MULTIMEDIA NETWORKING

Network is collection of many computers or devices interconnected together to form a group to transfer an information from one device to another device.

Multimedia Networking Applications

Multimedia Networking Applications also referred to as continuous media applications, it has streaming video, IP telephony, Internet radio, teleconferencing, Interactive games, virtual world distance learning & so on.

Many multimedia applications are highly sensitive to end-to-end delay and delay variation but can tolerate occassional loss of data.

Two things are important for networking multimedia applications,

1. Timing considerations
2. Tolerance of data loss

Timing considerations → packets that incur a sender to receiver delay of more than a few hundred millisec are essentially useless.

Loss in data → It causes because of glitches (unwanted delays) in the audio / video playback and those losses can be partially or fully canceled.

Examples of Multimedia Applications

1. Streaming stored Audio / Video
2. Streaming live Audio / video
3. Real-time Interactive Audio / video

1. Streaming stored Audio & Video

Client request on demand compressed audio or video files are stored on servers. stored audio files might contain audio from a professors lecture, rock songs, symphonies, archives of famous radio broadcasts or achived historical recordings.

Stored video files must contain video of professor's lecture, full length movies, pre recorded television shows, documentaries, video archieves of historical events, cartoons or music video clips.

3 key features,

1. Stored media
2. Streaming
3. Continuous playout

1. Stored media

The multimedia content has been prerecorded and is stored at the server. As a result a user may pause, rewind, fast-forward or index through the multimedia content.

2. Streaming

The client will be playing out audio/video from one location in the file while it is receiving later parts of the file from the server ⇒ streaming.

It avoids having to download the entire file before beginning playout.

3. Continuous playout

Once playout of the multimedia content begins it should proceed according to the original timing of the recording.

Data must be received from the server in time for its playout at the client.

Stream Live Audio & Video

Similar to traditional broadcast radio and television except that the transmission takes place over the Internet.

These application allow a user to receive a live radio or TV transmission emitted from the corner of the world.

Streaming live audio / video is not stored so a client cannot fast-forward through the media.

3. Real time Interactive Audio & video

This class of appln. allows people to use audio / video to communicate with each other in real time. Eg: Internet phone.

Multimedia Internet

The Internet moves each datagram from Sender to receiver as quickly as possible but it does not make sure about end-to-end delay for an individual Packet.

TCP and UDP run over IP, these transport Protocols makes any delay guarantees to invoking applns,

Internet phone & Real time interactive video has less successful than streaming stored audio/ video.

How Internet Support Multimedia Application,

1. We need a Protocol that on the behalf of applications, reserves link bandwidth on the path from the Senders to their receivers.

2. we must modify scheduling policies in the router queues so that BW reservations can be honored. With new scheduling policies not all packets get equal treatment instead reserve packets get more equal.

3. In order to honor reservations, the applications must give the n/w. description of the traffic.

4. The n/w. must have a means of determining whether it has sufficient available BW to support any new reservation request.

Audio and Video Compression

In a computer n/w. before transmitting audio and video it can be digitized and compressed.

Need for digitization => Transmit all the information in the form of bits so all transmitted information must be represented as a sequence of bits.

Uncompressed audio and video consume a huge amount of storage and BW.

Removing the inherent redundancies in digitized audio and video signals can reduce the amount of data that needs to be stored data and transmitted by orders of magnitude.

Audio Compression in the Internet

A continuous varying analog audio signal is converted to a digital signal.

The audio signal is first sampled at some fixed rate. Eg:- 8000 samples / sec.

Each samples is rounded to one of a finite no. of values → Quantization. The no. of finite values are called quantization value & it is typically a power of two.

Each of Quantization values is represented by a fixed no. of bits. Each of the samples is converted to its bit representation. The bit representations of all the samples are concatenated together to form the digital rep. of the sig.

Eg:

If an analog audio s/g → Sampled at 8000 Samples / sec. & each Sample is quantized and represented by 8 bits, Resulting d/g. s/g = 8000 × 8 = 64000 bits/sec.

This d/g. s/g. can be decoded to get original s/g. The decoded analog s/g. is different from original audio s/g. So by increasing the sampling rate and the no. of quantization values, the decoded s/g. can approximate the original analog signal.

Encoding Technique

Pulse Code Modulation (PCM) is the basic encoding method used to transmit audio s/g.

The audio Compact Disk (CD) also uses PCM with a Sampling rate of 44,100 Samples per second with 16 bits per sample.

A bit rate of 1411 Mbps for stereo music exceeds most access rates and even 64Mbps for Speech exceeds the access rate for a dial-up modem user. Hence, PCM encoded speech and music are rarely used in the Internet.

To overcome the drawback of PCM, some compression techniques are used to reduce the bit rates of stream. Popular compression techniques for speech include,

1. GSM (13kbps)
2. G.729 (8 kbps)
3. G.723.3 (both 6.4 & 5.3 kbps)

A popular compression technique for CD-quality stereo music is MPEG1 layer 3, commonly known as MP3.

MP3 encoders typically compress at rate of 96kbps, 128 kbps & 160 kbps to produce very little sound degradation.

Video Compression in the Internet

A video is a sequence of images, typically displayed at a constant rate.

Eg: At 24 or 30 images / second.

An uncompressed digitally encoded image has an array of pixels with each pixel encoded into a no. of bits to represent luminance and color.

Two types of Redundancy in Video,

1. Spatial Redundancy
2. Temporal Redundancy

Spatial Redundancy → Redundancy within a given image

Temporal Redundancy → Reflects repetition from image to subsequent image.

The MPEG compression technique standard is most popular compression technique used for video.

The MPEG compression include,

MPEG1 for CD-Rom Quality Video (1.5 Mbps)

MPEG2 for high-quality DVD Video (3-6 Mbps)

MPEG4 for object oriental video compression

H.261 can also be used for MPEG compression.

It is widely popular to use in Internet.

Streamed stored Audio and Video

In audio/video streaming, clients request compressed audio/video files that reside on servers. These servers can be ordinary web servers or special streaming servers for audio/video streaming application.

Based on direct request, the server directs an audio/video files to the client by sending the file into a socket. Both TCP and UDP socket connections are used.

Audio/ video files before being sent into the n/w, it must be segmented and segments are typically encapsulated with special headers appropriate for audio/ video traffic. The RTP is used.

Once requested audio/video file starts to arrive, the clients begins to render the file within a few seconds. The RTSP is a protocol for providing user interactively.

Users often request audio/video streaming through a web client but audio/video playout is not integrated directly into today's web clients. So we need a separate helper appln. for playing out audio/video.

Helper appln. also called media players, are real n/w. real player and Microsoft windows media player.

Decompression

Audio/video is always compressed to save disk storage and network Bandwidth. A media player must decompress the audio/video on fly during playout.

Jitter Removal

Packet jitter is the variability of packet delay within the same packet stream. Audio and video must be played out with the same timing with which it was

recorded and a receiver will buffer the received packets for a short period of time to remove this jitter.

Error Correction

Due to unpredictable congestion in the Internet, a fraction of packets in the packet stream can be lost.

