traffic on a network. Firewalls can be used to separate network nodes from external traffic sources, internal traffic sources, or even specific applications. Firewalls can be software, hardware, or cloud-based, with each type of firewall having its own unique pros and cons. The primary goal of a firewall is to block malicious traffic requests and data packets while allowing legitimate traffic through. Firewall types can be divided into several different categories based on their general structure and method of operation. Here are eight types of firewalls:

- Packet-filtering firewalls
- Circuit-level gateways
- Stateful inspection firewalls
- Application-level gateways (a.k.a. proxy firewalls)
- Next-gen firewalls
- Software firewalls
- Hardware firewalls
- Cloud firewalls

VLAN

VLAN is a logical grouping of networking devices. When we create VLAN, we actually break large broadcast domain in smaller broadcast domains. Consider VLAN as a subnet. Same as two different subnets cannot communicate with each other without router, different VLANs also requires router to communicate.

Advantage of VLAN

VLAN provides following advantages:-

- Solve broadcast problem
- Reduce the size of broadcast domains
- Allow us to add additional layer of security
- Make device management easier
- Allow us to implement the logical grouping of devices by function instead of location

DIFFERENCE BETWEEN LAN AND VLAN

Table 1.4 Difference between LAN and VLAN

LAN	VLAN
LAN stands for Local Area Network.	VLAN stands for Virtual Local Area Network.

The cost of Local Area Network is high.	The cost of Virtual Local Area Network is less.
The latency of Local Area Network is high.	The latency of Virtual Local Area Network is low.
The devices which are used in LAN are: Hubs, Routers and switch.	The devices which are used in VLAN are: Bridges and switch.
In local area network, the Packet is advertised to each device.	In virtual local area network, packet is send to specific broadcast domain.

There are 5 main types of VLANs depending on the type of the network they carry:

- **Default VLAN** –When the switch initially starts up, all switch ports become a member of the default VLAN (generally all switches have default VLAN named as VLAN 1), which makes them all part of the same broadcast domain. Using default VLAN allows any network device connected to any of the switch port to connect with other devices on other switch ports. One unique feature of Default VLAN is that it can't be rename or delete.
- **Data VLAN** –Data VLAN is used to divide the whole network into 2 groups. One group of users and other group of devices. This VLAN also known as a user VLAN, the data VLAN is used only for user-generated data. This VLAN carrying data only. It is not used for carrying management traffic or voice.
- **Voice VLAN** –Voice VLAN is configured to carry voice traffic. Voice VLANs are mostly given high transmission priority over other types of network traffic. To ensure voice over IP (VoIP) quality (delay of less than 150 milliseconds (ms) across the network), we must have separate voice VLAN as this will preserve bandwidth for other applications.
- **Management VLAN** –A management VLAN is configured to access the management capabilities of a switch (traffic like system logging, monitoring). VLAN 1 is the management VLAN by default (VLAN 1 would be a bad choice for the management VLAN). Any of a switch VLAN could be define as the management VLAN if admin as not configured a unique VLAN to serve as the management VLAN. This VLAN ensures that bandwidth for management will be available even when user traffic is high.
- **Native VLAN** –This VLAN identifies traffic coming from each end of a trunk link. A native VLAN is allocated only to an 802.1Q trunk port. The 802.1Q trunk port places untagged traffic (traffic that does not come from any VLAN) on the native VLAN. It is a best to configure the native VLAN as an unused VLAN.

VLAN TAGGING

VLAN Tagging, also known as Frame Tagging, is a method developed by Cisco to help identify packets travelling through trunk links. When an Ethernet frame traverses a trunk link, a special VLAN tag is added to the frame and sent across the trunk link.

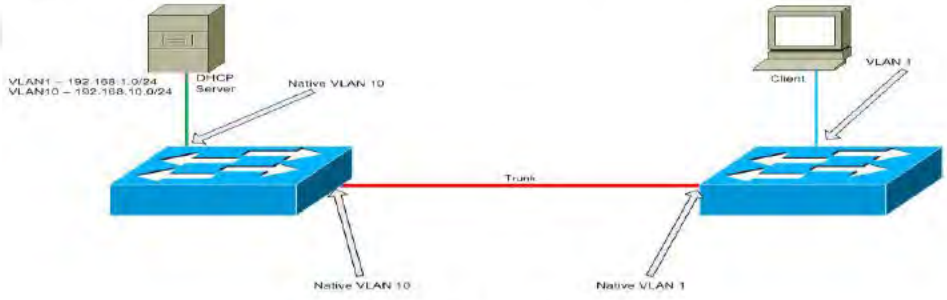

Figure 1.22 VLAN TAGGING

As it arrives at the end of the trunk link the tag is removed and the frame is sent to the correct access link port according to the switch's table, so that the receiving end is unaware of any VLAN information.

