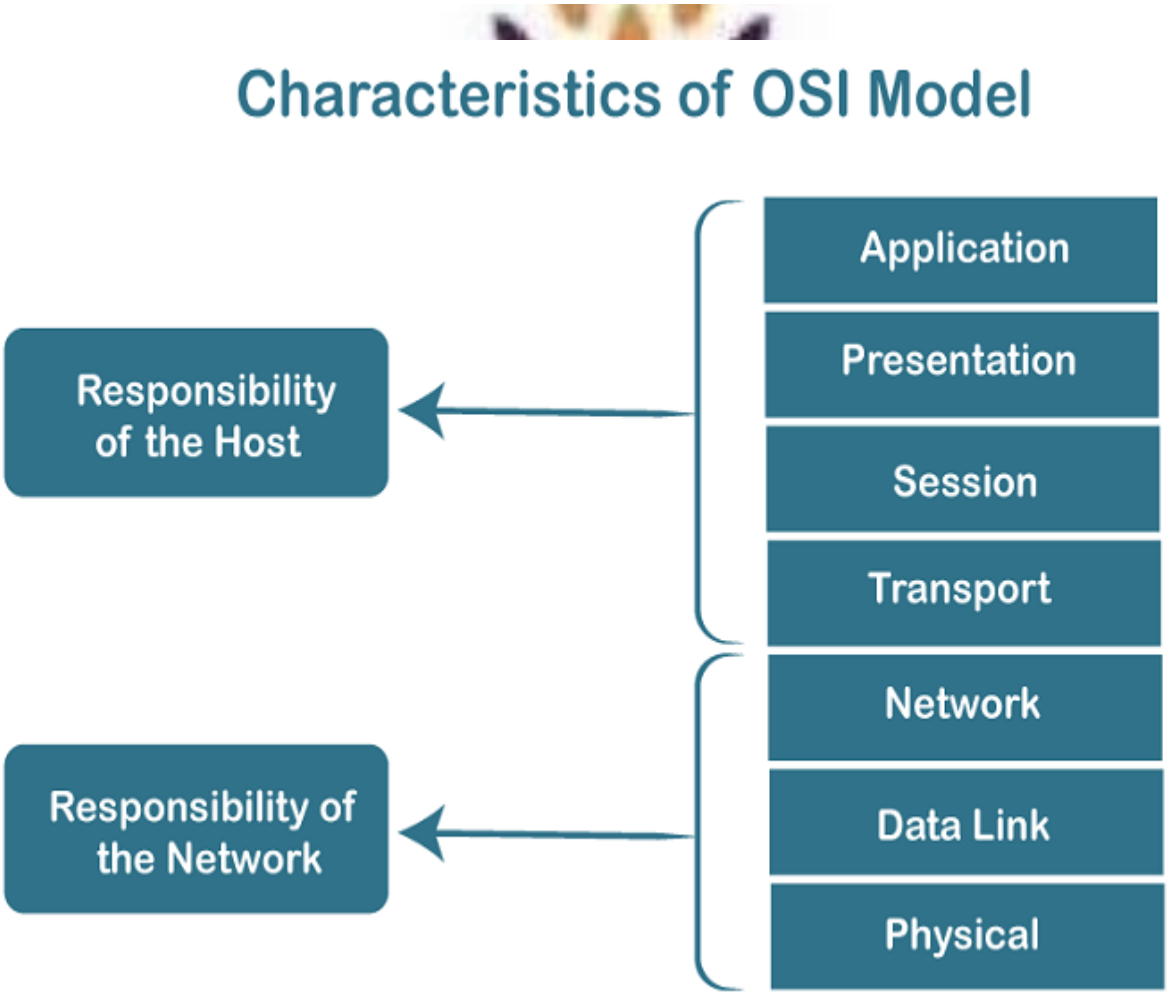
UNIT-I

OSI Model uses

- OSI stands for **Open System Interconnection** is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.

Characteristics of OSI Model:

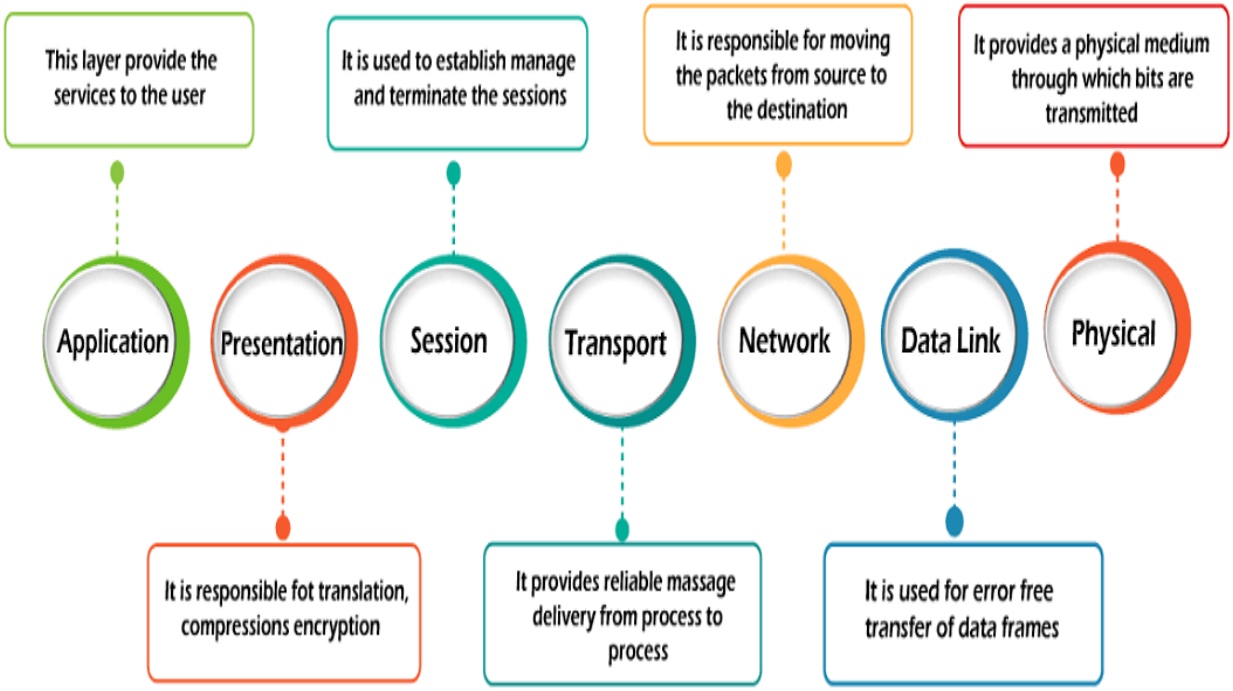


- The OSI model is divided into two layers: upper layers and lower layers.
- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
- The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

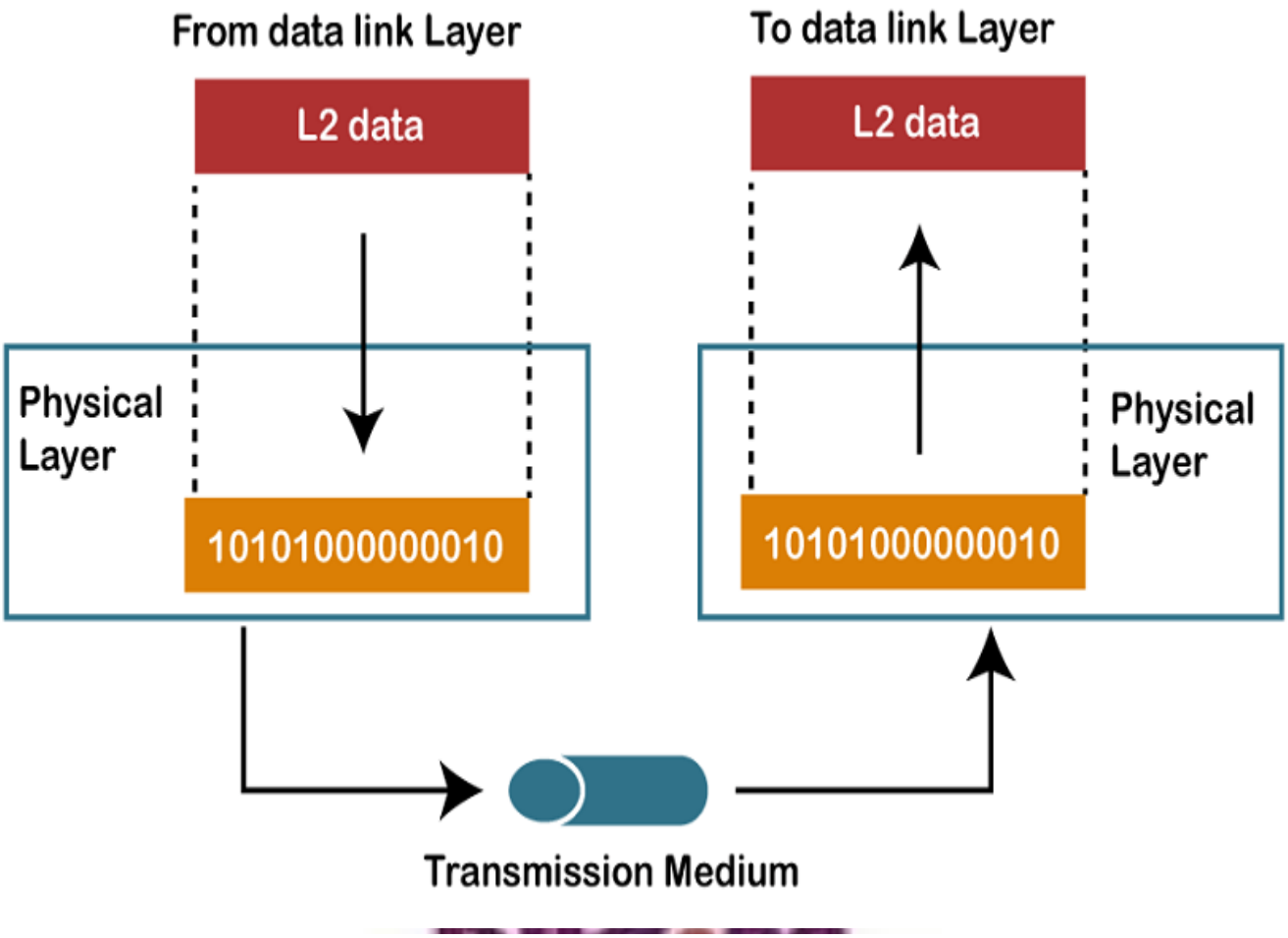
7 Layers of OSI Model

There are the seven OSI layers. Each layer has different functions. A list of seven layers are given below:

1. Physical Layer
2. Data-Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer



1) Physical layer

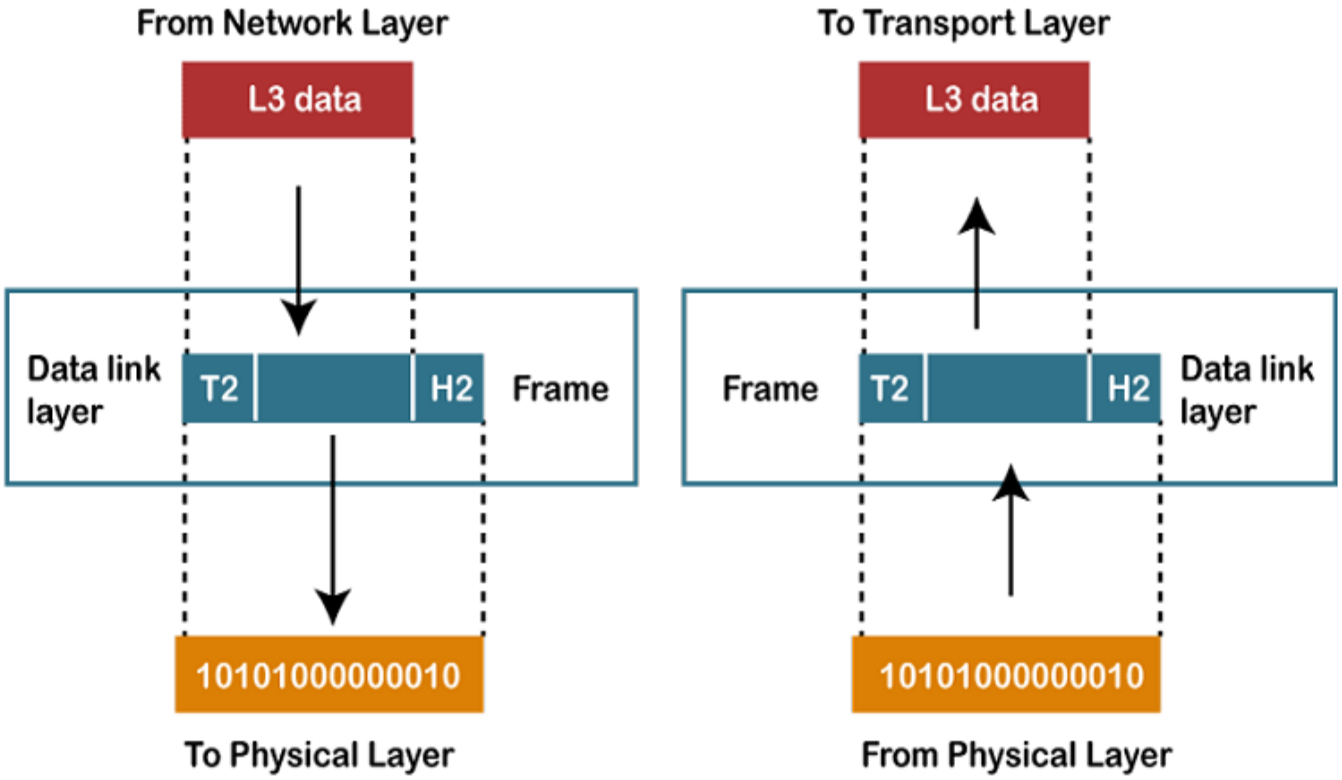


- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.
- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer:

- **Line Configuration:** It defines the way how two or more devices can be connected physically.
- **Data Transmission:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
- **Topology:** It defines the way how network devices are arranged.
- **Signals:** It determines the type of the signal used for transmitting the information.

2) Data-Link Layer



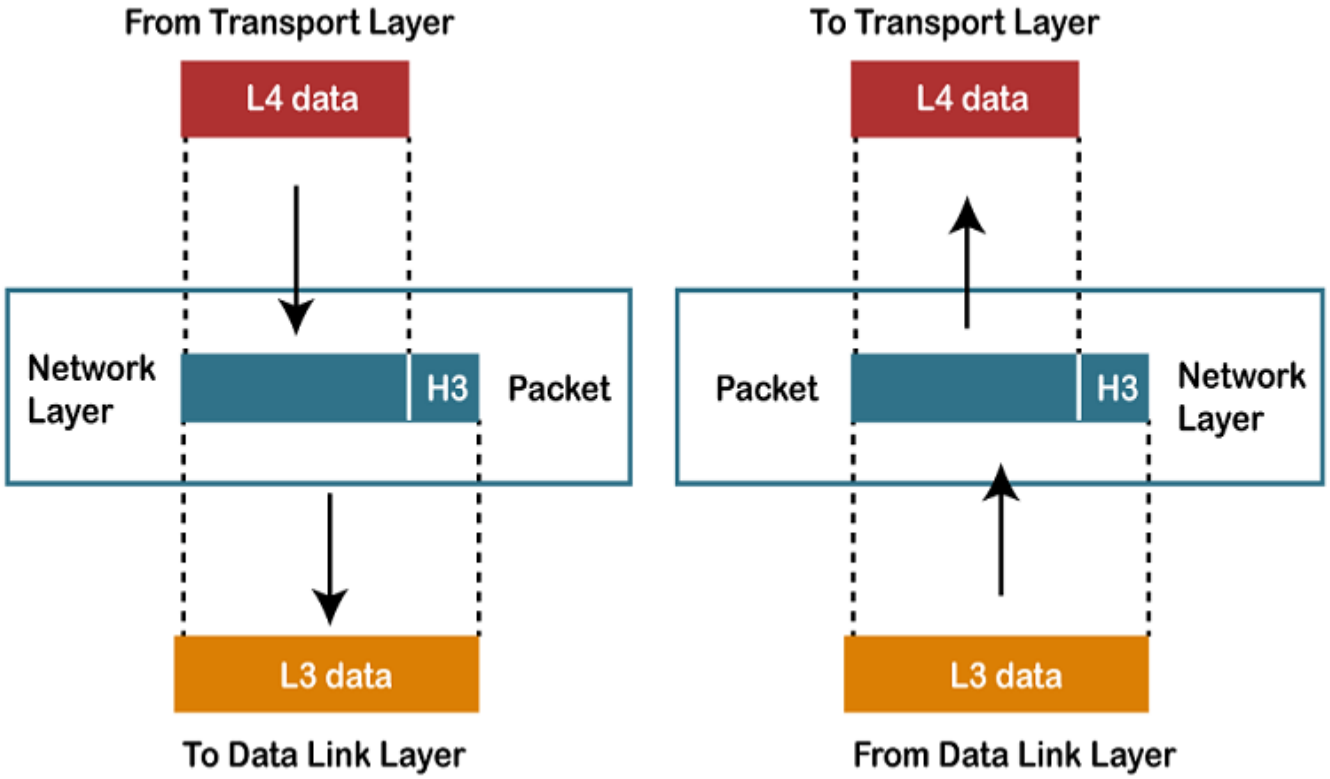
- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.
- It contains two sub-layers:
  - **Logical Link Control Layer**
    - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
    - It identifies the address of the network layer protocol from the header.
    - It also provides flow control.
  - **Media Access Control Layer**
    - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
    - It is used for transferring the packets over the network.

Functions of the Data-link layer

- **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.

- **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

3)NetworkLayer



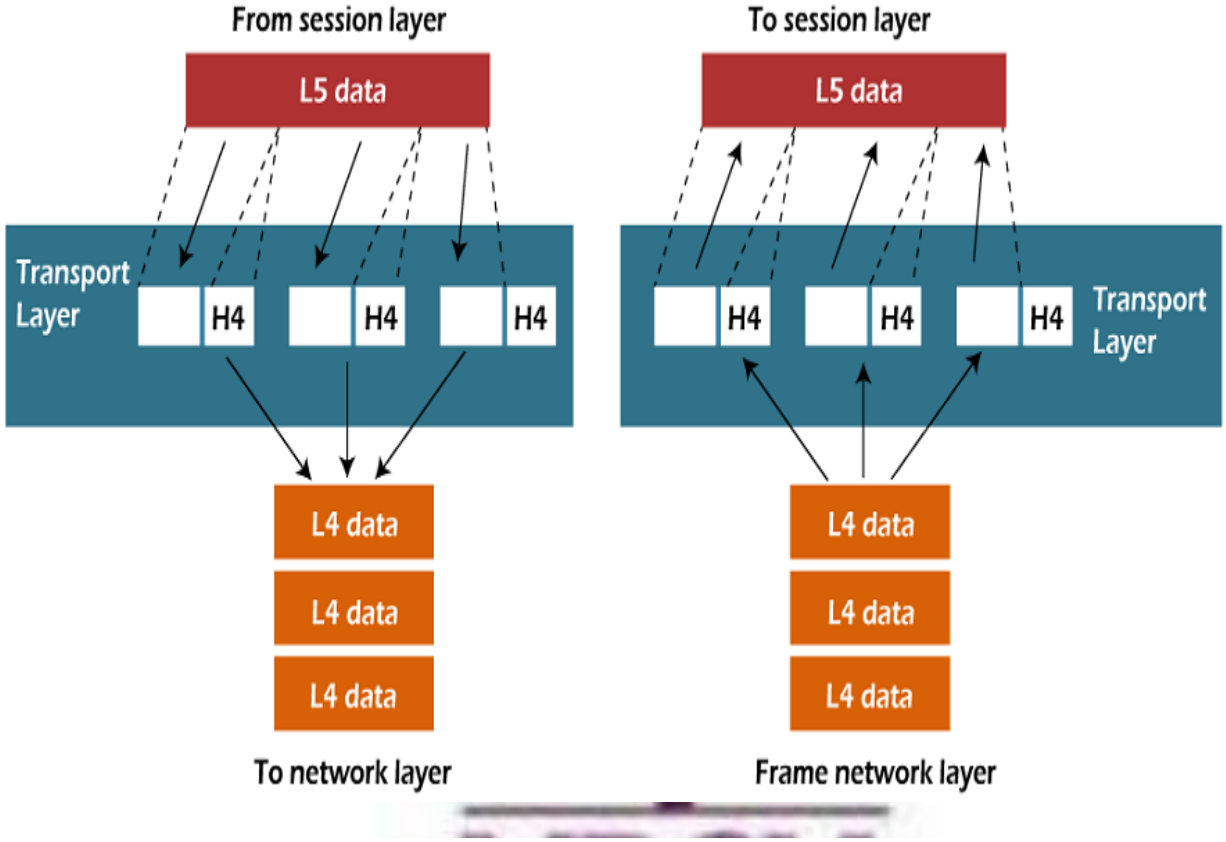
- It is a layer 3 that manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and forwarding the packets.
- Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions of Network Layer:

- **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- **Addressing:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
- **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.

- **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

4)TransportLayer



- The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

The two protocols used in this layer are:

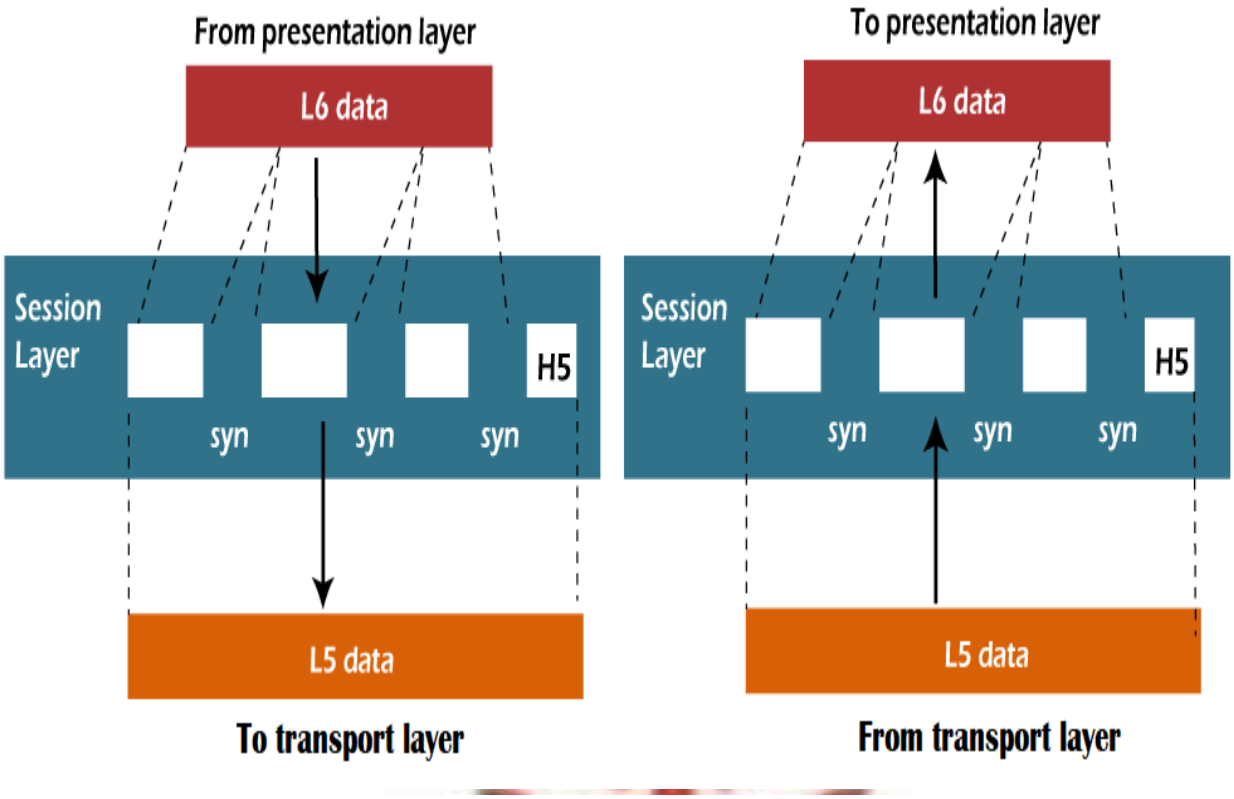
- **Transmission Control Protocol**
  - It is a standard protocol that allows the systems to communicate over the internet.
  - It establishes and maintains a connection between hosts.
  - When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.

- **User Datagram Protocol**
  - User Datagram Protocol is a transport layer protocol.
  - It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

Functions of Transport Layer:

- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
- **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
- **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
- **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

5) Session Layer

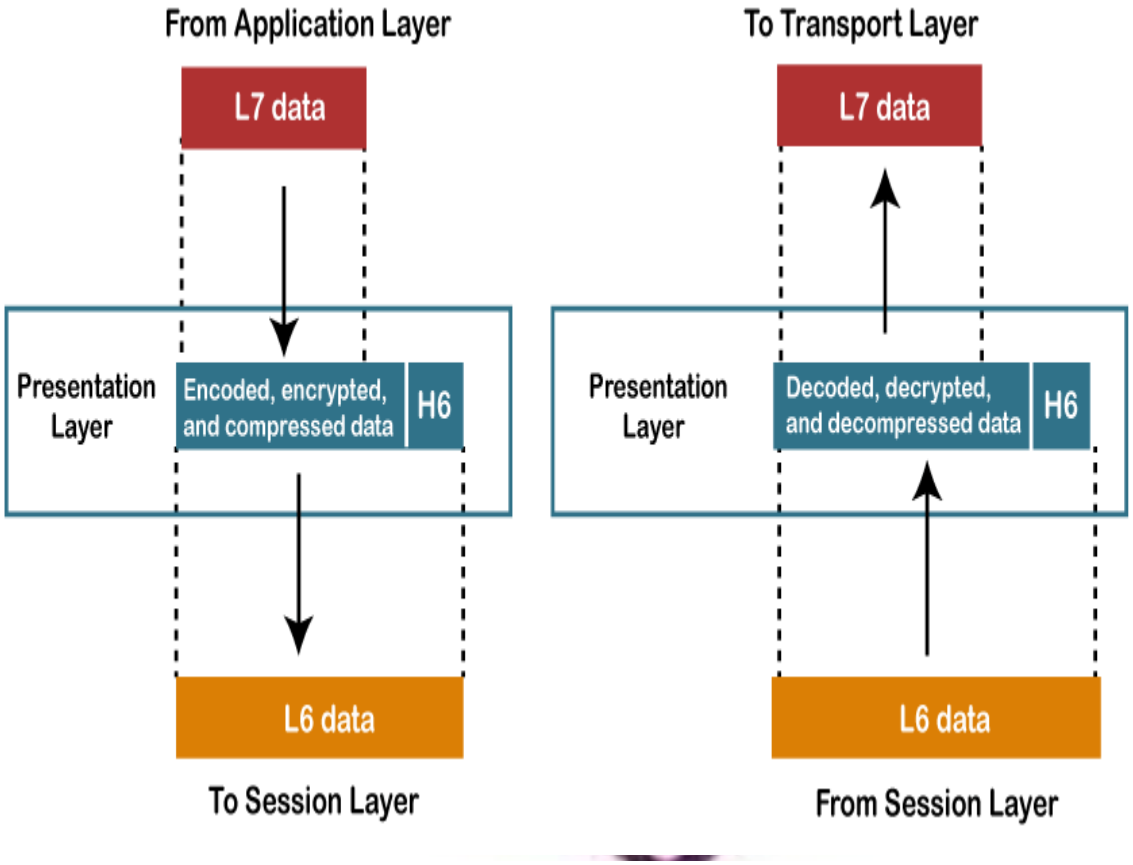


- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Functions of Session layer:

- **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
- **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

6) Presentation Layer

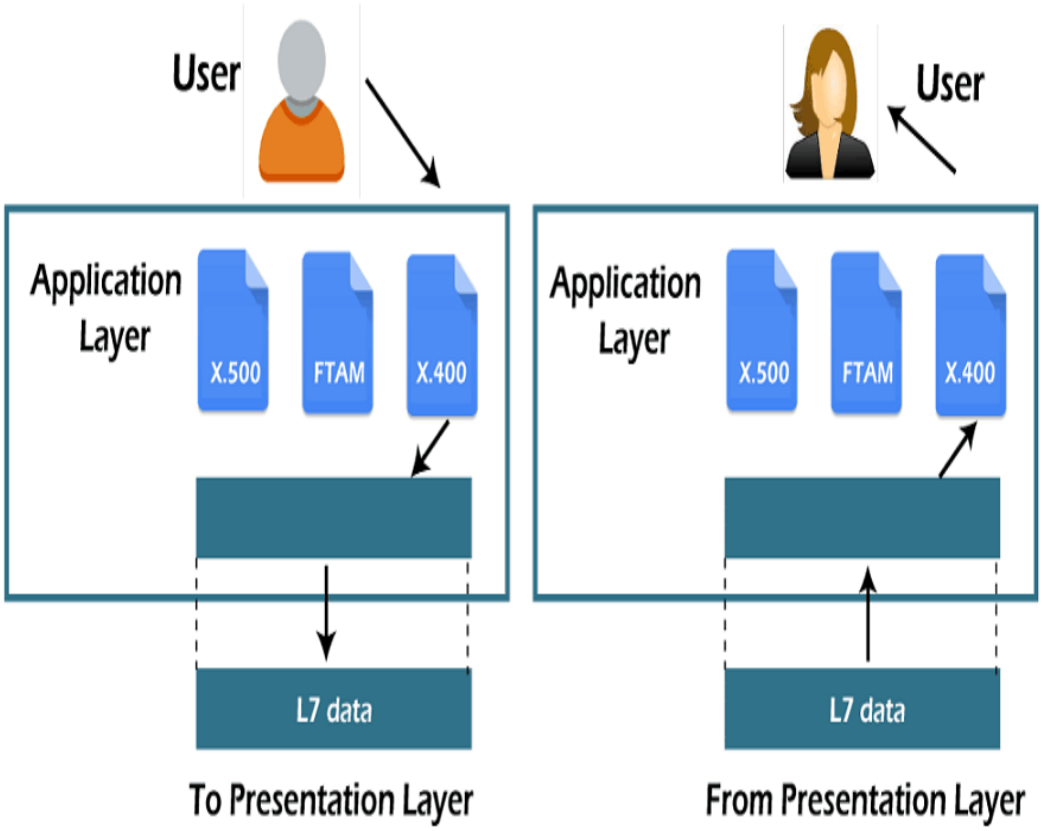


- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation layer is also known as the syntax layer.

Functions of Presentation layer:

- **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.
- **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
- **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

7) Application Layer



- An application layer serves as a window for users and application processes to access network service.
- It handles issues such as network transparency, resource allocation, etc.
- An application layer is not an application, but it performs the application layer functions.
- This layer provides the network services to the end-users.

Functions of Application layer:

- **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- **Mail services:** An application layer provides the facility for email forwarding and storage.
- Directory services: An application provides the distributed database sources and is used to provide that global information about various objects.

