UNIT V
INTERNET PROTOCOL

Internet Protocols are a set of rules that governs the communication and exchange of data over the internet. Both the sender and receiver should follow the same protocols in order to communicate the data. In order to understand it better, let’s take an example of a language. Any language has its own set of vocabulary and grammar which we need to know if we want to communicate in that language. Similarly, over the internet whenever we access a website or exchange some data with another device then these processes are governed by a set of rules called the internet protocols.

Working of Internet Protocol

The internet and many other data networks work by organizing data into small pieces called packets. Each large data sent between two network devices is divided into smaller packets by the underlying hardware and software. Each network protocol defines the rules for how its data packets must be organized in specific ways according to the protocols the network supports.

Need of Protocols

It may be that the sender and receiver of data are parts of different networks, located in different parts of the world having different data transfer rates. So, we need protocols to manage the flow control of data, and access control of the link being shared in the communication channel. Suppose there is a sender X who has a data transmission rate of 10 Mbps. And, there is a receiver Y who has a data receiving rate of 5Mbps. Since the rate of receiving the data is slow so some data will be lost during transmission. In order to avoid this, receiver Y needs to inform sender X about the speed mismatch so that sender X can adjust its transmission rate. Similarly, the access control decides the node which will access the link shared in the communication channel at a particular instant in time. If not the transmitted data will collide if many computers send data simultaneously through the same link resulting in the corruption or loss of data.

What is IP Addressing?

An IP address represents an Internet Protocol address. A unique address that identifies the device over the network. It is almost like a set of rules governing the structure of data sent over the Internet or through a local network. An IP address helps the Internet to distinguish between different routers, computers, and websites. It serves as a specific machine identifier in a specific network and helps to improve visual communication between source and destination.

INTERNET PROTOCOL FUNCTION

Function

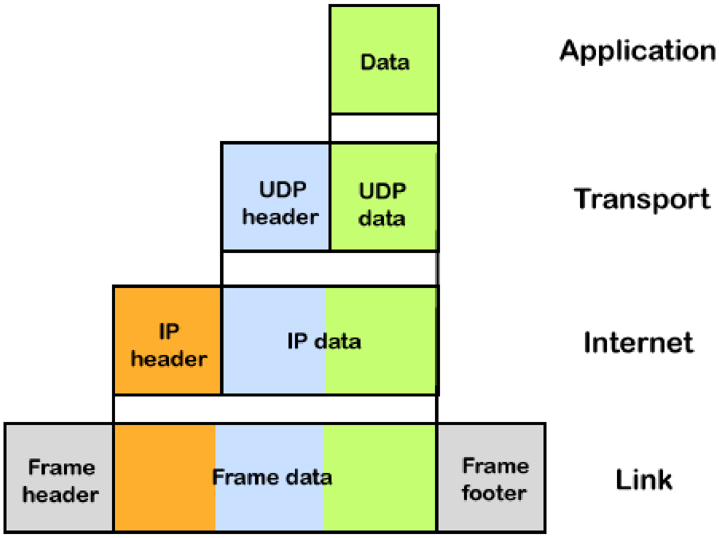
The main function of the internet protocol is to provide addressing to the hosts, encapsulating the data into a packet structure, and routing the data from source to the destination across one or more IP networks. In order to achieve these functionalities, internet protocol provides two major things which are given below.

An internet protocol defines two things:

- Format of IP packet
- IP Addressing system

What is an IP packet?

Before an IP packet is sent over the network, two major components are added in an IP packet, i.e., **header** and a **payload**.



An IP header contains lots of information about the IP packet which includes:

- Source IP address: The source is the one who is sending the data.
- Destination IP address: The destination is a host that receives the data from the sender.
- Header length
- Packet length
- TTL (Time to Live): The number of hops occurs before the packet gets discarded.
- Transport protocol: The transport protocol used by the internet protocol, either it can be TCP or UDP.

There is a total of 14 fields exist in the IP header, and one of them is optional.

Payload: Payload is the data that is to be transported.

How does the IP routing perform?

IP routing is a process of determining the path for data so that it can travel from the source to the destination. As we know that the data is divided into multiple packets, and each packet will pass through a web of the router until it reaches the final destination. The path that the data packet follows is determined by the routing algorithm. The routing algorithm considers various factors like the size of the packet and its header to determine the efficient route for the data from the source to the destination. When the data packet reaches some router, then the source address and destination address are used with a routing table to determine the next hop's address. This process goes on until it reaches the destination. The data is divided into multiple packets so all the packets will travel individually to reach the destination.

For example, when an email is sent from the email server, then the TCP layer in this email server divides the data into multiple packets, provides numbering to these packets and transmits them to the IP layer. This IP layer further transmits the packet to the destination email server. On the side of the destination server, the IP layer transmits these data packets to the TCP layer, and the TCP layer recombines these data packets into the message. The message is sent to the email application.

What is IP Addressing?

An IP address is a unique identifier assigned to the computer which is connected to the internet. Each IP address consists of a series of characters like 192.168.1.2. Users cannot access the domain name of each website with the help of these characters, so DNS resolvers are used that convert the human-readable domain names into a series of characters. Each IP packet contains two addresses, i.e., the IP address of the device, which is sending the packet, and the IP address of the device which is receiving the packet.

Types of IP addresses

IPv4 addresses are divided into two categories:

- **Public address**
- **Private address**

Public address

The public address is also known as an external address as they are grouped under the WAN addresses. We can also define the public address as a way to communicate outside the network. This address is used to access the internet. The public address available on our computer provides the remote access to our computer. With the help of a public address, we can set up the home server to access the internet. This address is generally assigned by the ISP (Internet Service Provider).

Key points related to public address are:

- The scope of the public address is global, which means that we can communicate outside the network.
- This address is assigned by the ISP (Internet Service Provider).
- It is not available at free of cost.
- We can get the Public IP by typing on Google "What is my IP".

Private address

A private address is also known as an internal address, as it is grouped under the LAN addresses. It is used to communicate within the network. These addresses are not routed on the internet so that no traffic can come from the internet to this private address. The address space for the private address is allocated using **InterNIC** to create our own network. The private addresses are assigned to mainly those computers, printers, smartphones, which are kept inside the home or the computers that are kept within the organization. For example, a private address is assigned to the printer, which is kept inside our home, so that our family member can take out the print from the printer.

If the computer is assigned with a private address, then the devices available within the local network can view the computer through the private ip address. However, the devices available outside the local network cannot view the computer through the private IP address, but they can access the computer if they know the router's public address. To access the computer directly, NAT (Network Address Translator) is to be used.

Key points related to private address are:

- Its scope is local, as we can communicate within the network only.
- It is generally used for creating a local area network.
- It is available at free of cost.
- We can get to know the private IP address by simply typing the "ipconfig" on the command prompt.

INTRODUCTION OF INTERNETWORKING

Internetworking is combined of 2 words, inter and networking which implies an association between totally different nodes or segments. This connection area unit is established through intercessor devices akin to routers or gateway. The first term for associate degree internetwork was catenet. This interconnection is often among or between public, private, commercial, industrial, or governmental networks. Thus, associate degree internetwork could be an assortment of individual networks, connected by intermediate networking devices, that function as one giant network. Internetworking refers to the trade, products, and procedures that meet the challenge of making and administering internet works.

To enable communication, every individual network node or phase is designed with a similar protocol or communication logic, that is Transfer Control Protocol (TCP) or Internet Protocol (IP). Once a network communicates with another network having constant communication procedures, it’s called Internetworking. Internetworking was designed to resolve the matter of delivering a packet of information through many links.

There is a minute difference between extending the network and Internetworking. Merely exploitation of either a switch or a hub to attach 2 local area networks is an extension of LAN whereas connecting them via the router is an associate degree example of Internetworking. Internetworking is enforced in Layer three (Network Layer) of the OSI-ISO model. The foremost notable example of internetworking is the Internet.

There is chiefly 3 units of Internetworking:

1. Extranet
2. Intranet
3. Internet

Intranets and extranets might or might not have connections to the net. If there is a connection to the net, the computer network or extranet area unit is usually shielded from being accessed from the net if it is not authorized. The net isn’t thought-about to be a section of the computer network or extranet, though it should function as a portal for access to parts of the associate degree extranet.