IPv6 address

An IPv6 address is 4 times larger than IPv4, but surprisingly, the header of an IPv6 address is only 2 times larger than that of IPv4. IPv6 headers have one Fixed Header and zero or more Optional (Extension) Headers. All the necessary information that is essential for a router is kept in the Fixed Header. The Extension Header contains optional information that helps routers to understand how to handle a packet/flow.

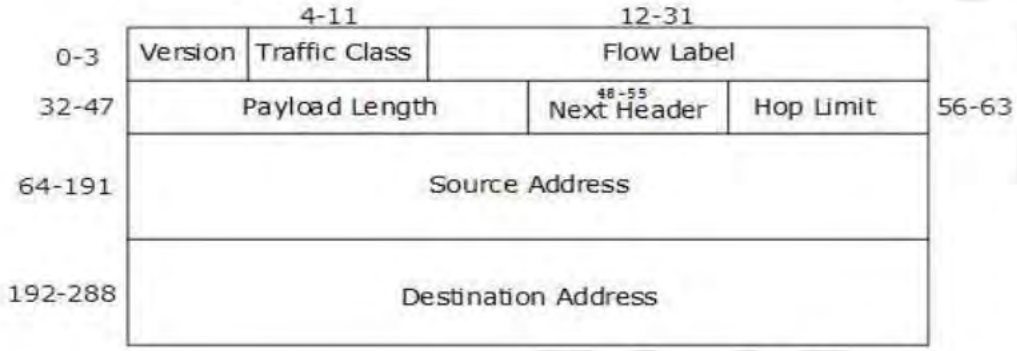

Figure 1.23 IPV6 Address

IPv6 fixed header is 40 bytes long and contains the following information.

Table 1.5 Header Format Details

S.N.	Field & Description
1	**Version** (4-bits): It represents the version of Internet Protocol, i.e. 0110.
2	**Traffic Class** (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).
3	**Flow Label** (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media.
4	**Payload Length** (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0.
5	**Next Header** (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4's.

6	**Hop Limit** (8-bits): This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0 the packet is discarded.
7	**Source Address** (128-bits): This field indicates the address of originator of the packet.
8	**Destination Address** (128-bits): This field provides the address of intended recipient of the packet.

ADDRESS STRUCTURE

An IPv6 address is made of 128 bits divided into eight 16-bits blocks. Each block is then converted into 4-digit Hexadecimal numbers separated by colon symbols.

For example, given below is a 128 bit IPv6 address represented in binary format and divided into eight 16-bits blocks:

0010000000000001 0000000000000000 0011001000111000 1101111111100001 0000000001100011 0000000000000000 0000000000000000 1111111011111011

Each block is then converted into Hexadecimal and separated by ':' symbol:

2001:0000:3238:DFE1:0063:0000:0000:FEFB

Even after converting into Hexadecimal format, IPv6 address remains long. IPv6 provides some rules to shorten the address. The rules are as follows:

Rule.1: Discard leading Zero(es):

In Block 5, 0063, the leading two 0s can be omitted, such as (5th block):

2001:0000:3238:DFE1:63:0000:0000:FEFB

Rule.2: If two of more blocks contain consecutive zeroes, omit them all and replace with double colon sign ::, such as (6th and 7th block):

2001:0000:3238:DFE1:63::FEFB

Consecutive blocks of zeroes can be replaced only once by :: so if there are still blocks of zeroes in the address, they can be shrunk down to a single zero, such as (2nd block):

2001:0:3238:DFE1:63::FEFB

IPv6 Address Space

The 128 bits of IPv6 addresses mean the size of the IPv6 address space is, quite literally, astronomical; like the numbers that describe the number of stars in a galaxy or the distance to the furthest pulsars, the number of addresses that can be supported in IPv6 is mind-boggling.

Since IPv6 addresses are 128 bits long, the theoretical address space if all addresses were used is 2^{128} addresses. Consider:

- It's enough addresses for many trillions of addresses to be assigned to every human being on the planet.
- The earth is about 4.5 billion years old. If we had been assigning IPv6 addresses at a rate of 1 billion per second since the earth was formed, we would have by now used up less than one trillionth of the address space.
- The earth's surface area is about 510 trillion square meters. If a typical computer has a footprint of about a tenth of a square meter, we would have to stack computers 10 billion high blanketing the entire surface of the earth to use up that same trillionth of the address space.

RGPVNOTES.IN

Thank you for using our services. Please support us so that we can improve further and help more people.
https://www.rgpvnotes.in/support-us

If you have questions or doubts, contact us on
WhatsApp at +91-8989595022 or by email at hey@rgpvnotes.in.

For frequent updates, you can follow us on
Instagram: https://www.instagram.com/rgpvnotes.in/.