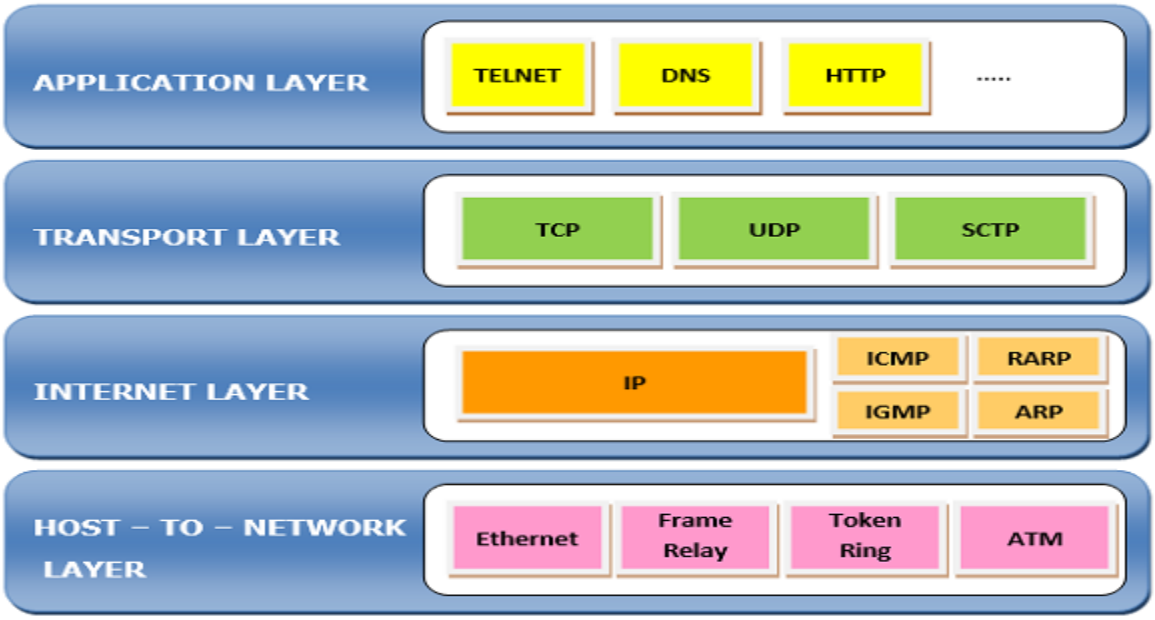
The TCP/IP Reference Model

TCP/IP Reference Model is a four-layered suite of communication protocols. It was developed by the DoD (Department of Defence) in the 1960s. It is named after the two main protocols that are used in the model, namely, TCP and IP. TCP stands for Transmission Control Protocol and IP stands for Internet Protocol.

The four layers in the TCP/IP protocol suite are −

- **Host-to- Network Layer** −It is the lowest layer that is concerned with the physical transmission of data. TCP/IP does not specifically define any protocol here but supports all the standard protocols.
- **Internet Layer** −It defines the protocols for logical transmission of data over the network. The main protocol in this layer is Internet Protocol (IP) and it is supported by the protocols ICMP, IGMP, RARP, and ARP.
- **Transport Layer** − It is responsible for error-free end-to-end delivery of data. The protocols defined here are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- **Application Layer** − This is the topmost layer and defines the interface of host programs with the transport layer services. This layer includes all high-level protocols like Telnet, DNS, HTTP, FTP, SMTP, etc.

The following diagram shows the layers and the protocols in each of the layers −



HTTP

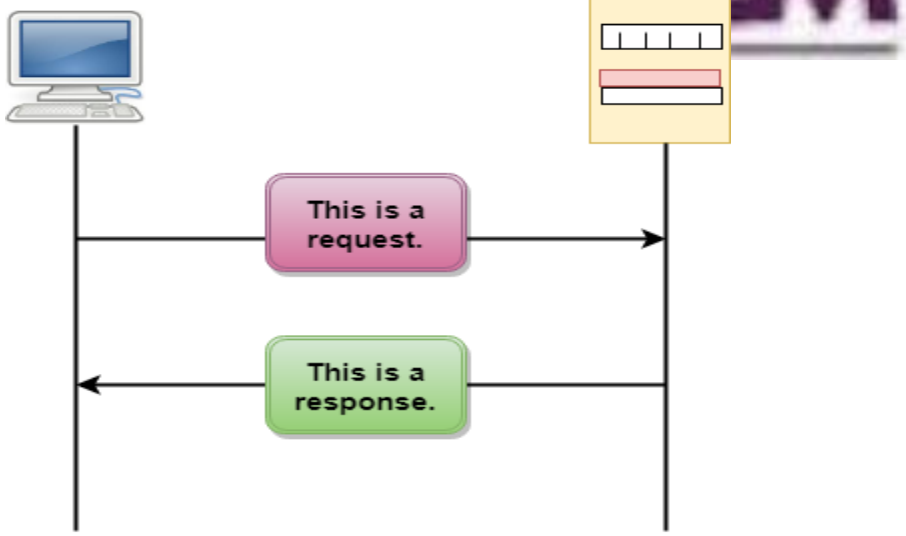
- HTTP stands for **HyperText Transfer Protocol**.
- It is a protocol used to access the data on the World Wide Web (www).
- The HTTP protocol can be used to transfer the data in the form of plain text, hypertext, audio, video, and so on.

- This protocol is known as HyperText Transfer Protocol because of its efficiency that allows us to use in a hypertext environment where there are rapid jumps from one document to another document.
- HTTP is similar to the FTP as it also transfers the files from one host to another host. But, HTTP is simpler than FTP as HTTP uses only one connection, i.e., no control connection to transfer the files.
- HTTP is used to carry the data in the form of MIME-like format.
- HTTP is similar to SMTP as the data is transferred between client and server. The HTTP differs from the SMTP in the way the messages are sent from the client to the server and from server to the client. SMTP messages are stored and forwarded while HTTP messages are delivered immediately.

Features of HTTP:

- **Connectionless protocol:** HTTP is a connectionless protocol. HTTP client initiates a request and waits for a response from the server. When the server receives the request, the server processes the request and sends back the response to the HTTP client after which the client disconnects the connection. The connection between client and server exist only during the current request and response time only.
- **Media independent:** HTTP protocol is a media independent as data can be sent as long as both the client and server know how to handle the data content. It is required for both the client and server to specify the content type in MIME-type header.
- **Stateless:** HTTP is a stateless protocol as both the client and server know each other only during the current request. Due to this nature of the protocol, both the client and server do not retain the information between various requests of the web pages.

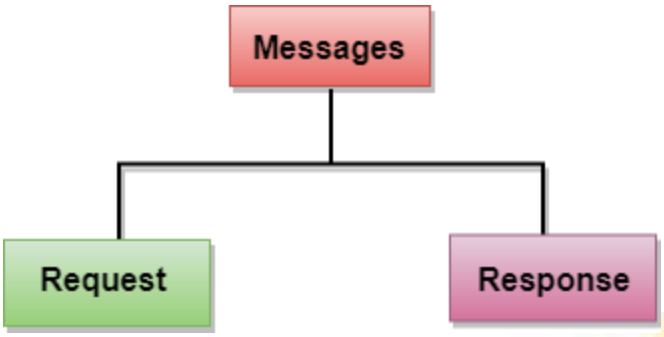
HTTP Transactions



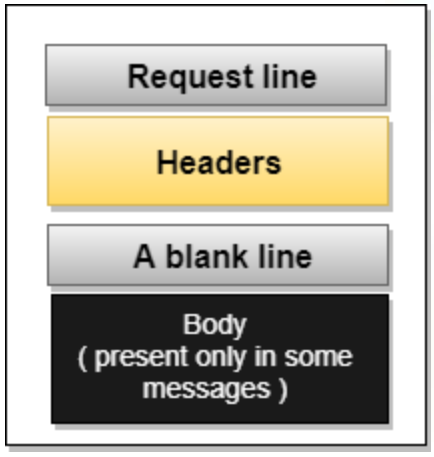
The above figure shows the HTTP transaction between client and server. The client initiates a transaction by sending a request message to the server. The server replies to the request message by sending a response message.

Messages

HTTP messages are of two types: request and response. Both the message types follow the same message format.



Request Message: The request message is sent by the client that consists of a request line, headers, and sometimes a body.



Response Message: The response message is sent by the server to the client that consists of a status line, headers, and sometimes a body.

HTTPS full form

- Difficulty Level : Basic
- Last Updated : 06 May, 2022

Read

Discuss

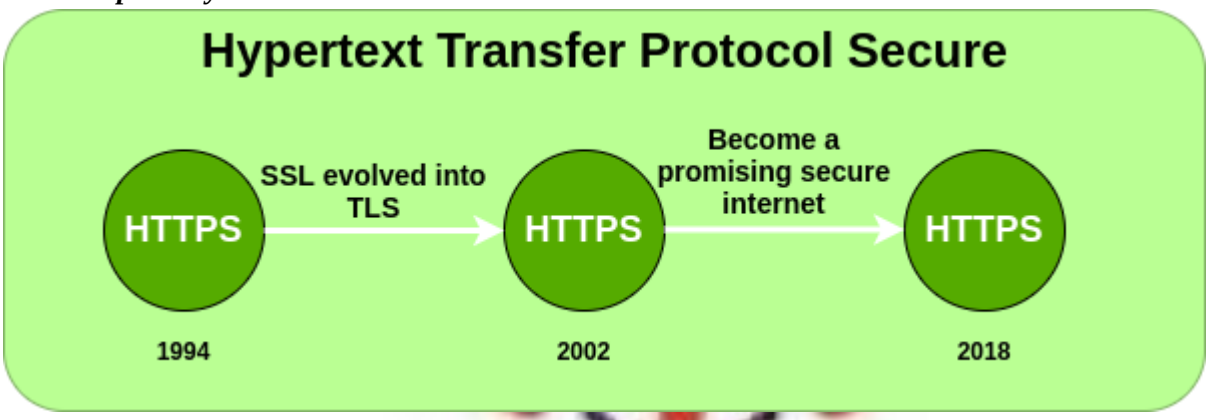
Courses

Practice

Video

HTTPS stands for **Hyper Text Transfer Protocol Secure**. HTTP Secure (HTTPS), could be a combination of the Hypertext Transfer Protocol with the SSL/TLS convention to supply encrypted communication and secure distinguishing proof of a arrange web server.
If the URL of that site is just HTTP, at that point anything you're perusing or whatever points of interest you're putting on that site, on the off chance that a programmer needs to take your data. Therefore, HTTPS is more secure than HTTP because HTTPS is certified by the SSL(Secure Socket Layer). Whatever website you are visiting on the internet, if its URL is HTTP, then that website is not secure. If a website has an SSL certificate installed then the URL of that website will be HTTPS that website will completely secure. You can give any information about your credit card, debit cards, OTP and anything else.

HTTP Improved years:



Characteristics of HTTPS:

- **Security:** Nowadays there's a lot of cyber-attacks on the web. And online installments have also expanded. That's why we need to be secure.If there is no security in any website,then no will use that website.
- **Need of SSL:** Some SEO specialists accept that by introducing SSL on the site, there are a few SEO benefits from Google. And by applying SSL, the positioning of the site in Google is additionally boosted.
- **Authentication:** HTTPS encrypts all message substance, including the HTTP headers and the request/response data.The verification perspective of HTTPS requires a trusted third party to sign server-side digital certificates.
- **Browsing Privately:** HTTPS is presently utilised more frequently by web clients than the first non-secure HTTP, fundamentally to ensure page genuineness on all sorts of websites,secure accounts and to keep client communications.

Advantages of HTTPS:

- Secures your information in-transit.
- Help you boost income per client.
- Protects your site from Phishing, MITM and other information breaches.
- Builds believe on your site visitors. Removes "NOT Secure" warnings.
- Help you move forward website ranking.

Disadvantages of HTTPS:

- A web ask with HTTPS is slower which regularly comes about in moderate page stacking.
- Pages with HTTPS can never be cached could be a shared cache.
- A few intermediary serves or firewall frameworks don't permit get to to locales with HTTPS.
- If you're making web site which has static contents or if there's no private information exchange, you'll select the HTTP.
- Overhead incorporates time to encrypt and decode the information, additional header input for encrypt information, handshaking some time recently exchanging genuine information.

LDAP(LIGHT WEIGHT ACCESS PROTOCOL)

Lightweight directory access protocol (LDAP) is a protocol that makes it possible for applications to query user information rapidly.

Someone within your office wants to do two things: Send an email to a recent hire and print a copy of that conversation on a new printer. LDAP (lightweight directory access protocol) makes both of those steps possible.

Set it up properly, and that employee doesn't need to talk with IT to complete the tasks.

What Is LDAP?

Companies store usernames, passwords, email addresses, printer connections, and other static data within directories. LDAP is an open, vendor-neutral application protocol for accessing and maintaining that data. LDAP can also tackle authentication, so users can sign on just once and access many different files on the server.

LDAP is a protocol, so it doesn't specify how directory programs work. Instead, it's a form of language that allows users to find the information they need very quickly.

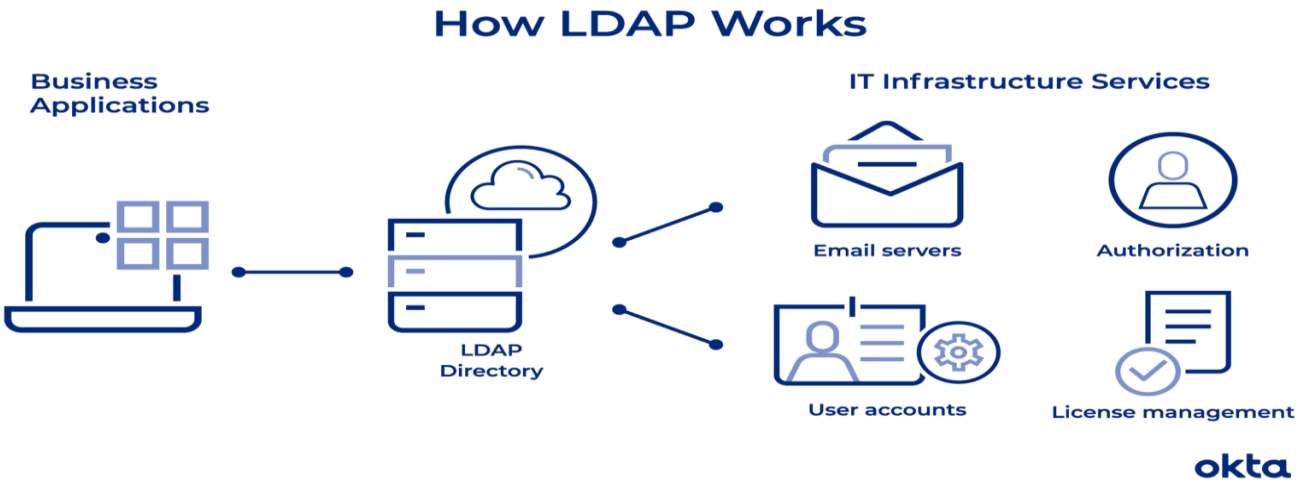
LDAP is vender-neutral, so it can be used with a variety of different directory programs. Typically, a directory contains data that is:

- **Descriptive.** Multiple points, such as name and location, come together to define an asset.
- **Static.** The information doesn’t change much, and when it does, the shifts are subtle.
- **Valuable.** Data stored within the directory is critical to core business functions, and it's touched over and over again.

Sometimes, people use LDAP in concert with other systems throughout the workday. For example, your employees may use LDAP to connect with printers or verify passwords. Those employees may then switch to Google for email, which doesn't rely on LDAP at all.

LDAP isn't new. The definitive whitepaper that describes how directory services work and how LDAP should interface was published in 2003. Despite its age, LDAP is still in widespread use today.

The LDAP Process Explained



The average employee connects with LDAP dozens or even hundreds of times per day. That person may not even know the connection has happened even though the steps to complete a query are intricate and complex.

An LDAP query typically involves:

- **Session connection.** The user connects to the server via an LDAP port.
- **Request.** The user submits a query, such as an email lookup, to the server.
- **Response.** The LDAP protocol queries the directory, finds the information, and delivers it to the user.
- **Completion.** The user disconnects from the LDAP port.

The search looks simple, but a great deal of coding makes the function possible. Developers must determine the size limit of the search, the time the server can spend processing it, how many variables can be included in a search, and more.

A person hopping from company to company might run searches with LDAP in each location. But the way the searches work and how they function can be quite different, depending on how the LDAP is configured.

Before any search commences, the LDAP must authenticate the user. Two methods are available for that work:

- **Simple.** The correct name and password connect the user to the server.
- **Simple Authentication and Security Layer (SASL).** A secondary service, such as Kerberos, performs authentication before the user can connect. For companies that require advanced security, this can be a good option.

Some queries originate within the company's walls, but some start on mobile devices or home computers. Most LDAP communication is sent without scrambling or encryption, and that could cause security problems. Most companies use Transport Layer Security (TLS) to ensure the safety of LDAP messages.

People can tackle all sorts of operations with LDAP. They can:

- **Add.** Enter a new file into the database.
- **Delete.** Take out a file from the database.
- **Search.** Start a query to find something within the database.
- **Compare.** Examine two files for similarities or differences.
- **Modify.** Make a change to an existing entry.

LDAP Terms to Understand

The average person tapping away at a computer doesn't need to know the ins and outs of LDAP. But people who work on network security and access must have a deep understanding of core concepts and structure. And the language people use to describe LDAP can be impenetrable for novices.

Common terms you'll see as you begin to learn about LDAP include:

- **Data models.** What types of information sit within your directory? Models help you understand the facets within your LDAP. You could have general information (such as an object class), names (how each item is uniquely referenced), functions (how the data is accessed), and security (how users move through authentication).
- **Distinguished name (DN).** This is a unique identifier of each entry that also describes location within the information tree.
- **Modifications.** These are requests LDAP users make to alter the data associated with an entry. Defined modification types include adding, deleting, replacing, and increasing.
- **Relative distinguished name (RDN).** This is a way of tying DNs together while specifying relative location.
- **Schema.** The coding that underpins your LDAP is known as schema. You'll use this language to describe the format and attributes of each item that sits on the server.
- **URLs.** This is a string that includes the address and port of a server, along with other data that can define a group, provide a location, or refer an operation to another server.
- **Uniform resource identifier (URI).** This is a string of characters that defines a resource.

This is just a hint of the language you'll need to master to implement LDAP protocols properly. But since LDAP is an open-source protocol, plenty of documents exist that can help you get started and coding like a professional in no time.

MIME Protocol

MIME stands for Multipurpose Internet Mail Extensions. It is used to extend the capabilities of Internet e-mail protocols such as SMTP. The MIME protocol allows the users to exchange various types of digital content such as pictures, audio, video, and various types of documents and files in the e-mail. MIME was created in 1991 by a computer scientist named Nathan Borenstein at a company called Bell Communications.

MIME is an e-mail extension protocol, i.e., it does not operate independently, but it helps to extend the capabilities of e-mail in collaboration with other protocols such as SMTP. Since MIME was able to transfer only text written file in a limited size English language with the help of the internet. At present, it is used by almost all e-mail related service companies such as Gmail, Yahoo-mail, Hotmail.

Need of MIME Protocol

MIME protocol is used to transfer e-mail in the computer network for the following reasons:

1. The MIME protocol supports multiple languages in e-mail, such as Hindi, French, Japanese, Chinese, etc.
2. Simple protocols can reject mail that exceeds a certain size, but there is no word limit in MIME.
3. Images, audio, and video cannot be sent using simple e-mail protocols such as SMTP. These require MIME protocol.
4. Many times, emails are designed using code such as HTML and CSS, they are mainly used by companies for marketing their product. This type of code uses MIME to send email created from HTML and CSS.

MIME Header

MIME adds five additional fields to the header portion of the actual e-mail to extend the properties of the simple email protocol. These fields are as follows:

1. MIME Version
2. Content Type
3. Content Type Encoding
4. Content Id
5. Content description

1. MIME Version

It defines the version of the MIME protocol. This header usually has a parameter value 1.0, indicating that the message is formatted using MIME.

2. Content Type

It describes the type and subtype of information to be sent in the message. These messages can be of many types such as Text, Image, Audio, Video, and they also have many subtypes such that the subtype of the image can be png or jpeg. Similarly, the subtype of Video can be WEBM, MP4 etc.

3. Content Type Encoding

In this field, it is told which method has been used to convert mail information into ASCII or Binary number, such as 7-bit encoding, 8-bit encoding, etc.

4. Content Id

In this field, a unique "Content Id" number is appended to all email messages so that they can be uniquely identified.

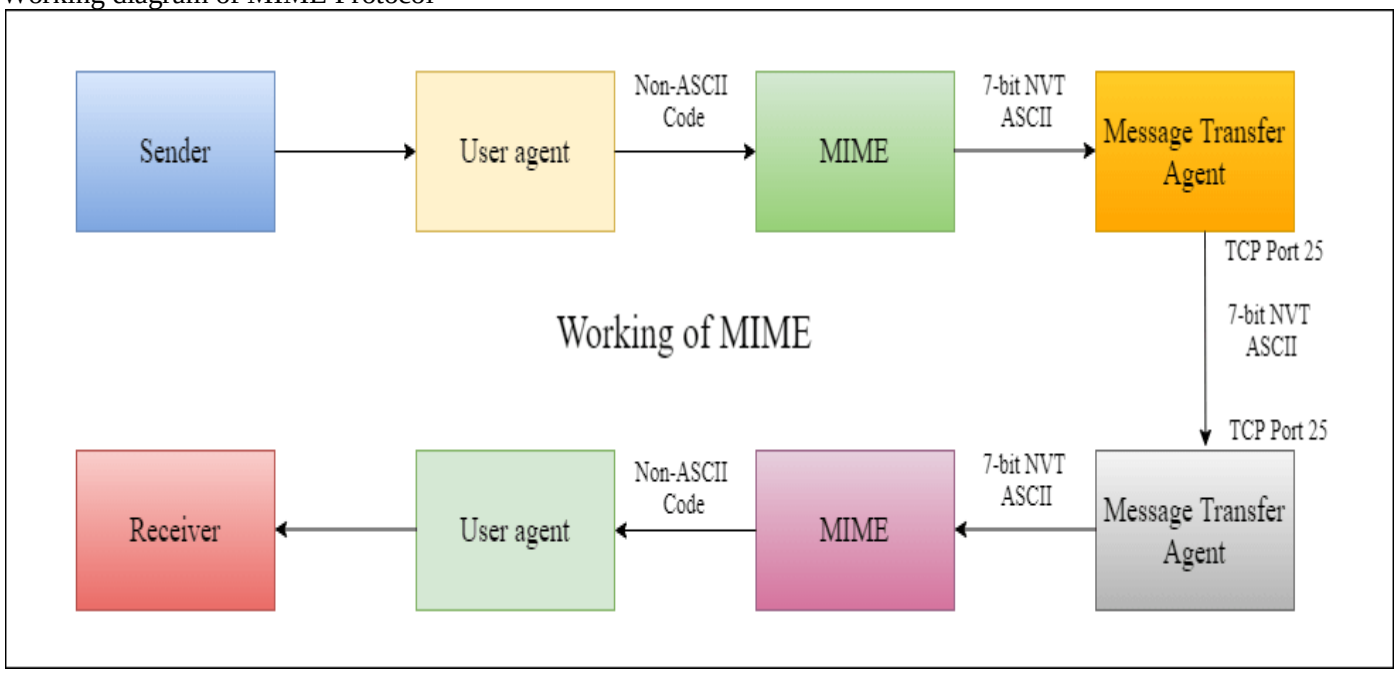
5. Content description

This field contains a brief description of the content within the email. This means that information about whatever is being sent in the mail is clearly in the "Content Description". This field also provides the information of name, creation date, and modification date of the file.

Example of Content description

```
Content-Description: attachment; filename = javatpoint.jpeg;
modification-date = "Wed, 12 Feb 1997 16:29:51 -0500";
```

Working diagram of MIME Protocol



Features of MIME Protocol

1. It supports multiple attachments in a single e-mail.
2. It supports the non-ASCII characters.
3. It supports unlimited e-mail length.
4. It supports multiple languages.

Advantage of the MIME

The MIME protocol has the following advantages:

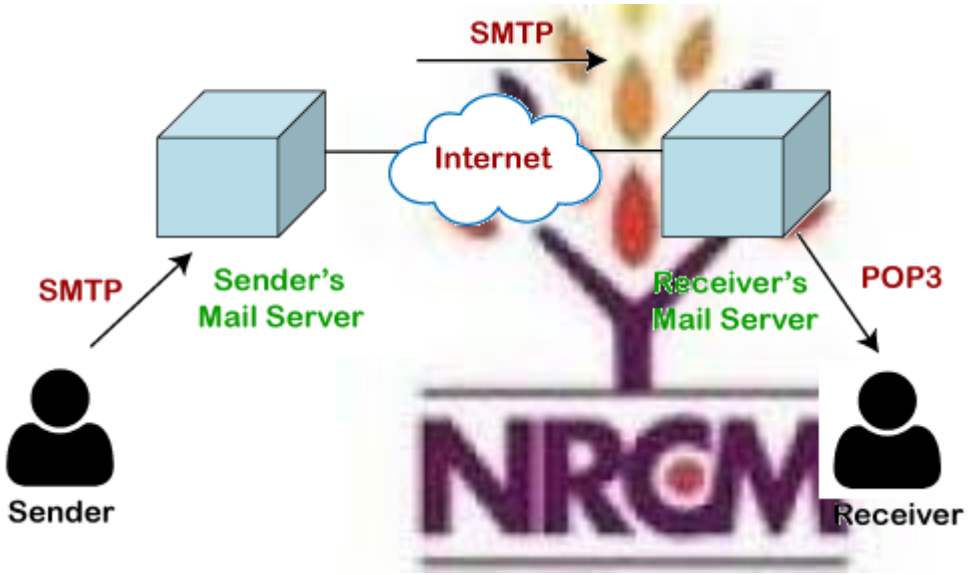
1. It is capable of sending various types of files in a message, such as text, audio, video files.

2. It also provides the facility to send and receive emails in different languages like Hindi, French, Japanese, Chinese etc.
3. It also provides the facility of connecting HTML and CSS to email, due to which people can design email as per their requirement and make it attractive and beautiful.
4. It is capable of sending the information contained in an email regardless of its length.
5. It assigns a unique id to all e-mails.

POP Protocol

The POP protocol stands for Post Office Protocol. As we know that SMTP is used as a message transfer agent. When the message is sent, then SMPT is used to deliver the message from the client to the server and then to the recipient server. But the message is sent from the recipient server to the actual server with the help of the Message Access Agent. The Message Access Agent contains two types of protocols, i.e., POP3 and IMAP.

How is mail transmitted?



Suppose sender wants to send the mail to receiver. First mail is transmitted to the sender's mail server. Then, the mail is transmitted from the sender's mail server to the receiver's mail server over the internet. On receiving the mail at the receiver's mail server, the mail is then sent to the user. The whole process is done with the help of Email protocols. The transmission of mail from the sender to the sender's mail server and then to the receiver's mail server is done with the help of the SMTP protocol. At the receiver's mail server, the POP or IMAP protocol takes the data and transmits to the actual user.

Since SMTP is a push protocol so it pushes the message from the client to the server. As we can observe in the above figure that SMTP pushes the message from the client to the recipient's mail server. The third stage of email communication requires a pull protocol, and POP is a pull protocol. When the mail is transmitted from the recipient mail server to the client which means that the client is pulling the mail from the server.

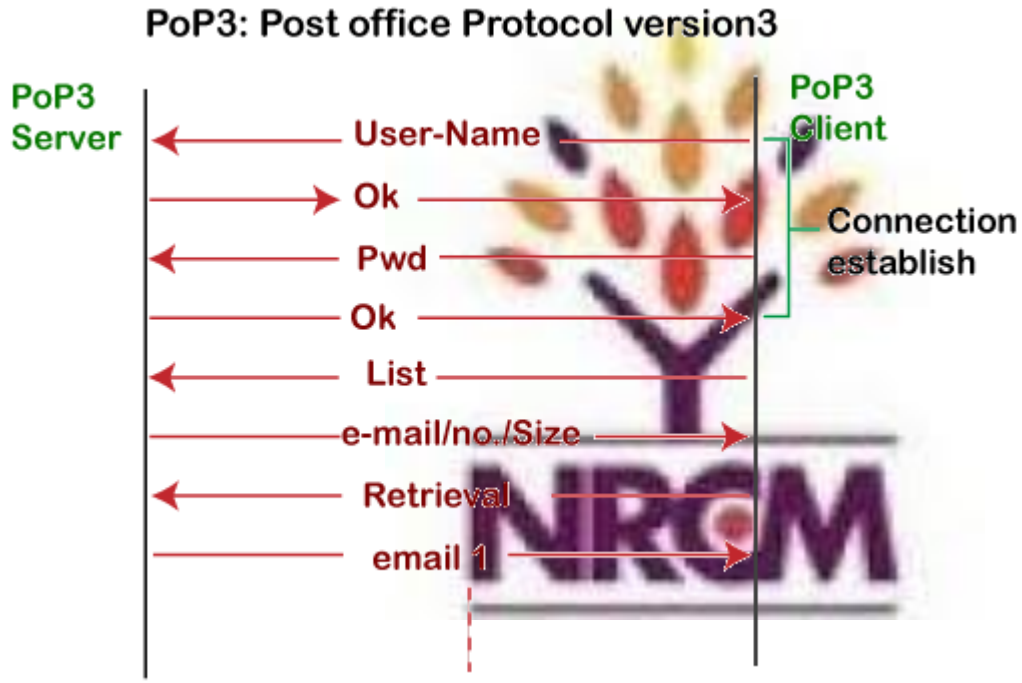
What is POP3?

The POP3 is a simple protocol and having very limited functionalities. In the case of the POP3 protocol, the POP3 client is installed on the recipient system while the POP3 server is installed on the recipient's mail server.

In 1985, the post office protocol version 2 was introduced in RFC 937, but it was replaced with the post office protocol version 3 in 1988 with the publication of RFC 1081. Then, POP3 was revised for the next 10 years before it was published. Once it was refined completely, it got published on 1996.

Although the POP3 protocol has undergone various enhancements, the developers maintained a basic principle that it follows a three-stage process at the time of mail retrieval between the client and the server. They tried to make this protocol very simple, and this simplicity makes this protocol very popular today.

Let's understand the working of the POP3 protocol.



To establish the connection between the POP3 server and the POP3 client, the POP3 server asks for the user name to the POP3 client. If the username is found in the POP3 server, then it sends the ok message. It then asks for the password from the POP3 client; then the POP3 client sends the password to the POP3 server. If the password is matched, then the POP3 server sends the OK message, and the connection gets established. After the establishment of a connection, the client can see the list of mails on the POP3 mail server. In the list of mails, the user will get the email numbers and sizes from the server. Out of this list, the user can start the retrieval of mail.

Once the client retrieves all the emails from the server, all the emails from the server are deleted. Therefore, we can say that the emails are restricted to a particular machine, so it would not be possible to access the same mails on another machine. This situation can be overcome by configuring the email settings to leave a copy of mail on the mail server.