1. Reconstructing lost packets through the transmission of redundant packets.
2. The client explicitly request retransmission of lost packets.
3. Masking loss by interpolating the missing data from the received data.

Accessing Audio and Video through a web server

Two kinds of locations such as,

1. It resides on a webserver that delivers the audio/video to the client over HTTP.
2. It also resides on an audio/video streaming server exter that delivers the audio/video over non-HTTP protocols.

Audio Streaming

When an audio file resides on a web server, the audio file is an ordinary object in the servers file sly, just as HTML & JPEG files.

When a user wants to hear the audio file then the user's host establishes a TCP connection with the webserver and sends HTTP req. for the object.

Based on receiving request, a web server encapsulates the audio file in an HTTP response message and sends the response message back to TCP connection.

Video Streaming

When a video file resides on a web server, the video file may be stored in two files.

Two separate HTTP request are sent to the server and the audio/video files arrive at the client in parallel.

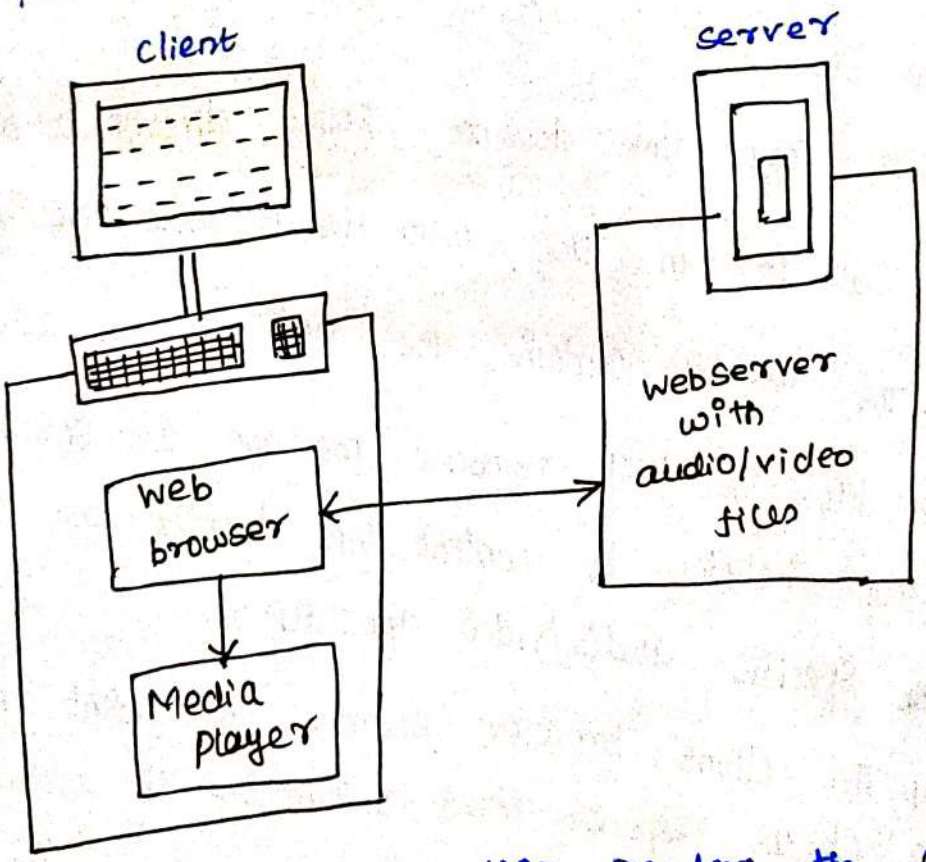
The audio/video is interleaved in the same file so that only one objects needs to be sent to the client.

Audio / video streaming

1. The browser process establishes a TCP connection with the web server and requests the audio/video file with an HTTP request message.

2. The webserver sends the audio/video file to the browser in HTTP response message.

3. The Content type header line in HTTP response message indicates a specific audio/video encoding. The client browser examines the content type of the response message, launches the associated media player and passes the file to the media player.



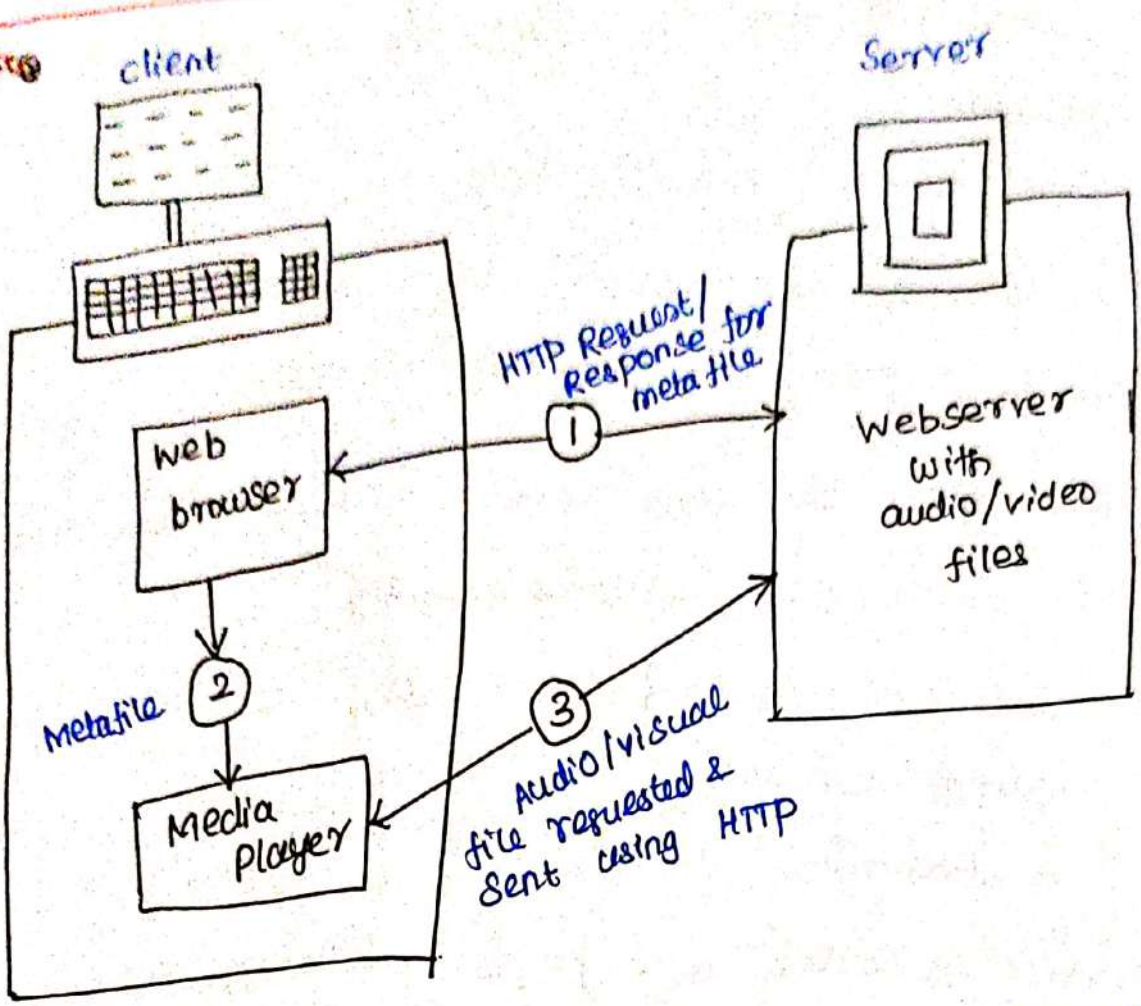
4. The media player then renders the audio/video file.