1. **Extranet –** It’s a network of the internetwork that’s restricted in scope to one organization or entity however that additionally has restricted connections to the networks of one or a lot of different sometimes, however not essential. It’s the very lowest level of Internetworking, usually enforced in an exceedingly personal area. Associate degree extranet may additionally be classified as a Man, WAN, or different form of network however it cannot encompass one local area network i.e. it should have a minimum of one reference to associate degree external network.
2. **Intranet –** This associate degree computer network could be a set of interconnected networks, which exploits the Internet Protocol and uses IP-based tools akin to web

browsers and FTP tools, that are underneath the management of one body entity. That body entity closes the computer network to the remainder of the planet and permits solely specific users. Most typically, this network is the internal network of a corporation or different enterprise. An outsized computer network can usually have its own internet server to supply users with browsable data.

3. **Internet –** A selected Internetworking, consisting of a worldwide interconnection of governmental, academic, public, and personal networks based mostly upon the Advanced analysis comes Agency Network (ARPANET) developed by ARPA of the U.S. Department of Defense additionally home to the World Wide Web (WWW) and cited as the 'Internet' to differentiate from all different generic Internetworks. Participants within the web, or their service suppliers, use IP Addresses obtained from address registries that manage assignments.

Internetworking has evolved as an answer to a few key problems: isolated LANs, duplication of resources, and an absence of network management. Isolated LANs created transmission problems between totally different offices or departments. Duplication of resources meant that constant hardware and code had to be provided to every workplace or department, as did a separate support employee. This lack of network management meant that no centralized methodology of managing and troubleshooting networks existed.

One more form of the interconnection of networks usually happens among enterprises at the Link Layer of the networking model, i.e. at the hardware-centric layer below the amount of the TCP/IP logical interfaces. Such interconnection is accomplished through network bridges and network switches. This can be typically incorrectly termed internetworking, however, the ensuing system is just a bigger, single subnetwork, and no internetworking protocol, akin to web Protocol, is needed to traverse these devices.

However, one electronic network is also reborn into associate degree internetwork by dividing the network into phases and logically dividing the segment traffic with routers. The Internet Protocol is meant to supply an associate degree unreliable packet service across the network. The design avoids intermediate network components maintaining any state of the network. Instead, this task is allotted to the endpoints of every communication session. To transfer information correctly, applications should utilize associate degree applicable Transport Layer protocol, akin to Transmission management Protocol (TCP), that provides a reliable stream. Some applications use a less complicated, connection-less transport protocol, User Datagram Protocol (UDP), for tasks that don't need reliable delivery of information or that need period of time service, akin to video streaming or voice chat.

Internetwork Addressing –

Internetwork addresses establish devices severally or as members of a bunch. Addressing schemes differ based on the protocol family and therefore the OSI layer. Three kinds of internetwork addresses area units are ordinarily used: data-link layer addresses, Media Access control (MAC) addresses, and network-layer addresses.

1. **Data Link Layer addresses:** A data-link layer address unambiguously identifies every physical network association of a network device. Data-link addresses typically area units

cited as physical or hardware addresses. Data-link addresses sometimes exist among a flat address area and have a pre-established and usually fastened relationship to a selected device. End systems usually have just one physical network association, and therefore have just one data-link address. Routers and different internetworking devices usually have multiple physical network connections and so eventually have multiple data-link addresses.

2. **MAC Addresses:** Media Access management (MAC) addresses encompass a set of data-link layer addresses. MAC addresses establish network entities in LANs that implement the IEEE MAC addresses of the data-link layer. MAC addresses different area units distinctively for every local area network interface. MAC addresses are forty-eight bits long and are expressed in form of twelve hexadecimal digits. The primary half dozen hexadecimal digits, which are usually administered by the IEEE, establish the manufacturer or merchant and therefore comprise the Organizational Unique Identifier (OUI). The last half dozen positional notation digits comprise the interface serial variety or another price administered by the particular merchant. MAC addresses are typically area units referred to as burned-in addresses (BIAs) as a result of being burned into read-only memory(ROM) and are traced into random-access memory (RAM) once the interface card initializes.
3. **Network-Layer Addresses:** Network addresses sometimes exist among a gradable address area and typically area units referred to as virtual or logical addresses. the connection between a network address and a tool is logical and unfixed, it usually relies either on physical network characteristics or on groupings that don't have any physical basis. finish systems need one network-layer address for every network-layer protocol they support. Routers and different Internetworking devices need one network-layer address per physical network association for every network-layer protocol supported.

Challenges to Internetworking –

Implementing useful internetwork isn't at any certainty. There are several challenging fields, particularly in the areas of dependableness, connectivity, network management, and adaptability, and each and every space is essential in establishing associate degree economical and effective internetwork. A few of them are:-

- The initial challenge lies when we are trying to connect numerous systems to support communication between disparate technologies. For example, Totally different sites might use different kinds of media, or they could operate at variable speeds.
- Another essential thought is reliable service that should be maintained in an internetwork. Individual users and whole organizations depend upon consistent, reliable access to network resources.
- Network management should give centralized support associate degree troubleshooting capabilities on the internetwork. Configuration, security, performance, and different problems should be adequately addressed for the internetwork to perform swimmingly.
- Flexibility, the ultimate concern, is important for network enlargement and new applications and services, among different factors.

Advantages:

Increased connectivity: Internetworking enables devices on different networks to communicate with each other, which increases connectivity and enables new applications and services.

Resource sharing: Internetworking allows devices to share resources across networks, such as printers, servers, and storage devices. This can reduce costs and improve efficiency by allowing multiple devices to share resources.

Improved scalability: Internetworking allows networks to be expanded and scaled as needed to accommodate growing numbers of devices and users.

Improved collaboration: Internetworking enables teams and individuals to collaborate and work together more effectively, regardless of their physical location.

Access to remote resources: Internetworking allows users to access resources and services that are physically located on remote networks, improving accessibility and flexibility.

Disadvantages:

Security risks: Internetworking can create security vulnerabilities and increase the risk of cyberattacks and data breaches. Connecting multiple networks together increases the number of entry points for attackers, making it more difficult to secure the entire system.

Complexity: Internetworking can be complex and requires specialized knowledge and expertise to set up and maintain. This can increase costs and create additional maintenance overhead.

Performance issues: Internetworking can lead to performance issues, particularly if networks are not properly optimized and configured. This can result in slow response times and poor network performance.

Compatibility issues: Internetworking can lead to compatibility issues, particularly if different networks are using different protocols or technologies. This can make it difficult to integrate different systems and may require additional resources to resolve.

Management overhead: Internetworking can create additional management overhead, particularly if multiple networks are involved. This can increase costs and require additional resources to manage effectively

IP OPERATIONS

Internet Protocol

Internet Protocols are of different types having different uses. These are mentioned below:

1. TCP/IP(Transmission Control Protocol/ Internet Protocol)
2. SMTP(Simple Mail Transfer Protocol)
3. PPP(Point-to-Point Protocol)
4. FTP (File Transfer Protocol)
5. SFTP(Secure File Transfer Protocol)
6. HTTP(Hyper Text Transfer Protocol)
7. HTTPS(HyperText Transfer Protocol Secure)

8. TELNET(Terminal Network)
9. POP3(Post Office Protocol 3)
10. IPv4
11. IPv6
12. ICMP
13. UDP
14. IMAP
15. SSH
16. Gopher

1. TCP/IP(Transmission Control Protocol/ Internet Protocol)

These are a set of standard rules that allows different types of computers to communicate with each other. The IP protocol ensures that each computer that is connected to the Internet is having a specific serial number called the IP address. TCP specifies how data is exchanged over the internet and how it should be broken into IP packets. It also makes sure that the packets have information about the source of the message data, the destination of the message data, the sequence in which the message data should be re-assembled, and checks if the message has been sent correctly to the specific destination. The TCP is also known as a connection-oriented protocol.

For more details, please refer TCP/IP Model article.

2. SMTP(Simple Mail Transfer Protocol)

These protocols are important for sending and distributing outgoing emails. This protocol uses the header of the mail to get the email id of the receiver and enters the mail into the queue of outgoing mail. And as soon as it delivers the mail to the receiving email id, it removes the email from the outgoing list. The message or the electronic mail may consider the text, video, image, etc. It helps in setting up some communication server rules.

3. PPP(Point-to-Point Protocol)

It is a communication protocol that is used to create a direct connection between two communicating devices. This protocol defines the rules using which two devices will authenticate with each other and exchange information with each other. For example, A user connects his PC to the server of an Internet Service Provider and also uses PPP. Similarly, for connecting two routers for direct communication it uses PPP.

4. FTP (File Transfer Protocol)

This protocol is used for transferring files from one system to the other. This works on a client-server model. When a machine requests for file transfer from another machine, the FTO sets up a connection between the two and authenticates each other using their ID and Password. And, the desired file transfer takes place between the machines.