Advantages of POP3 protocol

The following are the advantages of a POP3 protocol:

- It allows the users to read the email offline. It requires an internet connection only at the time of downloading emails from the server. Once the mails are downloaded from the server, then all the downloaded mails reside on our PC or hard disk of our computer, which can be accessed without the internet. Therefore, we can say that the POP3 protocol does not require permanent internet connectivity.
- It provides easy and fast access to the emails as they are already stored on our PC.
- There is no limit on the size of the email which we receive or send.
- It requires less server storage space as all the mails are stored on the local machine.
- There is maximum size on the mailbox, but it is limited by the size of the hard disk.
- It is a simple protocol so it is one of the most popular protocols used today.
- It is easy to configure and use.

Disadvantages of POP3 protocol

The following are the advantages of a POP3 protocol:

- If the emails are downloaded from the server, then all the mails are deleted from the server by default. So, mails cannot be accessed from other machines unless they are configured to leave a copy of the mail on the server.
- Transferring the mail folder from the local machine to another machine can be difficult.
- Since all the attachments are stored on your local machine, there is a high risk of a virus attack if the virus scanner does not scan them. The virus attack can harm the computer.
- The email folder which is downloaded from the mail server can also become corrupted.
- The mails are stored on the local machine, so anyone who sits on your machine can access the email folder.

What is RMON in the Computer Network?

RMON stands for Remote Network Monitoring. It is an extension of the Simple Network Management Protocol (SNMP) that allows detailed monitoring of network statistics for Ethernet networks.

RMON was initially developed to address remote site and local area network (LAN) segment management from a centralized location. The RMON standard determines a group of functions and statistics exchanged between RMON compatible network probes and console managers.

ROM Versions

There are two ROM Versions which are as follows −

RMON1 MIB

It has defined 10 MIB groups for basic network monitoring. It operates on the MAC layer and the physical layer.

- **Statistics MIB Group** − It contains a statistic measured by the probe for each monitored interface on this device. It includes statistics on packets dropped, packets sent, bytes, sent, broadcast packets, multicast packets, CRC errors, giants, packet fragments.
- **History** − It records periodic statistical samples from a network and stores them for retrieval. It contains the number of samples, items sampled in different periods.
- **Alarm** − It periodically takes statistical samples and compares them with the threshold set for events generation. It includes an alarm table & implementation of event group, Alarm type, interval, starting threshold, stop threshold.
- **HOST** − It contains statistics associated with each host discovered on the network. Statistics contains Host address, packets & bytes that are received and transmitted, broadcast packets, multicast packets, error packets.
- **HOST top N** − It prepares tables that describe the top hosts. It contains statistics on hosts, sample, and start and stop period, rate base duration.
- **Matrix** − It stores and retrieves statistics for conversations between sets of two addresses. Its elements are source & destination address pairs, their packets, bytes & errors for each pair.
- **Filters** − It enables packets to be matched by a filter equation for capturing packets or events. Its elements are bit-filter type, filter expression, conditional expression to other filters.
- **Packet Capture** − It enables packets to be captured after they flow through a channel. Its elements are the buffer size for captured packets, full status, and the number of captured packets.
- **Events** − It controls the generation and notification of events from a device. Its elements are event type, description, last time event sent.
- **Token ring** − It supports token rings.

RMON 2 MIB Group

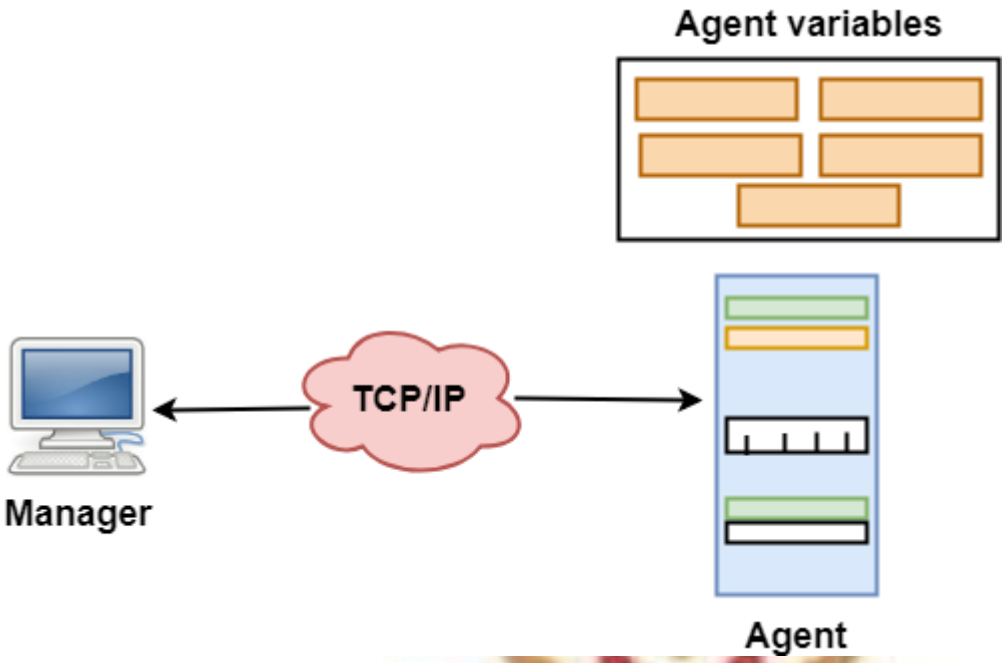
It operates on the above protocol layers of the OSI model: application, presentation, session, and transport & Network layer.

- **Protocol Delivery** − It is a simple and interoperable way for an RMON 2 application to establish which protocols a particular RMON 2 agent implements.
- **Protocol Distribution** − It maps the data collected by a probe to the correct protocol name displayed to the network manager.
- **Address Mapping** − It helps address translation from the MAC layer to network layer addresses that are easier to read. It also supports the SNMP management platform and will lead to improved topology.
- **Network Layer host** − It contains statistics for network layer traffic to or from each host.
- **Network Layer Matrix** − It contains network layer traffic statistics for conversations between pairs of hosts.
- **Application Layer Host** − It contains statistics for application layer traffic to or from each host.
- **Application Layer Matrix** − It stores and retrieves application layer statistics for conversation between sets of two addresses.
- **Probe Configuration** − It provides a standard way to remotely configure probe parameters such as trap destination and out-of-band management.
- **User History Collection** − It contains periodic samples of user-specified variables.

SNMP

- SNMP stands for **Simple Network Management Protocol**.
- SNMP is a framework used for managing devices on the internet.
- It provides a set of operations for monitoring and managing the internet.

SNMP Concept



- SNMP has two components Manager and agent.
- The manager is a host that controls and monitors a set of agents such as routers.
- It is an application layer protocol in which a few manager stations can handle a set of agents.
- The protocol designed at the application level can monitor the devices made by different manufacturers and installed on different physical networks.
- It is used in a heterogeneous network made of different LANs and WANs connected by routers or gateways.

Managers & Agents

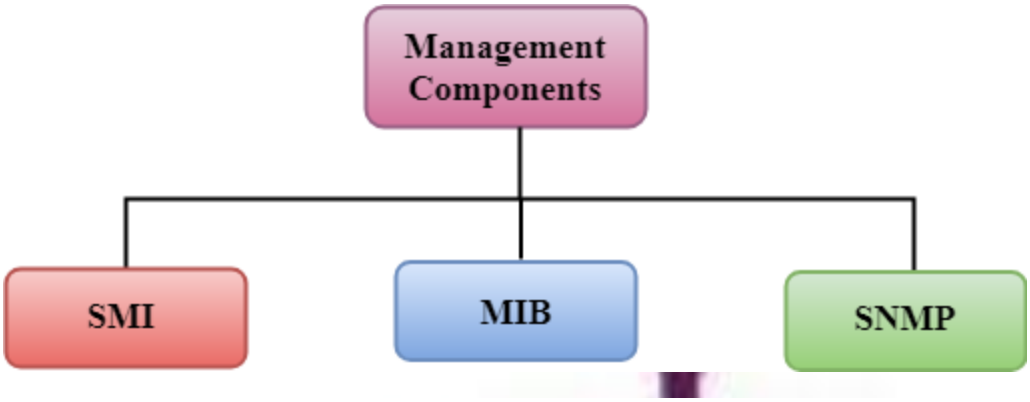
- A manager is a host that runs the SNMP client program while the agent is a router that runs the SNMP server program.
- Management of the internet is achieved through simple interaction between a manager and agent.
- The agent is used to keep the information in a database while the manager is used to access the values in the database. For example, a router can store the appropriate variables such as a number of packets received and forwarded while the manager can compare these variables to determine whether the router is congested or not.
- Agents can also contribute to the management process. A server program on the agent checks the environment, if something goes wrong, the agent sends a warning message to the manager.

Management with SNMP has three basic ideas:

- A manager checks the agent by requesting the information that reflects the behavior of the agent.
- A manager also forces the agent to perform a certain function by resetting values in the agent database.
- An agent also contributes to the management process by warning the manager regarding an unusual condition.

Management Components

- Management is not achieved only through the SNMP protocol but also the use of other protocols that can cooperate with the SNMP protocol. Management is achieved through the use of the other two protocols: SMI (Structure of management information) and MIB(management information base).
- Management is a combination of SMI, MIB, and SNMP. All these three protocols such as abstract syntax notation 1 (ASN.1) and basic encoding rules (BER).

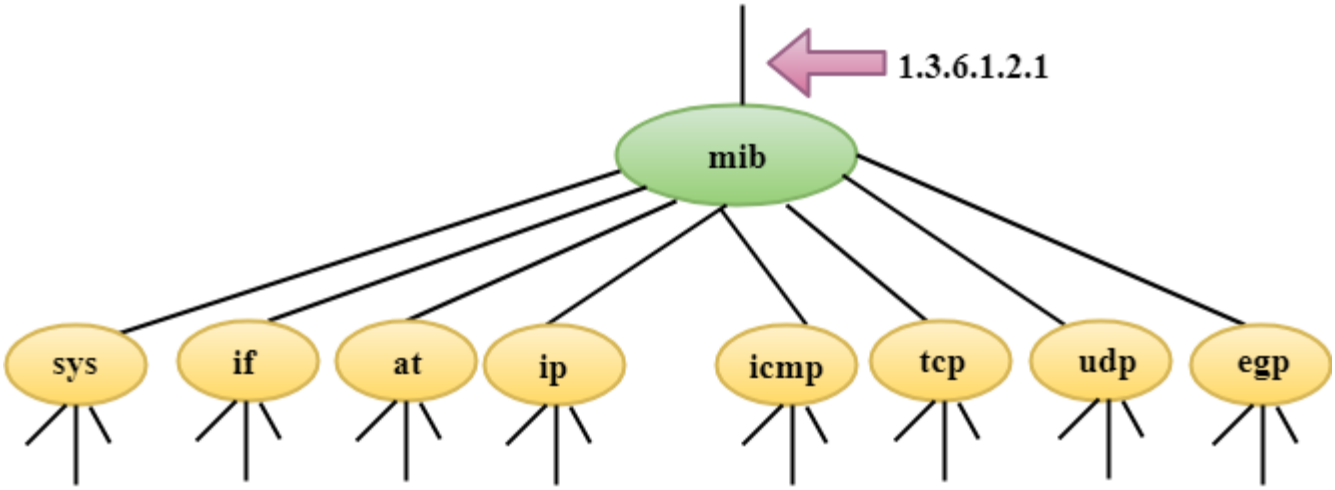


SMI

The SMI (Structure of management information) is a component used in network management. Its main function is to define the type of data that can be stored in an object and to show how to encode the data for the transmission over a network.

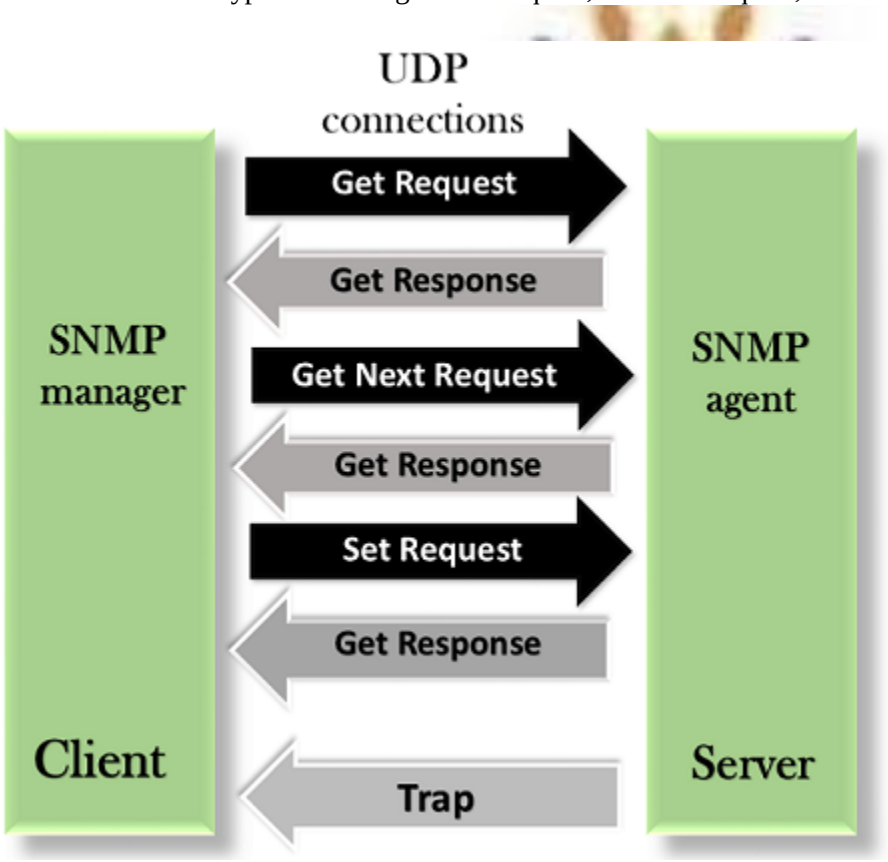
MIB

- The MIB (Management information base) is a second component for the network management.
- Each agent has its own MIB, which is a collection of all the objects that the manager can manage. MIB is categorized into eight groups: system, interface, address translation, ip, icmp, tcp, udp, and egp. These groups are under the mib object.



SNMP

SNMP defines five types of messages: GetRequest, GetNextRequest, SetRequest, GetResponse, and Trap.



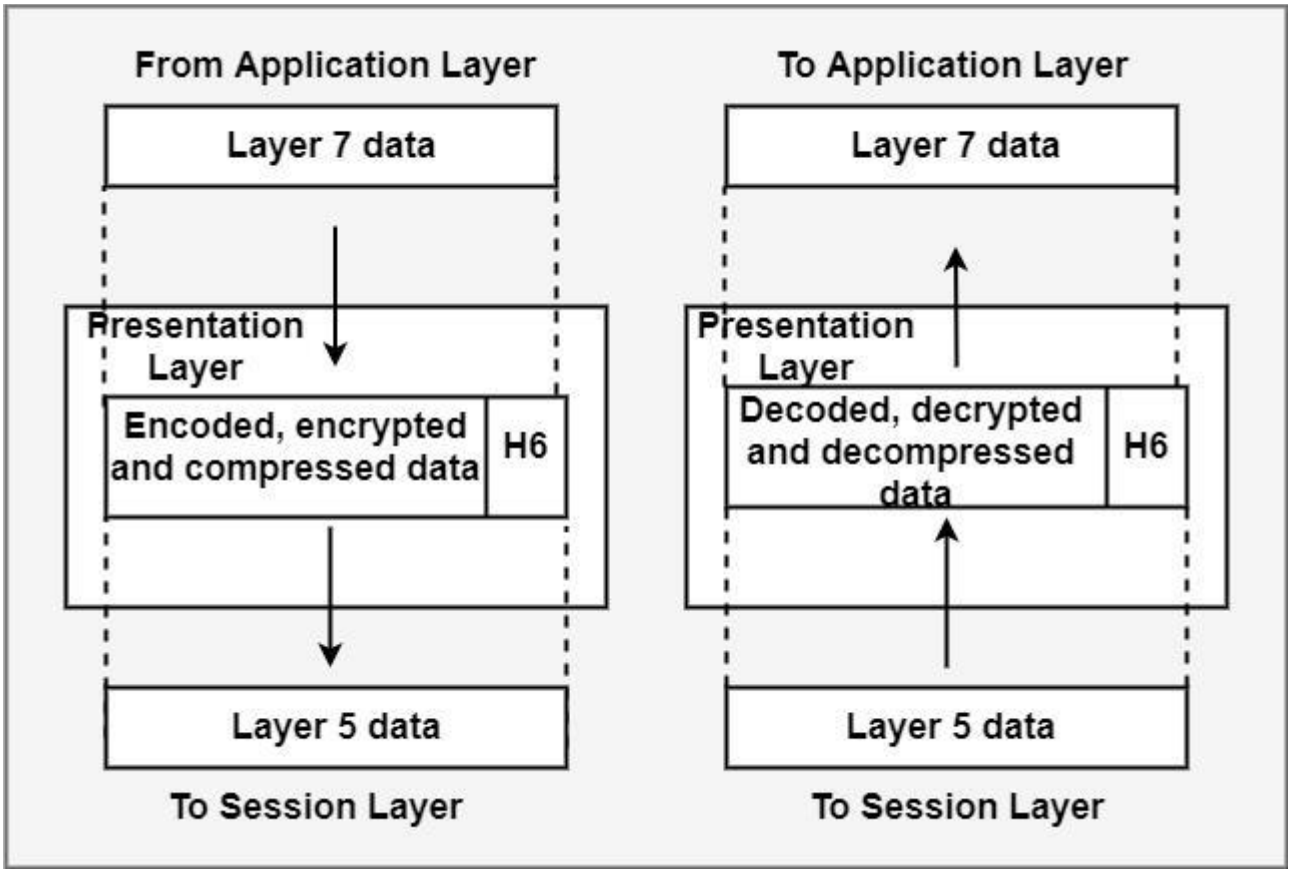
GetRequest: The GetRequest message is sent from a manager (client) to th

What is a presentation layer?

The presentation layer changes the data from an application layer into the device native internal mathematical structure and encodes communicated information into a displayable output format.

It executes the code changes, document compressions, security encryption, etc. It also defines the data as per the software/hardware environment of the hub. For instance, demonstrating UNIX structured data in windows.

The link between the presentation layer and the application and session layer has been shown in the diagram below –



It is concerned with the syntax of data.

Translation

The procedure in two frameworks are generally to exchange the data in the form of character strings, numbers etc. The data must be exchanged into a bitstream before being transmitted.

Encryption

To carry any sensitive data, the presentation layer encrypts the data at the sender's end and decrypts at the receiver's end.

Compression

Compression means the reduction of bits. It is required in the case of multiline text, audio and video.

Function of presentation layer

The functions of presentation layer are explained below −

- **Data Compression:** It decreases the various bits to be sent by shrinking the data.
- **Data Conversion:** It layouts the data on several hubs according to the software/hardware environment.
- **Code Conversion:** The form and syntax (language) of the two connecting frameworks can be different. One framework uses the American Standard Code for Information Interchange (ASCII) code to document transfer, and the other facilitates the Extended Binary Coded Decimal Interchange Code (EBCDIC) developed by the Computer hardware company IBM. It offers the "translation" from ASCII to EBCDIC and vice versa.
- **Data Encryption:** It encodes information in a particular format so that each user or application cannot understand it.
- All the receiver end performs the **decomposition, decoding and decryption.**

UNIT-II
Remote Procedure Call (RPC)

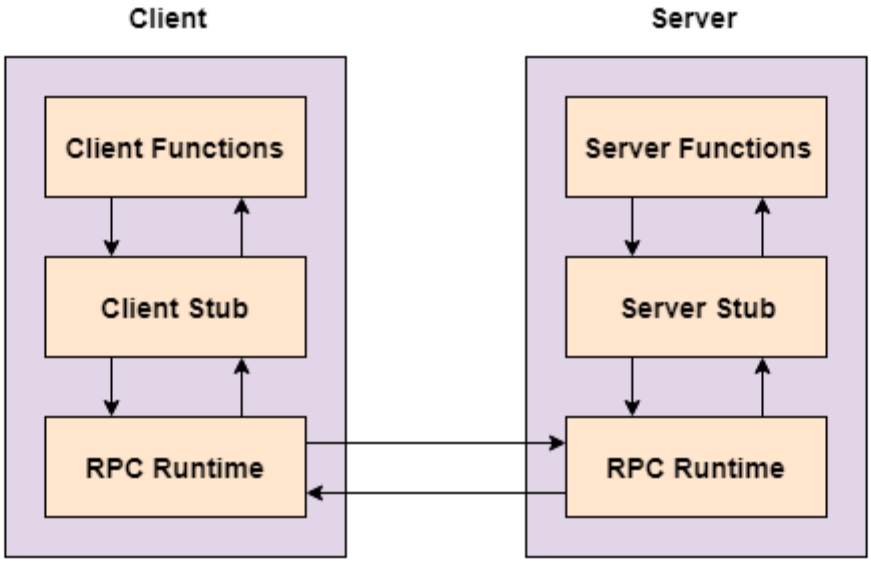
A remote procedure call is an interprocess communication technique that is used for client-server based applications. It is also known as a subroutine call or a function call.

A client has a request message that the RPC translates and sends to the server. This request may be a procedure or a function call to a remote server. When the server receives the request, it sends the required response back to the client. The client is blocked while the server is processing the call and only resumed execution after the server is finished.

The sequence of events in a remote procedure call are given as follows −

- The client stub is called by the client.
- The client stub makes a system call to send the message to the server and puts the parameters in the message.
- The message is sent from the client to the server by the client's operating system.
- The message is passed to the server stub by the server operating system.
- The parameters are removed from the message by the server stub.
- Then, the server procedure is called by the server stub.

A diagram that demonstrates this is as follows −



Advantages of Remote Procedure Call

Some of the advantages of RPC are as follows −

- Remote procedure calls support process oriented and thread oriented models.
- The internal message passing mechanism of RPC is hidden from the user.
- The effort to re-write and re-develop the code is minimum in remote procedure calls.
- Remote procedure calls can be used in distributed environment as well as the local environment.
- Many of the protocol layers are omitted by RPC to improve performance.

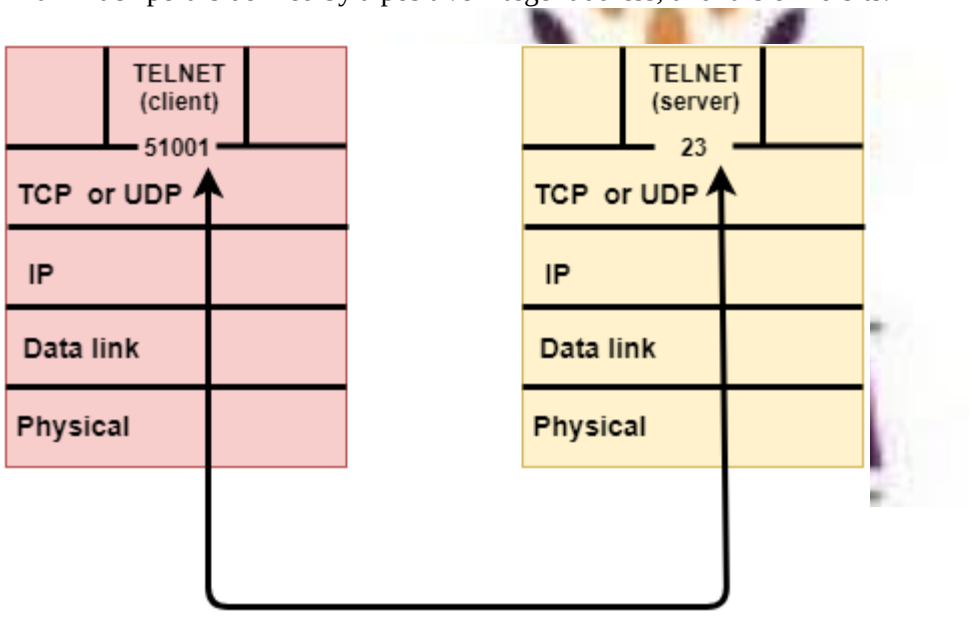
Disadvantages of Remote Procedure Call

Some of the disadvantages of RPC are as follows −

- The remote procedure call is a concept that can be implemented in different ways. It is not a standard.
- There is no flexibility in RPC for hardware architecture. It is only interaction based.
- There is an increase in costs because of remote procedure call.

Transport Layer protocols

- The transport layer is represented by two protocols: TCP and UDP.
- The IP protocol in the network layer delivers a datagram from a source host to the destination host.
- Nowadays, the operating system supports multiuser and multiprocessing environments, an executing program is called a process. When a host sends a message to other host means that source process is sending a process to a destination process. The transport layer protocols define some connections to individual ports known as protocol ports.
- An IP protocol is a host-to-host protocol used to deliver a packet from source host to the destination host while transport layer protocols are port-to-port protocols that work on the top of the IP protocols to deliver the packet from the originating port to the IP services, and from IP services to the destination port.
- Each port is defined by a positive integer address, and it is of 16 bits.

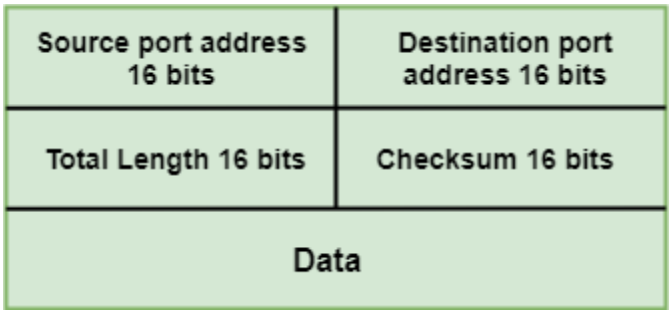


UDP

- UDP stands for **User Datagram Protocol**.
- UDP is a simple protocol and it provides nonsequenced transport functionality.
- UDP is a connectionless protocol.
- This type of protocol is used when reliability and security are less important than speed and size.
- UDP is an end-to-end transport level protocol that adds transport-level addresses, checksum error control, and length information to the data from the upper layer.
- The packet produced by the UDP protocol is known as a user datagram.

User Datagram Format

The user datagram has a 16-byte header which is shown below:



Where,

- **Source port address:** It defines the address of the application process that has delivered a message. The source port address is of 16 bits address.
- **Destination port address:** It defines the address of the application process that will receive the message. The destination port address is of a 16-bit address.
- **Total length:** It defines the total length of the user datagram in bytes. It is a 16-bit field.
- **Checksum:** The checksum is a 16-bit field which is used in error detection.

Disadvantages of UDP protocol

- UDP provides basic functions needed for the end-to-end delivery of a transmission.
- It does not provide any sequencing or reordering functions and does not specify the damaged packet when reporting an error.
- UDP can discover that an error has occurred, but it does not specify which packet has been lost as it does not contain an ID or sequencing number of a particular data segment.

TCP

- TCP stands for Transmission Control Protocol.
- It provides full transport layer services to applications.
- It is a connection-oriented protocol means the connection established between both the ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission.

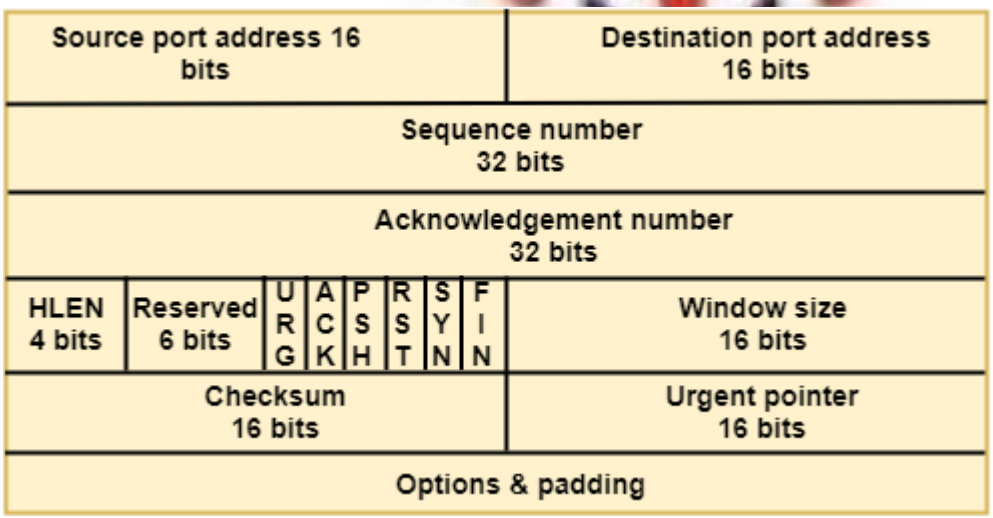
Features Of TCP protocol

- **Stream data transfer:** TCP protocol transfers the data in the form of contiguous stream of bytes. TCP group the bytes in the form of TCP segments and then passed it to the IP layer for transmission to the destination. TCP itself segments the data and forward to the IP.
- **Reliability:** TCP assigns a sequence number to each byte transmitted and expects a positive acknowledgement from the receiving TCP. If ACK is not received within a timeout interval, then the data is

retransmitted to the destination.
The receiving TCP uses the sequence number to reassemble the segments if they arrive out of order or to eliminate the duplicate segments.

- **Flow Control:** When receiving TCP sends an acknowledgement back to the sender indicating the number the bytes it can receive without overflowing its internal buffer. The number of bytes is sent in ACK in the form of the highest sequence number that it can receive without any problem. This mechanism is also referred to as a window mechanism.
- **Multiplexing:** Multiplexing is a process of accepting the data from different applications and forwarding to the different applications on different computers. At the receiving end, the data is forwarded to the correct application. This process is known as demultiplexing. TCP transmits the packet to the correct application by using the logical channels known as ports.
- **Logical Connections:** The combination of sockets, sequence numbers, and window sizes, is called a logical connection. Each connection is identified by the pair of sockets used by sending and receiving processes.
- **Full Duplex:** TCP provides Full Duplex service, i.e., the data flow in both the directions at the same time. To achieve Full Duplex service, each TCP should have sending and receiving buffers so that the segments can flow in both the directions. TCP is a connection-oriented protocol. Suppose the process A wants to send and receive the data from process B. The following steps occur:
  - Establish a connection between two TCPs.
  - Data is exchanged in both the directions.
  - The Connection is terminated.

TCP Segment Format



Where,

- **Source port address:** It is used to define the address of the application program in a source computer. It is a 16-bit field.
- **Destination port address:** It is used to define the address of the application program in a destination computer. It is a 16-bit field.
- **Sequence number:** A stream of data is divided into two or more TCP segments. The 32-bit sequence number field represents the position of the data in an original data stream.

- **Acknowledgement number:** A 32-field acknowledgement number acknowledge the data from other communicating devices. If ACK field is set to 1, then it specifies the sequence number that the receiver is expecting to receive.
- **Header Length (HLEN):** It specifies the size of the TCP header in 32-bit words. The minimum size of the header is 5 words, and the maximum size of the header is 15 words. Therefore, the maximum size of the TCP header is 60 bytes, and the minimum size of the TCP header is 20 bytes.
- **Reserved:** It is a six-bit field which is reserved for future use.
- **Control bits:** Each bit of a control field functions individually and independently. A control bit defines the use of a segment or serves as a validity check for other fields.