Drawback of this approach

1. The media player must interact with the server through a web browser as an intermediate
2. When a browser & intermediate then the entire object must be downloaded before the browser passes the object to a helper appln.
3. It causes a delay before playout.

To overcome these drawbacks, a direct socket connection is made between the server process and media player process,

1. The user clicks on a hyperlink for an audio/video file.
2. The hyper link does not point directly to audio/video file, but it can use meta file to point directly.
3. The metafile contains the URL of the actual audio/video file. The HTTP response message that encapsulates the meta file includes a content type header line that indicates the specific audio/video application.
4. The client browser examines the content type header line of the response messages, launches the associated media player and passes the entire body of the response message to the media player.



5. The media player sets up a TCP connection directly with the HTTP server. The media player sends an HTTP request message for audio/video file into the TCP connection.

6. The audio/video file is sent within an HTTP response message to the media player. The media player streams out audio/video file.

Sending Multimedia from a Streaming server to a Helper application.

In order to overcome the problem of using HTTP, the stored audio/video can be sent from a streaming server to the media player,

It will be sent over UDP → Better than HTTP to audio/video ~~servers~~ streaming.

Two kinds of servers such as,

1. HTTP server
2. Streaming server

HTTP server → Server web pages including meta files and streaming server, serves the audio/video files.

The media player and streaming server can interact using their own protocols.

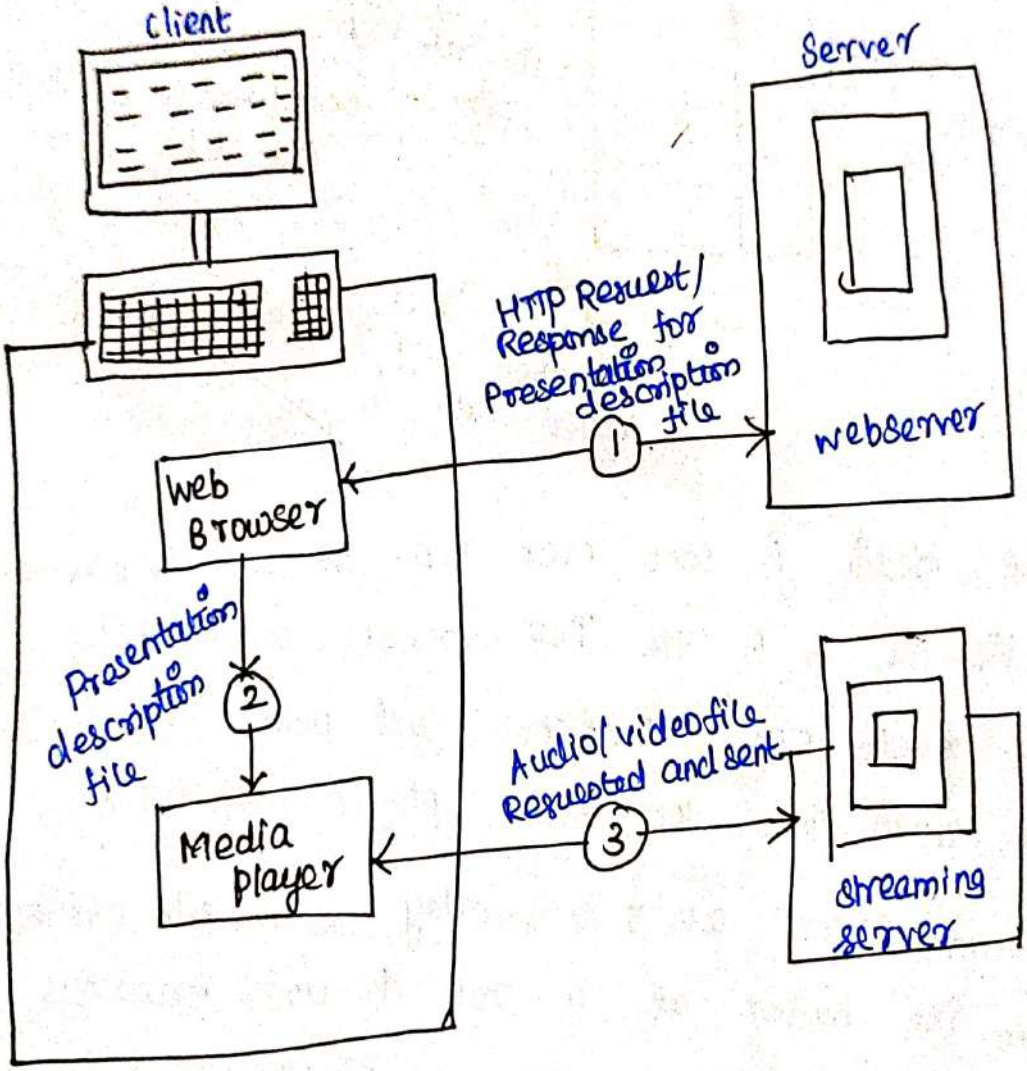
These protocols can allow for rich user interaction with the audio/video stream.

3 options are used for delivering the audio/video from the streaming server to the media player.

Option 1:

The audio/video is sent over UDP at a constant rate equal to the drain rate at the rcvr.

As soon as the client receives compressed audio/video from the nlw, it decompresses the audio/video and plays it back.



Option 2:

Similar to first option

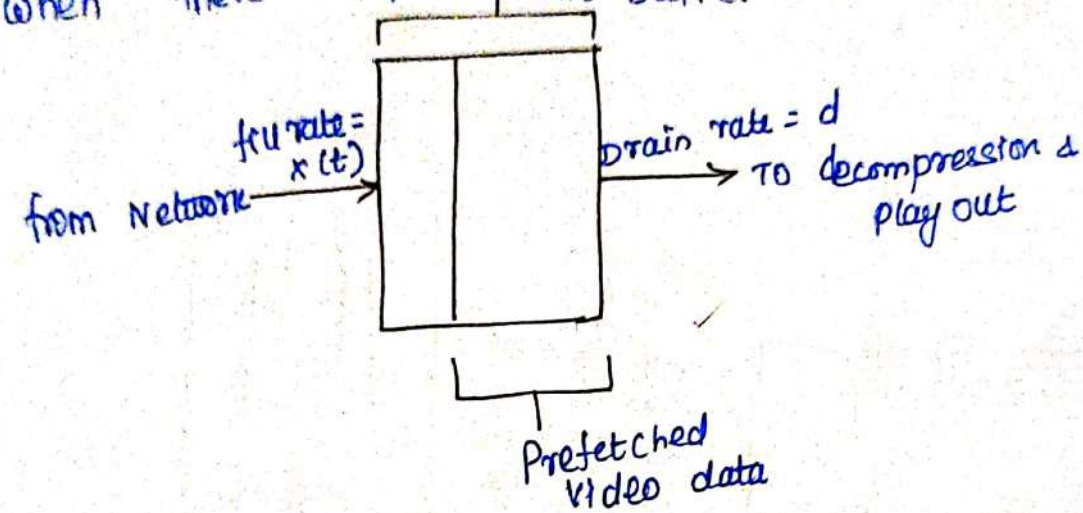
But the media player delays playout for two t

five sec. in order to eliminate n/w. induced jitter

The client performs this task by placing the compressed media that it receives from the n/w into a client buffer.

