**VLAN** is a custom network which is created from one or more local area networks. It enables a group of devices available in multiple networks to be combined into one logical network. The result becomes a virtual LAN that is administered like a physical LAN. The full form of VLAN is defined as Virtual Local Area Network.

The below topology depicts a network having all hosts inside the same virtual LAN:

Without VLANs, a broadcast sent from a host can easily reach all network devices. Each and every device will process broadcast received frames. It can increase the CPU overhead on each device and reduce the overall network security.

In case if you place interfaces on both switches into separate VLAN, a broadcast from host A can reach only devices available inside the same VLAN. Hosts of VLANs will not even be aware that the communication took place. This is shown in the below picture:

**ARP** Most of the computer programs/applications use **logical address (IP address)** to send/receive messages, however, the actual communication happens over the **physical address (MAC address)** i.e from layer 2 of the OSI model. So our mission is to get the destination MAC address which helps in communicating with other devices. This is where ARP comes into the picture, its functionality is to translate IP address to physical addresses.

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

When a new computer joins a LAN, it is assigned a unique IP address to use for identification and communication. When an incoming packet destined for a host machine on a particular LAN arrives at a gateway, the gateway asks the ARP program to find a MAC address that matches the IP address

**Router VS Switch**

R-The main objective of router is to connect various networks simultaneously.

S-While the main objective of switch is to connect various devices simultaneously.

R-It works in network layer.

S-While it works in data link layer.

R-Router is used by LAN as well as MAN.

S-While switch is used by only LAN.

R-Through the router, data is sent in the form of packets.

S-While through switch data is sent in the form of  frame.

R-There is less collision taking place in the router.

S-While there is no collision taking place in full duplex switch.

R-Router is compatible with NAT.

S-While it is not compatible with NAT.

R-The types of routing are: Adaptive and Non-adaptive routing.

S-The types of switching are: Circuit, Packet,and Message Switching.

**Broadcast and Multicast?**

Multicast is a one-to-many streaming over IP method similar to traditional broadcast. Multicast uses UDP (User Datagram Protocol) for “broadcasting” a stream over a closed IP network such as a LAN (Local Area Network) or an IP Service provider’s own network. Multicast streaming of live TV is commonly referred to as IPTV, whereas OTT is unicast over the internet.

In a multicast IP network, the content sender only needs to deliver a single stream, and the nodes along the network will replicate that stream across the entire network, as in a relay race. Using multicast for distributing video to hundreds or thousands of users is the preferred video delivery option for companies and organizations as it avoids flooding the network with duplicate streams.

Broadcasting sends out a signal to everyone all at once from a single source, and whoever has a receiver within range on a network can view the content. Predominantly used by television stations and cable tv channels for live content distribution, the biggest advantage of the broadcast approach is that it can reach audiences on a massive scale. Think one-to-all.

A single video source is broadcast over a specific antenna frequency direct to home or satellite and fiber links to satellite and cable TV services. Digital TV antennae, satellite dishes, and set-top boxes receive and decode the broadcast signal for viewing on a television set. The broadcast approach, however, is not suitable for viewing on mobile devices.

**CSMA/CD**

CSMA/CD (Carrier Sense Multiple Access/ Collision Detection) is a media access control method that was widely used in Early Ethernet technology/LANs When there used to be shared   
Bus Topology

Consider a scenario where there are ‘n’ stations on a link and all are waiting to transfer data through that channel. In this case, all ‘n’ stations would want to access the link/channel to transfer their own data. Problem arises when more than one station transmits the data at the moment. In this case, there will be collisions in the data from different stations.

CSMA/CD is one such technique where different stations that follow this protocol agree on some terms and collision detection measures for effective transmission. **This protocol decides which station will transmit when so that data reaches the destination without corruption.**

**How CSMA/CD works?**

* **Step 1:** Check if the sender is ready for transmitting data packets.
* **Step 2:** Check if the transmission link is idle?   
  Sender has to keep on checking if the transmission link/medium is idle. For this, it continuously senses transmissions from other nodes. Sender sends dummy data on the link. If it does not receive any collision signal, this means the link is idle at the moment. If it senses that the carrier is free and there are no collisions, it sends the data. Otherwise, it refrains from sending data.
* **Step 3:** Transmit the data & check for collisions.   
  Sender transmits its data on the link. CSMA/CD does not use an ‘acknowledgment’ system. It checks for successful and unsuccessful transmissions through collision signals. During transmission, if a collision signal is received by the node, transmission is stopped. The station then transmits a jam signal onto the link and waits for random time intervals before it resends the frame. After some random time, it again attempts to transfer the data and repeats the above process.
* **Step 4:** If no collision was detected in propagation, the sender completes its frame transmission and resets the counters.