5. SFTP(Secure File Transfer Protocol)

SFTP which is also known as SSH FTP refers to File Transfer Protocol (FTP) over Secure Shell (SSH) as it encrypts both commands and data while in transmission. SFTP acts as an extension to SSH and encrypts files and data then sends them over a secure shell data stream. This protocol is used to remotely connect to other systems while executing commands from the command line.

6. HTTP(Hyper Text Transfer Protocol)

This protocol is used to transfer hypertexts over the internet and it is defined by the www(world wide web) for information transfer. This protocol defines how the information needs to be formatted and transmitted. And, it also defines the various actions the web browsers should take in response to the calls made to access a particular web page. Whenever a user opens their web browser, the user will indirectly use HTTP as this is the protocol that is being used to share text, images, and other multimedia files on the World Wide Web.

Note: *Hypertext refers to the special format of the text that can contain links to other texts.*

7. HTTPS(HyperText Transfer Protocol Secure)

HTTPS is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network with the SSL/TLS protocol for encryption and authentication. So, generally, a website has an HTTP protocol but if the website is such that it receives some sensitive information such as credit card details, debit card details, OTP, etc then it requires an SSL certificate installed to make the website more secure. So, before entering any sensitive information on a website, we should check if the link is HTTPS or not. If it is not HTTPS then it may not be secure enough to enter sensitive information.

8. TELNET(Terminal Network)

TELNET is a standard TCP/IP protocol used for virtual terminal service given by ISO. This enables one local machine to connect with another. The computer which is being connected is called a remote computer and which is connecting is called the local computer. TELNET operation lets us display anything being performed on the remote computer in the local computer. This operates on the client/server principle. The local computer uses the telnet client program whereas the remote computer uses the telnet server program.

9. POP3(Post Office Protocol 3)

POP3 stands for Post Office Protocol version 3. It has two Message Access Agents (MAAs) where one is client MAA (Message Access Agent) and another is server MAA(Message Access Agent) for accessing the messages from the mailbox. This protocol helps us to retrieve and manage emails from the mailbox on the receiver mail server to the receiver’s computer. This is implied between the receiver and the receiver mail server. It can also be called a one-way client-server protocol. The POP3 WORKS ON THE 2 PORTS I.E. PORT 110 AND PORT 995.

10. IPv4

The fourth and initially widely used version of the Internet Protocol is called IPv4 (Internet Protocol version 4). It is the most popular version of the Internet Protocol and is in charge of distributing data packets throughout the network. Maximum unique addresses for IPv4 are 4,294,967,296 (232), which are possible due to the use of 32-bit addresses. The network address and the host address are the two components of each address. The host address identifies a particular device within the network, whereas the network address identifies the network to which the host belongs. In the “dotted decimal” notation, which is the standard for IPv4 addresses, each octet (8 bits) of the address is represented by its decimal value and separated by a dot (e.g. 192.168.1.1).

11. IPv6

The most recent version of the Internet Protocol, IPv6, was created to address the IPv4 protocol’s drawbacks. A maximum of 4.3 billion unique addresses are possible with IPv4’s 32-bit addresses. Contrarily, IPv6 uses 128-bit addresses, which enable a significantly greater number of unique addresses. This is significant because IPv4 addresses were running out and there are an increasing number of devices that require internet access. Additionally, IPv6 offers enhanced security features like integrated authentication and encryption as well as better support for mobile devices. IPv6 support has spread among websites and internet service providers, and it is anticipated to gradually displace IPv4 as the main internet protocol.

For more details, please refer Differences between IPv4 and IPv6 article.

12. ICMP

ICMP (Internet Control Message Protocol) is a network protocol that is used to send error messages and operational information about network conditions. It is an integral part of the Internet Protocol (IP) suite and is used to help diagnose and troubleshoot issues with network connectivity. ICMP messages are typically generated by network devices, such as routers, in response to errors or exceptional conditions encountered in forwarding a datagram. Some examples of ICMP messages include:

- Echo Request and Echo Reply (ping)
- Destination Unreachable
- Time Exceeded
- Redirect

ICMP can also be used by network management tools to test the reachability of a host and measure the round-trip time for packets to travel from the source to the destination and back. It should be noted that ICMP is not a secure protocol, it can be used in some types of network attacks like DDoS amplification.

13. UDP

UDP (User Datagram Protocol) is a connectionless, unreliable transport layer protocol. Unlike TCP, it does not establish a reliable connection between devices before transmitting data, and it does not guarantee that data packets will be received in the order they were sent or that they will be received at all. Instead, UDP simply sends packets of data to a destination without any error checking or flow control. UDP is typically used for real-time applications such as streaming video and audio, online gaming, and VoIP (Voice over Internet Protocol) where a small amount of lost data is acceptable and low latency is important. UDP is faster than TCP because it has less overhead. It doesn’t need to establish a connection, so it can send data packets immediately. It also doesn’t need to wait for confirmation that the data was received before sending more, so it can transmit data at a higher rate.

14. IMAP

IMAP (Internet Message Access Protocol) is a protocol used for retrieving emails from a mail server. It allows users to access and manage their emails on the server, rather than downloading them to a local device. This means that the user can access their emails from multiple devices and the emails will be synced across all devices. IMAP is more flexible than POP3 (Post Office Protocol version 3) as it allows users to access and organize their emails on the server, and also allows multiple users to access the same mailbox.

15. SSH

SSH (Secure Shell) is a protocol used for secure remote login and other secure network services. It provides a secure and encrypted way to remotely access and manage servers, network devices, and other computer systems. SSH uses public-key cryptography to authenticate the user and encrypt the data being transmitted, making it much more secure than traditional remote login protocols such as Telnet. SSH also allows for secure file transfers using the SCP (Secure Copy) and SFTP (Secure File Transfer Protocol) protocols. It is widely used in Unix-based operating systems and is also available for Windows. It is commonly used by system administrators, developers, and other technical users to remotely access and manage servers and other network devices.

16. Gopher

Gopher is a type of file retrieval protocol that provides downloadable files with some description for easy management, retrieving, and searching of files. All the files are arranged on a remote computer in a stratified manner. It is an old protocol and it is not much used nowadays.

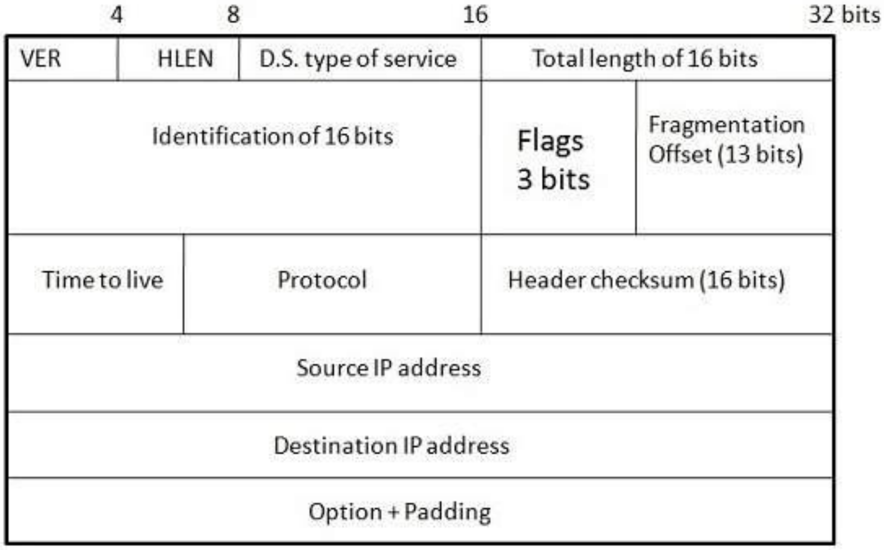
INTERNET PROTOCOL

Internet Protocol (IP)

Internet Protocol is **connectionless** and **unreliable** protocol. It ensures no guarantee of successfully transmission of data.

In order to make it reliable, it must be paired with reliable protocol such as TCP at the transport layer.