Once the client has prefetched a few sec of the media it begins to drain the buffer.

The fill rate $x(t)$ is equal to drain rate d, except when there is packet loss, in that case $x(t) < d$.



Option 3:

The media is sent over TCP. The server pushes the media file into the TCP socket as quickly the client reads from TCP socket and places the compressed video into the media player buffer.

After an initial 2 to 5 sec delay, the media player reads from its buffer at a rate d and forwards the compressed media to decompression & play back.

TCP retransmits lost packets and provide better sound quality than UDP.

Drawbacks in option 3:

The behavior of x(t) is very much depend on the size of client buffer.

If x(t) becomes much larger than d for long periods of time, then a larger portion of media is prefetched into client & subsequent client starvation is unlikely.

Real Time Streaming Protocol (RTSP)

It is a public domain protocol to provide user interactivity and it is defined in RFC - 2326.

RTSP does not do;

RTSP does not define compression scheme for audio & video.

Does not define how audio & video are encapsulated in packets for transmission over a n/w.

Doesnot restrict how streamed media player buffers the audio/video.

RTSP does do?

RTSP allows a media player to contr the transmission of a media stream control actions include pause/resume, playback, fast-forward and rewind.

RTSP messages are sent out of band because it is an out-of-band protocol.

It use a different port no.

The webbrowser first requests a presentation description file from webserver. It have references to several continuous media files.

Each will begins with the URL method.

Two audio recordings are used.

1. Low-fidelity recording
2. High-fidelity recording

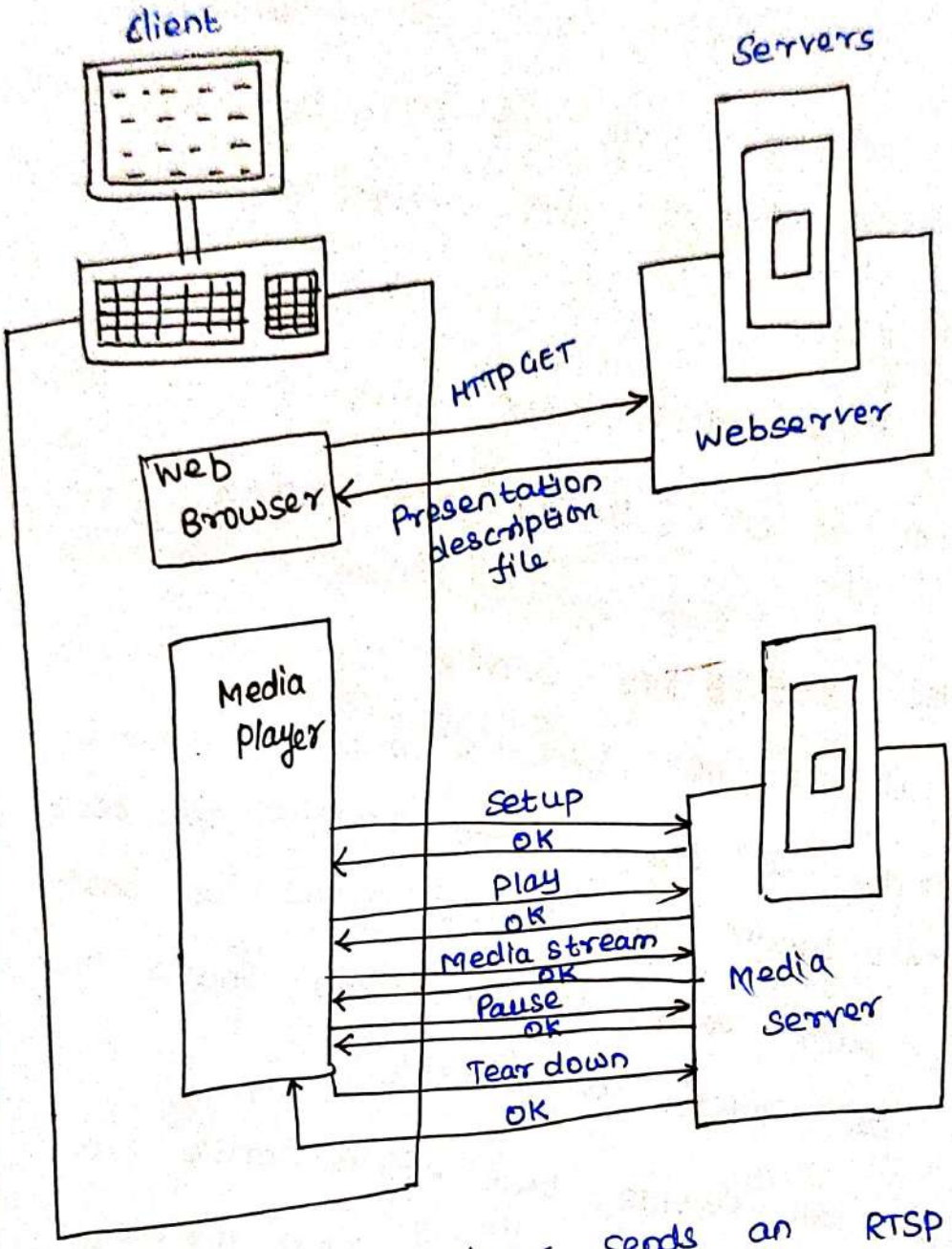
The web server encapsulates the presentation description file in an HTTP response message and sends the message to the browser.

The player sends an RTSP SETUP request and server responds with an RTSP OK message.

The player sends an RTSP PLAY request and the server responds with an RTSPOK message.

At this point the streaming server pumps the low fidelity audio into its own in-band channel.

Interaction between client and server using RTSP



Later the media player sends an RTSP PAUSE request and server responds with RTSP OK message.

When the user is finished, the media player sends an RTSP TEARDOWN Request & Server Confirms with an RTSP OK response.

* Similarity b/w HTTP & RTSP,

All request and response messages are in Ascii text, the client employs standardized methods and server responds with standardized reply codes.

Difference,

RTSP Server keeps track of the state of client for each ongoing RTSP session.

Making the Best Effort - Service

IP is the Internet's network protocol which provides a best effort service. The best effort service means the service makes its best effort to move each datagram from source to destination as quickly as possible.

IP will provide best effort service but it does not make any promises about certain events such as,

1. The extent of the end-to-end delay for an individual packet.

2. The extent of packet jitter and packet loss within the packet stream.

An Internet phone Eg:-

The speaker in Internet phone generates an audio sig. consisting of alternating talk spurts and silent periods.