**The Data link layer generally provides** or offers three types of services as given below :

* **1.Unacknowledged Connectionless Service -**Unacknowledged connectionless service simply provides datagram styles delivery without any error, issue, or flow control. In this service, source machine generally transmits independent frames to destination machine without having destination machine to acknowledge these frames.

This service is called as connectionless service because there is no connection established among sending or source machine and destination or receiving machine before data transfer or release after data transfer.

In Data Link Layer, if anyhow frame is lost due to noise, there will be no attempt made just to detect or determine loss or recovery from it. This simply means that there will be no error or flow control. An example can be Ethernet.

* **2.Acknowledged Connectionless Service -**This service simply provides acknowledged connectionless service i.e. packet delivery is simply acknowledged, with help of stop and wait for protocol.

In this service, each frame that is transmitted by Data Link Layer is simply acknowledged individually and then sender usually knows whether or not these transmitted data frames received safely. There is no logical connection established and each frame that is transmitted is acknowledged individually.

This mode simply provides means by which user of data link can just send or transfer data and request return of data at the same time. It also uses particular time period that if it has passed frame without getting acknowledgment, then it will resend data frame on time period.

This service is more reliable than unacknowledged connectionless service. This service is generally useful over several unreliable channels, like wireless systems, Wi-Fi services, etc.

* **3.Acknowledged Connection-Oriented Service -**In this type of service, connection is established first among sender and receiver or source and destination before data is transferred.

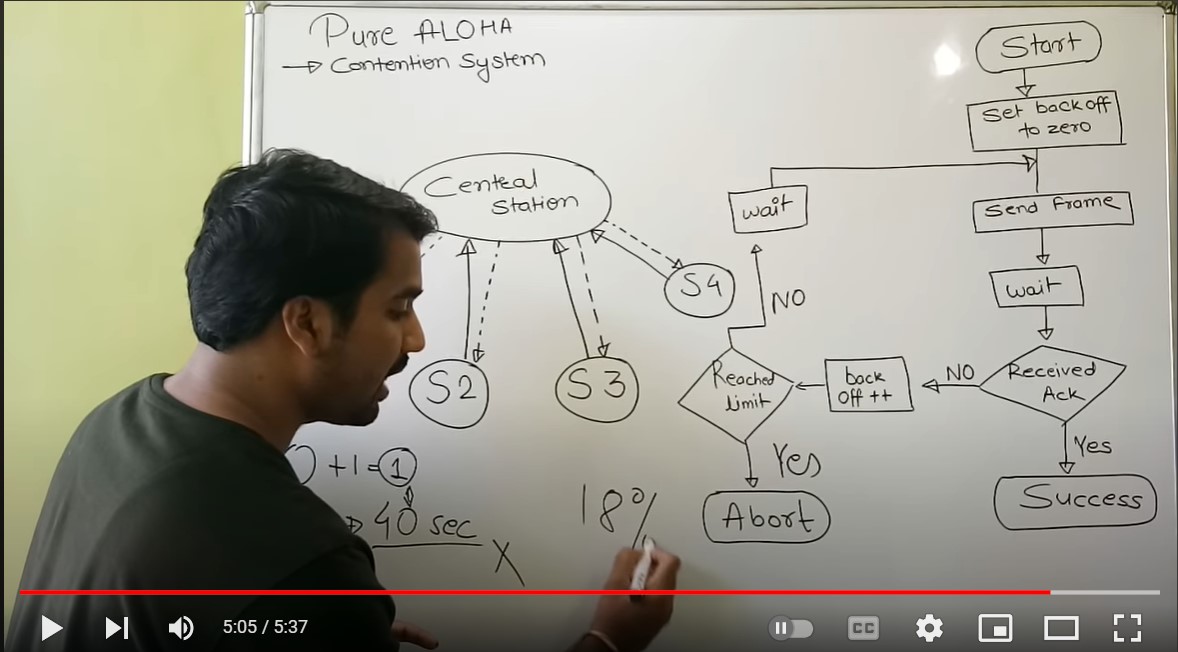
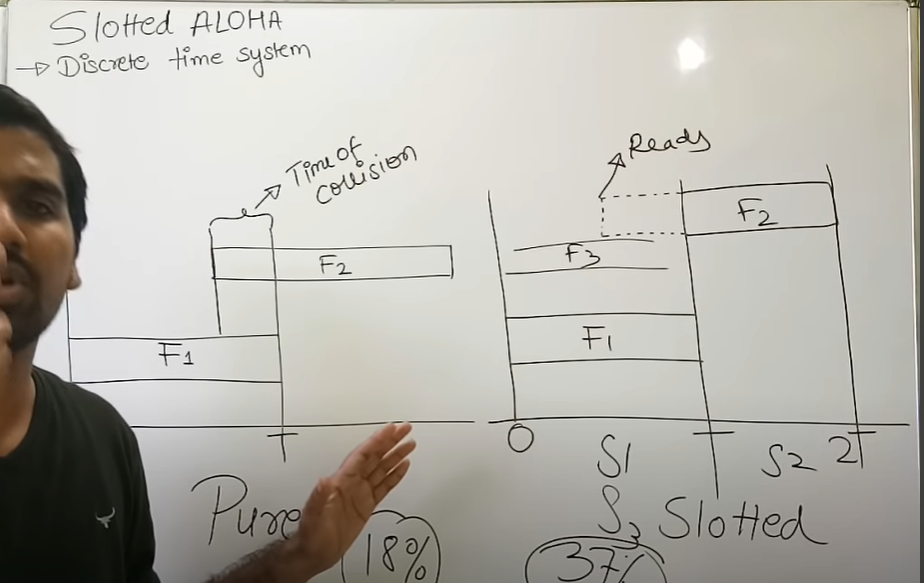
Then data is transferred or transmitted along with this established connection. In this service, each of frames that are transmitted is provided individual numbers first, so as to confirm and guarantee that each of frames is received only once that too in an appropriate order and sequence.