There are total six types of flags in control field:

- **URG:** The URG field indicates that the data in a segment is urgent.
- **ACK:** When ACK field is set, then it validates the acknowledgement number.
- **PSH:** The PSH field is used to inform the sender that higher throughput is needed so if possible, data must be pushed with higher throughput.
- **RST:** The reset bit is used to reset the TCP connection when there is any confusion occurs in the sequence numbers.
- **SYN:** The SYN field is used to synchronize the sequence numbers in three types of segments: connection request, connection confirmation (with the ACK bit set), and confirmation acknowledgement.
- **FIN:** The FIN field is used to inform the receiving TCP module that the sender has finished sending data. It is used in connection termination in three types of segments: termination request, termination confirmation, and acknowledgement of termination confirmation.
    - **Window Size:** The window is a 16-bit field that defines the size of the window.
    - **Checksum:** The checksum is a 16-bit field used in error detection.
    - **Urgent pointer:** If URG flag is set to 1, then this 16-bit field is an offset from the sequence number indicating that it is a last urgent data byte.
    - **Options and padding:** It defines the optional fields that convey the additional information to the receiver.

Differences b/w TCP & UDP

Basis for Comparison	**TCP**	**UDP**
Definition	TCP establishes a virtual circuit before transmitting the data.	UDP transmits the data directly to the destination computer without verifying whether the receiver is ready to receive or not.
Connection Type	It is a Connection-Oriented protocol	It is a Connectionless protocol

Speed	slow	high
Reliability	It is a reliable protocol.	It is an unreliable protocol.
Header size	20 bytes	8 bytes
acknowledgement		

Internet of Things (IoT) Enabling Technologies

IoT(internet of things) enabling technologies are

1. Wireless Sensor Network
2. Cloud Computing
3. Big Data Analytics
4. Communications Protocols
5. Embedded System

1. Wireless Sensor Network(WSN) :

A **WSN** comprises distributed devices with sensors which are used to monitor the environmental and physical conditions. A **wireless sensor network** consists of end nodes, routers and coordinators. End nodes have several sensors attached to them where the data is passed to a coordinator with the help of routers. The coordinator also acts as the gateway that connects WSN to the internet.
Example –

- Weather monitoring system
- Indoor air quality monitoring system
- Soil moisture monitoring system
- Surveillance system
- Health monitoring system

2. Cloud Computing :

It provides us the means by which we can access applications as utilities over the internet. Cloud means something which is present in remote locations.
With Cloud computing, users can access any resources from anywhere like databases, webservers, storage, any device, and any software over the internet.
Characteristics –

- Weather monitoring system
- Indoor air quality monitoring system
- Soil moisture monitoring system
- Surveillance system
- Health monitoring system

2. Cloud Computing :

It provides us the means by which we can access applications as utilities over the internet. Cloud means something which is present in remote locations.
With Cloud computing, users can access any resources from anywhere like databases, webservers, storage, any device, and any software over the internet.
Characteristics –

1. Broad network access
2. On demand self-services
3. Rapid scalability
4. Measured service

5. Pay-per-use

Provides different services, such as –

- **IaaS (**Infrastructure as a service**)**
  Infrastructure as a service provides online services such as physical machines, virtual machines, servers, networking, storage and data center space on a pay per use basis. Major IaaS providers are Google Compute Engine, Amazon Web Services and Microsoft Azure etc.
  Ex : Web Hosting, Virtual Machine etc.
- **PaaS (**Platform as a service**)**
  Provides a cloud-based environment with a very thing required to support the complete life cycle of building and delivering West web based (cloud) applications – without the cost and complexity of buying and managing underlying hardware, software provisioning and hosting. Computing platforms such as hardware, operating systems and libraries etc. Basically, it provides a platform to develop applications.
  Ex : App Cloud, Google app engine
- **SaaS (**Software as a service**)**
  It is a way of delivering applications over the internet as a service. Instead of installing and maintaining software, you simply access it via the internet, freeing yourself from complex software and hardware management. SaaS Applications are sometimes called web-based software on demand software or hosted software. SaaS applications run on a SaaS provider's service and they manage security availability and performance.
  Ex : Google Docs, Gmail, office etc.

3. Big Data Analytics :

It refers to the method of studying massive volumes of data or big data. Collection of data whose volume, velocity or variety is simply too massive and tough to store, control, process and examine the data using traditional databases.

Big data is gathered from a variety of sources including social network videos, digital images, sensors and sales transaction records.

Several steps involved in analyzing big data –

1. Data cleaning
2. Munging
3. Processing
4. Visualization

Examples –

- Bank transactions
- Data generated by IoT systems for location and tracking of vehicles
- E-commerce and in Big-Basket
- Health and fitness data generated by IoT system such as a fitness bands

4. Communications Protocols :

They are the backbone of IoT systems and enable network connectivity and linking to applications. Communication protocols allow devices to exchange data over the network. Multiple protocols often describe different aspects of a single communication. A group of protocols designed to work together is known as a protocol suite; when implemented in software they are a protocol stack.

They are used in

1. Data encoding
2. Addressing schemes

5. Embedded Systems :

It is a combination of hardware and software used to perform special tasks.

It includes microcontroller and microprocessor memory, networking units (Ethernet Wi-Fi adapters), input output units (display keyword etc.) and storage devices (flash memory).

It collects the data and sends it to the internet.

Embedded systems used in

Examples –

1. Digital camera
2. DVD player, music player
3. Industrial robots
4. Wireless Routers etc.

Remote Desktop Protocol (RDP)

RDP is based on, and is an extension of, the T-120 family of protocol standards. A multichannel capable protocol allows for separate virtual channels for carrying the following information:

- presentation data
- serial device communication
- licensing information
- highly encrypted data, such as keyboard, mouse activity

RDP is an extension of the core T.Share protocol. Several other capabilities are retained as part of the RDP, such as the architectural features necessary to support multipoint (multiparty sessions). Multipoint data delivery allows data from an application to be delivered in **real time** to multiple parties, such as Virtual Whiteboards. It doesn't require to send the same data to each session individually.

In this first release of Windows Terminal Server, we're concentrating on providing reliable and fast point-to-point (single-session) communications. Only one data channel is used in the initial release of Terminal Server 4.0. However, the flexibility of RDP gives plenty of room for functionality in future products.

One reason that Microsoft decided to implement RDP for connectivity purposes within Windows NT Terminal Server is that it provides an extensible base to build many more capabilities. RDP provides 64,000 separate channels for data transmission. However, current transmission activities are only using a single channel (for keyboard, mouse, and presentation data).

RDP is designed to support many different types of Network topologies, such as ISDN, POTS. RDP is also designed to support many LAN protocols, such as IPX, NetBIOS, TCP/IP. The current version of RDP will only run over TCP/IP. With customer feedback, other protocol support may be added in future versions.

The activity involved in sending and receiving data through the RDP stack is essentially the same as the seven-layer OSI model standards for common LAN networking today. Data from an application or service to be transmitted is passed down through the protocol stacks. It's sectioned, directed to a channel (through MCS), encrypted, wrapped, framed, packaged onto the network protocol, and finally addressed and sent over the wire to the client. The returned data works the same way only in reverse. The packet is stripped of its address, then unwrapped, decrypted, and so on. Finally the data is presented to the application for use. Key portions of the protocol stack modifications occur between the fourth and seventh layers, where the data is:

- encrypted
- wrapped
- framed
- directed to a channel
- prioritized

One of the key points for application developers is that, in using RDP, Microsoft has abstracted away the complexities of dealing with the protocol stack. It allows them to write clean, well-designed, well-behaved 32-bit applications. Then the RDP stack implemented by the Terminal Server and its client connections takes care of the rest.

For more information about how applications interact on the Terminal Server, and what to know when developing applications for a Windows Terminal Server infrastructure, see the following white paper: **Optimizing Applications for Windows NT Server 4.0, Terminal Server Edition**

Four components worth discussing within the RDP stack instance are:

- the Multipoint Communication Service (MCSMUX)
- the Generic Conference Control (GCC)
- Wdtshare.sys
- Tdtcp.sys

MCSmux and GCC are part of the International Telecommunication Union (ITU) T.120 family. The MCS is made up of two standards:

- T.122: It defines the multipoint services
- T.125: It specifies the data transmission protocol

MCSMux controls:

- channel assignment by multiplexing data onto predefined virtual channels within the protocol
- priority levels
- segmentation of data being sent

It essentially abstracts the multiple RDP stacks into a single entity, from the perspective of the GCC. GCC is responsible for management of those multiple channels. The GCC allows the creation and deletion of session connections and controls resources provided by MCS. Each Terminal Server protocol (currently, only RDP and Citrix's ICA are supported) will have a protocol stack instance loaded (a listener stack awaiting a connection request). The Terminal Server device driver coordinates and manages the RDP protocol activity. It's made up of smaller components:

- an RDP driver (Wdtshare.sys) for UI transfer, compression, encryption, framing, and so on.
- a transport driver (Tdtcp.sys) to package the protocol onto the underlying network protocol, TCP/IP.

RDP was developed to be entirely independent of its underlying transport stack, in this case TCP/IP. It means that we can add other transport drivers for other network protocols as customers needs for them grow, with little or no significant changes to the foundational parts of the protocol. They're key elements to the performance and extendibility of RDP on the network

User Datagram Protocol

The User Datagram Protocol (UDP) is simplest Transport Layer communication protocol available of the TCP/IP protocol suite. It involves minimum amount of communication mechanism. UDP is said to be an unreliable transport protocol but it uses IP services which provides best effort delivery mechanism.

In UDP, the receiver does not generate an acknowledgement of packet received and in turn, the sender does not wait for any acknowledgement of packet sent. This shortcoming makes this protocol unreliable as well as easier on processing.

Requirement of UDP

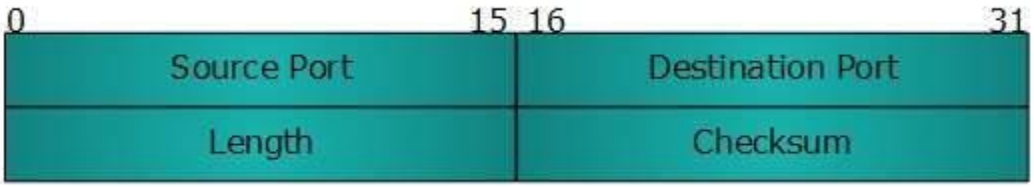
A question may arise, why do we need an unreliable protocol to transport the data? We deploy UDP where the acknowledgement packets share significant amount of bandwidth along with the actual data. For example, in case of video streaming, thousands of packets are forwarded towards its users. Acknowledging all the packets is troublesome and may contain huge amount of bandwidth wastage. The best delivery mechanism of underlying IP protocol ensures best efforts to deliver its packets, but even if some packets in video streaming get lost, the impact is not calamitous and can be ignored easily. Loss of few packets in video and voice traffic sometimes goes unnoticed.

Features

- UDP is used when acknowledgement of data does not hold any significance.
- UDP is good protocol for data flowing in one direction.
- UDP is simple and suitable for query based communications.
- UDP is not connection oriented.
- UDP does not provide congestion control mechanism.
- UDP does not guarantee ordered delivery of data.
- UDP is stateless.
- UDP is suitable protocol for streaming applications such as VoIP, multimedia streaming.

UDP Header

UDP header is as simple as its function.



UDP header contains four main parameters:

- **Source Port** - This 16 bits information is used to identify the source port of the packet.
- **Destination Port** - This 16 bits information, is used identify application level service on destination machine.
- **Length** - Length field specifies the entire length of UDP packet (including header). It is 16-bits field and minimum value is 8-byte, i.e. the size of UDP header itself.
- **Checksum** - This field stores the checksum value generated by the sender before sending. IPv4 has this field as optional so when checksum field does not contain any value it is made 0 and all its bits are set to zero.

UDP application

Here are few applications where UDP is used to transmit data:

- Domain Name Services
- Simple Network Management Protocol
- Trivial File Transfer Protocol
- Routing Information Protocol
- Kerberos

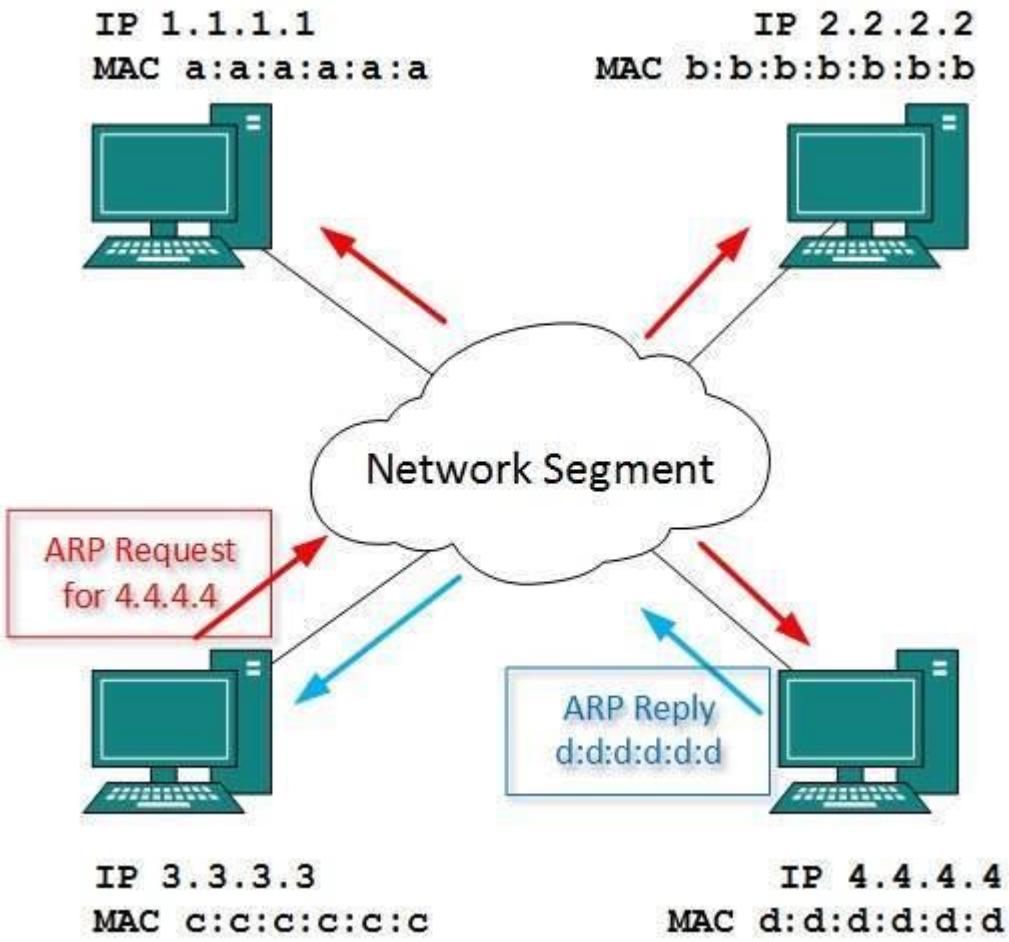
Network Layer Protocols

Every computer in a network has an IP address by which it can be uniquely identified and addressed. An IP address is Layer-3 (Network Layer) logical address. This address may change every time a computer restarts. A computer can have one IP at one instance of time and another IP at some different time.

Address Resolution Protocol(ARP)

While communicating, a host needs Layer-2 (MAC) address of the destination machine which belongs to the same broadcast domain or network. A MAC address is physically burnt into the Network Interface Card (NIC) of a machine and it never changes.

On the other hand, IP address on the public domain is rarely changed. If the NIC is changed in case of some fault, the MAC address also changes. This way, for Layer-2 communication to take place, a mapping between the two is required.



To know the MAC address of remote host on a broadcast domain, a computer wishing to initiate communication sends out an ARP broadcast message asking, “Who has this IP address?” Because it is a broadcast, all hosts on the network segment (broadcast domain) receive this packet and process it. ARP packet contains the IP address of destination host, the sending host wishes to talk to. When a host receives an ARP packet destined to it, it replies back with its own MAC address.

Once the host gets destination MAC address, it can communicate with remote host using Layer-2 link protocol. This MAC to IP mapping is saved into ARP cache of both sending and receiving hosts. Next time, if they require to communicate, they can directly refer to their respective ARP cache.

Reverse ARP is a mechanism where host knows the MAC address of remote host but requires to know IP address to communicate.

Internet Control Message Protocol (ICMP)

ICMP is network diagnostic and error reporting protocol. ICMP belongs to IP protocol suite and uses IP as carrier protocol. After constructing ICMP packet, it is encapsulated in IP packet. Because IP itself is a best-effort non-reliable protocol, so is ICMP.

Any feedback about network is sent back to the originating host. If some error in the network occurs, it is reported by means of ICMP. ICMP contains dozens of diagnostic and error reporting messages.

ICMP-echo and ICMP-echo-reply are the most commonly used ICMP messages to check the reachability of end-to-end hosts. When a host receives an ICMP-echo request, it is bound to send back an ICMP-echo-reply. If there is any problem in the transit network, the ICMP will report that problem.

Internet Protocol Version 4 (IPv4)

IPv4 is 32-bit addressing scheme used as TCP/IP host addressing mechanism. IP addressing enables every host on the TCP/IP network to be uniquely identifiable.

IPv4 provides hierarchical addressing scheme which enables it to divide the network into sub-networks, each with well-defined number of hosts. IP addresses are divided into many categories:

- **Class A** - it uses first octet for network addresses and last three octets for host addressing
- **Class B** - it uses first two octets for network addresses and last two for host addressing
- **Class C** - it uses first three octets for network addresses and last one for host addressing
- **Class D** - it provides flat IP addressing scheme in contrast to hierarchical structure for above three.
- **Class E** - It is used as experimental.

IPv4 also has well-defined address spaces to be used as private addresses (not routable on internet), and public addresses (provided by ISPs and are routable on internet).

Though IP is not reliable one; it provides ‘Best-Effort-Delivery’ mechanism.

Internet Protocol Version 6 (IPv6)

Exhaustion of IPv4 addresses gave birth to a next generation Internet Protocol version 6. IPv6 addresses its nodes with 128-bit wide address providing plenty of address space for future to be used on entire planet or beyond.

IPv6 has introduced Anycast addressing but has removed the concept of broadcasting. IPv6 enables devices to self-acquire an IPv6 address and communicate within that subnet. This auto-configuration removes the dependability of Dynamic Host Configuration Protocol (DHCP) servers. This way, even if the DHCP server on that subnet is down, the hosts can communicate with each other.

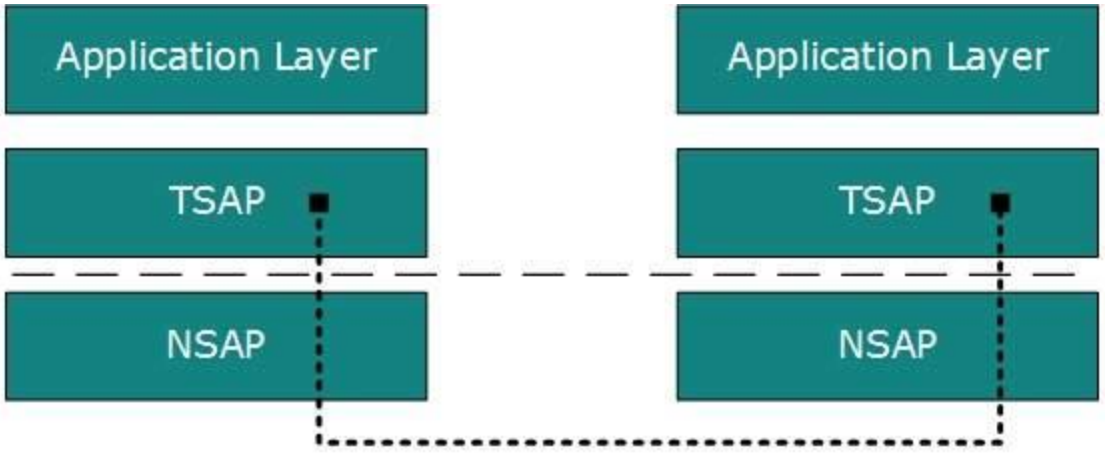
IPv6 provides new feature of IPv6 mobility. Mobile IPv6 equipped machines can roam around without the need of changing their IP addresses.

IPv6 is still in transition phase and is expected to replace IPv4 completely in coming years. At present, there are few networks which are running on IPv6. There are some transition mechanisms available for IPv6 enabled networks to speak and roam around different networks easily on IPv4. These are:

- Dual stack implementation
- Tunneling
- NAT-PT

End-to-End Communication

A process on one host identifies its peer host on remote network by means of TSAPs, also known as Port numbers. TSAPs are very well defined and a process which is trying to communicate with its peer knows this in advance.



For example, when a DHCP client wants to communicate with remote DHCP server, it always requests on port number 67. When a DNS client wants to communicate with remote DNS server, it always requests on port number 53 (UDP).

The two main Transport layer protocols are:

- **Transmission Control Protocol**
  It provides reliable communication between two hosts.
- **User Datagram Protocol**
  It provides unreliable communication between two hosts.

Transmission Control Protocol

The transmission Control Protocol (TCP) is one of the most important protocols of Internet Protocols suite. It is most widely used protocol for data transmission in communication network such as internet.

Features

- TCP is reliable protocol. That is, the receiver always sends either positive or negative acknowledgement about the data packet to the sender, so that the sender always has bright clue about whether the data packet is reached the destination or it needs to resend it.
- TCP ensures that the data reaches intended destination in the same order it was sent.
- TCP is connection oriented. TCP requires that connection between two remote points be established before sending actual data.
- TCP provides error-checking and recovery mechanism.
- TCP provides end-to-end communication.

- TCP provides flow control and quality of service.
- TCP operates in Client/Server point-to-point mode.
- TCP provides full duplex server, i.e. it can perform roles of both receiver and sender.

Header

The length of TCP header is minimum 20 bytes long and maximum 60 bytes.

- **Source Port (16-bits)** - It identifies source port of the application process on the sending device.
- **Destination Port (16-bits)** - It identifies destination port of the application process on the receiving device.
- **Sequence Number (32-bits)** - Sequence number of data bytes of a segment in a session.
- **Acknowledgement Number (32-bits)** - When ACK flag is set, this number contains the next sequence number of the data byte expected and works as acknowledgement of the previous data received.
- **Data Offset (4-bits)** - This field implies both, the size of TCP header (32-bit words) and the offset of data in current packet in the whole TCP segment.
- **Reserved (3-bits)** - Reserved for future use and all are set zero by default.
- **Flags (1-bit each)**
  - **NS** - Nonce Sum bit is used by Explicit Congestion Notification signaling process.
  - **CWR** - When a host receives packet with ECE bit set, it sets Congestion Windows Reduced to acknowledge that ECE received.
  - **ECE** -It has two meanings:
    - If SYN bit is clear to 0, then ECE means that the IP packet has its CE (congestion experience) bit set.
    - If SYN bit is set to 1, ECE means that the device is ECT capable.
  - **URG** - It indicates that Urgent Pointer field has significant data and should be processed.
  - **ACK** - It indicates that Acknowledgement field has significance. If ACK is cleared to 0, it indicates that packet does not contain any acknowledgement.
  - **PSH** - When set, it is a request to the receiving station to PUSH data (as soon as it comes) to the receiving application without buffering it.
  - **RST** - Reset flag has the following features:
    - It is used to refuse an incoming connection.
    - It is used to reject a segment.
    - It is used to restart a connection.
  - **SYN** - This flag is used to set up a connection between hosts.
  - **FIN** - This flag is used to release a connection and no more data is exchanged thereafter. Because packets with SYN and FIN flags have sequence numbers, they are processed in correct order.
- **Windows Size** - This field is used for flow control between two stations and indicates the amount of buffer (in bytes) the receiver has allocated for a segment, i.e. how much data is the receiver expecting.
- **Checksum** - This field contains the checksum of Header, Data and Pseudo Headers.
- **Urgent Pointer** - It points to the urgent data byte if URG flag is set to 1.

- **Options** - It facilitates additional options which are not covered by the regular header. Option field is always described in 32-bit words. If this field contains data less than 32-bit, padding is used to cover the remaining bits to reach 32-bit boundary.

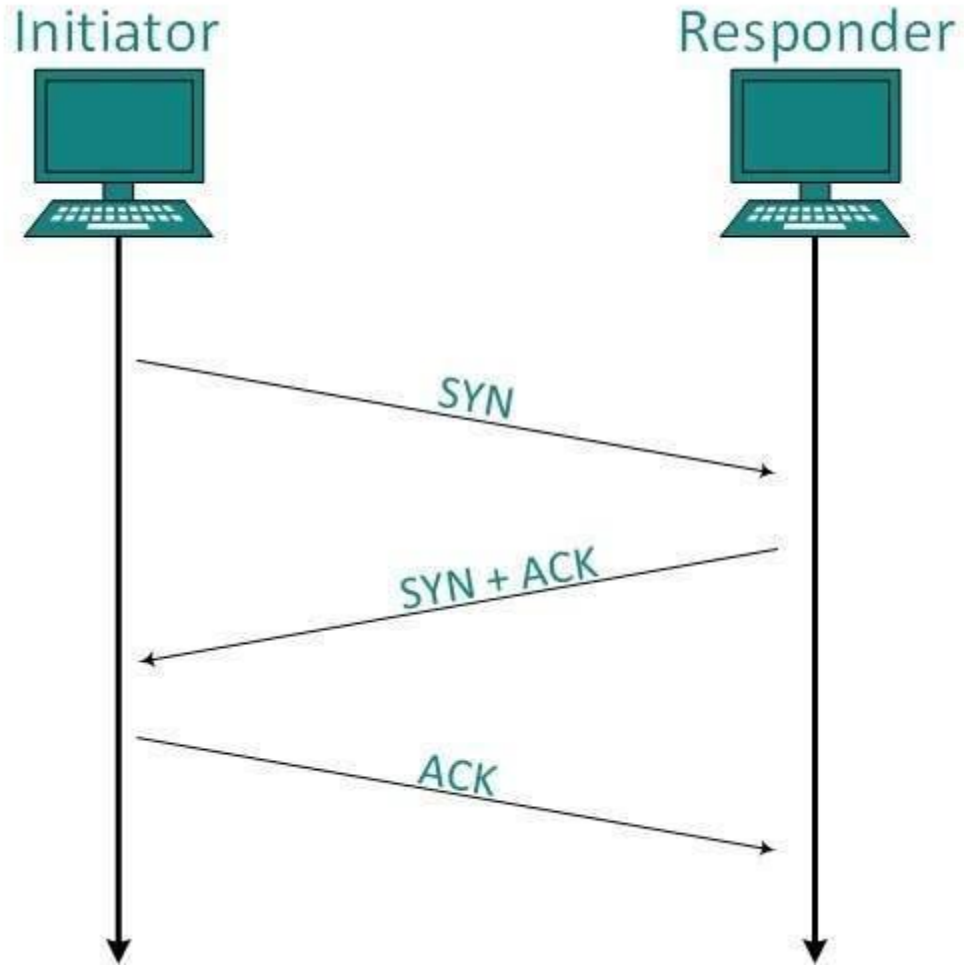
Addressing

TCP communication between two remote hosts is done by means of port numbers (TSAPs). Ports numbers can range from 0 – 65535 which are divided as:

- System Ports (0 – 1023)
- User Ports (1024 – 49151)
- Private/Dynamic Ports (49152 – 65535)

Connection Management

TCP communication works in Server/Client model. The client initiates the connection and the server either accepts or rejects it. Three-way handshaking is used for connection management.



Establishment

Client initiates the connection and sends the segment with a Sequence number. Server acknowledges it back with its own Sequence number and ACK of client's segment which is one more than client's Sequence number. Client after receiving ACK of its segment sends an acknowledgement of Server's response.

Release

Either of server and client can send TCP segment with FIN flag set to 1. When the receiving end responds it back by ACKnowledging FIN, that direction of TCP communication is closed and connection is released.

Bandwidth Management

TCP uses the concept of window size to accommodate the need of Bandwidth management. Window size tells the sender at the remote end, the number of data byte segments the receiver at this end can receive. TCP uses slow start phase by using window size 1 and increases the window size exponentially after each successful communication.

For example, the client uses windows size 2 and sends 2 bytes of data. When the acknowledgement of this segment received the windows size is doubled to 4 and next sent the segment sent will be 4 data bytes long. When the acknowledgement of 4-byte data segment is received, the client sets windows size to 8 and so on.

If an acknowledgement is missed, i.e. data lost in transit network or it received NACK, then the window size is reduced to half and slow start phase starts again.

Error Control &and Flow Control

TCP uses port numbers to know what application process it needs to handover the data segment. Along with that, it uses sequence numbers to synchronize itself with the remote host. All data segments are sent and received with sequence numbers. The Sender knows which last data segment was received by the Receiver when it gets ACK. The Receiver knows about the last segment sent by the Sender by referring to the sequence number of recently received packet.

If the sequence number of a segment recently received does not match with the sequence number the receiver was expecting, then it is discarded and NACK is sent back. If two segments arrive with the same sequence number, the TCP timestamp value is compared to make a decision.

Multiplexing

The technique to combine two or more data streams in one session is called Multiplexing. When a TCP client initializes a connection with Server, it always refers to a well-defined port number which indicates the application process. The client itself uses a randomly generated port number from private port number pools.

Using TCP Multiplexing, a client can communicate with a number of different application process in a single session. For example, a client requests a web page which in turn contains different types of data (HTTP, SMTP, FTP etc.) the TCP session timeout is increased and the session is kept open for longer time so that the three-way handshake overhead can be avoided.

This enables the client system to receive multiple connection over single virtual connection. These virtual connections are not good for Servers if the timeout is too long.

Congestion Control

When large amount of data is fed to system which is not capable of handling it, congestion occurs. TCP controls congestion by means of Window mechanism. TCP sets a window size telling the other end how much data segment to send. TCP may use three algorithms for congestion control:

- Additive increase, Multiplicative Decrease
- Slow Start
- Timeout React

Timer Management

TCP uses different types of timer to control and management various tasks:

Keep-alive timer:

- This timer is used to check the integrity and validity of a connection.
- When keep-alive time expires, the host sends a probe to check if the connection still exists.

Retransmission timer:

- This timer maintains stateful session of data sent.
- If the acknowledgement of sent data does not receive within the Retransmission time, the data segment is sent again.

Persist timer:

- TCP session can be paused by either host by sending Window Size 0.
- To resume the session a host needs to send Window Size with some larger value.
- If this segment never reaches the other end, both ends may wait for each other for infinite time.
- When the Persist timer expires, the host re-sends its window size to let the other end know.
- Persist Timer helps avoid deadlocks in communication.

Timed-Wait:

- After releasing a connection, either of the hosts waits for a Timed-Wait time to terminate the connection completely.
- This is in order to make sure that the other end has received the acknowledgement of its connection termination request.
- Timed-out can be a maximum of 240 seconds (4 minutes).

Crash Recovery

TCP is very reliable protocol. It provides sequence number to each of byte sent in segment. It provides the feedback mechanism i.e. when a host receives a packet, it is bound to ACK that packet having the next sequence number expected (if it is not the last segment).

When a TCP Server crashes mid-way communication and re-starts its process it sends TPDU broadcast to all its hosts. The hosts can then send the last data segment which was never unacknowledged and carry onwards.