In order to conserve BW, Internet phone appln. generates packets only during talk spurts.

During a talk spurt the sender generates bytes at a rate of 8000 bytes / sec and every 20msec the sender gethers bytes into chunks.

The no. of bytes in a chunk (20msec) · (8000 bytes/sec)
160 bytes.

The Receiver must do,

1. When to play back a chunk
2. What to do with a missing chunk

Limitations of Best effort service

1. Packet Loss
2. End-to-End delay
3. Packet Jitter

1. Packet loss

Internet layer use two kinds of protocols for packet transmission such as TCP and UDP.

using UDP

The UDP segment is encapsulated in an IP datagram and it passes through buffers in the routers in order to access out bound links.

One or more of the buffers in the route from Sender to receiver are full and cannot admit the IP datagram. In this case, the IP datagram is discarded and never to arrive at the receiving appln.

using TCP

Packet losses are eliminated by TCP because TCP retransmits packets that do not arrive at destination.

Due to TCP congestion control, after packet loss the retransmission rate at the Sender can be reduced to a rate that is lower than the rate at rxr.

Almost all Internet phone appln, run over UDP and donot bother to retransmit lost packets.

End-to-End Delay

It is accumulation of transmission, Processing and queuing delays in routers, propagations. Delays in the links and end sly.

Processing delays.

Internet phone appln. has end-to-end delays smaller than 150msec.

3. Packet Jitter

A Crucial Component of end-to-end delays is the random queuing delays in the routers. Because of these varying delays within the n/w, the time from when a packet is generated at source until it is received at the rxr. Can fluctuate from packet to packet ⇒ This is called as Jitter.

Recovering from packet loss

Loss recovery schemes are used to preserve acceptable audio quality in the presence of packet loss.

Two types of loss anticipation schemes are,

1. Forward Error correction (FEC)
2. Interleaving

1. Forward Error Correction (FEC)

To add redundant information to the original packet stream and the redundant information can be used to reconstruct approximations or exact versions of some of the lost packets.

It has 2 mechanisms,

Mechanism I

It sends a redundant encoded chunk after every n chunks. The redundant chunk is obtained by Ex-OR ing the n original chunks.

In this way if any one packet of group n+1 packets is lost then the rcvr. can fully reconstruct the lost packet.

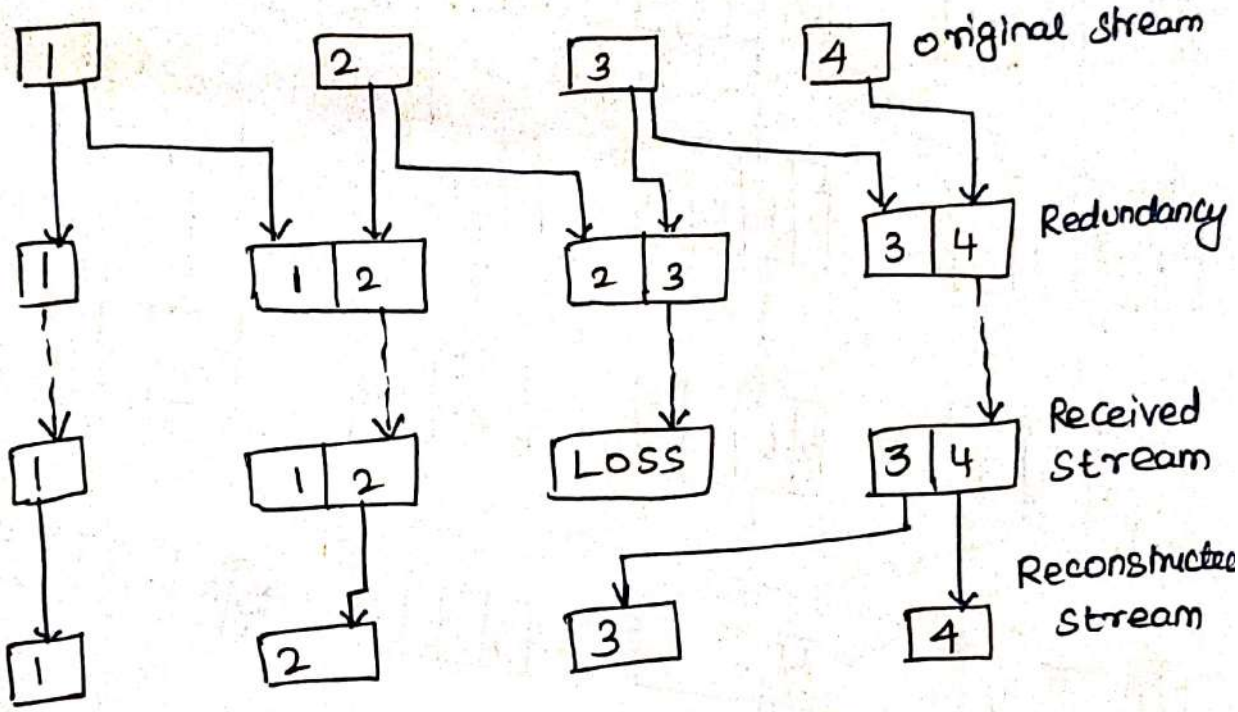
But if two or more packets in a group are lost then the rcvr. cannot reconstruct the lost packets.

The transmission ~~delay~~ rate will increases by a factor of 1/n and this scheme increases the playout delay, the rcvr. must wait to receive the entire group of packets before it can begin playout.

Mechanism II

It Sends a lower resolution audio stream as the redundant information.

The Sender Constructs the n^{th} packet by taking the n^{th} chunk from the nominal stream and appending to it the $(n-1)^{st}$ chunk from the redundant stream.