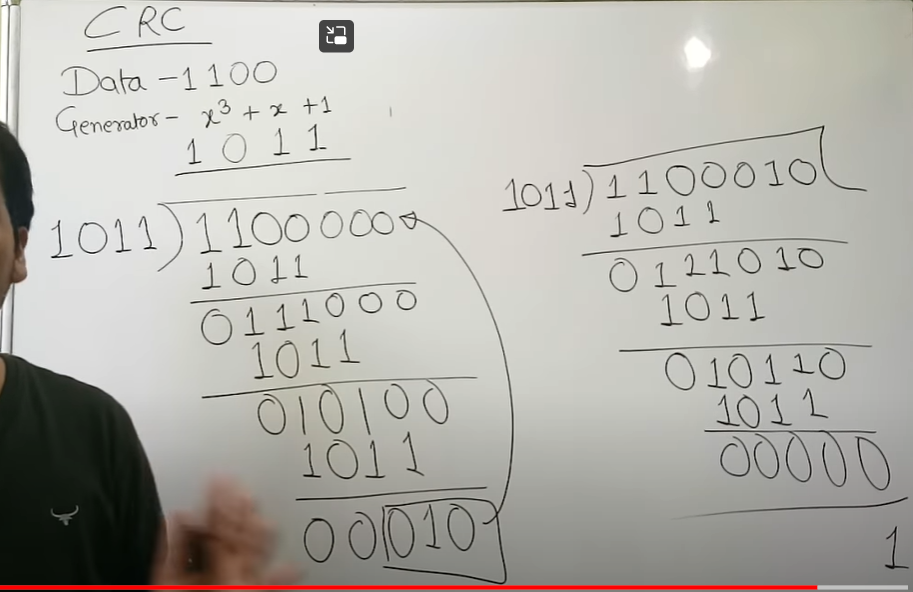
**SLOTTED ALOHA VS PURE ALOHA**

Pure aloha is used when data is available for sending over a channel at stations. In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost.