What is Secure Socket Layer (SSL)?

Secure Sockets Layer

Secure Sockets Layer (SSL) is a standard technique for transmitting documents securely across a network. SSL technology, created by Netscape, establishes a secure connection between a Web server and a browser, ensuring private and secure data transmission. SSL communicates using the Transport Control Protocol (TCP).

The term "socket" in SSL refers to the method of sending data via a network between a client and a server.

A Web server requires an SSL certificate to establish a secure SSL connection while using SSL for safe Internet transactions. SSL encrypts network connection segments atop the transport layer, a network connection component above the program layer.

SSL is based on an asymmetric cryptographic process in which a Web browser generates both a public and a private (secret) key. A certificate signing request is a data file that contains the public key (CSR). Only the recipient receives the private key.

How Does SSL Work?

SSL encrypts data communicated across the web to guarantee a high level of privacy. Anyone attempting to intercept this data will meet a jumbled mess of characters nearly hard to decrypt.

SSL begins an authentication process known as a handshake between two communicating devices to confirm that both devices are who they say they are.

SSL also digitally certifies data to ensure data integrity, ensuring that it has not been tampered with before reaching its intended receiver.

SSL has gone through multiple incarnations, each one more secure than the last. TLS (Transport Layer Security) was introduced in 1999, replacing SSL.

Objectives of SSL

The goals of SSL are as follows −

- *Data integrity* − Information is safe from tampering. The SSL Record Protocol, SSL Handshake Protocol, SSL Change CipherSpec Protocol, and SSL Alert Protocol maintain data privacy.
- *Client-server authentication* − The SSL protocol authenticates the client and server using standard cryptographic procedures.
- SSL is the forerunner of Transport Layer Security (TLS), a cryptographic technology for secure data transfer over the Internet.

How to Obtain an SSL/TLS Certificate?

Are you ready to protect your website? The following is the fundamental approach for requesting a publicly trusted SSL/TLS website certificate −

- The individual or organization requesting the certificate generates a pair of public and private keys, which should be stored on the server being protected.
- A certificate signing request is generated using the public key, the domain name(s) to be protected, and (for OV and EV certificates) organizational information about the company requesting the certificate (CSR).
- A publicly trusted CA receives the CSR (such as SSL.com). The CA verifies the information in the CSR and generates a signed certificate that the requester can install on their web server.

What is Transport Layer Security (TLS) Handshake?

Transport layer security protocol is one of the security protocols which are designed to facilitate privacy and data security for communications over the Internet. The main use of TLS is to encrypt the communication between web applications and servers, like web browsers loading a website.

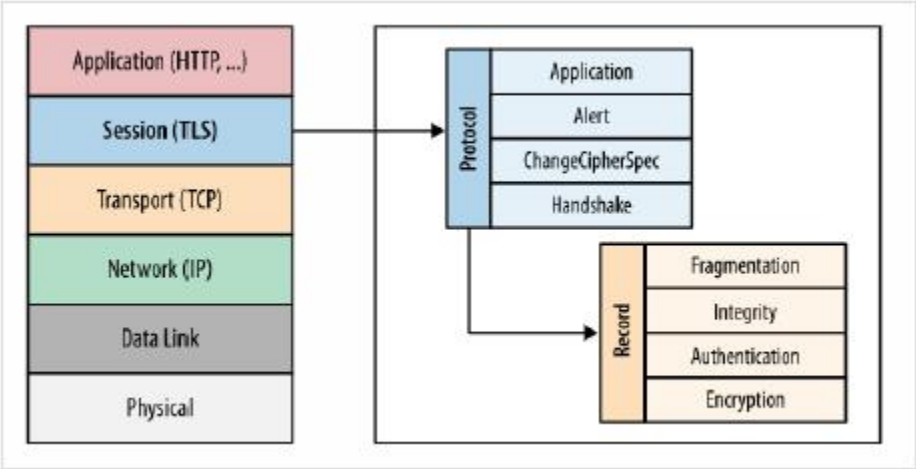
TLS is used to encrypt other communications like email, messaging, and voice over IP (VoIP). TLS was proposed by the Internet Engineering Task Force (IETF), which is an international standards organization.

Components

The three main components that TLS accomplishes are as follows −

- **Encryption** − It is used to hide the data being transferred from third parties.
- **Authentication** − It always ensures that the parties exchanging information are who they claim to be.
- **Integrity** − Integrity verifies that the data has not been tampered with.

Given below is the pictorial representation of the **Transport layer security protocol (TLS)** −



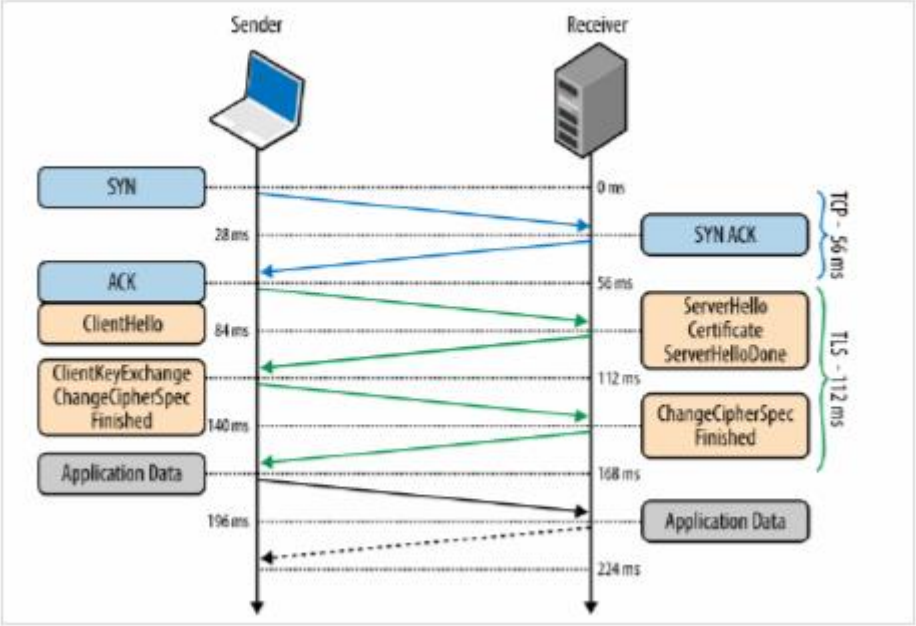
Advantages

The advantages of TLS are as follows−

- Encryption
- Interoperability
- Flexibility
- Easy of deployment
- Easy to use.

TLS handshake Protocol

The working condition of the TLS Handshake protocol is shown below −



Here,

- A client sends a synchronous message "client hello" requesting a connection and presents a list of supported cipher suites and a random string of bytes.
- The server responds with a "server hello" message containing a server certificate.
- The server is sending its SSL certificate to the client for the purpose of authentication. The client then authenticates the server by verifying the server's SSL certificate, and also sends a certificate for authentication if requested by the server.
- The client sends the client key exchange, change Cipher specification finished message to the server.
- The server decrypts the message sent by client secret with the private key.
- Both client and server generate session keys from the client random, the server random, and the secret message.
- The client sends a "finished" message that has been encrypted with a session key.
- The server responds with a finished message which was encrypted with a session key.
- The client and server have successfully achieved secure symmetric encryption, meaning the handshake is complete and communication can continue with the established session keys.
- Finally transfer the application data.

DTLS (Datagram Transport Layer Security)

What is DTLS?

DTLS: A quick definition

DTLS stands for Datagram Transport Layer Security. It's a session layer communications protocol designed to protect data privacy. It allows datagram-based applications to communicate while preventing tampering, eavesdropping, and message forgery.

DTLS is based on the Transport Layer Security (TLS) protocol, which provides security to computer-based communications networks. It was developed with TLS for applications with an unreliable transport layer, such as in the case of the IoT, video conferencing, VoIP, VPN, and online gaming.

Alongside Secure Real-time Transport Protocol (SRTP), DTSL is one of the security protocols used for Web Real-Time Communication (WebRTC) technology, which includes web browsing, mail, instant messaging, and internet telephony.

The original DTLS 1.0 (defined in **IETF document** RFC 4347) was replaced by DTLS 1.2 (RFC 5246 and RFC 6347) and later 1.3, each based on the corresponding TLS 1 protocol version.

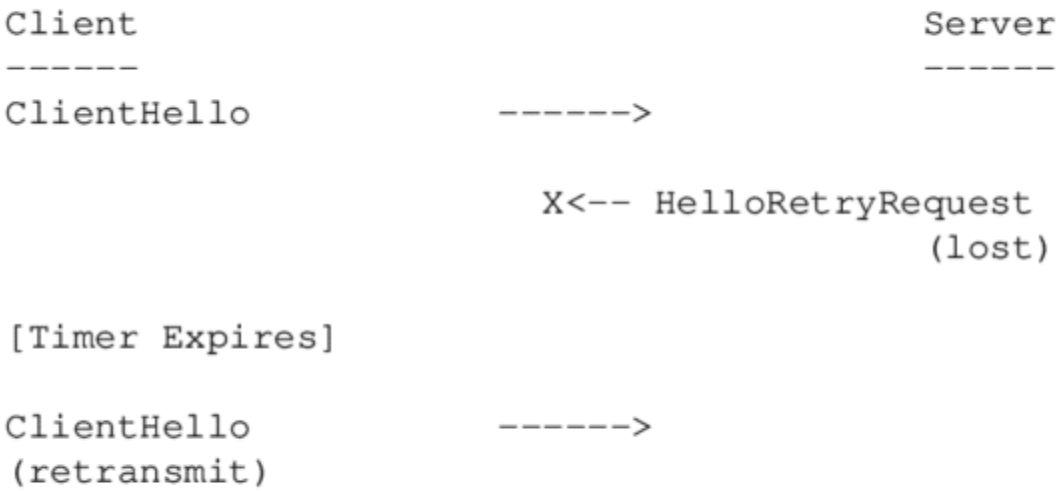
How does DTLS work?

A datagram (the "D" in DTLS) is a bit like a telegram, but with digital data. These data "packets" don't require any prior connection between sender and receiver because they contain enough information to find their own way to the destination.

User Datagram Protocol (UDP) is mainly used to establish low-latency connections between applications on the internet. As UDP prioritises fast data transfer and short response times, it's useful for time-sensitive communications like VoIP, DNS lookup, and video or audio playback.

However, with no confirmation or flow control, the connection is unreliable. The sender doesn't know whether the message has been received, and if data packets overtake each other on route, the recipient can't be sure they've arrived in the correct order. That's where DTLS comes in.

The DTLS protocol is like an extra layer of privacy for UDP communications, and it's designed to prevent data packages from getting lost or arriving in the wrong order. DTLS uses a simple retransmission timer for this, with each endpoint continuing to retransmit its last message until a reply is received.



DTLS vs TLS

Although DTLS is based on TLS, they are two different things. Whereas DTLS is built on UDP, TLS uses Transmission Control Protocol (TCP). TLS cannot go directly on top of UDP because it's unable to cope with the packet loss or reordering that may occur.

In this instance, the TLS handshake layer will assume that handshake messages have been delivered reliably, and will break the connection if messages get lost. Because its mission is to deliver data reliably and with end-to-end encryption via TCP, it can't be used to secure unreliable datagram traffic.

DTLS is also designed to deliver authenticated and **encrypted** application data, but it enables lower latency—which means it can process a very high volume of data messages with minimal delay. As we mentioned in the previous section, DTLS solves the problems of reordering or packet loss using a retransmission timer.

TLS's traffic encryption layer does not allow packets to be decrypted independently, since the integrity check depends on the sequence number. DTLS uses explicit (rather than implicit) sequence numbers to resolve this.

However, there are many similarities. DTLS is basically a datagram-compatible version of TLS, specifically designed so that minimal changes are required to solve the problems that TLS can't fix. Since DTLS is so similar, pre-existing TLS protocol infrastructure and implementations can be reused.

UNIT-III

Data-link Layer Introduction

Data Link Layer is second layer of OSI Layered Model. This layer is one of the most complicated layers and has complex functionalities and liabilities. Data link layer hides the details of underlying hardware and represents itself to upper layer as the medium to communicate.

Data link layer works between two hosts which are directly connected in some sense. This direct connection could be point to point or broadcast. Systems on broadcast network are said to be on same link. The work of data link layer tends to get more complex when it is dealing with multiple hosts on single collision domain.

Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware. At the receiving end, Data link layer picks up data from hardware which are in the form of electrical signals, assembles them in a recognizable frame format, and hands over to upper layer.

Data link layer has two sub-layers:

- **Logical Link Control:** It deals with protocols, flow-control, and error control
- **Media Access Control:** It deals with actual control of media

Functionality of Data-link Layer

Data link layer does many tasks on behalf of upper layer. These are:

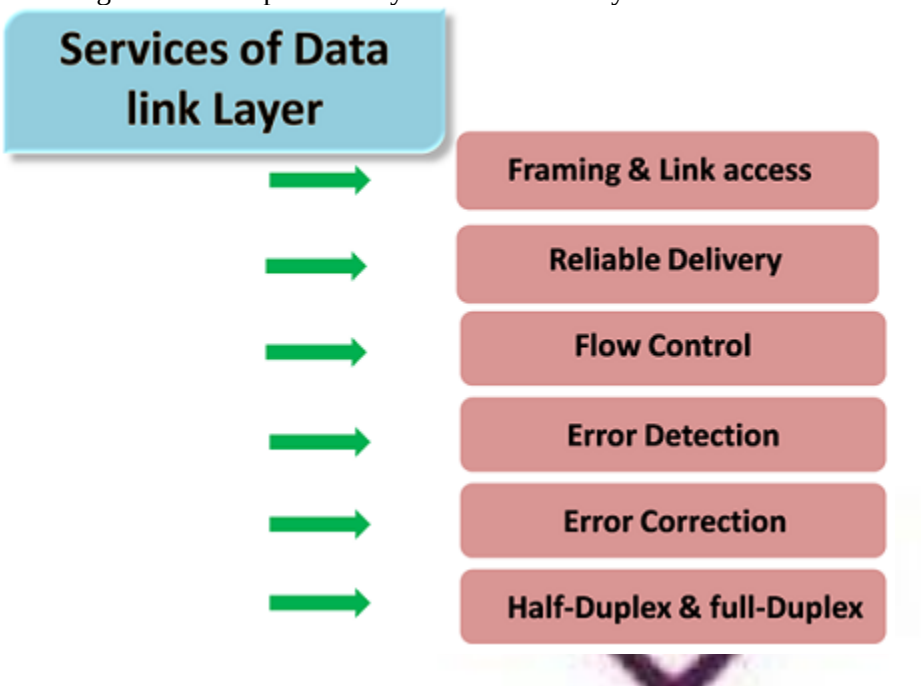
- **Framing**
  Data-link layer takes packets from Network Layer and encapsulates them into Frames.Then, it sends each frame bit-by-bit on the hardware. At receiver' end, data link layer picks up signals from hardware and assembles them into frames.
- **Addressing**
  Data-link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.
- **Synchronization**
  When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.
- **Error Control**
  Sometimes signals may have encountered problem in transition and the bits are flipped.These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.
- **Flow Control**
  Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machine to exchange data on same speed.
- **Multi-Access**
  When host on the shared link tries to transfer the data, it has a high probability of collision. Data-link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple System.

Data Link Layer

- In the OSI model, the data link layer is a 4^{th} layer from the top and 2^{nd} layer from the bottom.
- The communication channel that connects the adjacent nodes is known as links, and in order to move the datagram from source to the destination, the datagram must be moved across an individual link.
- The main responsibility of the Data Link Layer is to transfer the datagram across an individual link.
- The Data link layer protocol defines the format of the packet exchanged across the nodes as well as the actions such as Error detection, retransmission, flow control, and random access.

- The Data Link Layer protocols are Ethernet, token ring, FDDI and PPP.
- An important characteristic of a Data Link Layer is that datagram can be handled by different link layer protocols on different links in a path. For example, the datagram is handled by Ethernet on the first link, PPP on the second link.

Following services are provided by the Data Link Layer:

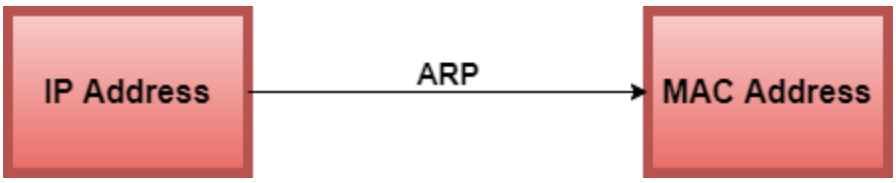


- **Framing & Link access:** Data Link Layer protocols encapsulate each network frame within a Link layer frame before the transmission across the link. A frame consists of a data field in which network layer datagram is inserted and a number of data fields. It specifies the structure of the frame as well as a channel access protocol by which frame is to be transmitted over the link.
- **Reliable delivery:** Data Link Layer provides a reliable delivery service, i.e., transmits the network layer datagram without any error. A reliable delivery service is accomplished with transmissions and acknowledgements. A data link layer mainly provides the reliable delivery service over the links as they have higher error rates and they can be corrected locally, link at which an error occurs rather than forcing to retransmit the data.

- **Flow control:** A receiving node can receive the frames at a faster rate than it can process the frame. Without flow control, the receiver's buffer can overflow, and frames can get lost. To overcome this problem, the data link layer uses the flow control to prevent the sending node on one side of the link from overwhelming the receiving node on another side of the link.
- **Error detection:** Errors can be introduced by signal attenuation and noise. Data Link Layer protocol provides a mechanism to detect one or more errors. This is achieved by adding error detection bits in the frame and then receiving node can perform an error check.
- **Error correction:** Error correction is similar to the Error detection, except that receiving node not only detect the errors but also determine where the errors have occurred in the frame.
- **Half-Duplex & Full-Duplex:** In a Full-Duplex mode, both the nodes can transmit the data at the same time. In a Half-Duplex mode, only one node can transmit the data at the same time.

Address Resolution Protocol (ARP)

ARP stands for **Address Resolution Protocol**, which is used to find the MAC address of the device from its known IP address. This means, the source device already knows the IP address but not the MAC address of the destination device. The MAC address of the device is required because you cannot communicate with a device in a local area network (Ethernet) without knowing its MAC address. So, the Address Resolution Protocol helps to obtain the MAC address of the destination device.



Scenario 1: When the data packet is lost or erroneous.

The purpose of ARP is to convert the 32-bit logical address (IPv4 address) to the 48-bit physical address (MAC address). This protocol works between layer 2 and layer 3 of the OSI model. The MAC address resides at layer 2, which is also known as the data link layer and IP address resides at layer 3, this layer is also known as the network layer.

Note: The ARP request is generated only when both the devices (source and destination) are in the same network.

Example: Suppose two devices (device A and device B) want to communicate with each other. The device A already knows the IP address of the Device B. But in order to communicate with the device B, device A still needs the MAC address of the device B. The **IP address** is used to locate a device on a local area network and the **MAC address** is used to identify the actual device. The device A first look at its internal list known as ARP cache (table) to check if the IP address of the device B already consists of its MAC address or not. If the ARP table consists of the MAC address of the device B, then device A simply use that MAC address and start communication.

If the table does not consist of the MAC address of device B, then device A sends an ARP broadcast message on the network to know which device has that specific IP address and ask for the MAC address of that particular device. Then the device that has matching IP address to the source address sends an ARP response message that consists of the MAC address of the device B. When device A obtains the MAC address of the device B, it will store the information in the ARP cache (table). The ARP cache is used to make the network more efficient. It stores the IP address of the device along with its MAC address. The stored information is used when device A wants to communicate with device B on a network, and it does not need to broadcast a message on the network again. It will simply check the ARP cache for the entries and then use it for communication.

Note: The ARP request message is broadcast in nature, but the ARP response message is unicast.

Types of Mapping in ARP

There are two different ways to map the IP address into the MAC address, which are given below:

- Static Mapping
- Dynamic Mapping

Static Mapping - In the static mapping, a table consists of a logical address and corresponding physical address of the destination device. In this, the IP and MAC address of the device is entered manually in an ARP table. The source device has to access the table first if a source wants to communicate with the destination device.

Dynamic Mapping - In the dynamic mapping, if a device knows the logical address of the other device, then by using the Address Resolution protocol, this device will also find the physical address of the device. The dynamic entries are created automatically when the source device sends an ARP broadcast request. These entries are not permanent and cleared periodically.

IPv6 - Overview

Internet Protocol version 6 is a new addressing protocol designed to incorporate all the possible requirements of future Internet known to us as Internet version 2. This protocol as its predecessor IPv4, works on the Network Layer (Layer-3). Along with its offering of an enormous amount of logical address space, this protocol has ample features to which address the shortcoming of IPv4.

Why New IP Version?

So far, IPv4 has proven itself as a robust routable addressing protocol and has served us for decades on its best-effort-delivery mechanism. It was designed in the early 80's and did not get any major change afterward. At the time of its birth, Internet was limited only to a few universities for their research and to the Department of Defense. IPv4 is 32 bits long and offers around 4,294,967,296 (2^{32}) addresses. This address space was considered more than enough that time. Given below are the major points that played a key role in the birth of IPv6:

- Internet has grown exponentially and the address space allowed by IPv4 is saturating. There is a requirement to have a protocol that can satisfy the needs of future Internet addresses that is expected to grow in an unexpected manner.
- IPv4 on its own does not provide any security feature. Data has to be encrypted with some other security application before being sent on the Internet.
- Data prioritization in IPv4 is not up to date. Though IPv4 has a few bits reserved for Type of Service or Quality of Service, but they do not provide much functionality.
- IPv4 enabled clients can be configured manually or they need some address configuration mechanism. It does not have a mechanism to configure a device to have globally unique IP address.

Why Not IPv5?

Till date, Internet Protocol has been recognized has IPv4 only. Version 0 to 3 were used while the protocol was itself under development and experimental process. So, we can assume lots of background activities remain active before putting a protocol into production. Similarly, protocol version 5 was used while experimenting with the stream protocol for Internet. It is known to us as Internet Stream Protocol which used Internet Protocol number 5 to encapsulate its datagram. It was never brought into public use, but it was already used.

Here is a table of IP versions and how they are used:

Decimal	Keyword	Version
0-1		Reserved
2-3		Unassigned
4	IP	Internet Protocol
5	ST	ST Datagram mode
6	IPv6	Internet Protocol version 6
7	TP/IX	TP/IX: The Next Internet
8	PIP	The P Internet Protocol
9	TUBA	TUBA
10-14		Unassigned
15		Reserved

Brief History

After IPv4's development in the early 80s, the available IPv4 address pool begun to shrink rapidly as the demand of addresses exponentially increased with Internet. Taking pre-cognizance of the situation that might arise, IETF, in 1994, initiated the development of an addressing protocol to replace IPv4. The progress of IPv6 can be tracked by means of the RFC published:

- 1998 – RFC 2460 – Basic Protocol
- 2003 – RFC 2553 – Basic Socket API
- 2003 – RFC 3315 – DHCPv6
- 2004 – RFC 3775 – Mobile IPv6
- 2004 – RFC 3697 – Flow Label Specification
- 2006 – RFC 4291 – Address architecture (revision)
- 2006 – RFC 4294 – Node requirement

On June 06, 2012, some of the Internet giants chose to put their Servers on IPv6. Presently they are using Dual Stack mechanism to implement IPv6 parallel in with IPv4.

Wide Area Network Protocols and Data Transmission

What is a WAN?

A wide-area network (WAN) is the technology that connects your offices, data centers, cloud applications, and cloud storage together. It is called a wide-area network because it spans beyond a single building or large campus to include multiple locations spread across a specific geographic area, or even the world. For example, businesses with many international branch offices use a WAN to connect office networks together. The world's largest WAN is the internet because it is a collection of many international networks that connect to each other. This article focuses on enterprise WANs and their uses and benefits.

What is the purpose of a WAN connection?

Wide-area networks (WANs) are the backbone of enterprise today. With the digitization of resources, companies use WANs to do the following:

- Communicate using voice and video.

- Share resources between employees and customers.
- Access data storage and remotely back up data.
- Connect to applications running in the cloud.
- Run and host internal applications.

WAN technology innovations help organizations access information in a secure, fast, and reliable way. WANs are important for business productivity and continuity.

What is WAN architecture?

Wide-area network (WAN) architectures are based on the Open Systems Interconnection (OSI) model that conceptually defines and standardizes all telecommunication. The OSI model visualizes any computer network to work in seven layers. Different networking technologies operate on each of these different layers and together make a working WAN.

We will show you these layers in a top-down approach and provide an example to help you understand them:

Layer 7 – Application layer

The application layer is closest to the user and defines how the user interacts with the network. It contains the application logic and is unaware of the network implementation. For example, if you have a calendar booking system in your enterprise, this layer manages booking logic such as sending invitations, converting time zones, and more.

Layer 6 – Presentation layer

The presentation layer prepares data for transmission across the network. For example, it adds some encryption so that cybercriminals watching your WAN can't hack your sensitive meeting data.

Layer 5 – Session layer

The session layer manages the connections or sessions between local and remote applications. It can open, close, or terminate the connection between two devices. For example, your booking system is located on a web server in the central office, and you are working from home. The session layer opens a connection between your computer and the web server after authentication. This connection is a logical connection, not an actual physical connection.

Layer 4 – Transport layer

The transport layer defines the functions and procedures for data transmission. It classifies and dispatches the data for transfer. It may also package the data into data packets. For example, when you visit the booking site, the Transmission Control Protocol (TCP) manages communication by sorting it into request and response packets.

ATM Networks

Layer 3 – Network layer

The network layer manages how the data packets travel through the network. For example, it defines the rules for packet routing, load balancing, and packet loss.

Layer 2 – Data link layer

The data link layer is responsible for establishing communication rules or protocols on the physical layer operations. For example, it decides when to start or terminate a direct connection. This layer function forwards packets from one device to another until they reach their destination.

Layer 1 – Physical layer

The physical layer manages the transfer of raw data in the form of digital bits, optical signals, or electromagnetic waves across the different network transmission media, such as optical fibers and wireless technologies.

What are WAN protocols?

Wide-area network (WAN) protocols, or networking protocols, define the rules of communication across any network. The following are some examples:

Frame relay

Frame relay is an early technology that packages data in the form of frames and transmits it over a private line to a frame relay node. Frame relay works on layers 1 and 2 and facilitates information transfer from one LAN to another over multiple switches and routers.

Asynchronous transfer mode

Asynchronous Transfer Mode (ATM) is also an early WAN technology that formats data into 53-byte data cells. ATM network devices use time-division multiplexing, which converts digital signals into fixed-sized cells, transmits them, and then reassembles them at their destination.

Packet over SONET/SDH

Packet over SONET/SDH (POS) is a communication protocol that defines how point-to-point links communicate when using optical fiber.

TCP/IP

The Transmission Control Protocol/Internet Protocol (TCP/IP) defines end-to-end communication by specifying how data should be packetized, addressed, transmitted, routed, and received. IPv6 is the latest version of the most commonly used method.

What are local area networks?

Local area networks (LANs) are the building blocks of a WAN. A LAN consists of interconnected computers and other devices limited to a small place, such as a building, school, or office.

LAN vs. WAN

LANs are smaller networks with limited capacity but higher speeds. They are easier and more cost effective to design, set up, and manage. They are private networks that typically use a single connection technology.

On the other hand, WANs connect LANs together. A single WAN can have many different types of networking technologies to communicate across LANs. Its communication speed is slow, but its capacity is high. Because a WAN is a large network, you may find it more complex to set up and manage.

How does a WAN work?

Enterprises have resources running in different on-premises data centers, branch offices, and virtual private clouds (VPCs). To connect these resources, enterprises use multiple network connections and internet services. Since companies cannot build their own network infrastructure across multiple geographical boundaries, they typically rent it from a third-party service provider.

The following are some common types of connections:

Leased lines

A leased line is a direct network connection that you can rent from a large network provider, such as an ISP. It can connect two LAN endpoints together. Leased lines are not necessarily physical lines. They may be virtual connections that the service providers implement over other network infrastructure.

Tunneling

Tunneling is a way to encrypt data packets as they move over the public internet. In tunneling, you use an internet connection to access enterprise servers in another country. But you send them as encapsulated packets, forming your own virtual private network (VPN).

Multiprotocol label switching

Multiprotocol Label Switching (MPLS) is a technique that routes data traffic based on predetermined labels. It attempts to route critical data traffic across shorter or faster network paths, improving network performance. It works between Open Systems Interconnection (OSI) layers 2 and 3. You can use it to create a unified network across existing infrastructure, such as IPv6, frame relay, ATM, or ethernet. You can use MPLS leased lines or MPLS with VPNs to create efficient and secure networks.

Software-defined WAN

Software-defined wide-area network (SD-WAN) is the further evolution of MPLS technology. It abstracts the MPLS functions into a software layer. Because SD-WAN works over commodity broadband internet connections, it can often reduce networking costs and provide greater flexibility than a fixed connection.

MPLS vs. SD-WAN

MPLS can slow down cloud integration because it routes traffic through corporate headquarters, which act as central choke points. On the other hand, SD-WAN is cloud-aware and integrates much better with modern cloud infrastructure. SD-WAN is also cost effective. It can work over MPLS so you can use bandwidth more efficiently on expensive MPLS lease lines.

What is WAN optimization?

Wide-area network (WAN) optimization is a collection of techniques that improve WAN performance metrics such as throughput, congestion, and latency. WAN design, technology choices, and traffic flow arrangements all affect WAN performance. The following are some common techniques for WAN optimization.

Traffic flow management

Traffic flow management includes techniques that minimize the amount of data sent over the network. Here are some examples:

- Caching frequently stored information on local servers
- Identifying and eliminating redundant data copies for data backup and disaster recovery applications

- Compressing or zipping data files

Protocol acceleration

Some WAN protocols are chatty—that is, they may require a lot of back-and-forth data communication for a single request. For example, both client and server may send acknowledgment data back to confirm that they have received data. Protocol acceleration bundles chatty protocol communications to lower the number of data packets on the network.

Rate and connection limits

Network administrators can limit the number of open internet access links, the number of users, and the amount of bandwidth each user can access at a time. For example, they can set rules to prevent employees from streaming videos on the enterprise WAN.

Network segmentation

Traffic shaping controls data flow for specific applications, which divides network bandwidth optimally between applications. The network operator can choose to prioritize certain critical applications to improve their performance.

How can AWS help you with WAN management?

AWS Cloud WAN is a fully managed service to build, manage, and monitor your global wide-area networks (WANs). It provides a central dashboard for making connections between your branch offices, data centers, and virtual private clouds (VPCs) in just a few clicks. It generates a complete view of your on-premises and AWS networks to help you monitor network health, security, and performance. You can also use network policies to automate network management and security tasks from one location.

You gain these benefits:

- Use your choice of local network providers to connect to AWS, and then use the AWS global network to connect your locations and VPCs.
- Save time by automating routine networking tasks, such as adding new connections, branch locations, and VPCs.
- Track network traffic, view the health of your network, improve performance, and minimize downtime.