Internet protocol transmits the data in form of a datagram as shown in the following diagram:



4	8	16		32 bits
VER	HLEN	D.S. type of service	Total length of 16 bits	
Identification of 16 bits			Flags 3 bits	Fragmentation Offset (13 bits)
Time to live	Protocol		Header checksum (16 bits)	
Source IP address				
Destination IP address				
Option + Padding				

Points to remember:

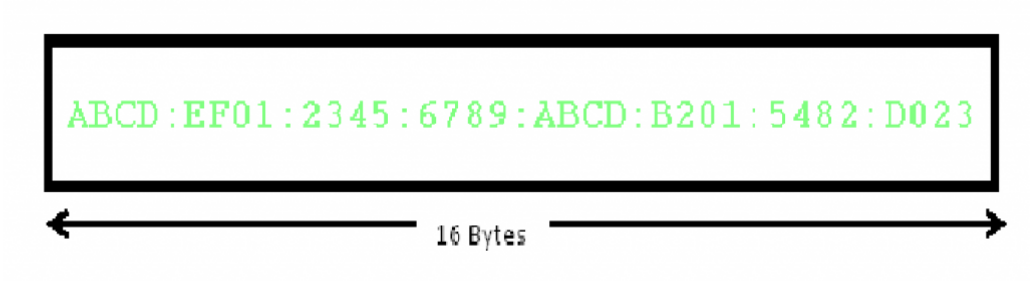
- The length of datagram is variable.
- The Datagram is divided into two parts: **header** and **data.**
- The length of header is 20 to 60 bytes.
- The header contains information for routing and delivery of the packet.

INTERNET PROTOCOL VERSION 6 (IPV6)

IPv6 was developed by Internet Engineering Task Force (IETF) to deal with the problem of IPv4 exhaustion. IPv6 is a 128-bits address having an address space of 2^{128}, which is way bigger than IPv4. IPv6 use Hexa-Decimal format separated by colon (:) .

Components in Address format :

1. There are 8 groups and each group represents 2 Bytes (16-bits).
2. Each Hex-Digit is of 4 bits (1 nibble)
3. Delimiter used – colon (:)



Need for IPv6:

The Main reason of IPv6 was the address depletion as the need for electronic devices rose quickly when Internet Of Things (IOT) came into picture after the 1980s & other reasons are related to the slowness of the process due to some unnecessary processing, the need for new options, support for multimedia, and the desperate need for security. IPv6 protocol responds to the above issues using the following main changes in the protocol:

1. Large address space

An IPv6 address is 128 bits long .compared with the 32 bit address of IPv4, this is a huge(2 raised 96 times) increases in the address space.

2. Better header format

IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and the upper layer data . This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.

3. New options

IPv6 has new options to allow for additional functionalities.

4. Allowance for extension

IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.

5. Support for resource allocation

In IPv6,the type of service field has been removed, but two new fields , traffic class and flow label have been added to enables the source to request special handling of the packet . this mechanism can be used to support traffic such as real-time audio and video.

6. Support for more security

The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

In IPv6 representation, we have three addressing methods :

- Unicast
- Multicast
- Anycast

Addressing methods

1. Unicast Address

Unicast Address identifies a single network interface. A packet sent to a unicast address is delivered to the interface identified by that address.

2. Multicast Address

Multicast Address is used by multiple hosts, called as **groups**, acquires a multicast destination address. These hosts need not be geographically together. If any packet is sent to this multicast address, it will be distributed to all interfaces corresponding to that multicast address. And every node is configured in the same way. In simple words, one data packet is sent to multiple destinations simultaneously.

3. Anycast Address

Anycast Address is assigned to a group of interfaces. Any packet sent to an anycast address will be delivered to only one member interface (mostly nearest host possible).

Note: Broadcast is not defined in IPv6.

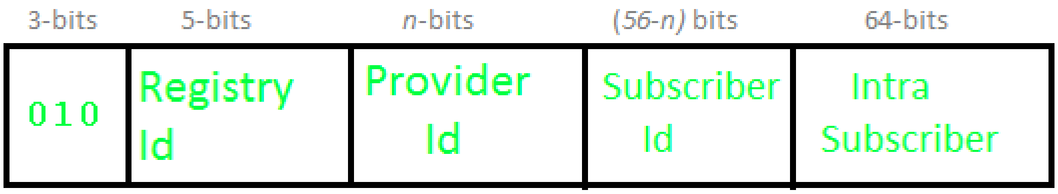
Types of IPv6 address:

We have 128 bits in IPv6 address but by looking at the first few bits we can identify what type of address it is.

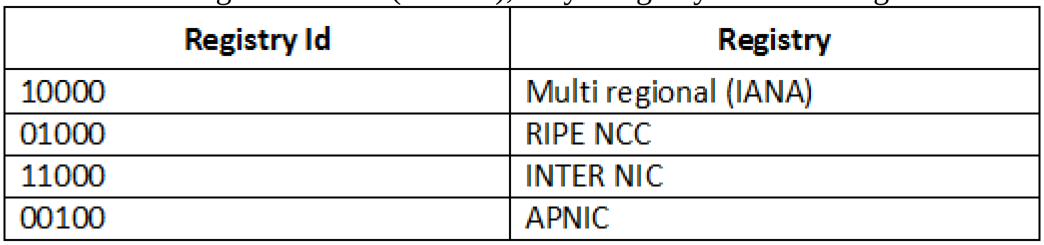
Prefix	**Allocation**	**Fraction of Address Space**
0000 0000	Reserved	1/256
0000 0001	Unassigned (UA)	1/256
0000 001	Reserved for NSAP	1/128
0000 01	UA	1/64
0000 1	UA	1/32
0001	UA	1/16
001	Global Unicast	1/8
010	UA	1/8
011	UA	1/8
100	UA	1/8
101	UA	1/8
110	UA	1/8
1110	UA	1/16
1111 0	UA	1/32
1111 10	UA	1/64
1111 110	UA	1/128
1111 1110 0	UA	1/512
1111 1110 10	Link-Local Unicast Addresses	1/1024
1111 1110 11	Site-Local Unicast Addresses	1/1024
1111 1111	Multicast Address	1/256

Note: In IPv6, all 0’s and all 1’s can be assigned to any host, there is not any restriction like IPv4.

Provider-based Unicast address : These are used for global communication.



The First 3 bits identify it as of this type. **Registry Id (5-bits):** Registry Id identifies the region to which it belongs. Out of 32 (i.e. 2^5), only 4 registry IDs are being used.



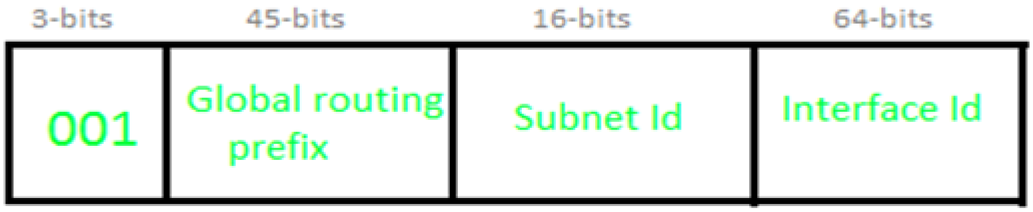
Registry Id	Registry
10000	Multi regional (IANA)
01000	RIPE NCC
11000	INTER NIC
00100	APNIC

Provider Id: Depending on the number of service providers that operate under a region, certain bits will be allocated to the Provider Id field. This field need not be fixed. Let's say if Provider Id = 10 bits then Subscriber Id will be 56 – 10 = 46 bits.

Subscriber Id: After Provider Id is fixed, the remaining part can be used by ISP as a normal IP address.

Intra Subscriber: This part can be modified as per the need of the organization that is using the service.

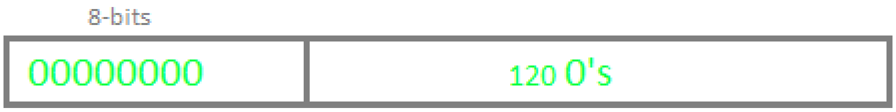
Geography based Unicast address :



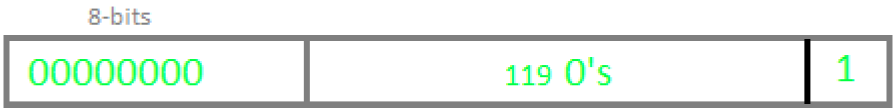
Global routing prefix: Global routing prefix contains all the details of Latitude and Longitude. As of now, it is not being used. In Geography-based Unicast address routing will be based on location.

Interface Id: In IPv6, instead of using Host Id, we use the term Interface Id.