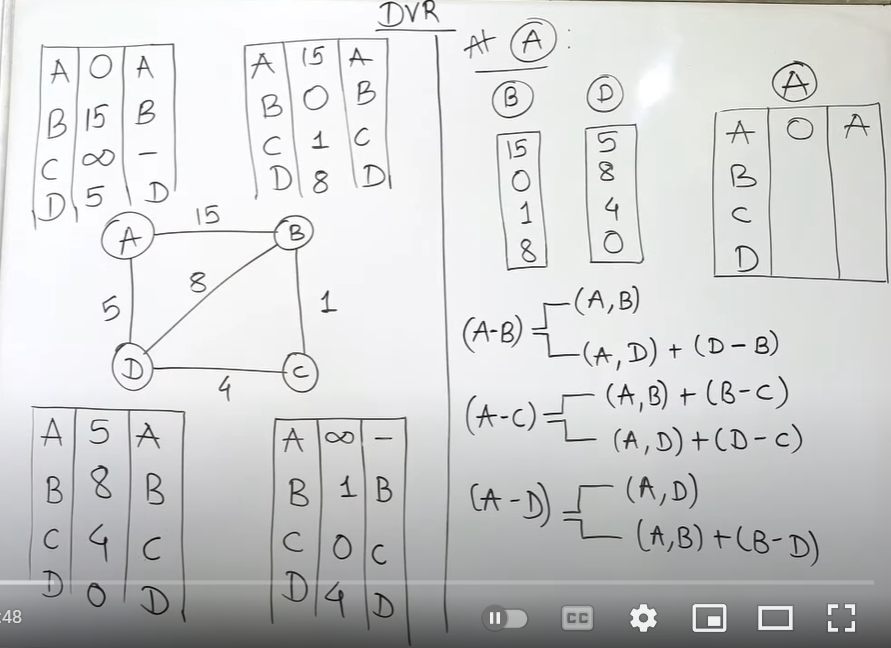
When a station transmits the data frame to a channel without checking whether the channel is free or not, there will be a possibility of the collision of data frames. Station expects the acknowledgement from the receiver, and if the acknowledgement of the frame is received at the specified time, then it will be OK; otherwise, the station assumes that the frame is destroyed. Then station waits for a random amount of time, and after that, it retransmits the frame until all the data are successfully transmitted to the receiver.

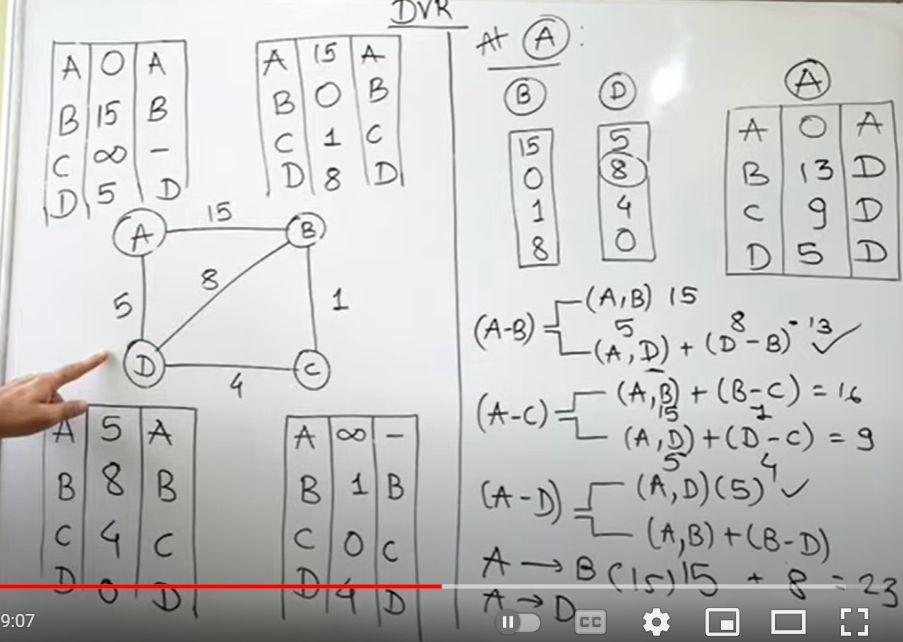
There is a high possibility of frame hitting in pure aloha, so slotted aloha is designed to overcome it. Unlike pure aloha, slotted aloha does not allow the transmission of data whenever the station wants to send it.In slotted Aloha, the shared channel is divided into a fixed time interval called slots. So that, if a station wants to send a frame to a shared channel, the frame can only be sent at the beginning of the slot, and only one frame is allowed to be sent to each slot. If the station is failed to send the data, it has to wait until the next slot.