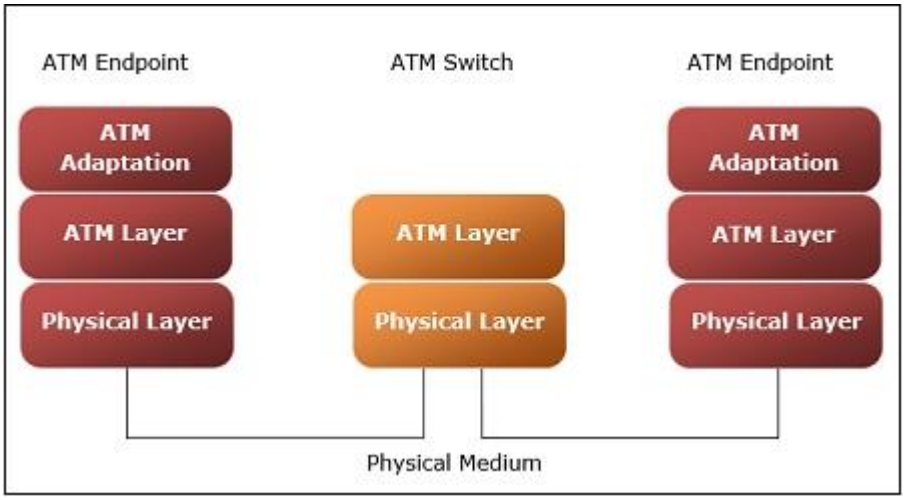
Get started with Cloud WAN by creating an AWS accouting

ATM and ATM Networks

ATM stands for Asynchronous Transfer Mode. It is a switching technique that uses time division multiplexing (TDM) for data communications.

ATM networks are connection oriented networks for cell relay that supports voice, video and data communications. It encodes data into small fixed - size cells so that they are suitable for TDM and transmits them over a physical medium.

The size of an ATM cell is 53 bytes: 5 byte header and 48 byte payload. There are two different cell formats - user-network interface (UNI) and network-network interface (NNI). The below image represents the Functional Reference Model of the Asynchronous Transfer Mode.



Benefits of ATM Networks are

- It provides the dynamic bandwidth that is particularly suited for bursty traffic.
- Since all data are encoded into identical cells, data transmission is simple, uniform and predictable.
- Uniform packet size ensures that mixed traffic is handled efficiently.
- Small sized header reduces packet overload, thus ensuring effective bandwidth usage.
- ATM networks are scalable both in size and speed.

ATM reference model comprises of three layers

- **Physical Layer** − This layer corresponds to physical layer of OSI model. At this layer, the cells are converted into bit streams and transmitted over the physical medium. This layer has two sub layers: PMD sub layer (Physical Medium Dependent) and TC (Transmission Convergence) sub layer.
- **ATM Layer** −This layer is comparable to data link layer of OSI model. It accepts the 48 byte segments from the upper layer, adds a 5 byte header to each segment and converts into 53 byte cells. This layer is responsible for routing of each cell, traffic management, multiplexing and switching.
- **ATM Adaptation Layer (AAL)** −This layer corresponds to network layer of OSI model. It provides facilities to the existing packet switched networks to connect to ATM network and use its services. It accepts the data and converts them into fixed sized segments. The transmissions can be of fixed or variable data rate. This layer has two sub layers − Convergence sub layer and Segmentation and Reassembly sub layer.
- **ATM endpoints** − It contains ATM network interface adaptor. Examples of endpoints are workstations, routers, CODECs, LAN switches, etc.
- **ATM switch** −It transmits cells through the ATM networks. It accepts the incoming cells from ATM endpoints (UNI) or another switch (NNI), updates cell header and retransmits cell towards destination.

Point-to-Point Protocol (PPP)
Computer EngineeringComputerNetworkMCA

Point - to - Point Protocol (PPP) is a communication protocol of the data link layer that is used to transmit multiprotocol data between two directly connected (point-to-point) computers. It is a byte - oriented protocol that is widely used in broadband communications having heavy loads and high speeds. Since it is a data link layer protocol, data is transmitted in frames. It is also known as RFC 1661.

Services Provided by PPP

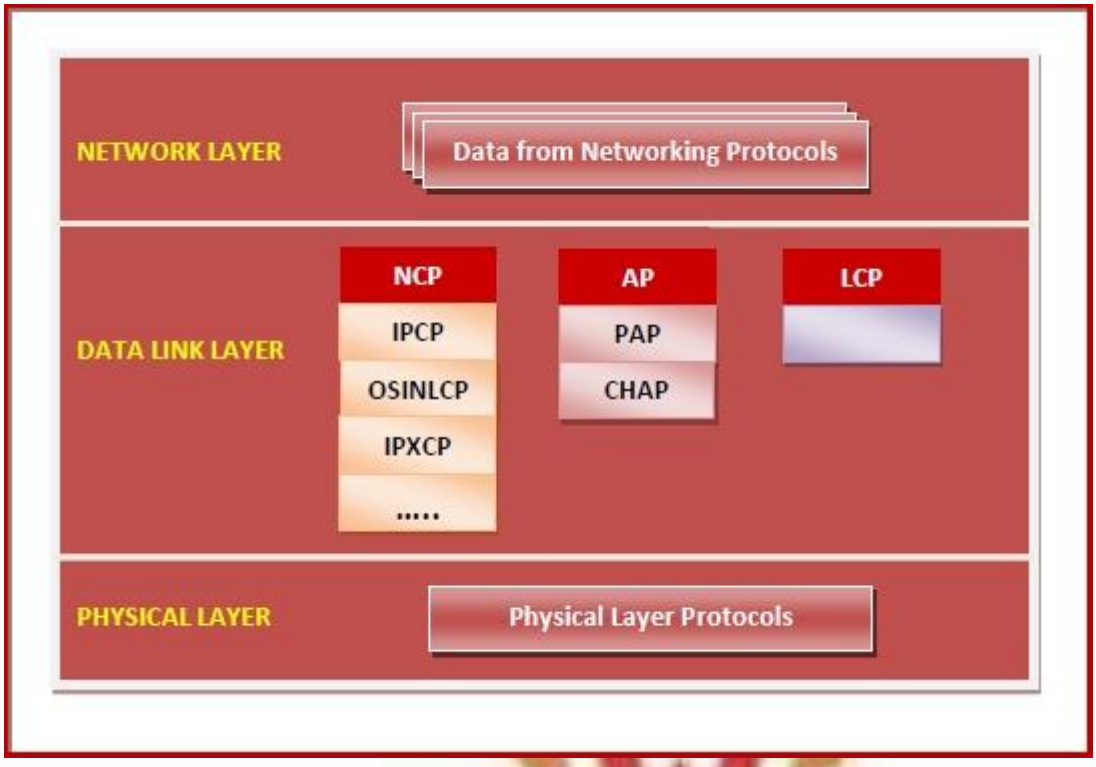
The main services provided by Point - to - Point Protocol are −

- Defining the frame format of the data to be transmitted.
- Defining the procedure of establishing link between two points and exchange of data.
- Stating the method of encapsulation of network layer data in the frame.
- Stating authentication rules of the communicating devices.
- Providing address for network communication.
- Providing connections over multiple links.
- Supporting a variety of network layer protocols by providing a range os services.

Components of PPP

Point - to - Point Protocol is a layered protocol having three components −

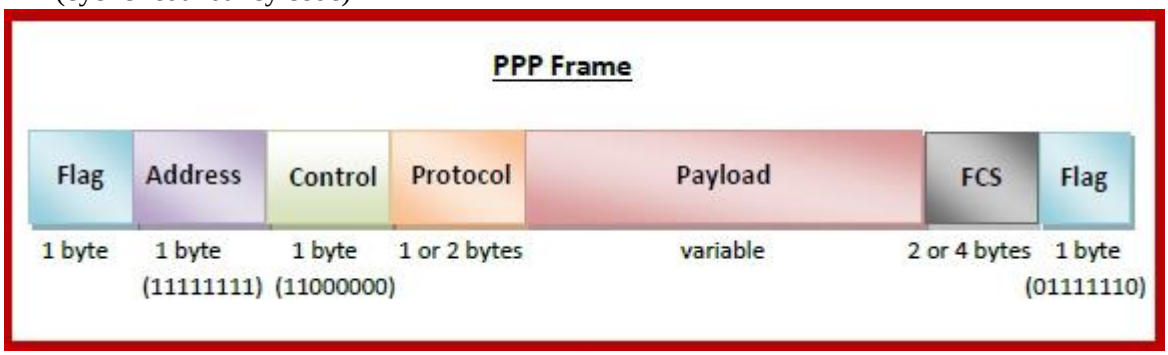
- **Encapsulation Component** − It encapsulates the datagram so that it can be transmitted over the specified physical layer.
- **Link Control Protocol (LCP)** − It is responsible for establishing, configuring, testing, maintaining and terminating links for transmission. It also imparts negotiation for set up of options and use of features by the two endpoints of the links.
- **Authentication Protocols (AP)** − These protocols authenticate endpoints for use of services. The two authentication protocols of PPP are −
  - Password Authentication Protocol (PAP)
  - Challenge Handshake Authentication Protocol (CHAP)
- **Network Control Protocols (NCPs)** − These protocols are used for negotiating the parameters and facilities for the network layer. For every higher-layer protocol supported by PPP, one NCP is there. Some of the NCPs of PPP are −
  - Internet Protocol Control Protocol (IPCP)
  - OSI Network Layer Control Protocol (OSINLCP)
  - Internetwork Packet Exchange Control Protocol (IPXCP)
  - DECnet Phase IV Control Protocol (DNCP)
  - NetBIOS Frames Control Protocol (NBFCP)
  - IPv6 Control Protocol (IPV6CP)



PPP Frame

PPP is a byte - oriented protocol where each field of the frame is composed of one or more bytes. The fields of a PPP frame are −

- **Flag** − 1 byte that marks the beginning and the end of the frame. The bit pattern of the flag is 01111110.
- **Address** − 1 byte which is set to 11111111 in case of broadcast.
- **Control** − 1 byte set to a constant value of 11000000.
- **Protocol** − 1 or 2 bytes that define the type of data contained in the payload field.
- **Payload** − This carries the data from the network layer. The maximum length of the payload field is 1500 bytes. However, this may be negotiated between the endpoints of communication.
- **FCS** − It is a 2 byte or 4 bytes frame check sequence for error detection. The standard code used is CRC (cyclic redundancy code)



Byte Stuffing in PPP Frame − Byte stuffing is used is PPP payload field whenever the flag sequence appears in the message, so that the receiver does not consider it as the end of the frame. The escape byte, 01111101, is stuffed before every byte that contains the same byte as the flag byte or the escape byte. The receiver on receiving the message removes the escape byte before passing it onto the network layer.

UNIT-IV

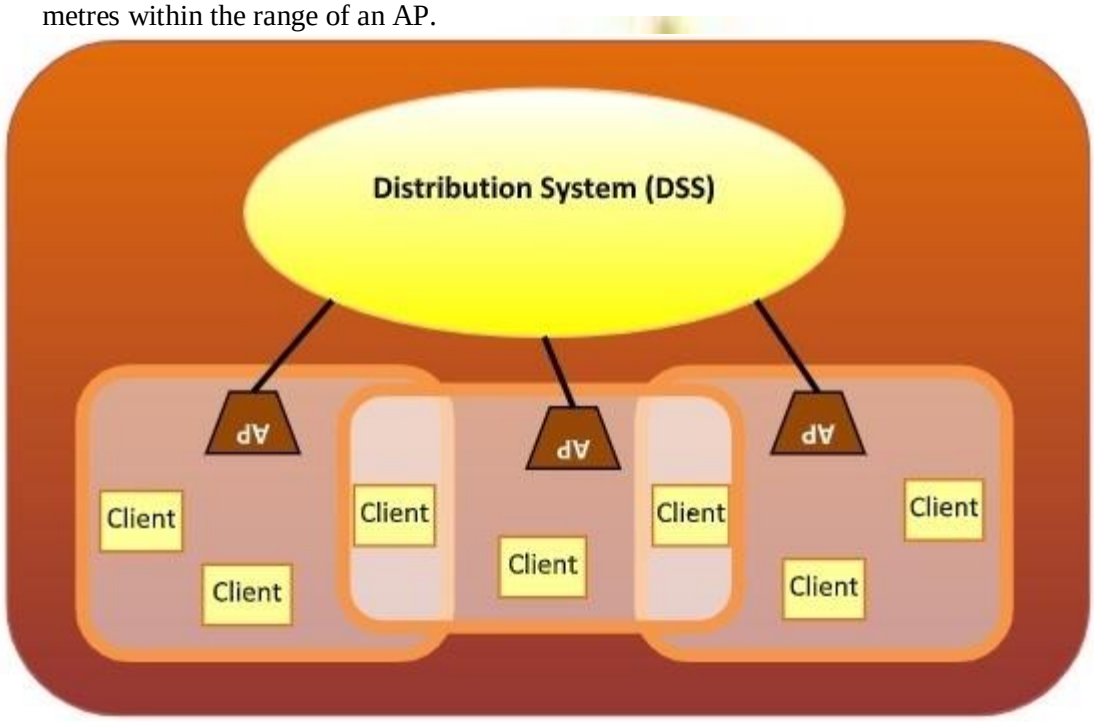
Wireless LAN Protocols

Wireless LANs refer to LANs (Local Area Networks) that use high frequency radio waves instead of cables for connecting the devices. It can be conceived as a set of laptops and other wireless devices communicating by radio signals. Users connected by WLANs can move around within the area of network coverage. Most WLANs are based upon the standard IEEE 802.11 or WiFi.

Configuration of Wireless LANs

Each station in a Wireless LAN has a wireless network interface controller. A station can be of two categories −

- **Wireless Access Point (WAP)** − WAPs or simply access points (AP) are generally wireless routers that form the base stations or access points. The APs are wired together using fiber or copper wires, through the distribution system.
- **Client** − Clients are workstations, computers, laptops, printers, smart phones etc. They are around tens of metres within the range of an AP.



Types of WLAN Protocols

IEEE 802.11 or WiFi has a number of variations, the main among which are −

- **802.11a Protocol**− This protocol supports very high transmission speeds of 54Mbps. It has a high frequency of 5GHz range, due to which signals have difficulty in penetrating walls and other obstructions. It employs Orthogonal Frequency Division Multiplexing (OFDM).
- **802.11b Protocol** − This protocol operates within the frequency range of 2.4GHz and supports 11Mbps speed. It facilitates path sharing and is less vulnerable to obstructions. It uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with Ethernet protocol.
- **802.11g Protocol** − This protocol combines the features of 802.11a and 802.11b protocols. It supports both the frequency ranges 5GHz (as in 802.11a standard) and 2.4GHz (as in 802.11b standard). Owing to its dual

features, 802.11g is backward compatible with 802.11b devices. 802.11g provides high speeds, varying signal range, and resilience to obstruction. However, it is more expensive for implementation.

- **802.11n Protocol** − Popularly known as Wireless N, this is an upgraded version of 802.11g. It provides very high bandwidth up to 600Mbps and provides signal coverage. It uses Multiple Input/Multiple Output (MIMO), having multiple antennas at both the transmitter end and receiver ends. In case of signal obstructions, alternative routes are used. However, the implementation is highly expensive.

Ethernet Tutorial – Part I: Networking Basics

Computer networking has become an integral part of business today. Individuals, professionals and academics have also learned to rely on computer networks for capabilities such as electronic mail and access to remote databases for research and communication purposes. Networking has thus become an increasingly pervasive, worldwide reality because it is fast, efficient, reliable and effective. Just how all this information is transmitted, stored, categorized and accessed remains a mystery to the average computer user.

This tutorial will explain the basics of some of the most popular technologies used in networking, and will include the following:

- Types of Networks – including LANs, WANs and WLANs
- The Internet and Beyond – The Internet and its contributions to intranets and extranets
- Types of LAN Technology – including Ethernet, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, ATM, PoE and Token Ring
- Networking and Ethernet Basics – including standard code, media, topographies, collisions and CSMA/CD
- Ethernet Products – including transceivers, network interface cards, hubs and repeaters

Types of Networks

In describing the basics of networking technology, it will be helpful to explain the different types of networks in use.

Local Area Networks (LANs)

A network is any collection of independent computers that exchange information with each other over a shared communication medium. Local Area Networks or LANs are usually confined to a limited geographic area, such as a single building or a college campus. LANs can be small, linking as few as three computers, but can often link hundreds of computers used by thousands of people. The development of standard networking protocols and media has resulted in worldwide proliferation of LANs throughout business and educational organizations.

Wide Area Networks (WANs)

Often elements of a network are widely separated physically. Wide area networking combines multiple LANs that are geographically separate. This is accomplished by connecting the several LANs with dedicated leased lines such as a T1 or a T3, by dial-up phone lines (both synchronous and asynchronous), by satellite links and by data packet carrier services. WANs can be as simple as a modem and a remote access server for employees to dial into, or it can be as complex as hundreds of branch offices globally linked. Special routing protocols and filters minimize the expense of sending data over vast distances.

Wireless Local Area Networks (WLANs)

Wireless LANs, or WLANs, use radio frequency (RF) technology to transmit and receive data over the air. This minimizes the need for wired connections. WLANs give users mobility as they allow connection to a local area

network without having to be physically connected by a cable. This freedom means users can access shared resources without looking for a place to plug in cables, provided that their terminals are mobile and within the designated network coverage area. With mobility, WLANs give flexibility and increased productivity, appealing to both entrepreneurs and to home users. WLANs may also enable network administrators to connect devices that may be physically difficult to reach with a cable.

The Institute for Electrical and Electronic Engineers (IEEE) developed the 802.11 specification for wireless LAN technology. 802.11 specifies over-the-air interface between a wireless client and a base station, or between two wireless clients. WLAN 802.11 standards also have security protocols that were developed to provide the same level of security as that of a wired LAN.
The first of these protocols is Wired Equivalent Privacy (WEP). WEP provides security by encrypting data sent over radio waves from end point to end point.

Virtual Local Area Networks (VLANs)

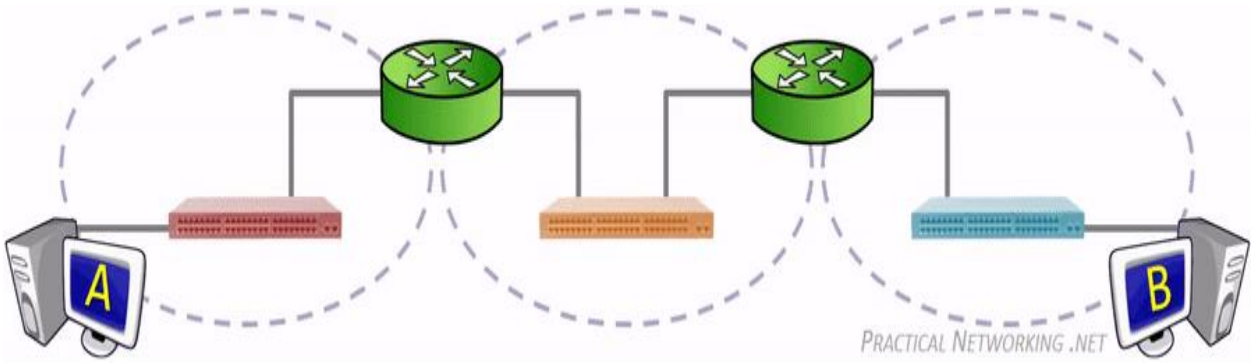
Virtual Local Area Networks, or **VLANs**, are a very simple concept that has been very poorly defined by the industry.

This article will explain VLANs from a *practical* perspective. It will be framed around the two major functions of VLANs, and concluded with an explanation of the idea behind the Native VLAN.

Finally, at the end of the article is a two question comprehension challenge – if you can successfully answer these two questions, then you can consider yourself to fully understand the *concept* of VLANs — the topic of configuring VLANs will be covered in another article.

Two Major Functions of VLANs

Below is a network with three different physical switches. The switches facilitate communication within networks, and the Routers facilitate communication between networks.



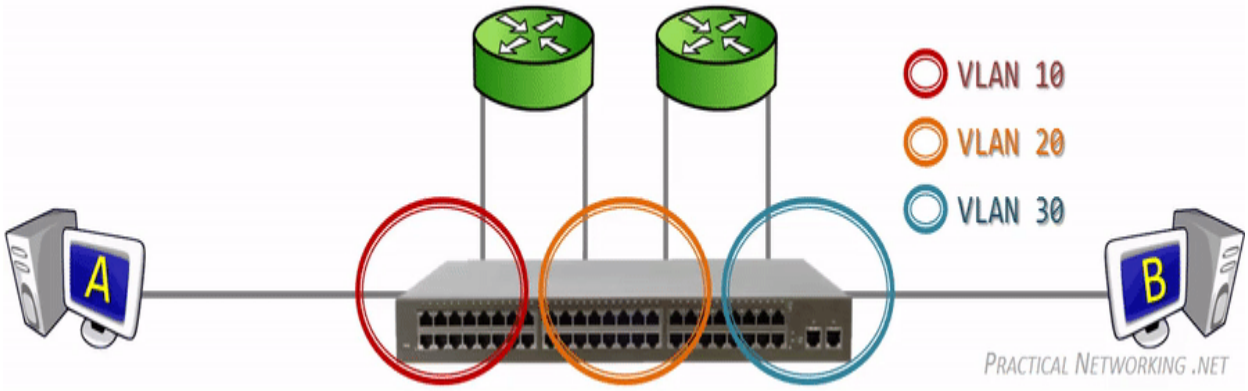
Each switch above independently perform all the functions of a switch.

If each of these switches have 24 ports and only two are in use, then 22 ports are left wasted on each switch. Moreover, what if you need to replicate this network elsewhere and you do not have three physical switches to accommodate?

That is where the first major function of a VLAN comes into play: **A VLAN allows you to take one physical switch, and break it up into smaller *mini-switches***.

Breaking up one Physical Switch into multiple Virtual Switches

Consider each circle on the switch below as its own *mini-switch* (or *virtual* switch). Each of these *mini-switches* are a collection of switch ports which *operate completely independent* from the others — exactly as they would had there been three *different* physical switches.



Traffic flow through the single *switch* of this topology operates exactly as it did in the topology above it with three separate physical switches. The routers are configured and operate exactly as they did above.

Each *virtual* switch, or *VLAN*, is simply a number assigned to each switch port. For example, the two switch ports in the red *mini-switch* might be assigned to VLAN #10. The two ports in the orange *mini-switch* might be assigned to VLAN #20. And lastly the two switch ports in the blue *mini-switch* might be assigned to VLAN #30.

Any switch port which is *not* explicitly assigned a VLAN number, resides in the *default* VLAN. Which for most vendors corresponds to **VLAN** 1.

Traffic arriving on a switch port assigned to one VLAN will only ever be forwarded out another switch port that belongs to the *same* VLAN – **a switch will never allow traffic to cross a VLAN boundary**. Again, each VLAN operates as if it were a completely separate physical switch.

In the first illustration, traffic from the red switch cannot magically appear on the orange switch without first passing through a router. Similarly, in the second illustration, traffic in VLAN #10 cannot magically appear on VLAN #20 without also passing through a router.

When a frame arrives on a switchport in VLAN #10, it can only leave a switchport in VLAN #10. You and I can see that the same frame is traversing all three VLANs, but from the Switch's perspective, it is **three different instances** of **a frame arriving on *one port* in *one VLAN***, and **leaving on *another port* in the *same VLAN***.

VLANs and MAC Address Tables

By definition, a Switch is a device whose primary purpose is to move data *within* IP Networks. To accomplish this goal, every switch maintains a MAC Address Table, which is a mapping of the MAC addresses connected to every Switchport. A simple representation of a single entry in a MAC address table would be: MAC Address | Port.

A Switch which supports VLANs will *also* include the VLAN # for *each* entry of the MAC Address Table. A simple representation of a single entry in a MAC address table of a VLAN aware switch would be: VLAN# | MAC Address | Port.

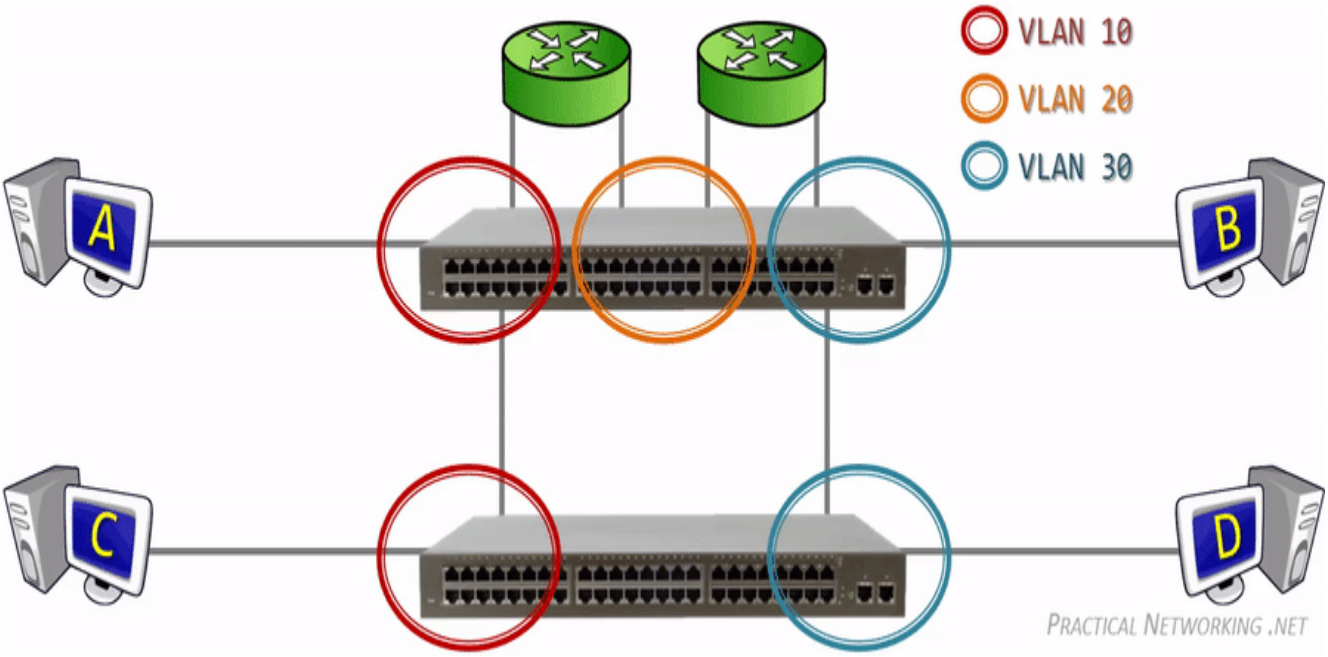
In a way, it's almost as if each VLAN maintains their own independent MAC address table. If Host A were to send a frame with a destination MAC address of Host B, that frame would *still* only be flooded solely to the switch ports in VLAN #10. Even if a MAC address table entry for Host B existed associated to VLAN #30.

Ultimately, assigning different ports to different VLANs allows you to re-use a single physical switch for multiple purposes. This is the first major function of a VLAN.

But that isn't all VLANs allow you to do. The second major function is **VLANs allow you to extend the smaller Virtual switches across multiple Physical switches**.

Extending Virtual Switches across multiple Physical Switches

To illustrate this point, we will expand the topology above with an additional physical switch and two additional hosts:



Notice how a VLAN# 10 and VLAN# 30 have been extended onto a second switch. This enables Host A and Host C to exist in the same VLAN, despite being connected to different physical switches located in potentially different areas.

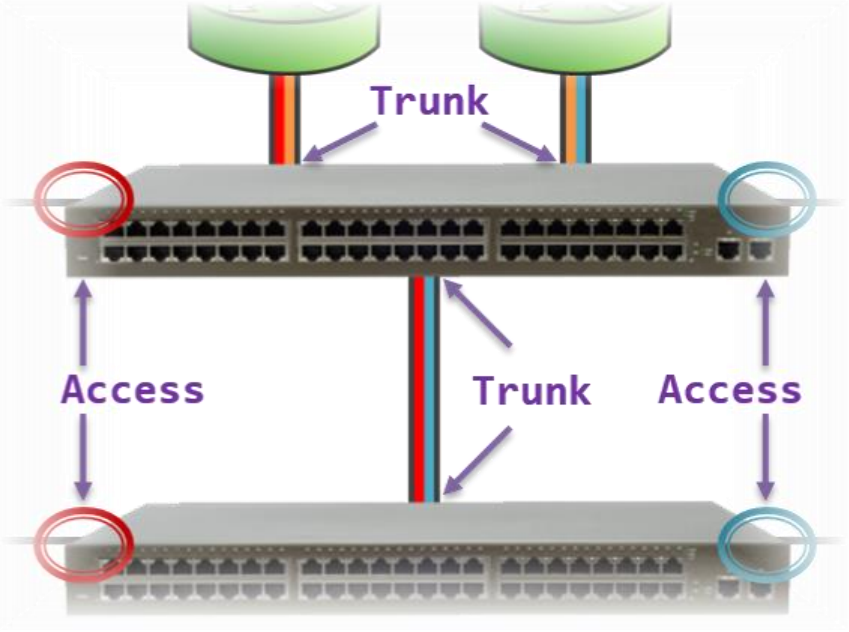
The primary benefit of extending a VLAN to different physical switches is that the Layer 2 topology no longer has to be tied to the Physical Topology. A single VLAN can span across multiple rooms, floors, or office buildings.

Each connected switch port in the topology above is a member of only a single VLAN. This is referred to as an **Access** port. **An Access port is a switch port that is a member of *only one* VLAN**.

When configuring a port as an Access port, the administrator also designates the VLAN number that port is a member of. Whenever the switch receives any traffic on an Access port, it accepts the traffic onto the configured VLAN.

In order to extend a VLAN to the second switch, a connection is made between *one* Access port on *both* switches for *each* VLAN. While functional, this strategy does not scale. Imagine if our topology was using ten VLANs, on a 24 port switch nearly half of the ports would be taken up by the inter-switch links.

Instead, there is a mechanism which allows a single switch port to carry traffic from multiple VLANs. This is referred to as a **Trunk** port. **A Trunk port is a switch port that carries traffic for *multiple* VLANs**.



We can use Trunk ports to reduce the amount of switch ports required for the topology above. This enables us to leave more ports available to add hosts to the network in the future.

This physical topology operates (logically) identically to the illustration above it, but requires far fewer switch ports.

We were able to use a total of four Trunk ports (across both switches) to replace eight different Access ports in the prior illustration.

Typically, **switch ports connected to end-host devices are configured as Access ports** (e.g., workstations, printers, servers). Conversely, **switch ports connected to other network devices are configured as Trunk ports** (e.g., other switches, routers). We will uncover the reason for this later in this article.

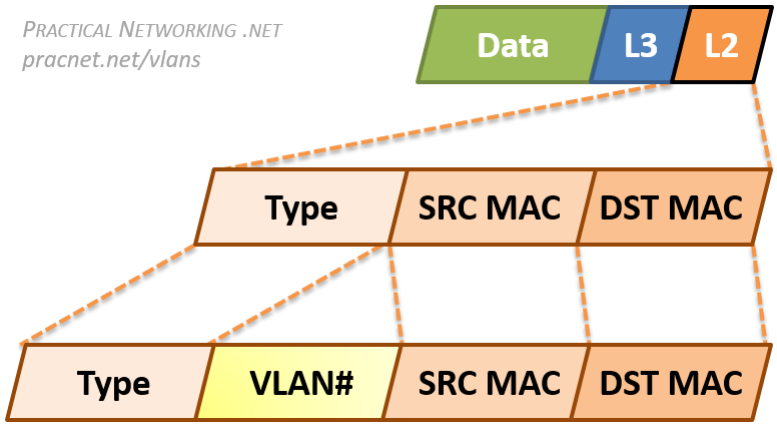
Tagged Ports and Untagged Ports

A Trunk port on a switch can receive traffic for more than one VLAN. For example, in the illustration above, the link between the two switches is carrying traffic for both VLAN 10 and VLAN 30.