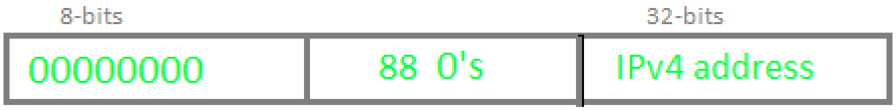
Some special addresses: Unspecified



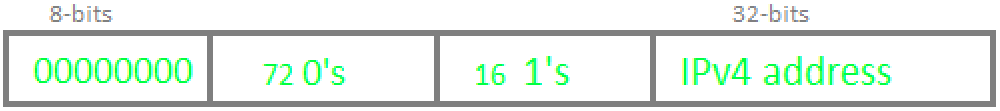
Loopback



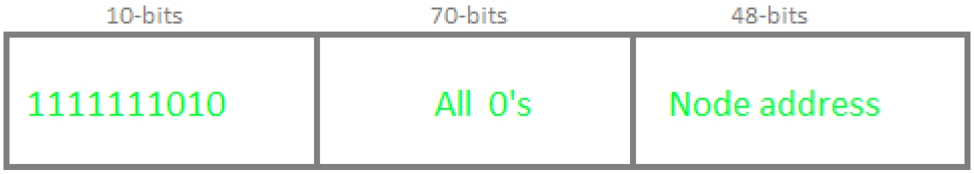
IPv4 Compatible



IPv4 mapped

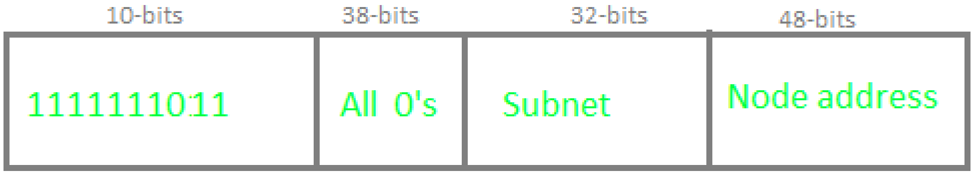


Local Unicast Addresses :
These are of two types: ***Link-local*** and ***Site-Local***
1. Link-local address:



A link-local address is used for addressing a single link. It can also be used to communicate with nodes on the same link. The link-local address always begins with 1111111010 (i.e. FE80). The router will not forward any packet with Link-local address.

2. Site local address:



Site local addresses are equivalent to a private IP address in IPv4. Likely, some address space is reserved, which can only be routed within an organization. The first 10-bits are set to 1111111011, which is why Site local addresses always begin with FEC0. The following 32 bits are Subnet IDs, which can be used to create a subnet within the organization. The node address is used to uniquely identify the link; therefore, we use a 48-bits MAC address here.

Advantages of IPv6 :
1. Realtime Data Transmission : Realtime data transmission refers to the process of transmitting data in a very fast manner or **immediately**. Example : Live streaming services such as cricket matches, or other tournament that are streamed on web exactly as soon as it happens with a maximum delay of 5-6 seconds.

2. IPv6 supports authentication: Verifying that the data received by the receiver from the sender is exactly what the sender sent and came through the sender only not from any third party. Example : Matching the hash value of both the messages for verification is also done by IPv6.
3. IPv6 performs Encryption: Ipv6 can encrypt the message at network layer even if the protocols of application layer at user level didn't encrypt the message which is a major advantage as it takes care of encryption.
4. Faster processing at Router: Routers are able to process data packets of Ipv6 much faster due to smaller **Base header** of fixed size – 40 bytes which helps in decreasing processing time resulting in more efficient packet transmission. Whereas in Ipv4, we have to calculate the length of header which lies between 20-60 bytes.

VIRTUAL PRIVATE NETWORK (VPN)

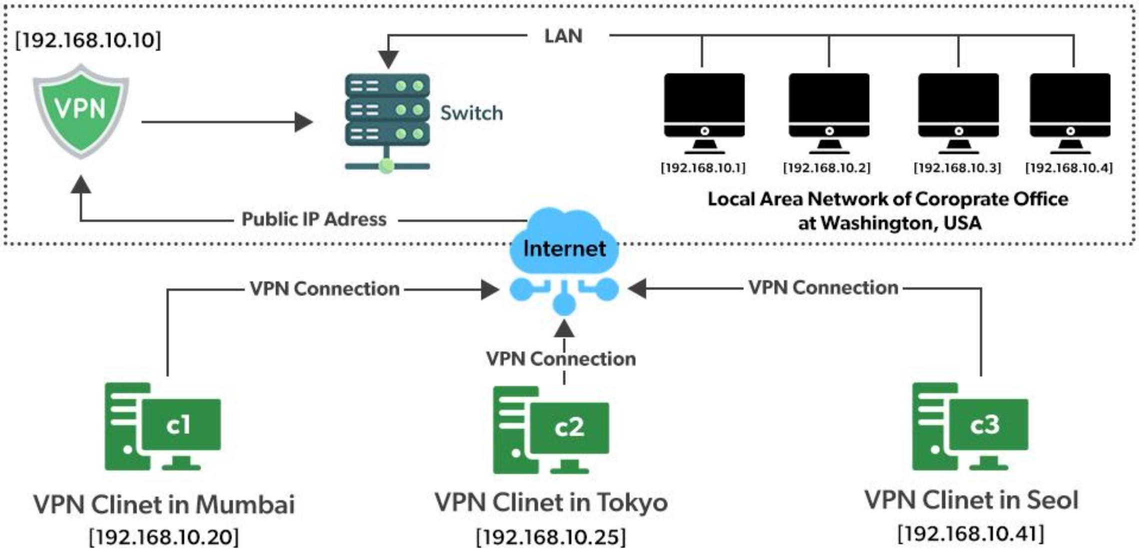
VPN stands for the virtual private network. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. A Virtual Private Network is a way to extend a private network using a public network such as the internet. The name only suggests that it is a Virtual "private network" i.e. user can be part of a local network sitting at a remote location. It makes use of tunneling protocols to establish a secure connection.

Lets understand VPN by an example:

Think of a situation where corporate office of a bank is situated in Washington, USA. This office has a local network consisting of say 100 computers. Suppose other branches of the bank are in Mumbai, India, and Tokyo, Japan. The traditional method of establishing a secure connection between head office and branch was to have a leased line between the branches and head office which was a very costly as well as troublesome job. VPN lets us overcome this issue in an effective manner.

The situation is described below:

- All 100 hundred computers of the corporate office at Washington are connected to the VPN server(which is a well-configured server containing a public IP address and a switch to connect all computers present in the local network i.e. in US head office).
- The person sitting in the Mumbai office connects to The VPN server using a dial-up window and the VPN server returns an IP address that belongs to the series of IP addresses belonging to a local network of the corporate office.
- Thus person from the Mumbai branch becomes local to the head office and information can be shared securely over the public internet.
- So this is the intuitive way of extending the local network even across the geographical borders of the country.



VPN is well exploited all across the globe

We will explain to you with an example. Suppose we are using smartphones regularly. Spotify-a Swedish music app which is not active in India But we are making full use of it sitting in India. So how ?? VPN can be used to camouflage our geolocation.

- Suppose the Ip address is 101.22.23.3 which belongs to India. That's why our device is not able to access the Spotify music app.
- But the magic begins when we used the Psiphon app which is an android app and is used to change the device IP address to the IP address of the location we want(say US where Spotify works in a seamless manner).
- The IP address is changed using VPN technology. Basically what happens is that your device will connect to a VPN server of the respective country that you have entered in your location textbox of the Psiphon app and now you will inherit a new IP from this server.