****

****

**DVR NUMERICAL**

****

****

**Routing Information Protocol** (RIP) is a dynamic routing protocol that uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance-vector routing protocol that has an AD value of 120 and works on the Network layer of the OSI model. RIP uses port number 520.

#### ****Hop Count****

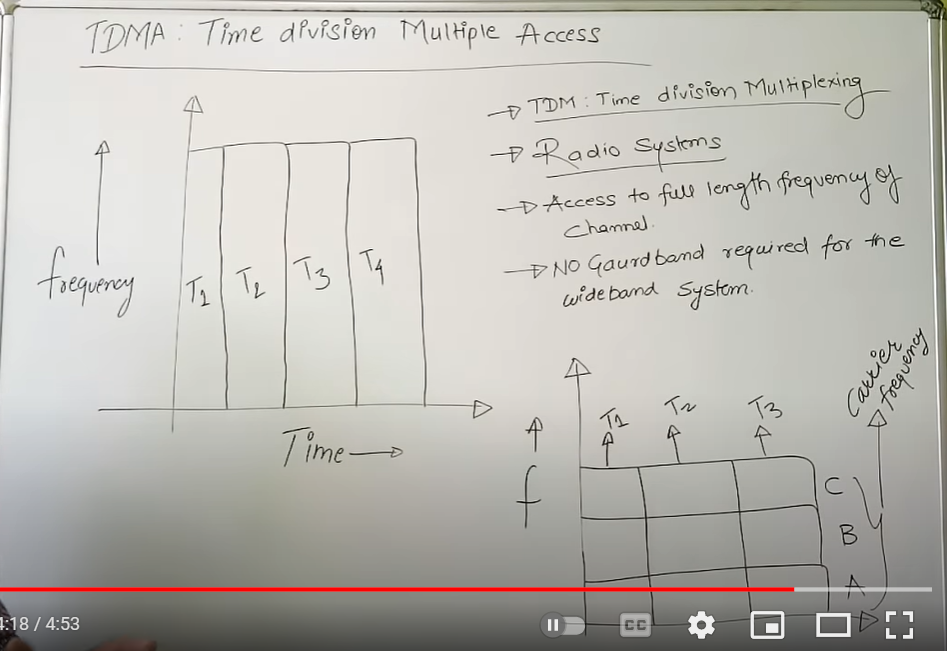
Hop count is the number of routers occurring in between the source and destination network. The path with the lowest hop count is considered as the best route to reach a network and therefore placed in the routing table. RIP prevents routing loops by limiting the number of hops allowed in a path from source and destination. The maximum hop count allowed for RIP is 15 and a hop count of 16 is considered as network unreachable.

### ****Features of RIP****

1. Updates of the network are exchanged periodically.   
2. Updates (routing information) are always broadcast.   
3. Full routing tables are sent in updates.   
4. Routers always trust routing information received from neighbor routers. This is also known as *Routing on*rumors.

* **OSPF** - Open Shortest Path First (OSPF) is a link-state routing protocol that is used to find the best path between the source and the destination router using its own Shortest Path First. OSPF is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e, the protocol which aims at moving the packet within a large autonomous system or routing domain. It is a network layer protocol which works on protocol number 89 and uses AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router(DR)/Backup Designated Router (BDR).
* **BGP** - Border Gateway Protocol (BGP) is used to Exchange routing information for the internet and is the protocol used between ISP which are different ASes. The protocol can connect together any internetwork of autonomous system using an arbitrary topology. The only requirement is that each AS have at least one router that is able to run BGP and that is router connect to at least one other AS BGP router. BGP’s main function is to exchange network reachability information with other BGP systems. Border Gateway Protocol constructs an autonomous systems’ graph based on the information exchanged between BGP routers.