But in both cases, traffic is leaving one switch as a series of frames, and arriving on the other switch as a series of frames. Which begs the question, **how will the receiving switch determine which frames belong to** VLAN #10**, and which frames belong to** VLAN #30?

To account for this, **whenever a Switch is sending frames out a Trunk port, it adds to each frame a *tag* to indicate to the other end what VLAN that frame belongs to**. This allows the receiving switch to read the VLAN tag in order to determine what VLAN the incoming traffic should be associated to.

An *Access* port, by comparison, can only ever carry or receive traffic for a single VLAN. Therefore, **there is no need to add a VLAN Tag to traffic leaving an Access port**.

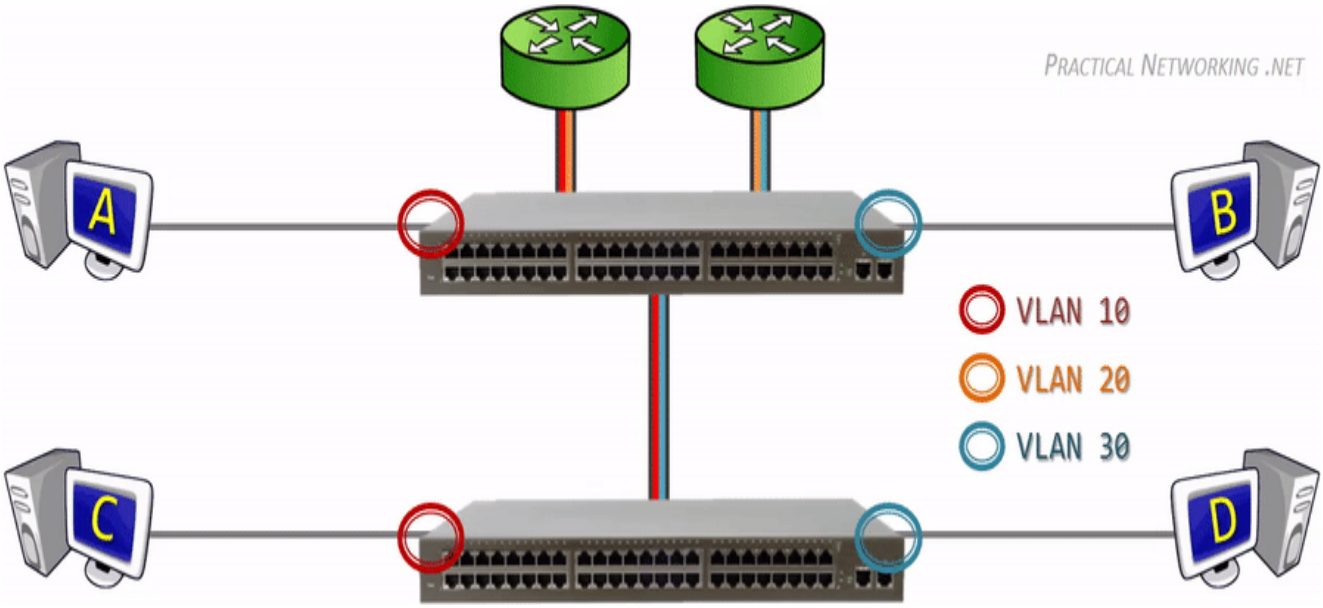


Since VLANs are a Layer 2 technology, the VLAN Tag is inserted within the Layer 2 header. The standard Layer 2 header in modern networks is the Ethernet header, which has three fields: *Destination MAC Address*, *Source MAC Address*, and *Type*.

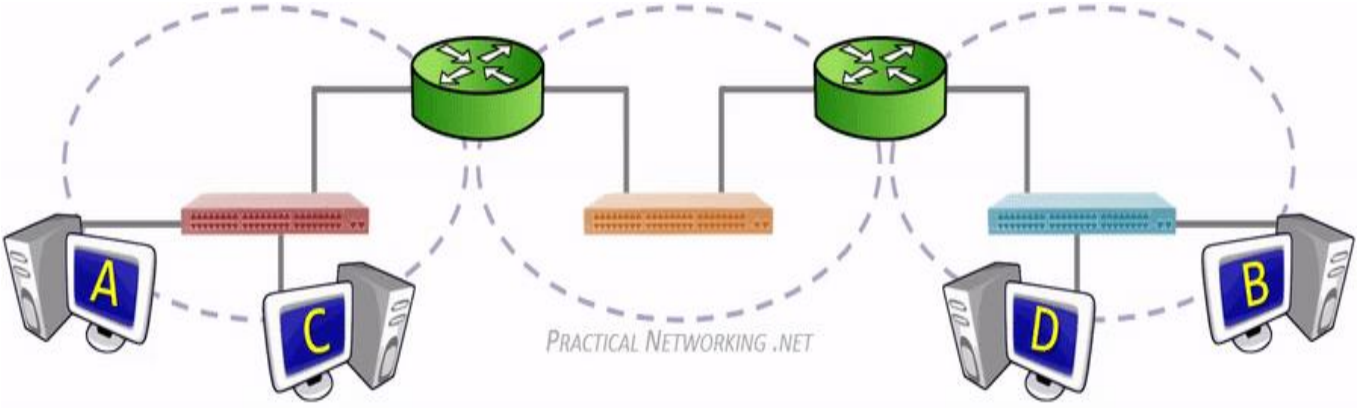
When an Ethernet frame is exiting a Trunk port, the switch will insert a VLAN Tag between the *Source MAC address* and the *Type* fields.

This allows the receiving switch to associate the frame with the appropriate VLAN.

To summarize, the final topology with traffic traveling between Host C and Host D through Access ports and Trunk ports will look like this:



The physical topology above will work exactly like the logical topology below. The hosts will not know whether they are going through two physical switches (or three or four), or what VLANs they are in. They operate exactly as they would in any situation which involves moving packets through a network.



Access Ports and End-Host Devices

Earlier we mentioned **Access ports typically face end-host devices** like workstations or printers or servers.

Part of the reason for this is that switches do not add a VLAN tag when sending traffic out an Access Port.

This allows a host to operate without any knowledge of the VLAN they are connected to.

In a way, the hosts are, intentionally, completely blind to the existence or use of VLANs. Hosts simply send data on a network without any knowledge of VLANs, or the switches they might be connected to.

There was a point in the early days of Networking where certain end-devices would react negatively if they received a frame with a VLAN tag. For such systems, which were *strictly* expecting *only* the typical fields in an Ethernet header, the frames which included a VLAN tag might appear as a malformed Ethernet header.

However, this was rare, as the construction of the VLAN tag was intentionally designed to avoid being interpreted as a malformed frame (this will make more sense in the next section).

Either way, the general precedent is **traffic to end-hosts should *not* include any VLAN tags**, Hosts can and should remain blissfully ignorant of what VLANs they are in, or even whether VLANs are being utilized at all.

A possible **exception would be if a single Physical Host is hosting multiple Virtual Machines (VMs)** — like a Hypervisor. In some cases, each of those VMs need to exist in separate VLANs. Therefore, the Physical Host must be connected to a Trunk port, and must send and received VLAN tags in order to confine the virtual machine traffic to a specific VLAN.

Terminology

Finally, a quick note on terminology. The terms *Access* port and *Trunk* port are usually associated with the Cisco world. But VLANs are an open standard, therefore other vendors are able to implement VLANs as well.

What Cisco calls a *Trunk* port (i.e., a switch port that carries traffic for more than one VLAN), other vendors refer to as a **Tagged** port – referring to the addition of a VLAN tag to all traffic leaving such a port.

What Cisco calls an *Access* port (i.e., a switch port that carries traffic for only one VLAN), other vendors refer to as an **Untagged** port – referring to the traffic leaving the switch port without a VLAN tag.

These terms are not exhaustive, there are some vendors that may yet use other terminology, other vendors may even mix and match these terms. Regardless of the terminology used, all the concepts discussed above still apply.

802.1Q VLAN Tag

VLAN tags requires adding and removing bits to Ethernet frames. The specific sequence of bits to add is governed by an open standard, which allow any vendor to implement VLANs on their devices.

The exact format of the VLAN Tag is governed by the 802.1Q standard. This is an open, IEEE standard which is the ubiquitous method of VLAN tagging in use today.

To demonstrate exactly how the VLAN Tag modifies a packet, take a look at the packet capture below of the same frame before and after it exits a Trunk port.

The portion of the frame highlighted in yellow is the added VLAN tag. Notice it is inserted between the *Source MAC address* and *Type* field of the original Ethernet header.

You can view this capture yourself in Cloudshark, or you can download the capture file and open it in Wireshark.

No other modification to the frame or its payload is made by the addition or removal of the VLAN tag. That said, since even the slight modification displayed above is made, adding and removing the VLAN tag also involves recalculating the CRC — which is a simple hash algorithm devised to detect transmissions errors on the wire.

There is an older method of VLAN tagging which is a closed, Cisco proprietary method. This method was called Inter-Switch Link, or **ISL**. ISL fully encapsulated the L2 frame in a new header which included the VLAN identification number.

But these days, even newer Cisco products do not support ISL, as the entire industry has moved to the superior, open standard of 802.1Q.

Native VLAN

There is one final concept associated with VLANs that often brings confusion. That is the concept of the **Native VLAN**.

The Native VLAN is the answer to how a switch processes traffic it receives on a Trunk port which does not contain a VLAN Tag.

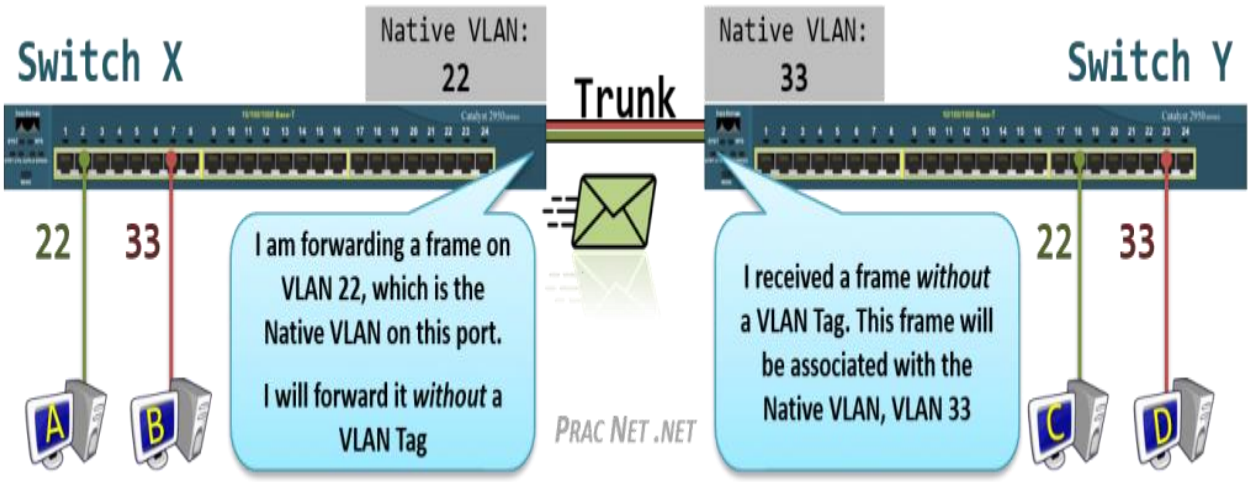
Without the tag, the switch will not know what VLAN the traffic belongs to, therefore the switch associates the untagged traffic with what is configured as the Native VLAN. Essentially, **the Native VLAN is the VLAN that any received untagged traffic gets assigned to on a Trunk port**.

Additionally, any traffic the switch forwards out a Trunk port that is associated with the Native VLAN is forwarded *without* a VLAN Tag.

To see the Native VLAN in action on a live trunk port, check out this video.

The Native VLAN can be configured on any Trunk port. If the Native VLAN is not explicitly designated on a Trunk port, the default configuration of VLAN #1 is used.

That being said, it is crucially important that both sides of a Trunk port are configured with the same Native VLAN. This illustration explains why:



Above we have four Hosts (A, B, C, D) all connected to Access Ports in VLAN #22 or VLAN #33, and Switch X and Switch Y connected to each other with a Trunk port.

Host A is attempting to send a frame to Host C. When it arrives on the switch, Switch X associates the traffic with VLAN #22. When the frame is forwarded out Switch X's Trunk port,

no tag is added since the Native VLAN for the Trunk Port on Switch X is also VLAN #22.

But when the frame arrives on Switch Y without a tag, Switch Y has no way of knowing the traffic should belong to VLAN #22. All it can do is associate the untagged traffic with what Switch Y's

-Trunk port has configured as the Native VLAN, which in this case is VLAN #33.

Since Switch Y will never allow VLAN #33 traffic to exit a VLAN #22 port, Host C will never get this traffic. Even worse, due to a Switch'

s flooding behavior, Host D might inadvertently get the traffic that was destined to Host C.

Finally, it should be noted that the Native VLAN is an 802.1Q feature. The antiquated tagging mechanism of ISL simply dropped traffic receive on a Trunk port that did not include the ISL tag.

Also, remember that **the Native VLAN concept only applies to Trunk ports** — traffic leaving and arriving on an Access port is always expected to be untagged.

VLAN Comprehension Challenge

To test yourself to see if you fully understand how VLANs work, there is a simple challenge we can offer.

Below is a (poorly) configured topology, featuring five switches and twelve hosts. Each switch port is configured as either an Access

port in the displayed VLAN, or a Trunk Port with the Native VLAN displayed.

What is the full form of MAN

MAN: Metropolitan Area Network

MAN stands for Metropolitan Area Network. The acronym is Metropolitan Area Network. It is a computer system that links multiple local-area networks (LANs) to form a larger network that allows for sharing of computer resources. This kind of network has a wider coverage area than a LAN, but it is still less than a WAN, which is meant to cover a whole city. MAN is specifically made to give consumers access to high-speed connectivity with a range of Mbps speeds. The MAN's intricate architecture makes it difficult to create and keep up with. MAN is between WAN and LAN in size. The scope and scale of the various computer designs can be used in networking as a classification method. Area network types frequently include LAN, WLAN, WAN, SAN, PAN, CAN, DAN, & MAN.

In this article, we will solely discuss MAN in its complete form and its benefits and drawbacks. MAN is positioned among LAN and WAN since it is larger than LAN and less significant than WAN. It includes a city's underground area network.

What Does MAN Stand for in Computer Language?

In computer networking, the MAN is formally known as Metropolitan Area Network. A MAN could be a single network, similar to the cable television network. Still, it typically connects numerous LANs using high-capacity backbone technologies, including fiber-optic cables and offers up-link services to a WAN. Between five and several hundred miles in length, MAN travels at speeds between 1.5 and 10 Mbps. Examples of MANs are FDDI (Fiber Distribution Data Transfer) and ATM (MAN full name: Metropolitan Area Network) (Asynchronous Transfer

Mode).

How Are MAN Networks Constructed?

Similar to WANs, a MAN is composed of interconnected LANs. Since data does not need to travel long distances, MANs are typically more efficient than WANs. Instead of being run by a single organization, MANs often combine the networks of several different organizations.deo

The majority of MANs connect LANs via fiber optic lines. A MAN frequently uses "black fiber"-traffic-carrying fiber optic cables previously idle. Leasing these fiber optic lines from private Internet service providers is an option (ISP). A city government may construct and maintain a metropolitan fiber optic network before leasing dark fiber to private businesses in particular instances.

Background of MAN

To link LANs when they were first established in 1994 to allow data connectivity in buildings and offices, enterprises mostly relied on mobile switching telephone networks. The telephone network, however, could not handle that amount of traffic. To address this issue, it was suggested that LANs be linked via single-mode fiber optic lines, creating metropolitan area networks (MAN) to connect LANs efficiently. These fiber optic MANs are run and owned by private companies or organizations, and they may not have been completely integrated through gateways with the public wide area network (WAN).

MAN Characteristics

The characteristics of MAN include;

- It can transport information from a collection of buildings to the entire city across a range of 5 to 50 kilometers.
- Data rates in MAN range from average to high.
- The most often used media in MAN, optical fibers, allows for high-speed communication.
- MAN, networks have a very low error rate, which makes them highly reliable.

Benefits of MAN (Metropolitan Area Network)

In terms of area network coverage, MAN outperforms LAN and is in the middle of LAN and WAN. Let's go over the benefits of the MAN in more detail. The advantages are as follows:

- It provides quick communication through fiber optic cables and other high-speed carriers.
- It offers increased access to WANs and strong support for networks of a large size.
- Data transfer in both directions can happen simultaneously thanks to the dual bus of the MAN network.
- A MAN network typically consists of a city's entirety or specific neighborhoods.

The Drawbacks of MAN (Metropolitan Area Network)

Each network design has advantages and disadvantages. We know its excellent coverage of the entire city and continued network connectivity. Let's now examine its drawbacks. The drawbacks are as follows:

- To build a MAN link from one location to another, an extra cable is required.
- It is challenging to make the systems hacker-proof in the MAN network.
- Compared to LANs, the data transfer rate in MAN is poor.

MAN examples include

- Network on cable TV.
- Used by government institutions.
- College campuses.

SAN

SAN is an abbreviation of the **Storage Area Network**. Storage Area Network is a dedicated, specialized, and high-speed network which provides block-level data storage. It delivers the shared pool of storage devices to more than one server.

The main aim of SAN is to transfer the data between the server and storage device. It also allows for transferring the data between the storage systems.

Storage Area networks are mainly used for accessing storage devices such as tape libraries and disk-based devices from the servers.

It is a dedicated network which is not accessible through the LAN. It consists of hosts, switches, and storage devices which are interconnected using the topologies, protocols, and technologies.

rotocols of SAN

Following are the most common protocols of SAN (Storage Area Network):

- FCP (Fibre Channel Protocol)
- iSCSI
- FCoE
- NVMe

FCP (Fibre Channel Protocol)

It is the most commonly used protocol of the Storage Area Network. It is a mapping of SCSI command over the Fibre Channel (FC) network.

ISCSI

It stands for Internet SCSI or Internet Small Computer System Interface. It is the second-largest block or SAN protocol. It puts the SCSI commands inside an ethernet frame and then transports them over an Internet protocol (IP) ethernet.

FCoE

FCoE stands for "Fibre Channel Over Internet". It is a protocol which is similar to the iSCSI. It puts the Fibre channel inside the ethernet datagram and then transports over an IP Ethernet network.

NVMe

NVMe stands for Non-Volatile Memory Express. It is also a protocol of SAN, which access the flash storage by the PCI Express bus.

How SAN is different from NAS

The following table describes the difference between Storage Area Network and Network Attached Storage:

SAN	NAS
1. SAN stands for Storage Area Network.	1. NAS is an abbreviation of Network Attached Storage.
2. It uses the fibre channel for connecting the several data storage devices.	2. It is a hardware device which attaches to LAN through an ethernet connection.
3. It is used in enterprise and professional environments.	3. It is typically used in homes.
4. It needs more administration for managing.	4. It is managed easily.
5. In this, data is identified by the disk block.	5. In NAS (Network Attached Storage), both file name and byte offset are used for identifying the data.
6. Storage Area Network is more complex than the Network Attached Storage.	6. Network Attached Storage is less complex than the Storage Area Network.
7. It is more costly than the Network Attached Storage.	7. Its cost is less than the SAN.
8. It depends on the Local Area Network and requires the TCP/IP network.	8. It does not depend on the Local Area Network but uses the high-speed fibre channel network.

9. ISCSI, FCoE, FCP, and Fc-NVMe are the protocols used in SAN.	9. AFP, NFS, and SMB are the protocols used in NAS.
10. In SAN, block by block technique is used for backup and recovery.	10. Files in NAS are used for backup and recovery.
11. It works easily with the virtualization technique.	11. NAS is a file storage device that does not work with the virtualization technique.
12. The file system is managed and controlled by the servers in SAN.	12. The file system is managed by the head unit in NAS.

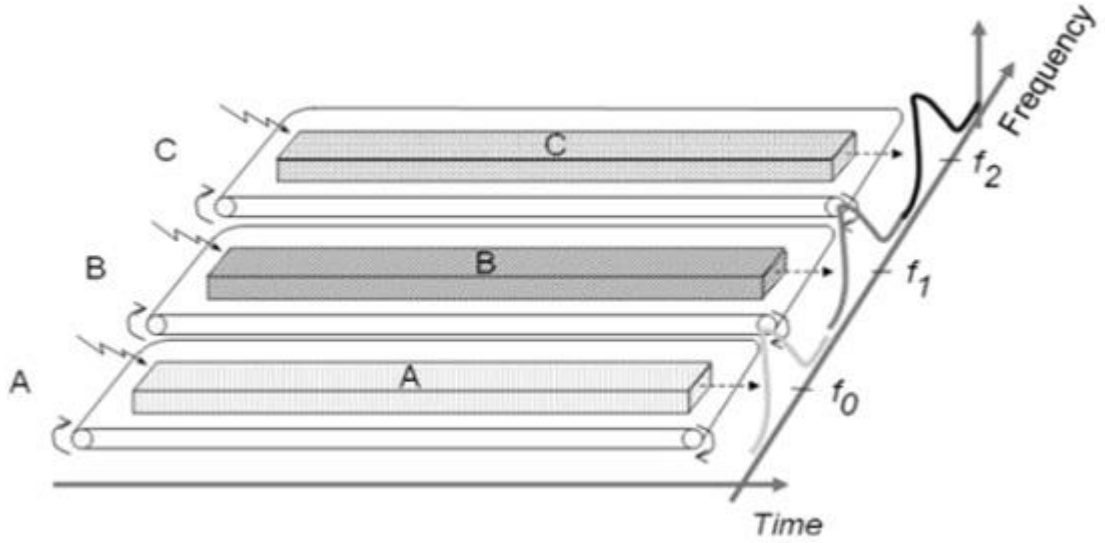
UNIT-V

FDMA - Technology

Frequency Division Multiple Access (FDMA) is one of the most common analogue multiple access methods. The frequency band is divided into channels of equal bandwidth so that each conversation is carried on a different frequency (*as shown in the figure below*).

FDMA Overview

In FDMA method, guard bands are used between the adjacent signal spectra to minimize crosstalk between the channels. A specific frequency band is given to one person, and it will received by identifying each of the frequency on the receiving end. It is often used in the first generation of analog mobile phone.



Advantages of FDMA

As FDMA systems use low bit rates (large symbol time) compared to average delay spread, it offers the following advantages −

- Reduces the bit rate information and the use of efficient numerical codes increases the capacity.
- It reduces the cost and lowers the inter symbol interference (ISI)
- Equalization is not necessary.
- An FDMA system can be easily implemented. A system can be configured so that the improvements in terms of speech encoder and bit rate reduction may be easily incorporated.
- Since the transmission is continuous, less number of bits are required for synchronization and framing.

Disadvantages of FDMA

Although FDMA offers several advantages, it has a few drawbacks as well, which are listed below −

- It does not differ significantly from analog systems; improving the capacity depends on the signal-to-interference reduction, or a signal-to-noise ratio (SNR).
- The maximum flow rate per channel is fixed and small.
- Guard bands lead to a waste of capacity.

- Hardware implies narrowband filters, which cannot be realized in VLSI and therefore increases the cost.

What is WiMAX?

WiMAX stands for "Worldwide Interoperability for Microwave Access," a telecommunications standard that describes fixed and fully mobile Internet access services. The protocol follows some aspects of the IEEE 802.16 Standard.

WiMAX products and services are most likely to be found in "last mile" applications. WiMAX enables ISPs and carriers to deliver Internet access to homes and businesses without the need for physical cabling (copper, cable, etc.) to reach the customer's location.

Difference between WiMAX and WiFi

WiMAX is sometimes compared to WiFi because both technologies rely on wireless Internet connectivity and are complementary.

Following are some of the major differences between WiMAX and WiFi −

- WiMAX's range is measured in kilometers, but WiFi's range is measured in meters and is only available locally. The reliability and range of WiMAX make it ideal for providing Internet access to significant urban areas.
- WiFi uses an unlicensed spectrum, whereas WiMAX uses a licensed or unlicensed band.
- WiFi is increasingly being used by end-user devices such as laptops, desktops, and cellphones. As a result, WiMAX service providers typically give a WiMAX subscriber unit to the consumer. This device connects to the provider's network and provides customers with WiFi access and convenience inside the WiFi range.

Architecture of WiMAX

- *The physical layer* – The physical layer is in charge of signal encoding and decoding and bit transmission and receiving. It turns MAC layer frames into transmittable signals. QPSK, QAM-16, and QAM-64 are some of the modulation methods utilized on this layer.
- *MAC Layer* – This layer serves as a link between the WiMax protocol stack's convergence and physical layers. It is based on CSMA/CA and allows point-to-multipoint communication (Carrier Sense Multiple Access with Collision Avoidance).
- *Convergence Layer* – This layer provides information from the external network. It takes higher-layer protocol data units (PDUs) and converts them into lower-layer PDUs. It has different functions depending on whatever service is used.

Advantages of WiMAX

WiMAX offers the following benefits −

- It allows for very high-speed voice and data transmission over extended distances.
- Hundreds of users can be served by a single WiMAX BS.
- It is seen as a less expensive alternative to broadband wired technologies such as ADSL, cable modem, etc.
- Higher speeds are possible.
- With mobile WiMAX, you can get a more comprehensive coverage range and cellular-like performance.

Disadvantages of WiMAX

WiMAX has the following drawbacks −

- Subscribers located far away from the WiMAX BS require a LOS (Line of Sight) connection.
- Bad weather, such as rain, will disrupt the WiMAX signal and frequently result in a loss of connection.
- Wimax is a power-hungry technology that necessitates a lot of electrical assistance.
- It is not backward compatible with any wireless cellular technologies, so the initial cost of starting a WiMax is very high.
- WiMax BS and towers must be set up from scratch. Since skilled workforce is needed, it results in significant starting expenses and higher operational expenditures.

IPv6 - Mobility

When a host is connected to a link or network, it acquires an IP address and all communication take place using that IP address on that link. As soon as, the same host changes its physical location, that is, moves into another area / subnet / network / link, its IP address changes accordingly, and all the communication taking place on the host using old IP address, goes down.

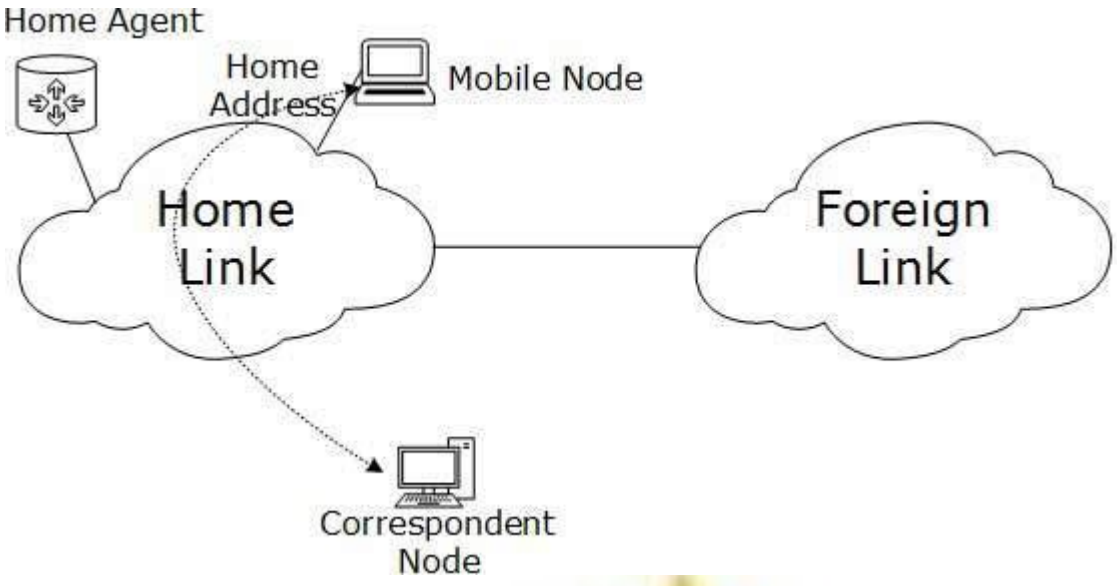
IPv6 mobility provides a mechanism for the host to roam around different links without losing any communication/connection and its IP address.

Multiple entities are involved in this technology:

- **Mobile Node**: The device that needs IPv6 mobility.
- **Home Link**: This link is configured with the home subnet prefix and this is where the Mobile IPv6 device gets its Home Address.
- **Home Address**: This is the address which the Mobile Node acquires from the Home Link. This is the permanent address of the Mobile Node. If the Mobile Node remains in the same Home Link, the communication among various entities take place as usual.
- **Home Agent**: This is a router that acts as a registrar for Mobile Nodes. Home Agent is connected to Home Link and maintains information about all Mobile Nodes, their Home Addresses, and their present IP addresses.
- **Foreign Link**: Any other Link that is not Mobile Node's Home Link.
- **Care-of Address**: When a Mobile Node gets attached to a Foreign Link, it acquires a new IP address of that Foreign Link's subnet. Home Agent maintains the information of both Home Address and Care-of Address. Multiple Care-of addresses can be assigned to a Mobile Node, but at any instance, only one Care-of Address has binding with the Home Address.
- **Correspondent Node**: Any IPv6 enabled device that intends to have communication with Mobile Node.

Mobility Operation

When Mobile Node stays in its Home Link, all communications take place on its Home Address as shown below:



[*Image: Mobile Node connected to Home Link*]

When a Mobile Node leaves its Home Link and is connected to some Foreign Link, the Mobility feature of IPv6 comes into play. After getting connected to a Foreign Link, the Mobile Node acquires an IPv6 address from the Foreign Link. This address is called Care-of Address. The Mobile Node sends a binding request to its Home Agent with the new Care-of Address. The Home Agent binds the Mobile Node's Home Address with the Care-of Address, establishing a Tunnel between both.

Whenever a Correspondent Node tries to establish connection with the Mobile Node (on its Home Address), the Home Agent intercepts the packet and forwards to Mobile Node's Care-of Address over the Tunnel which was already established.

What is RSVP (Resource Reservation Protocol)?

Computer NetworkComputerEngineeringMCA

RSVP is a transport layer protocol that is used to reserve resources in a computer network to get different quality of services (QoS) while accessing Internet applications. It operates over Internet protocol (IP) and initiates resource reservations from the receiver's end.