IP SECURITY

IP Sec (Internet Protocol Security) is an Internet Engineering Task Force (IETF) standard suite of protocols between two communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted, and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

Uses of IP Security

IPsec can be used to do the following things:

- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPsec tunneling in which all data being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

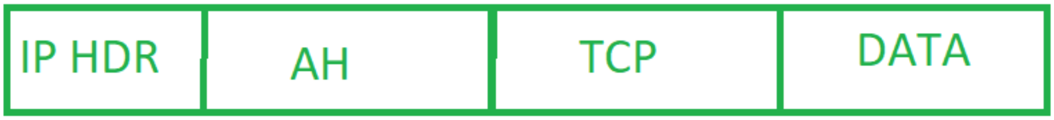
Components of IP Security

It has the following components:

1. Encapsulating Security Payload (ESP)
2. Authentication Header (AH)
3. Internet Key Exchange (IKE)

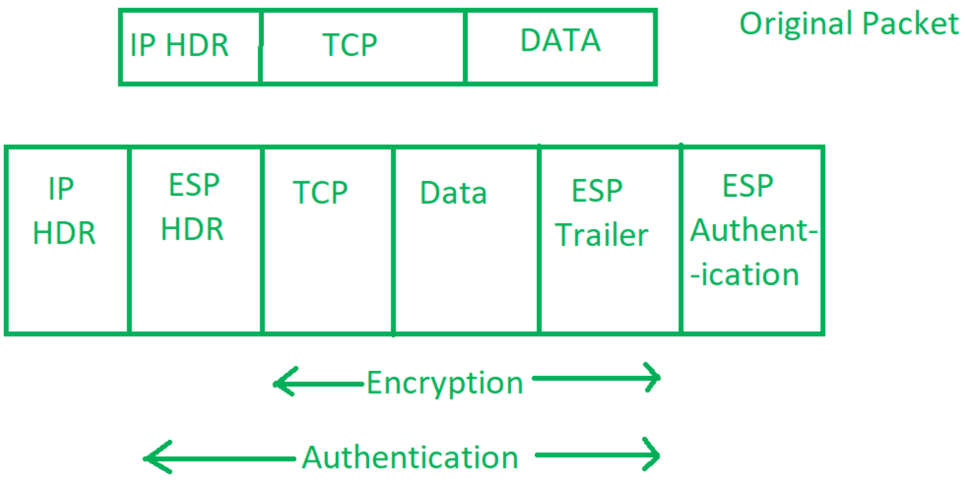
1. Encapsulating Security Payload (ESP): It provides data integrity, encryption, authentication, and anti-replay. It also provides authentication for payload.

2. Authentication Header (AH): It also provides data integrity, authentication, and anti-replay and it does not provide encryption. The anti-replay protection protects against the unauthorized transmission of packets. It does not protect data confidentiality.



IP Header

3. Internet Key Exchange (IKE): It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. The Key Management Protocol (ISAKMP) and Internet Security Association provides a framework for authentication and key exchange. ISAKMP tells how the setup of the Security Associations (SAs) and how direct connections between two hosts are using IPsec. Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5. The algorithm's IP sec users produce a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not. Packets that are not authorized are discarded and not given to the receiver.

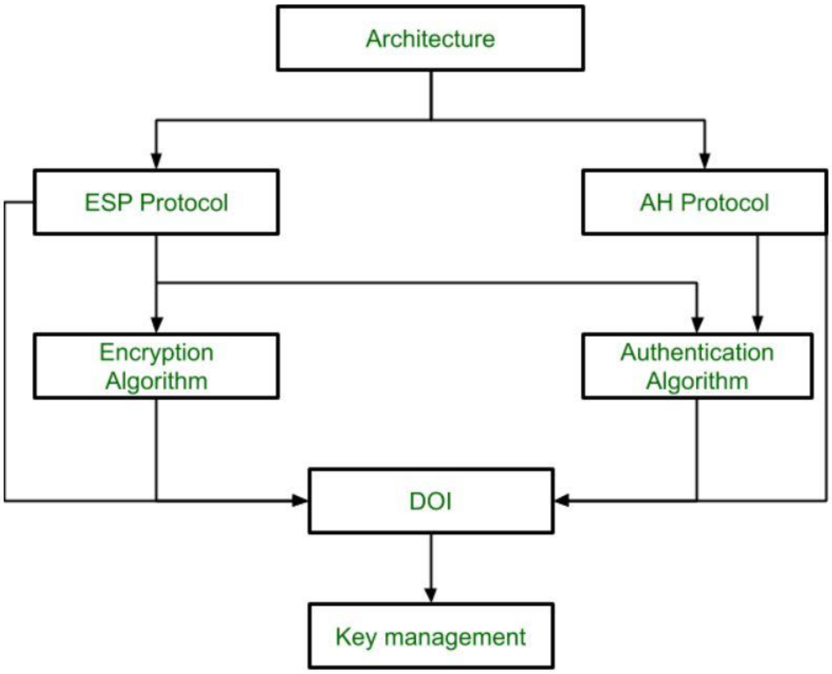


Packets in Internet Protocol

IP Security Architecture

IPSec (IP Security) architecture uses two protocols to secure the traffic or data flow. These protocols are ESP (Encapsulation Security Payload) and AH (Authentication Header). IPSec Architecture includes protocols, algorithms, DOI, and Key Management. All these components are very important in order to provide the three main services:

- Confidentiality
- Authenticity
- Integrity



IP Security Architecture

Working on IP Security

- The host checks if the packet should be transmitted using IPsec or not. This packet traffic triggers the security policy for itself. This is done when the system sending the packet applies appropriate encryption. The incoming packets are also checked by the host that they are encrypted properly or not.
- Then IKE Phase 1 starts in which the 2 hosts(using IPsec) authenticate themselves to each other to start a secure channel. It has 2 modes. The Main mode provides greater security and the Aggressive mode which enables the host to establish an IPsec circuit more quickly.
- The channel created in the last step is then used to securely negotiate the way the IP circuit will encrypt data across the IP circuit.
- Now, the IKE Phase 2 is conducted over the secure channel in which the two hosts negotiate the type of cryptographic algorithms to use on the session and agree on secret keying material to be used with those algorithms.
- Then the data is exchanged across the newly created IPsec encrypted tunnel. These packets are encrypted and decrypted by the hosts using IPsec SAs.
- When the communication between the hosts is completed or the session times out then the IPsec tunnel is terminated by discarding the keys by both hosts.

Features of IPSec

1. **Authentication:** IPSec provides authentication of IP packets using digital signatures or shared secrets. This helps ensure that the packets are not tampered with or forged.
2. **Confidentiality:** IPSec provides confidentiality by encrypting IP packets, preventing eavesdropping on the network traffic.

3. **Integrity:** IPSec provides integrity by ensuring that IP packets have not been modified or corrupted during transmission.
4. **Key management:** IPSec provides key management services, including key exchange and key revocation, to ensure that cryptographic keys are securely managed.
5. **Tunneling:** IPSec supports tunneling, allowing IP packets to be encapsulated within another protocol, such as GRE (Generic Routing Encapsulation) or L2TP (Layer 2 Tunneling Protocol).
6. **Flexibility:** IPSec can be configured to provide security for a wide range of network topologies, including point-to-point, site-to-site, and remote access connections.
7. **Interoperability:** IPSec is an open standard protocol, which means that it is supported by a wide range of vendors and can be used in heterogeneous environments.

Advantages of IPSec

1. **Strong security:** IPSec provides strong cryptographic security services that help protect sensitive data and ensure network privacy and integrity.
2. **Wide compatibility:** IPSec is an open standard protocol that is widely supported by vendors and can be used in heterogeneous environments.
3. **Flexibility:** IPSec can be configured to provide security for a wide range of network topologies, including point-to-point, site-to-site, and remote access connections.
4. **Scalability:** IPSec can be used to secure large-scale networks and can be scaled up or down as needed.
5. **Improved network performance:** IPSec can help improve network performance by reducing network congestion and improving network efficiency.

Disadvantages of IPSec

1. **Configuration complexity:** IPSec can be complex to configure and requires specialized knowledge and skills.
2. **Compatibility issues:** IPSec can have compatibility issues with some network devices and applications, which can lead to interoperability problems.
3. **Performance impact:** IPSec can impact network performance due to the overhead of encryption and decryption of IP packets.
4. **Key management:** IPSec requires effective key management to ensure the security of the cryptographic keys used for encryption and authentication.
5. **Limited protection:** IPSec only provides protection for IP traffic, and other protocols such as ICMP, DNS, and routing protocols may still be vulnerable to attacks.

CONNECTION-ORIENTED SERVICE

Connection-Oriented Service is basically a technique that is typically used to transport and send data at session layer. The data streams or packets are transferred or delivered to receiver in a similar order in which they have seen transferred by sender. It is actually a data transfer method among two devices or computers in a different network, that is designed and developed after telephone system. Whenever a network implements this service, it sends or transfers data or message from sender or source to receiver or destination in correct order and manner.

This connection service is generally provided by protocols of both network layer (signifies different path for various data packets that belongs to same message) as well as transport layer (use to exhibits independence among packets rather than different paths that various packets belong to same message will follow).

Operations :

There is a sequence of operations that are needed to b followed by users. These operations are given below :

1. **Establishing Connection –**
   It generally requires a session connection to be established just before any data is transported or sent with a direct physical connection among sessions.
2. **Transferring Data or Message –**
   When this session connection is established, then we transfer or send message or data.
3. **Releasing the Connection –**
   After sending or transferring data, we release connection.