**TDMA** Time Division Multiple Access (TDMA) is a digital cellular telephone communication technology.

****

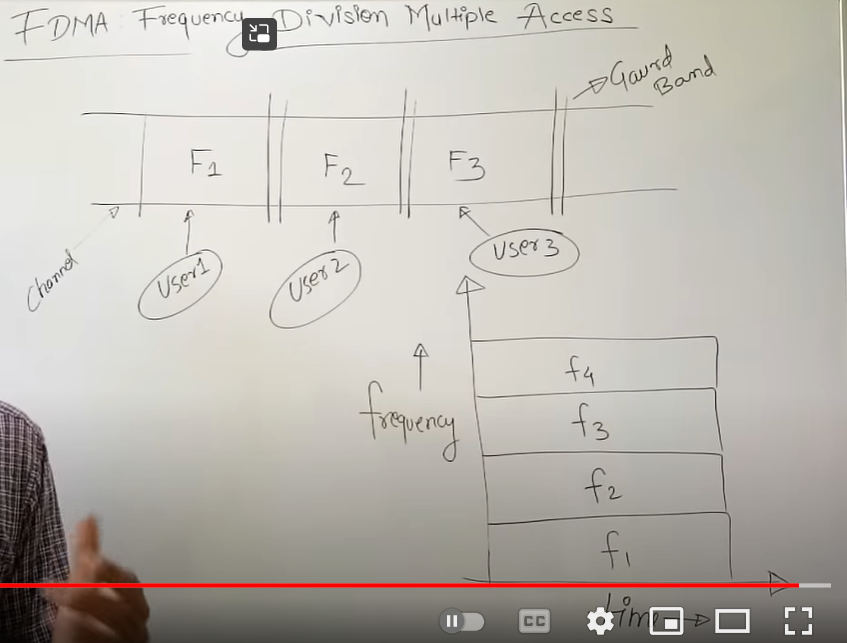
It facilitates many users to share the same frequency without interference. Its technology divides a signal into different time slots, and increases the data carrying capacity.

* No guard band required for the wideband system.
* No narrowband filter required for the wideband system.

**FDMA**

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.

* 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)

****

**UNIT-3**

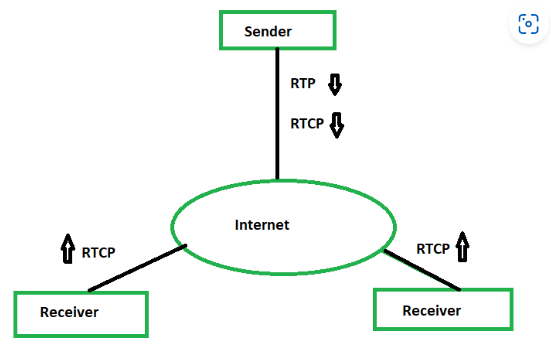
**RTCP**

**Rtp (real time transport protocol) which allows only that type messages which carries data from source to destination. But in some cases we need other type of messages in the session.**

**The messages that can control transmission quality of data as well as allow the recipient to send feedback to the source. The protocol designed for this purpose is RTCP.**

**RTCP stands for real time transport control protocol.**

**Use udp and tcp protocol and works at network layer.**

****

**Rtcp has 5 types of messages:-**

**1)Sender report – It is sent after an fixed interval by an active sender in a conference to report transmission. The report sent by sender contains detail of absolute time stamp.**

**2)Reciever report- used to inform the sender and other receiver about the quality of service.**

**3)sender descripotion msg (sdm)-source sends a sdm after a fixes interval to give som extra info about itself.**

**4)Bye msg – to shut down a stream , a source sends a type of message which is known as bye msg ,used by the source to announce for leaving the conference .**

**5)application spefici mesggae (ASM)-it can be used to extend the type of application.**

**RTP(Real time transport protocol)**

**This is protocol is designed to handle real time traffic real (audio and video) of the internet is known as Real time transport protocol. Rtp must be used with udp .**

**It does not provide any delievery mechanism like multicating and port numbers.**

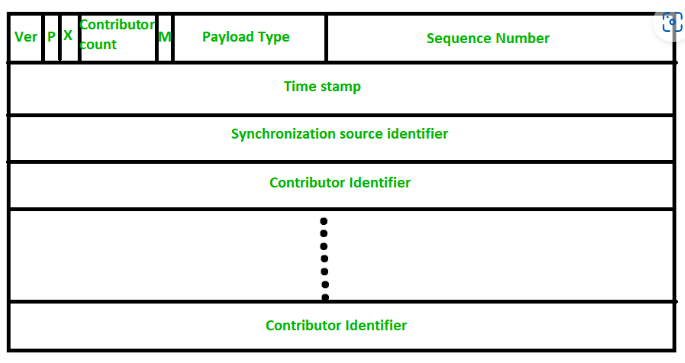
**RTP support different formats like mpeg and mjpeg**