Features

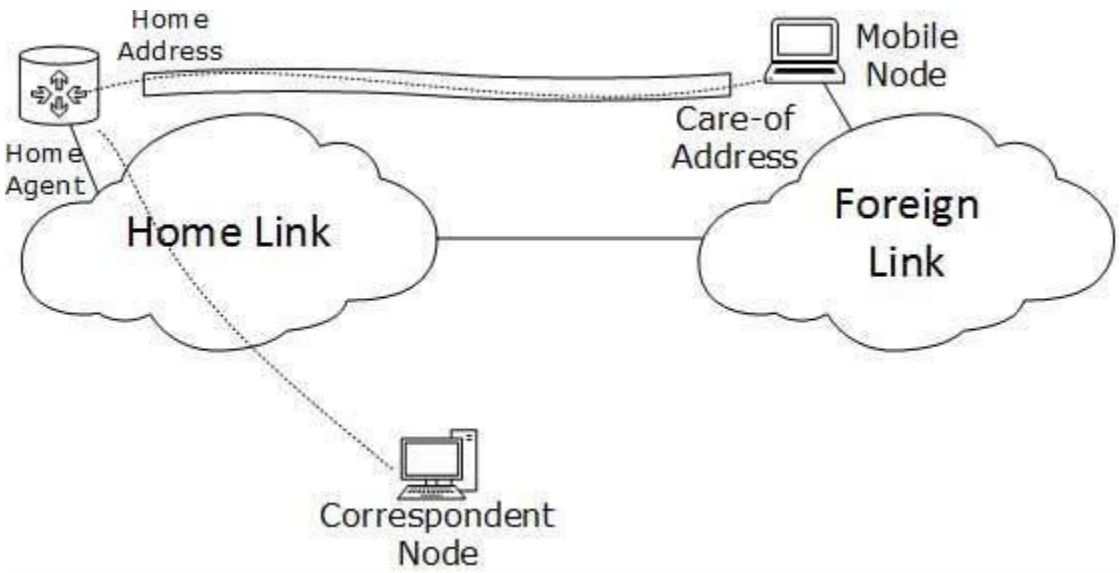
- RSVP is a receiver oriented signalling protocol. The receiver initiates and maintains resource reservation.
- It is used both for unicasting (sending data from one source to one destination) and multicasting (sending data simultaneously to a group of destination computers).
- RSVP supports dynamic automatic adaptation to changes in network.
- It provides a number of reservation styles. It also provides support for addition of future styles.

RSVP Messages

There are two types of RSVP messages −

- **Path Messages (path):** A path message is sent by the sender to all receivers by multicasting storing the path state at each node in its path. It stores the necessary information so that the receivers can make the reservation.

- **Reservation messages (resv):** The resv message is sent by the receiver to the sender along the reverse path of the path message. It identifies the resources that is requires by the data flow.



[*Image: Mobile Node connected to Foreign Link*]

Route Optimization

When a Correspondent Node initiates a communication by sending packets to Mobile the Node on the Home Address, these packets are tunneled to the Mobile Node by the Home Agent. In Route Optimization mode, when the Mobile Node receives a packet from the Correspondent Node, it does not forward replies to the Home Agent. Rather, it sends its packet directly to the Correspondent Node using Home Address as Source Address. This mode is optional and not used by default.

What is IPv4 Address and its Role in the Network?

IPv4 or Internet Protocol version 4, address is a 32-bit string of numbers separated by periods. It uniquely identifies a network interface in a device. IP is a part of the TCP/IP (Transmission Control Protocol/Internet Protocol) suite, where IP is the principal set of rules for communication on the Internet. An IP address is needed to be allocated on the devices, such as PCs, printers, servers, routers, switches, etc., to be able to communicate with each other in the network and out the Internet.

IPv4 Address Format

IPv4 addresses are expressed as a set of four numbers in decimal format, and each set is separated by a dot. Thus, the term ‘dotted decimal format.’ Each set is called an ‘octet’ because a set is composed of 8 bits. The figure below shows the binary format of each octet in the 192.168.10.100 IP address:

Format	1st Octet	2nd Octet	3rd Octet	4th Octet
Dotted Decimal	192	168	10	100
Binary	1100 0000	1010 1000	0000 1010	0110 0100

A number in an octet can range from 0 to 255. Therefore, the full IPv4 address space goes from 0.0.0.0 to 255.255.255.255. The IPv4 address has two parts, the network part and the host part. A subnet mask is used to identify these parts.

Network Part

The network part of the IPv4 address is on the left-hand side of the IP address. It specifies the particular network to where the IPv4 address belongs. The network portion of the address also identifies the IP address class of the IPv4 address.

For example, we have the IPv4 address 192.168.10.100 and a /24 subnet mask. /24 simply means that the first 24 bits, starting from the left side, is the network portion of the IPv4 address. The 8 remaining bits of the 32 bits will be the host portion.

Format	1st Octet	2nd Octet	3rd Octet	4th Octet
Dotted Decimal	192	168	10	100
Binary	1100 0000	1010 1000	0000 1010	0110 0100

Host Part

The host portion of the IPv4 address uniquely identifies the device or the interface on your network. Hosts that have the same network portion can communicate with one another directly, without the need for the traffic to be routed.

IPv4 Address Allocation

The Internet Protocol address can be allocated to hosts or interfaces either manually or dynamically.

- **Static** – static IP address is set manually on the device. It is best practice to set static IP addresses on network devices, such as routers and switches, and on servers as well.
- **Dynamic** – dynamic IP address can be automatically allocated to a device via Dynamic Host Configuration Protocol (DHCP). Dynamic IP addresses are best to be used on end devices, such as PCs.

Types of IPv4 Addresses

We have two types of IP addresses, namely public IP addresses and private IP addresses.

- **Public IP address** – used to route Internet traffic. This is used on the Internet and is given out by Internet Service Providers (ISPs) to their customers.
- **Private IP address** – used in private networks for internal traffics within the LAN. Private addresses are not routable out the Internet.

What is Generic Routing Encapsulation (GRE)?

Computer NetworkInternetMCA

Generic Routing Encapsulation (GRE) is a routing protocol developed by Cisco Systems in 1994 that allows a wide range of network-layer protocols to be contained inside virtual point-to-point or point-tomultipoint links over an Internet Protocol network. Protocol encapsulation, not GRE specifically, breaks the layering sequence, according to the OSI principles of protocol layering.

GRE can be thought of as a barrier between two protocol stacks, one of which serves as a carrier for the other. IP protocol type 47 is used for GRE packets enclosed within IP. It is a tunnelling protocol and is defined by RFC 2784. GRE provides both stateless and private connection.

GRE establishes a secure, stateless connection. The protocol establishes a connection that is comparable to that of a Virtual Private Network (VPN). Over an IP network, it can carry any OSI layer three protocol.

GRE establishes a tunnel between two routers over the Internet to allow communication between two hosts of different private networks. With the help of Virtual Tunnel Interface, the GRE connection endpoints can be terminated.

GRE Tunnelling

GRE creates a private way for packets to travel through an otherwise public network by encapsulating or tunnelling the packets. Tunnel endpoints that encapsulate or de-encapsulate the traffic are used in GRE tunnelling.

Encapsulating packets within other packets is known as **tunnelling**. GRE tunnels are often set up between two routers, with each router acting as the tunnel's end. The routers are configured to send and receive GRE packets directly.

Within an outer IP packet, GRE encapsulates a payload, an inner packet that must be transferred to a target network. GRE tunnel endpoints route encapsulated packets via intervening IP networks to convey payloads across GRE tunnels. GRE tunnels are used to connect different subnetworks.

Advantages of GRE

Some of the advantages of using GRE are listed below −

- IPv4 broadcast and multicast traffic can be encapsulated using the GRE protocol.
- IPv6 is also supported.
- It's a straightforward and adaptable protocol.
- Numerous protocols are encapsulated in a single GRE tunnel.
- It can connect multiple discontinuous sub-networks and is easy to debug.

Disadvantages of GRE

The drawbacks of using GRE are as follows −

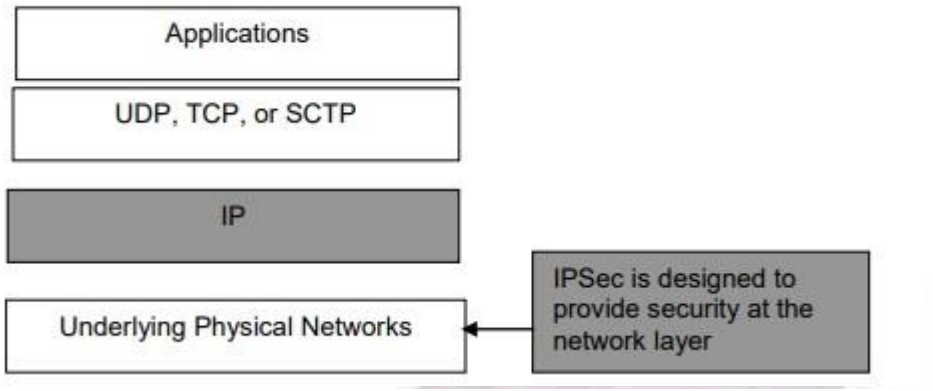
- It does not provide a data encryption facility, and it needs to be integrated with other security protocols to provide network security.
- Defining GRE tunnels is a laborious process, hence it is less scalable.

There are quite a few protocols available for data transfer via a secure network. Protocols were created for a reason, and they're getting better all the time. Whether it's greater security or ease of use and configuration, we always have various aspects to consider when picking the optimal protocol for a network.

What is IPsec in computer networks?

Computer NetworkInternetMCA

IP Security (IPSec) is a collection of protocols which is designed by Internet Engineering Task Force (IETF) to provide security for a packet at the network level. It helps to create confidential and authenticated and packets for the IP layer as shown in below diagram −



IPSec protocol aim is to provide security services for IP packets like encrypting sensitive data/packets, authentication, and protection against replay and data confidentiality. It can be configured to operate in two different modes −

- Tunnel Mode
- Transport mode.

The original packet is generated as follows −

IP Header	UDP Header	Data

Let us discuss each mode in detail.

Tunnel mode

IPSec tunnel mode is the default mode. IPSec Tunnel mode is most widely used to create site-to-site IPSec VPN.

Let see the packet format of IPSec tunnel mode with ESP header −

|□-----Original Packet----------□|

NewIP Header	ESP Header	IP Header	TCP/UDP Header	Data	ESP Trailer	EXP Auth.trailer

|□-------Encrypted--------------------------□|

|----------------------Authenticated----------------------□|

From the above format we can conclude the following −

- The encrypted part of the packet contains the following −

IP Header	UDP Header	Data	ESP Trailer

- The authenticated part of the packet contains the following −

ESP Header	IP Header	UDP Header	Data	ESP Trailer

Transport Mode

IPSec Transport mode is used for end-to-end communications. In this only, the Data Payload of the IP datagram is secured by IPSec.

IP Header	ESP Header	TCP/UDP Header	Data	ESP Trailer	EXP Auth.trailer

|□-------Encrypted-------------□|

|----------------------Authenticated---------□|

From the above format we conclude the following −

- The encrypted part of the packet contains the following −

UDP Header	Data	ESP Trailer

- The authenticated part of the packet contains the follow

What is Tunnelling in Computer Networks?

Computer NetworkInternetMCA

Tunnelling is a protocol for transferring data securely from one network to another. Using a method known as *encapsulation*, Tunnelling allows private network communications to be sent across a public network, such as the Internet. Encapsulation enables data packets to appear general to a public network when they are private data packets, allowing them to pass unnoticed.

Note *− Port forwarding is another name for Tunnelling.*

When data is tunnelled, it is split into smaller parts called *packets*, as it travels through the tunnel. The packets are encrypted via the tunnel, and another process known as *encapsulation* takes place. For transmission, private

network data and protocol details are encased in public network transmission units. The units have the appearance of public data, allowing them to be sent via the Internet. Encapsulation enables packets to reach their intended destination. De-capsulation and decryption take place at the final destination.

Tunnelling is possible thanks to a variety of procedures, including −

- Point-to-Point Tunnelling Protocol (PPTP)

Tunnelling is possible thanks to a variety of procedures, including −

- Point-to-Point Tunnelling Protocol (PPTP)
- Layer Two Tunnelling Protocol (L2TP)

PPTP (Point-to-Point Tunnelling Protocol)

PPTP protects confidential information even when transmitted via public networks. An Internet service provider can provide authorized users with access to a private network called a virtual private network. Because it was built in a tunnelled environment, this is a "virtual" private network.

Layer Two Tunnelling Protocol (L2TP)

This tunnelling protocol combines PPTP with Layer 2 Forwarding.

Tunnelling is a technique for communicating over a public network while going through a private network. This is especially beneficial in a corporate situation, and it also includes security measures like encryption.

The IP packet in this scenario does not have to deal with the WAN, and neither do the hosts A and B. IP, and WAN packets will be understood by the multiprotocol routers M1 and M2. As a result, the WAN can be compared to a large tunnel connecting multiprotocol routers M1 and M2, and the process is known as Tunnelling.

Tunnelling makes use of a layered protocol paradigm like the OSI or TCP/IP protocol suite. In other words, when data travels from host A to host B, it traverses all levels of the specified protocol (OSI, TCP/IP, and so on), and data conversion (encapsulation) to suit different interfaces of the particular layer is referred to as Tunnelling.

Applications of Tunnelling

Several protocols use a public network, such as the Internet, to transfer private network data by establishing a VPN (Virtual Private Network), making data transmissions more secure, especially when using unencrypted data.

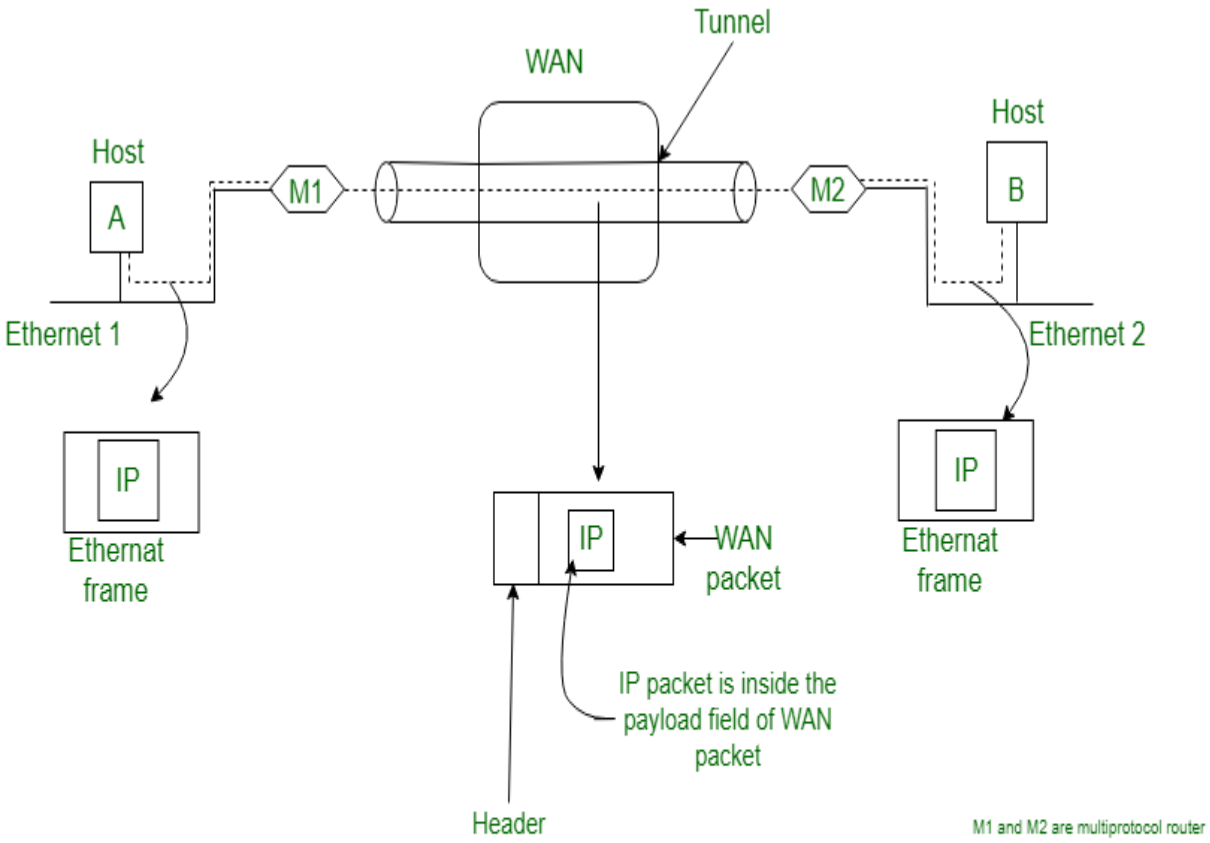
IPsec (GPRS tunnelling protocol), SSH (Secure Socket Tunnelling Protocol), PPTP (Point-to-Point Tunnelling Protocol), and others are standard protocols, each designed for a specific tunnelling task or purpose.

Some examples of how tunnelling protocols are used are as follows −

- Although a foreign protocol is not supported to run over a specific network, a tunnelling protocol can run IP-v6 over IP-v4.
- When the corporate network does not include the user's physical network address, it is also used to deliver unfeasible fundamental network services, such as a corporate network address) to a remote user.
- Tunnelling allows users to get around a firewall by using an unblocked protocol such as HTTP and the technique of "wrapping" to piggyback/ slip past the firewall rules.
- Another option is to use the HTTP CONNECT tunnel's command/ technique. The HTTP proxy establishes a TCP connection to a specific server when the client issues an HTTP CONNECT command to the proxy server. This security flaw is exploited to use the HTTP proxy to transmit data between the client connection and the designated port. Usually, HTTP proxies enable connections like 443 but deny other proxy servers' access to the CONNECT command.

tunneling

A technique of internetworking called **Tunneling** is used when source and destination networks of same type are to be connected through a network of different type. For example, let us consider an Ethernet to be connected to another Ethernet through a WAN as:



Tunneling

Computer Network AAA (Authentication, Authorization and Accounting)

Although the administrator can use a console to access a router or other device, doing so is quite difficult if he is sitting distant from where the equipment is located. Therefore, he will eventually need to use remote access to that gadget.

However, since remote devices can be accessed using an IP address, we must implement authentication as a security mechanism because it is possible for an unauthorized user to gain access using the same IP address. Additionally,

the packets transmitted between the devices should be encrypted to prevent unauthorized access to that sensitive data. Therefore, a framework known as **AAA** is used to *add that extra layer of security.*

AAA (Authentication, Authorization and Accounting)

A standard-based framework called AAA is used to manage who is allowed to access network resources, what they are allowed to do, and record the actions taken while doing so (via authentication and Authorization). Or we can say, the AAA is a structural framework used to access computer resources, enforce policies, conduct audits, provide vital data for service billing, and perform other network administration and security tasks.

- The primary purpose of this operation is to grant specific, Authorized user's access to network and software application resources.
- The AAA idea is widely used in regard to the network protocol **RADIUS**.
- A technique for monitoring and controlling user access to network resources on an IP-based network is authentication, Authorization, and accounting (AAA). Frequently, AAA is configured as a dedicated server.
- Authorization is the process of granting or denying specific user's access to a computer network and its resources. Users can be given several Authorization levels, restricting their access to the network and its resources. Accounting is known for monitoring and documenting user activities on a computer network.

Authentication -

It is a method of determining if a user who wants to access network resources is legitimate or not, and it is done by requesting certain credentials, such as a username and password. Authentication can be enabled on **console ports, AUX ports, or vty lines, among other places.**

If someone wants to enter the network, we, as network administrators, can manage how a user is authenticated. These techniques include utilising the router's internal database or submitting authentication requests to a remote server, such as the ACS server. A default or custom authentication method list is used to specify the authentication method to be utilised.

Authorization -

After the user has obtained access to the network resources through authentication, it offers the ability to enforce policies on those resources. When authentication is successful, Authorization can be used to identify which resources and processes the user is permitted to access.

For instance, if a junior network engineer wants access to the device but shouldn't have access to all the resources, then administrator can construct a view that would only allow him to perform certain commands. The administrator can designate how a user is Authorized to access network resources using the Authorization method list, such as through a local database or an ACS server.

Accounting -

It offers tracking and recording of user actions as they use network resources. Even the length of the user's network access is tracked. The administrator can construct an accounting method list to designate what should be accounted for and who should receive the accounting records.

Implementation of AAA

Utilizing the device's local database or an external ACS server are viable options for implementing AAA.

1. ACS Server - This approach is frequently employed. For AAA, an external ACS server?which could be an ACS device or software running on VMware?is utilised, and both the router and the ACS need to be configured. A user is created as part of the configuration, along with a unique customised method list for authentication, Authorization, and accounting.

According to the credentials given by the user, the ACS server decides whether to provide the user access to the network resource or not after receiving authentication requests from the client or Network Access Server (NAS).

Note: The administrator must include utilising the device's local database as a backup in the method list for implementing AAA in case the ACS server cannot authenticate

2. Local Database - We must first create users for authentication and grant them privilege levels for Authorization if we want to deploy AAA using the local running configuration of the router or switch.

Advantages of AAA framework:

The AAA framework enhances the scalability of a network. Scalability is the ability of a system to handle an increasing amount of work by adding resources to the system. Some of the main advantages of the AAA framework are listed below:

- It enables the network to be more controllable and adaptable.
- It helps the network to Standardize its protocol usage.
- Each user is given their own set of credentials using RADIUS.
- There will be a single point of contact for the users and system authentication for IT administrators.

Disadvantages of AAA framework:

Some of the main disadvantages of the AAA framework are listed below:

- RADIUS server configuration, particularly the initial configuration, can be challenging and time-consuming.
- It can be challenging to select the best RADIUS server software and deployment strategy for your company.
- On-site hardware upkeep can be

What is IGMP(Internet Group Management Protocol)?

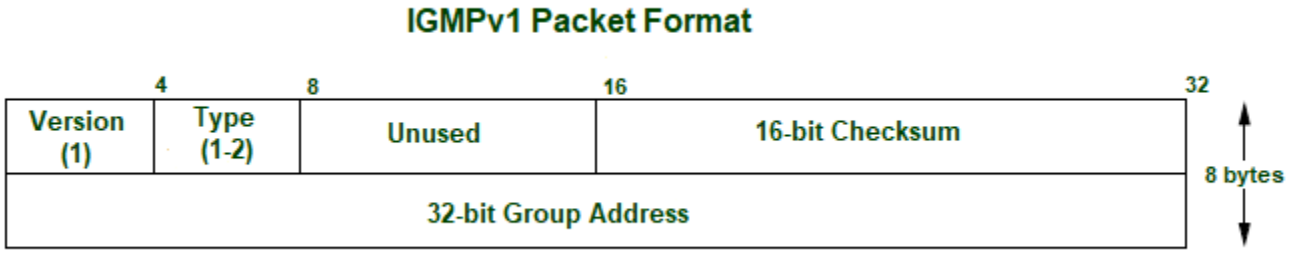
IGMP is acronym for **Internet Group Management Protocol**. IGMP is a communication protocol used by hosts and adjacent routers for multicasting communication with IP networks and uses the resources efficiently to transmit the message/data packets. Multicast communication can have single or multiple senders and receivers and thus,

IGMP can be used in streaming videos, gaming or web conferencing tools. This protocol is used on IPv4 networks and for using this on IPv6, multicasting is managed by Multicast Listener Discovery (MLD). Like other network protocols, IGMP is used on network layer. MLDv1 is almost same in functioning as IGMPv2 and MLDv2 is almost similar to IGMPv3. The communication protocol, IGMPv1 was developed in 1989 at Stanford University. IGMPv1 was updated to IGMPv2 in year 1997 and again updated to IGMPv3 in year 2002.

Applications:

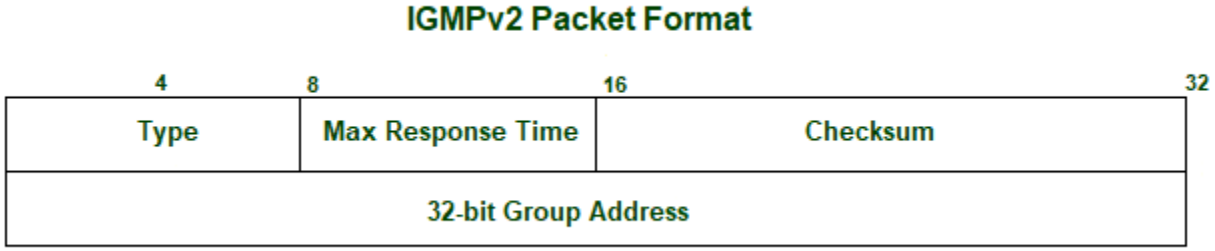
- **Streaming –** Multicast routing protocol are used for audio and video streaming over the network i.e., either one-to-many or many-to-many.
- **Gaming –** Internet group management protocol is often used in simulation games which has multiple users over the network such as online games.
- **Web Conferencing tools –** Video conferencing is a new method to meet people from your own convenience and IGMP connects to the users for conferencing and transfers the message/data packets efficiently.

Types: There are 3 versions of IGMP. These versions are backward compatible. Following are the versions of IGMP: **1. IGMPv1 :** The version of IGMP communication protocol allows all the supporting hosts to join the multicast groups using membership request and include some basic features. But, host cannot leave the group on their own and have to wait for a timeout to leave the group. The message packet format in IGMPv1:



- **Version –** Set to 1.
- **Type –** 1 for Host Membership Query and Host Membership Report.
- **Unused –** 8-bits of zero which are of no use.
- **Checksum –** It is the one's complement of the sum of IGMP messages.
- **Group Address –** The group address field is zero when sent and ignored when received in membership query message. In a membership report message, the group address field takes the IP host group address of the group being reported.

2. IGMPv2 : IGMPv2 is the revised version of IGMPv1 communication protocol. It has added functionality of leaving the multicast group using group membership. The message packet format in IGMPv2:



Type:

0x11 for Membership Query

0x12 for IGMPv1 Membership Report

0x16 for IGMPv2 Membership Report

0x22 for IGMPv3 Membership Report

0x17 for Leave Group

- **Max Response Time –** This field is ignored for message types other than membership query. For membership query type, it is the maximum time allowed before sending a response report. The value is in units of 0.1 seconds.
- **Checksum –** It is the one's complement of the sum of IGMP message.
- **Group Address –** It is set as 0 when sending a general query. Otherwise, multicast address for group-specific or source-specific queries.

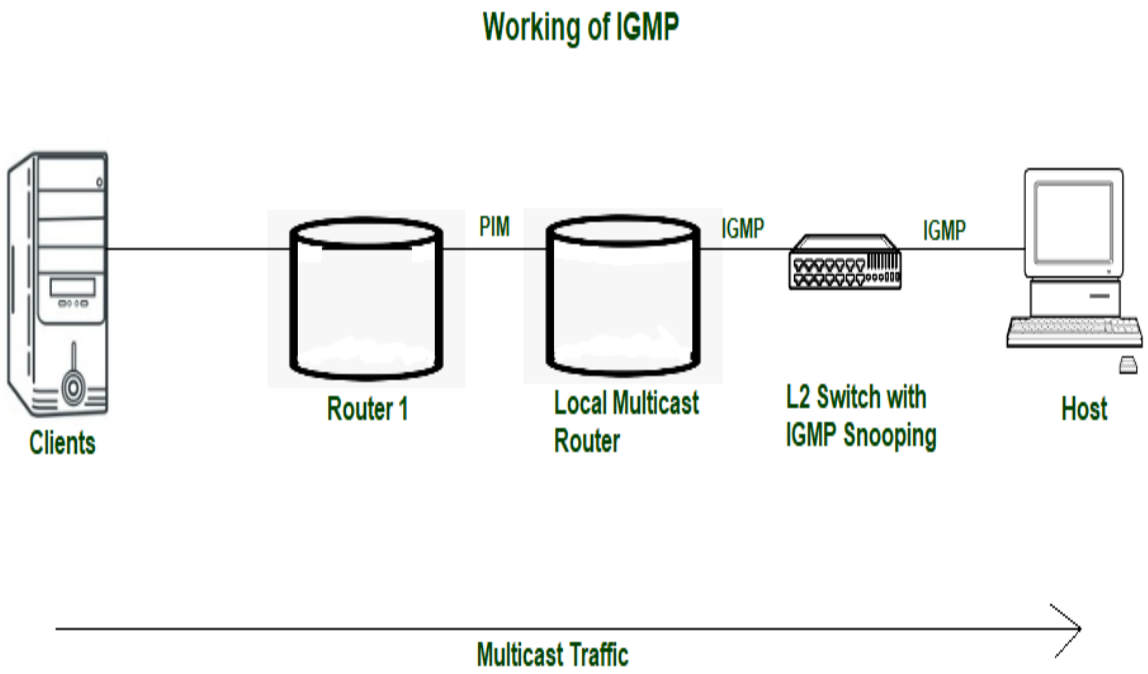
3. IGMPv3 : IGMPv2 was revised to IGMPv3 and added source-specific multicast and membership report aggregation. These reports are sent to 224.0.0.22. The message packet format in IGMPv3:

IGMPv3 Packet Format

Bit Offset	0-3	4	5-7	8-15	16-31
0	Type = 0x11			Max Response Code	Checksum
32	Group Address				
64	Resv	S	QRV	QQIC	Number of Sources (N)
96	Source Address[1]				
128	Source Address[2]				
	Source Address[N]				

- **Max Response Time –** This field is ignored for message types other than membership query. For membership query type, it is the maximum time allowed before sending a response report. The value is in units of 0.1 seconds.
- **Checksum –** It is the one's complement of the one's complement of the sum of IGMP message.
- **Group Address –** It is set as 0 when sending a general query. Otherwise, multicast address for group-specific or source-specific queries.
- **Resv –** It is set zero of sent and ignored when received.
- **S flag –** It represents Suppress Router-side Processing flag. When the flag is set, it indicates to suppress the timer updates that multicast routers perform upon receiving any query.
- **QRV –** It represents Querier's Robustness Variable. Routers keeps on retrieving the QRV value from the most recently received query as their own value until the most recently received QRV is zero.
- **QQIC –** It represents Querier's Query Interval Code.
- **Number of sources –** It represents the number of source addresses present in the query. For general query or group-specific query, this field is zero and for group-and-source-specific query, this field is non-zero.
- **Source Address[i] –** It represents the IP unicast address for N fields.

Working: IGMP works on devices that are capable of handling multicast groups and dynamic multicasting. These devices allows the host to join or leave the membership in the multicast group. These devices also allows to add and remove clients from the group. This communication protocol is operated between host and local multicast router. When a multicast group is created, the multicast group address is in range of class D (224-239) IP addresses and is forwarded as destination IP address in the packet.



L2 or Level-2 devices such as switches are used in between host and multicast router for IGMP snooping. IGMP snooping is a process to listen to the IGMP network traffic in controlled manner. Switch receives the message from host and forwards the membership report to the local multicast router. The multicast traffic is further forwarded to remote routers from local multicast routers using PIM (Protocol Independent Multicast) so that clients can receive the message/data packets. Clients wishing to join the network sends join message in the query and switch intercepts the message and adds the ports of clients to its multicast routing table.

Advantages:

- IGMP communication protocol efficiently transmits the multicast data to the receivers and so, no junk packets are transmitted to the host which shows optimized performance.
- Bandwidth is consumed totally as all the shared links are connected.
- Hosts can leave a multicast group and join another.

Disadvantages:

- It does not provide good efficiency in filtering and security.
- Due to lack of TCP, network congestion can occur.
- IGMP is vulnerable to some attacks such as DOS attack (Denial-Of-Service).