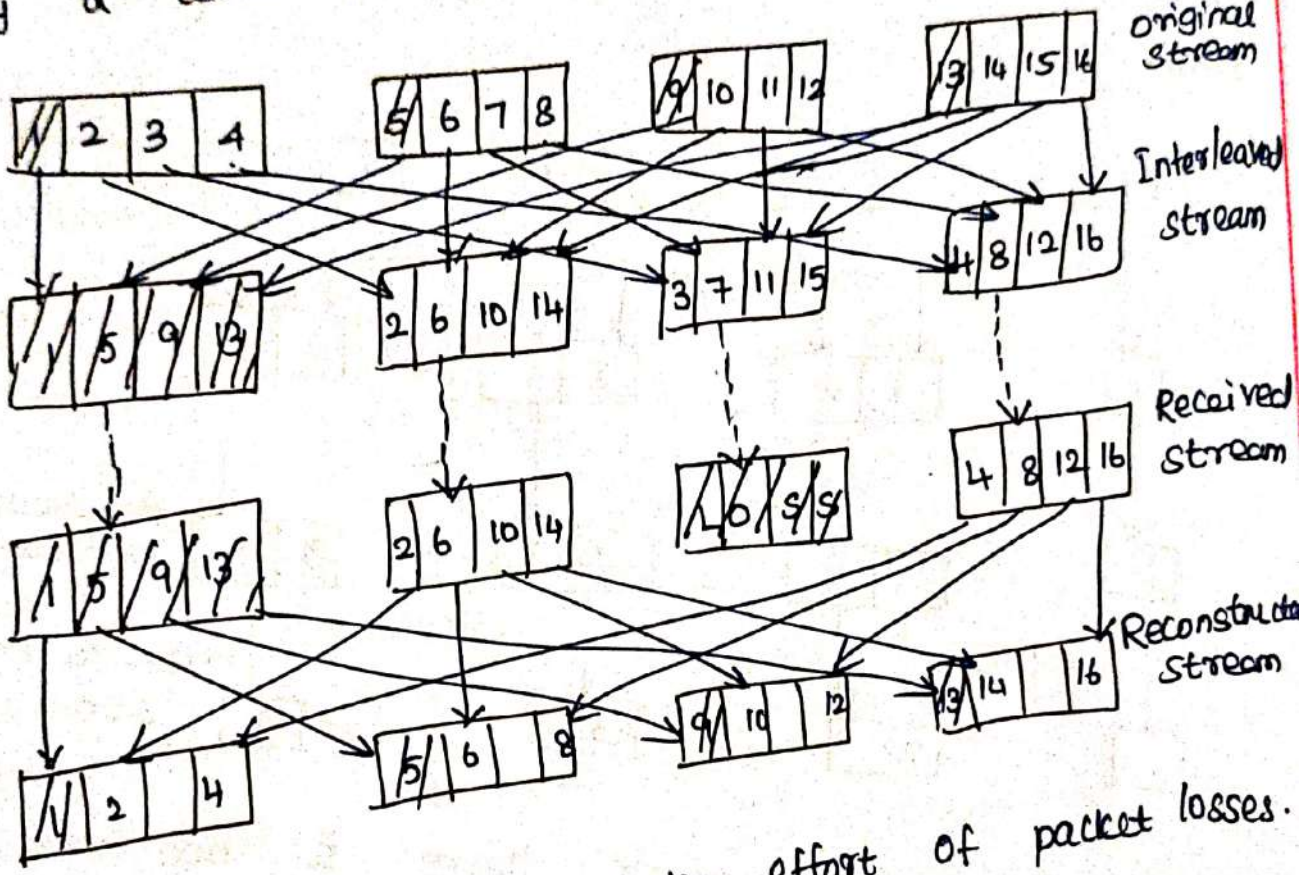


In this way, whenever there is non-Consecuti Packet loss then the receiver can cancel the loss by play out the low bit rate chunks give lower quality than the nominal chunks.

The receiver only has to receive two packets before playback so that increased play out delay is small.

Interleaving

An alternative to redundant transmission, an Internet phone appln. can send interleaved audio. The sender resequences units of audio data before transmission so that originally adjacent units are separated by a certain distance in the transmitted stream.



Interleaving can mitigate the effort of packet losses. The loss of a single packet from an interleaved stream results in multiple small gaps in the reconstructed stream.

Merits

1. Does not increase the BW requirement of a stream
2. Improves the perceived quality of an audio stream
3. low overhead

De-merits

It increases latency

Removing Jitter at the receiver for Audio

for a voice appln, such as Internet phone or audio on demand, the rxr. should attempt to Provide Synchronous playout of voice chunks in the Presence of random network Jitter.

3 mechanisms

1. Prefacing Each chunk with a Sequence number

The sender increments the sequence no. by one for each of the packets it generates.

2. prefacing Each chunk with a Time stamp

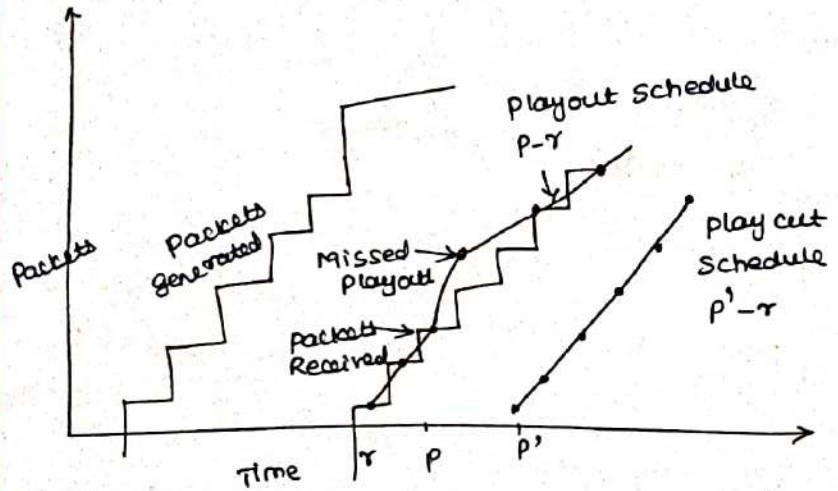
The sender stamps each chunk with the time at which the chunk was generated.

3. Delaying playout of chunks at the Time stamp

The playout delay of the received audio Chunks must be long enough so that most of the Packets are rxed. before their scheduled playout times.

Fixed playout Delay

The receiver attemps to playout each chunk exactly q msec after the chunk is generated. If a chunk is time stamped at time t then the rxr. plays out the chunk at time t+q assuming the chunk has arrived by that time.



Adaptive playout Delay

The adaptive adjustment of playout delays at the beginning of the talk spurts will cause the Senders silent periods to be compressed & elongated.

ti => The timestamp of ith packet = time the packet was generated by the sender

ri => time packet i is received by the receiver

Pi => Time packet i is played at receiver

The end-to-end network delay of ith packet is ri - ti.

This estimate is reconstructed from the timestamps as,

$$d_i = (1-u)\, d_{i-1} + u\,(r_i - t_i)$$

where

u => fixed constant.

from timestamps

$$v_i = (1-u)v_{i-1} + u\,|r - t_i - d_i|$$

The estimates di and vi are calculated for every packet received, although they are used only to determine the playout point for the first packet in any talk spurt.

If packet 1 is the first packet of a talk Spurt, its playout time Pi is computed as,

$$p_i = t_i + d_i + k v_i$$

k => positive constant

The purpose of Kvi term is to set the play out time for future so that only small fraction of arriving packets in the talk spurt will be lost due to late arrivals.

$q_i = p_i - t_i$ be the length of time from when the first packet in the talk spurt is generated until it is played out.

If packet j also belongs to this talk spurt then it is played out at time.

$$p_j = t_j + q_i$$

Streaming stored Audio and Video

Streaming stored audio and video applications also typically use sequence numbers, time stamps and playout delay to eliminate the effects of network jitter.

Protocols for Real Time Interactive Applications

Real time Interactive applications including Internet phone and video conferencing use 3 kinds of protocols.

1. RTP
2. SIP
3. H.323

1. RTP

RTP can be used for transporting common formats such as PCM, GSM and MP3 for sound and MPEG and H.263 for video.

It can also be used for transporting sound and video formats.

RTP Basics

RTP runs on top of UDP. The sending side encapsulates a media chunk within an RTP packet and then encapsulates the packet in a UDP segment and then hands the segment to IP.