**Mainly helps in :**

**1)VoIp (voiceOver Internet Protocol)**

**2)video conferencing.**

**RTP Header Format**

****

**SIP**

**Stands for session initiation protocol.**

**It is a lightweight protocol that –**

* 1. **Provides mechanism for establishing calls b/w a caller and a callee over an IP network.**
  2. **Provides mechanism for caller to determine the current IP address of the callee.**
  3. **Provides mechanism for call management like adding new people to call , call transfer , call holding.**
  4. **An interesting feature is that they can be included in web pages(just like email address are included in web Pages with mail to url.**

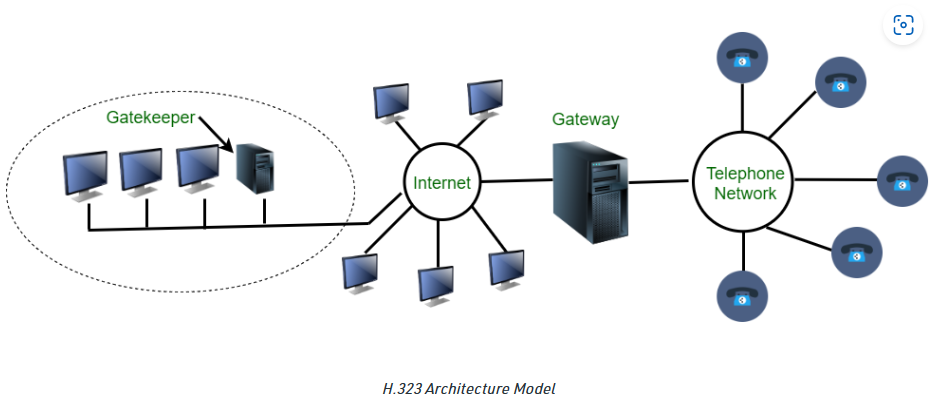
**H.323**

**It is a set of protocols for voice , video and data conferencing over packet – based network such as internet.**

**Designed to operate above transport layer of underlying network.**

**Can be used on top of any packet – based network transport like Ethernet to provide real time multimedia comm.**

**It uses internet protocol(IP) for inter-network conferencing.**

****

**Streaming**

**It is the technology of transmitting audio and video files in a continuos flow over a wired or wireless connection.**

**It refers to any media content(live/recorded) delievered to computer or any mobile device via internet.**

* **Working of streaming**

**Just like any other data sent over internet audio and video is broken down into data packets.Each packet contains a small piece of file , an audio or video player in the browser takes the data packet and interpret them as audio/video.**

**Streaming stored video**

**Streaming stored video involves , storing of prerecorded videos on servers.**

**User send request to server.**

**User may watch the video from start to end , pause it anytime cam forward or reverse skip or reverse it.**

**Types of video streaming**

**1)UDP streaming**

**2)http Streaming**

**3)Adaptive http streaming**

**1. UDP STREAMING:**  
**UDP servers send video chunks (Chunk: unit of information that contains either control information or user data) to clients, based on client’s consumption rate. It transmits chunks at a rate, that matches client’s video consumption rate by clocking out video chunks over UDP over steady state.**

**For example,**

**Video consumption rate = 2Mbps**

**Capacity of one UDP packet = 8000 bits**

**Therefore,**

**Transmission rate = 8000 bits/2 Mbps = 4000 msec**

**2. HTTP STREAMING:  
Video is stored in an HTTP server as a simple ordinary file with a unique URL. Client establishes TCP connection with server and issues a HTTP GET request for that URL. Server sends the video file along with an HTTP RESPONSE. Now the client buffer grabs the video and then displayed on user screen.**