Different Ways :

There are two ways in which connection-oriented services can be done. These ways are given below :

1. **Circuit-Switched Connection –**
   Circuit-switching networks or connections are generally known as connection-oriented networks. In this connection, a dedicated route is being established among sender and receiver, and whole data or message is sent through it. A dedicated physical route or a path or a circuit is established among all communication nodes, and after that, data stream or message is sent or transferred.
2. **Virtual Circuit-Switched Connection**
   Virtual Circuit-Switched Connection or Virtual Circuit Switching is also known as Connection-Oriented Switching. In this connection, a preplanned route or path is established before data or messages are transferred or sent. The message Is transferred over this network is such a way that it seems to user that there is a dedicated route or path from source or sender to destination or receiver.

Types of Connection-Oriented Service :

Service	**Example**
Reliable Message Stream	Sequence of pages, etc.
Reliable Byte Stream	Song Download, etc.
Unreliable Connection	VoIP (Voice Over Internet Protocol)

Advantages :

- It kindly support for quality of service is an easy way.
- This connection is more reliable than connectionless service.
- Long and large messages can be divided into various smaller messages so that it can fit inside packets.
- Problems or issues that are related to duplicate data packets are made less severe.

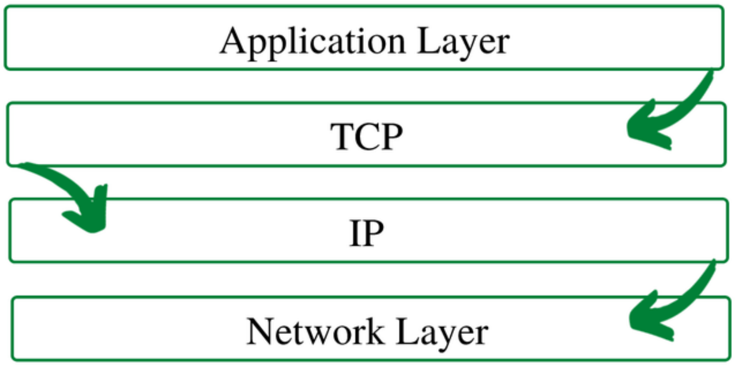
Disadvantages :

□ In this connection, cost is fixed no matter how traffic is.
□ It is necessary to have resource allocation before communication.

- If any route or path failures or network congestions arise, there is no alternative way available to continue communication.

TCP

TCP (Transmission Control Protocol) is one of the main protocols of the Internet protocol suite. It lies between the Application and Network Layers which are used in providing reliable delivery services. It is a connection-oriented protocol for communications that helps in the exchange of messages between different devices over a network. The Internet Protocol (IP), which establishes the technique for sending data packets between computers, works with TCP.

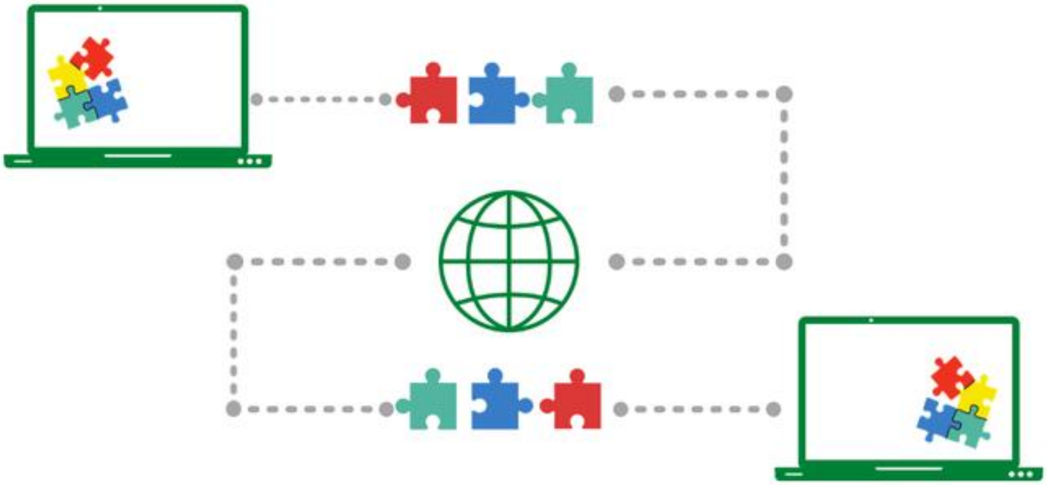


TCP/IP Layer

Working of TCP

To make sure that each message reaches its target location intact, the TCP/IP model breaks down the data into small bundles and afterward reassembles the bundles into the original message on the opposite end. Sending the information in little bundles of information makes it simpler to maintain efficiency as opposed to sending everything in one go.

After a particular message is broken down into bundles, these bundles may travel along multiple routes if one route is jammed but the destination remains the same.



We can see that the message is being broken down, then reassembled from a different order at the destination

For example, When a user requests a web page on the internet, somewhere in the world, the server processes that request and sends back an HTML Page to that user. The server makes use of a protocol called the HTTP Protocol. The HTTP then requests the TCP layer to set the required connection and send the HTML file.

Now, the TCP breaks the data into small packets and forwards it toward the Internet Protocol (IP) layer. The packets are then sent to the destination through different routes.

The TCP layer in the user's system waits for the transmission to get finished and acknowledges once all packets have been received.

Features of TCP/IP

Some of the most prominent features of Transmission control protocol are

1. Segment Numbering System

- TCP keeps track of the segments being transmitted or received by assigning numbers to each and every single one of them.
- A specific *Byte Number* is assigned to data bytes that are to be transferred while segments are assigned *sequence numbers*.
- *Acknowledgment Numbers* are assigned to received segments.

2. Connection Oriented

- It means sender and receiver are connected to each other till the completion of the process.
- The order of the data is maintained i.e. order remains same before and after transmission.

3. Full Duplex

- In TCP data can be transmitted from receiver to the sender or vice – versa at the same time.
- It increases efficiency of data flow between sender and receiver.

4. Flow Control

- Flow control limits the rate at which a sender transfers data. This is done to ensure reliable delivery.
- The receiver continually hints to the sender on how much data can be received (using a sliding window)

5. Error Control

- TCP implements an error control mechanism for reliable data transfer
- Error control is byte-oriented
- Segments are checked for error detection
- Error Control includes – *Corrupted Segment & Lost Segment Management, Out-of-order segments, Duplicate segments,* etc.

6. Congestion Control

- TCP takes into account the level of congestion in the network
- Congestion level is determined by the amount of data sent by a sender

Advantages

- It is a reliable protocol.
- It provides an error-checking mechanism as well as one for recovery.
- It gives flow control.
- It makes sure that the data reaches the proper destination in the exact order that it was sent.
- Open Protocol, not owned by any organization or individual.

- It assigns an IP address to each computer on the network and a domain name to each site thus making each device site to be distinguishable over the network.

Disadvantages

- TCP is made for Wide Area Networks, thus its size can become an issue for small networks with low resources.
- TCP runs several layers so it can slow down the speed of the network.
- It is not generic in nature. Meaning, it cannot represent any protocol stack other than the TCP/IP suite. E.g., it cannot work with a Bluetooth connection.
- No modifications since their development around 30 years ago

TCP CONGESTION CONTROL

TCP uses a congestion window and a congestion policy that avoid congestion. Previously, we assumed that only the receiver can dictate the sender's window size. We ignored another entity here, the network. If the network cannot deliver the data as fast as it is created by the sender, it must tell the sender to slow down. In other words, in addition to the receiver, the network is a second entity that determines the size of the sender's window.

Congestion policy in TCP –

1. Slow Start Phase: starts slowly increment is exponential to threshold
2. Congestion Avoidance Phase: After reaching the threshold increment is by 1
3. Congestion Detection Phase: Sender goes back to Slow start phase or Congestion avoidance phase.

Slow Start Phase : exponential increment – In this phase after every RTT the congestion window size increments exponentially.

Initially cwnd = 1
After 1 RTT, cwnd = 2^(1) = 2
2 RTT, cwnd = 2^(2) = 4
3 RTT, cwnd = 2^(3) = 8

Congestion Avoidance Phase : additive increment – This phase starts after the threshold value also denoted as *ssthresh*. The size of *cwnd*(congestion window) increases additive. After each RTT cwnd = cwnd + 1.