The receiving side extracts the RTP packet from UDP segment then extracts the media chunk from RTP packet and then passes the chunk to the media player for decoding & rendering.

The sending side precedes each chunk of the audio data with an RTP header that includes

the type of audio encoding, a sequence number and a time stamp.

The RTP header is normally 12 bytes.

RTP does not provide any mechanism to ensure timely delivery of data or other quality of service(QoS).

RTP encapsulation is seen only at the end systems. Routers do not distinguish b/w IP datagrams that carry RTP packets and IP datagrams that donot carry RTP packets.

(Many Popular encoding techniques including MPEG1 and MPEG2 bundle the audio and video into a single stream during the encoding process.)

RTP can also be sent over one-to-many and many-to many multicast trees. (1 to many, many to many)

RTP Packet Header Fields

4 main parts

1. Payload type - 7 bits long
2. Sequence number - 16 "
3. Timestamp - 32 "
4. Source Identifier Fields - 32 bits long

1. Payload type field

It is 7 bits long.

for an audio stream, this field is used to indicate the type of audio encoding that is being used.

for a video stream, the payload type is used to indicate the type of video encoding. The Sender can change video encoding on the fly during a session.

2. Source Sequence Number Field

It is 16 bits long

It increments by one for each RTP Packet sent and may be used by the receiver to detect packet loss and to restore packet sequence.

3. Timestamp

It is 32 bits long

It reflects the sampling instant of the first byte in the RTP data packet.

4. Source Identifier Field

The Synchronization Source Identifier (SSRC) is 32 bits long. It identifies the source of RTP stream.

RTCP

RTP Control Protocol

RTCP is a protocol that a networked multimedia appln. can use in conjuction with RTP. RTCP Packets are transmitted by each Participant in an RTP session to all other participants in the using IP multicast.

RTCP Port no. = RTP Port no. +1

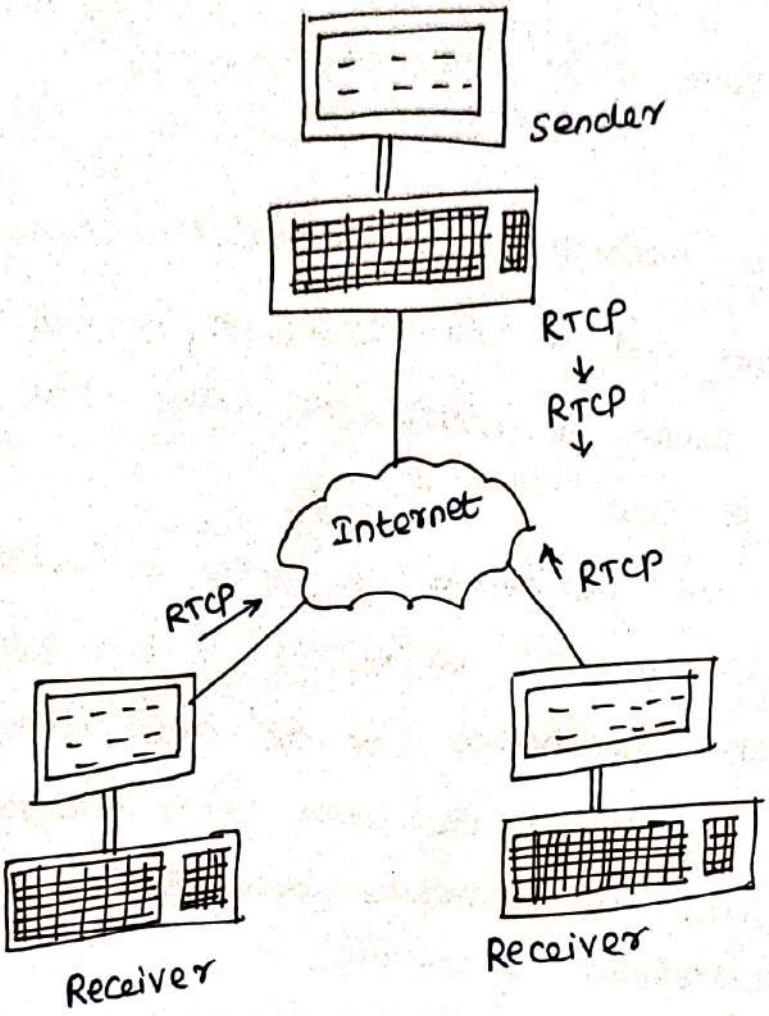
RTCP packets do not encapsulate chunks of audio or video. RTCP packets are sent periodically and contain sender / receiver reports that announce statistics that can be useful to the appln. These statistics include no. of packets sent, no. of packets lost and interarrival jitter

RTCP Packet types

1. The SSRC of RTP stream
2. Last sequence no. received
3. The Interarrival Jitter

RTCP Packets are stackable i.e. receiver reception reports, Sender reports and source descriptions can be concatenated into a single packet.

Both Senders and Receivers send RTCP messages



RTCP Bandwidth scaling

The period for transmitting RTCP packets for a

Sender is,

$$T = \frac{\text{NO. of senders}}{.25 \cdots 05 \cdot \text{Session BW}} \text{ (avg. RTCP Packet size)}$$

Receiver is,

$$T = \frac{\text{NO. of receivers}}{.75 \cdots 05 \cdot \text{session BW}} \text{ (avg. RTCP Packet size)}$$

SIP

Session Initiation Protocol

It is light weight protocol

Functions:

1. It provides mechanisms for establishing calls between a caller and a callee over an IP network. It allows the caller to notify the callee that it wants to start a call.

2. It allows the participants to agree an media encodings and also allows participants to end calls.

3. It provides mechanisms for the caller to determine the current IP address of the callee users do not have a single, fixed IP addresses because they may be assigned addresses dynamically.

4. It provides mechanisms for call management such as adding new media streams during the call, changing the encoding during the call, inviting new participants during the call, calltransfer & call holding.

SIP characteristics

1. SIP is an out of band protocol, the SIP messages are sent and received in sockets that are different from those used for sending and receiving the media data.

2. The SIP messages are ASCII readable and resemble HTTP messages.

3. SIP requires all messages to be acknowledged so it can run over UDP or TCP.

SIP Messages

Whenever an SIP message passes through a SIP device a Vit attaches via header. It indicates the IP address of the device.

The SIP message includes a from header line and a to header line. The message includes a Call-ID. The Call-ID identifies the call and includes a Content-type header line.