**Youtube and Netflix uses HTTP streaming mechanism.**

**3. ADAPTIVE HTTP STREAMING:  
The major drawbacks of HTTP streaming, lead to development of new type of HTTP based streaming referred to as DASH (Dynamic Adaptive Streaming over HTTP). Videos are encoded into different bit rate versions, having different quality. The host makes a dynamic video request of few seconds in length from different bit versions. When bandwidth is high, high bit rate chunks are received hence high quality similarly, low quality video during low bandwidth.**

**So the client dynamically selects the video and audio chunks and synchronizes it locally in the play-out.**

**Uses:  
COMCAST uses DASH for streaming high quality video contents**.

**RTSP(Real time streaming protocol)**

**SNMP**

**If an organization has 1000 devices then to check all devices, one by one every day, are working properly or not is a hectic task. To ease these up, Simple Network Management Protocol (SNMP) is used.**

**Simple Network Management Protocol (SNMP) –   
SNMP is an application layer protocol that uses UDP port number 161/162.SNMP is used to monitor the network, detect network faults, and sometimes even used to configure remote devices.**

**SNMP components –   
There are 3 components of SNMP:**

1. **SNMP Manager –   
   It is a centralized system used to monitor network. It is also known as Network Management Station (NMS).**
2. **SNMP agent –   
   It is a software management software module installed on a managed device. Managed devices can be network devices like PC, routers, switches, servers, etc.**
3. **Management Information Base –   
   MIB consists of information on resources that are to be managed.**

**SNMP messages –   
Different variables are:**

1. **GetRequest –   
   SNMP manager sends this message to request data from the SNMP agent**
2. **GetNextRequest –   
   This message can be sent to discover what data is available on an SNMP agent.**
3. **GetBulkRequest –   
   This message is used to retrieve large data at once by the SNMP manager from the SNMP agent.**
4. **SetRequest –   
   It is used by the SNMP manager to set the value of an object instance on the SNMP agent.**
5. **Response –   
   It is a message sent from the agent upon a request from the manager.**
6. **Trap –   
   These are the message sent by the agent without being requested by the manager. It is sent when a fault has occurred.   
    Informatio request-**
7. **The agents can be configured to send trap message continuously until it receives an Inform message. It is the same as a trap but adds an acknowledgement that the trap doesn’t provide.**

**SNMP versions –   
There are 3 versions of SNMP:**

1. **SNMPv1 –   
   It uses community strings for authentication and uses UDP only.**
2. **SNMPv2c –   
   It uses community strings for authentication. It uses UDP but can be configured to use TCP.**
3. **SNMPv3 –   
   It uses Hash-based MAC with MD5 or SHA for authentication and DES-56 for privacy. This version uses TCP. Therefore, the conclusion is the higher the version of SNMP, the more secure it will be.**

SNMP Framework Components As we will explore in more detail later, the Internet Standard Management Framework is entirely information-oriented. It includes the following primary components o Structure of Management Information (SMI): To ensure interoperability of various devices, we want to have a consistent way of describing the characteristics of devices to be managed using SNMP. In computer science, a data description language (DDL) is the tool for this job. The Structure of Management Information (SMI) is a standard that defines the structure, syntax and characteristics of management information in SNMP. o Management Information Bases (MIBs): Each managed device contains a set of variables that is used to manage it. These variables represent information about the operation of the device that is sent to a network management station, and/or parameters sent to the managed device to control it. The management information base (MIB) is the full set of these variables that describe the management characteristics of a particular type of device.Each variable in a MIB is called a MIB object, and is defined using the SMI data description language. A device may have many objects, corresponding to the different hardware and software elements it contains. o Initially, a single document defined the MIB for SNMP, but this model was inflexible. To allow new MIB objects to be more easily defined, groups of related MIB objects are now defined in separate RFC standards called MIB modules. Over 100 such MIB modules have been defined so far. o Simple Network Management Protocol (SNMP): This is the actual SNMP protocol itself. It defines how information is exchanged between SNMP agents and network management stations. The SNMP protocol operations define the various SNMP messages and how they are created and used. SNMP transport mappings describe how SNMP can be used over various underlying internetworks, such as TCP/IP, IPX and others. o Security and Administration: To the three main architectural components above, the SNMP Framework adds a number of supporting elements. These provide enhancements to the operation of the SNMP protocol for security, and address issues related to SNMP implementation, version transition and other administrative issue