Initially cwnd = i
After 1 RTT, cwnd = i+1
2 RTT, cwnd = i+2
3 RTT, cwnd = i+3

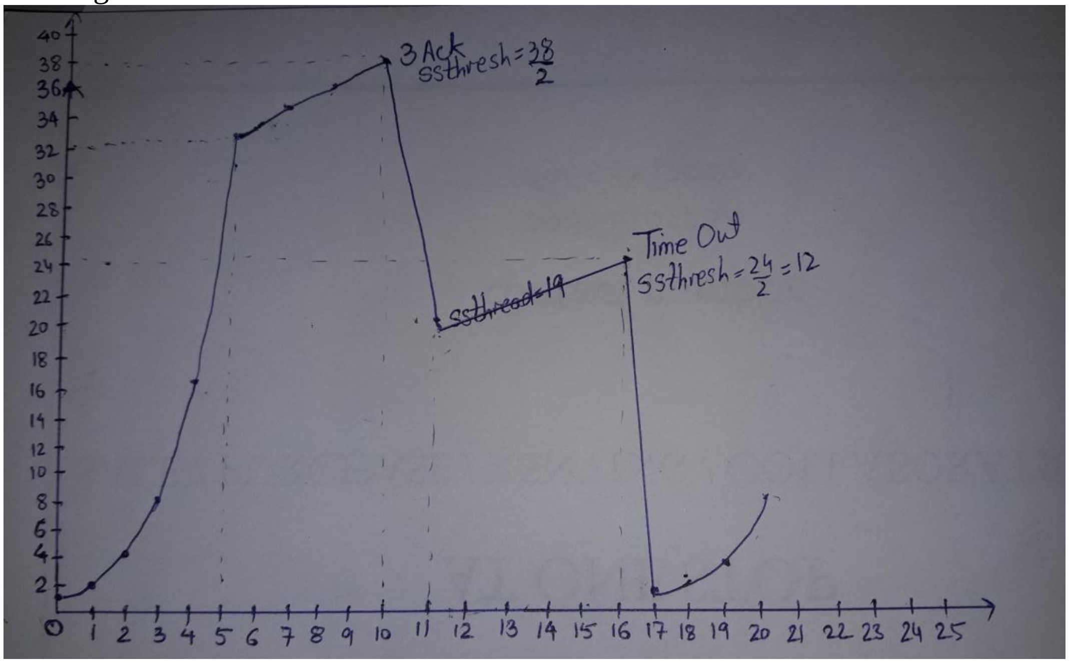
Congestion Detection Phase : multiplicative decrement – If congestion occurs, the congestion window size is decreased. The only way a sender can guess that congestion has occurred is the need to retransmit a segment. Retransmission is needed to recover a missing packet that is assumed to have been dropped by a router due to congestion. Retransmission can occur in one of two cases: when the RTO timer times out or when three duplicate ACKs are received.

- **Case 1 : Retransmission due to Timeout –** In this case congestion possibility is high.

(a) ssthresh is reduced to half of the current window size.
(b) set cwnd = 1
(c) start with slow start phase again.

- **Case 2 : Retransmission due to 3 Acknowledgement Duplicates** – In this case congestion possibility is less.
  (a) ssthresh value reduces to half of the current window size.
  (b) set cwnd= ssthresh
  (c) start with congestion avoidance phase

Example – Assume a TCP protocol experiencing the behavior of slow start. At 5th transmission round with a threshold (ssthresh) value of 32 goes into congestion avoidance phase and continues till 10th transmission. At 10th transmission round, 3 duplicate ACKs are received by the receiver and enter into additive increase mode. Timeout occurs at 16th transmission round. Plot the transmission round (time) vs congestion window size of TCP segments.



GATE CS Corner Questions –

Practicing the following questions will help you test your knowledge. All questions have been asked in GATE in previous years or in GATE Mock Tests. It is highly recommended that you practice them.

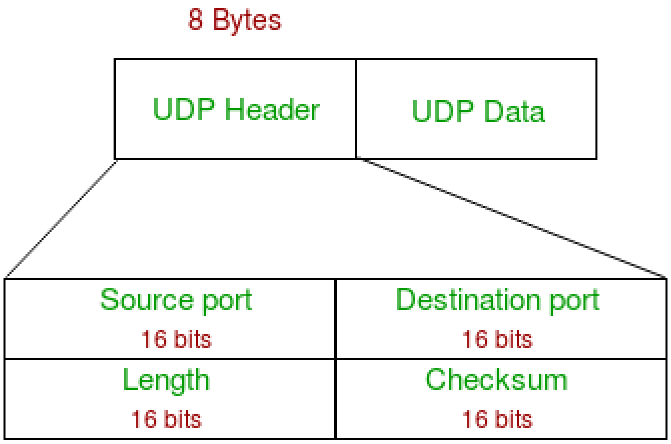
1. GATE CS 2008, Question 56
2. GATE CS 2012, Question 65
3. GATE CS 2014 (Set 1), Question 65
4. GATE IT 2005, Question 73

UDP

User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of the Internet Protocol suite, referred to as UDP/IP suite. Unlike TCP, it is an **unreliable and connectionless protocol.** So, there is no need to establish a connection prior to data transfer. The UDP helps to establish low-latency and loss-tolerating connections establish over the network.The UDP enables process to process communication.

Though Transmission Control Protocol (TCP) is the dominant transport layer protocol used with most of the Internet services; provides assured delivery, reliability, and much more but all these services cost us additional overhead and latency. Here, UDP comes into the picture. For real-time services like computer gaming, voice or video communication, live conferences; we need UDP. Since high performance is needed, UDP permits packets to be dropped instead of processing delayed packets. There is no error checking in UDP, so it also saves bandwidth. User Datagram Protocol (UDP) is more efficient in terms of both latency and bandwidth.

UDP Header –
UDP header is an **8-bytes** fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes. The first 8 Bytes contains all necessary header information and the remaining part consist of data. UDP port number fields are each 16 bits long, therefore the range for port numbers is defined from 0 to 65535; port number 0 is reserved. Port numbers help to distinguish different user requests or processes.



1. **Source Port:** Source Port is a 2 Byte long field used to identify the port number of the source.
2. **Destination Port:** It is a 2 Byte long field, used to identify the port of the destined packet.
3. **Length:** Length is the length of UDP including the header and the data. It is a 16-bits field.
4. **Checksum:** Checksum is 2 Bytes long field. It is the 16-bit one’s complement of the one’s complement sum of the UDP header, the pseudo-header of information from the IP header, and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

Notes – Unlike TCP, the Checksum calculation is not mandatory in UDP. No Error control or flow control is provided by UDP. Hence UDP depends on IP and ICMP for error reporting. Also UDP provides port numbers so that is can differentiate between users requests.

Applications of UDP:

- Used for simple request-response communication when the size of data is less and hence there is lesser concern about flow and error control.
- It is a suitable protocol for multicasting as UDP supports packet switching.
- UDP is used for some routing update protocols like RIP(Routing Information Protocol).
- Normally used for real-time applications which can not tolerate uneven delays between sections of a received message.
- UDP is widely used in online gaming, where low latency and high-speed communication is essential for a good gaming experience. Game servers often send small, frequent packets of data to clients, and UDP is well suited for this type of communication as it is fast and lightweight.
- Streaming media applications, such as IPTV, online radio, and video conferencing, use UDP to transmit real-time audio and video data. The loss of some packets can be tolerated in these applications, as the data is continuously flowing and does not require retransmission.
- VoIP (Voice over Internet Protocol) services, such as Skype and WhatsApp, use UDP for real-time voice communication. The delay in voice communication can be noticeable if packets are delayed due to congestion control, so UDP is used to ensure fast and efficient data transmission.
- DNS (Domain Name System) also uses UDP for its query/response messages. DNS queries are typically small and require a quick response time, making UDP a suitable protocol for this application.
- DHCP (Dynamic Host Configuration Protocol) uses UDP to dynamically assign IP addresses to devices on a network. DHCP messages are typically small, and the delay caused by packet loss or retransmission is generally not critical for this application.
- Following implementations uses UDP as a transport layer protocol:
    - NTP (Network Time Protocol)
    - DNS (Domain Name Service)
    - BOOTP, DHCP.
    - NNP (Network News Protocol)
    - Quote of the day protocol
    - TFTP, RTSP, RIP.
- The application layer can do some of the tasks through UDP-
    - Trace Route
    - Record Route
    - Timestamp
- UDP takes a datagram from Network Layer, attaches its header, and sends it to the user. So, it works fast.
- Actually, UDP is a null protocol if you remove the checksum field.

1. Reduce the requirement of computer resources.
2. When using the Multicast or Broadcast to transfer.
3. The transmission of Real-time packets, mainly in multimedia applications.