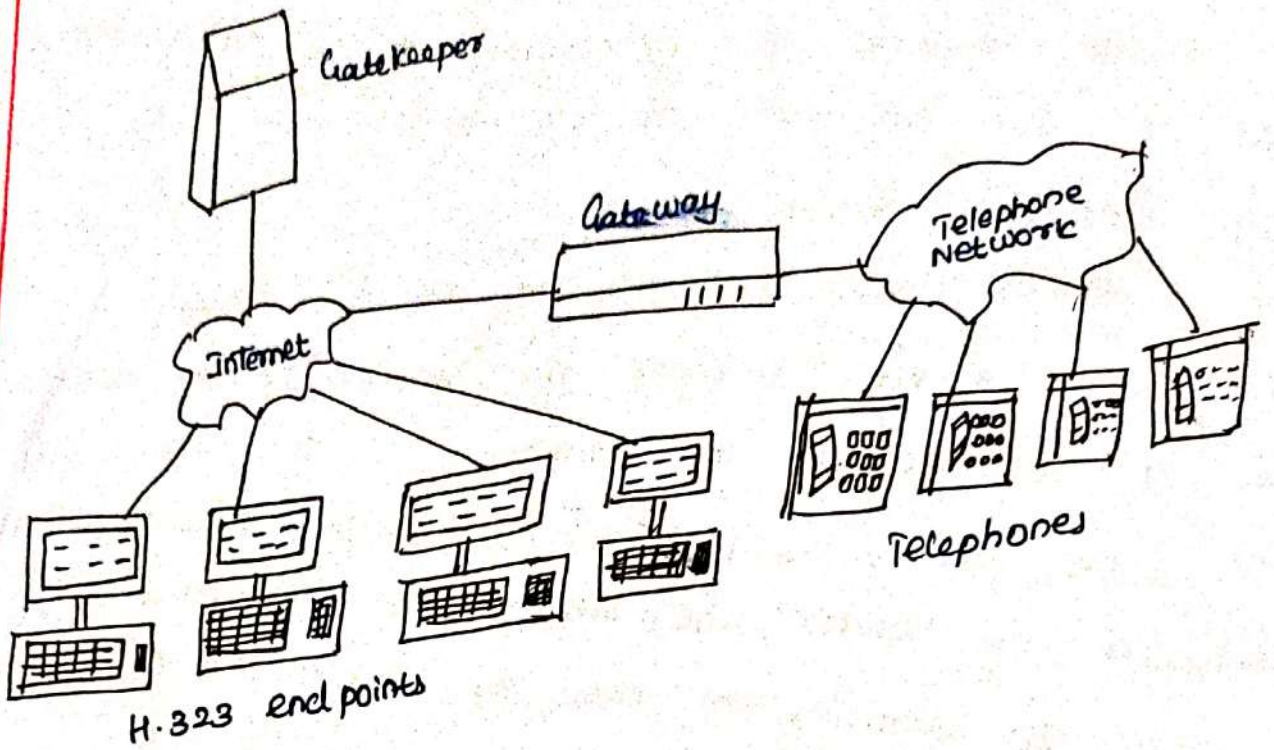
Content type header line defines the format used to describe the Content contained in the SIP messages and also includes a Content length header line.

H.323

H.323 is an alternative to SIP.

It is a popular standard for real time audio and video conferencing among end systems on the Internet.

The H.323 standard is an umbrella specification



Specifications,

1. A specification for how endpoints negotiate common audio / video encodings.

2. A specification for how audio and video chunks are encapsulated and sent over the network.

3. A specification for how endpoints communicate with their respective gatekeepers.

4. A specification for how Internet phones communicate through a gateway with ordinary phones in the Public Circuit Switched telephone network.

Each H.323 end point must support the G.711 speech compression standard. G.711 uses PCM to generate digitized speech at either 56kbps or 64kbps.

Comparison H.323 and SIP

H.323	SIP
1. H.323 is a complete vertically integrated suite of protocols for multimedia conferencing, signaling, registration, admission control, transport and codecs.	1. SIP is addresses only session initiation and management. It is a single component. SIP works with RTP but do not mandate them. It works with G.711 speech codecs & QCIF H.261 video codecs but does not mandate them. It can be combined with other protocols & services.
2. H.323 comes from ITU	2. SIP comes from IETF.
3. H.323 is an umbrella standard. It is large & complex	3. SIP uses kiss principle. It is simple.

Distributing Multimedia

Distributing multimedia has two problems such as,

1. A client may be very far from the server and server-to-client packets may pass through many ISPs. It will increase the delay and loss.

2. If the video is very popular then the video will be sent many times through the same ISPs. It will consume very large Bandwidth.

Content Distribution Networks (CDNs) will provide an alternative approach to distributing stored multimedia Content.

In CDNs method the client can't come to the Content and the Content should be brought to the client.

CDNs use a different model than web caching. In CDNs the paying customers are no longer the ISPs but the content providers must be present.

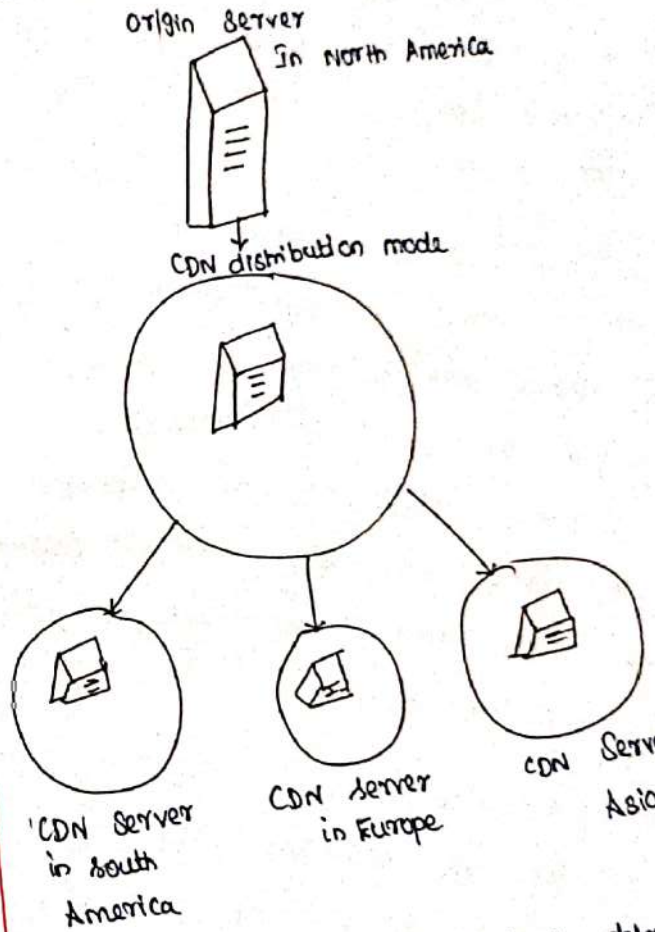
A Content provider with a video to distribute pays a CDN company to get its video to requesting users with the shortest possible delays.

Content distribution services,

1. CDN company installs hundreds of CDN servers throughout the Internet. CDN company places the CDN Servers in a data center.

2. A data center is owned and run by a third party. It is a building filled with server hosts. These data Centers are in lower-tier ISPs, close to ISP access networks and the clients.

3. The CDN replicates its customer's Content in the CDN Servers. whenever a Customer updates its Content, the CDN redistributes the fresh Content to the CDN Servers.



The Content provider first determines which of its objects and it wants to distribute.

The Content provider tag pushes the content to a CDN node and all its CDN Servers.

The CDN Company may own a private network for Pushing the Content from the CDN node to the CDN servers.

Whenever the Content provider modifies a CDN distributed Object, it pushes the fresh version to the CDN node, which again immediately replicates and distributes the Object to the CDN Servers.

Beyond Best effort Service

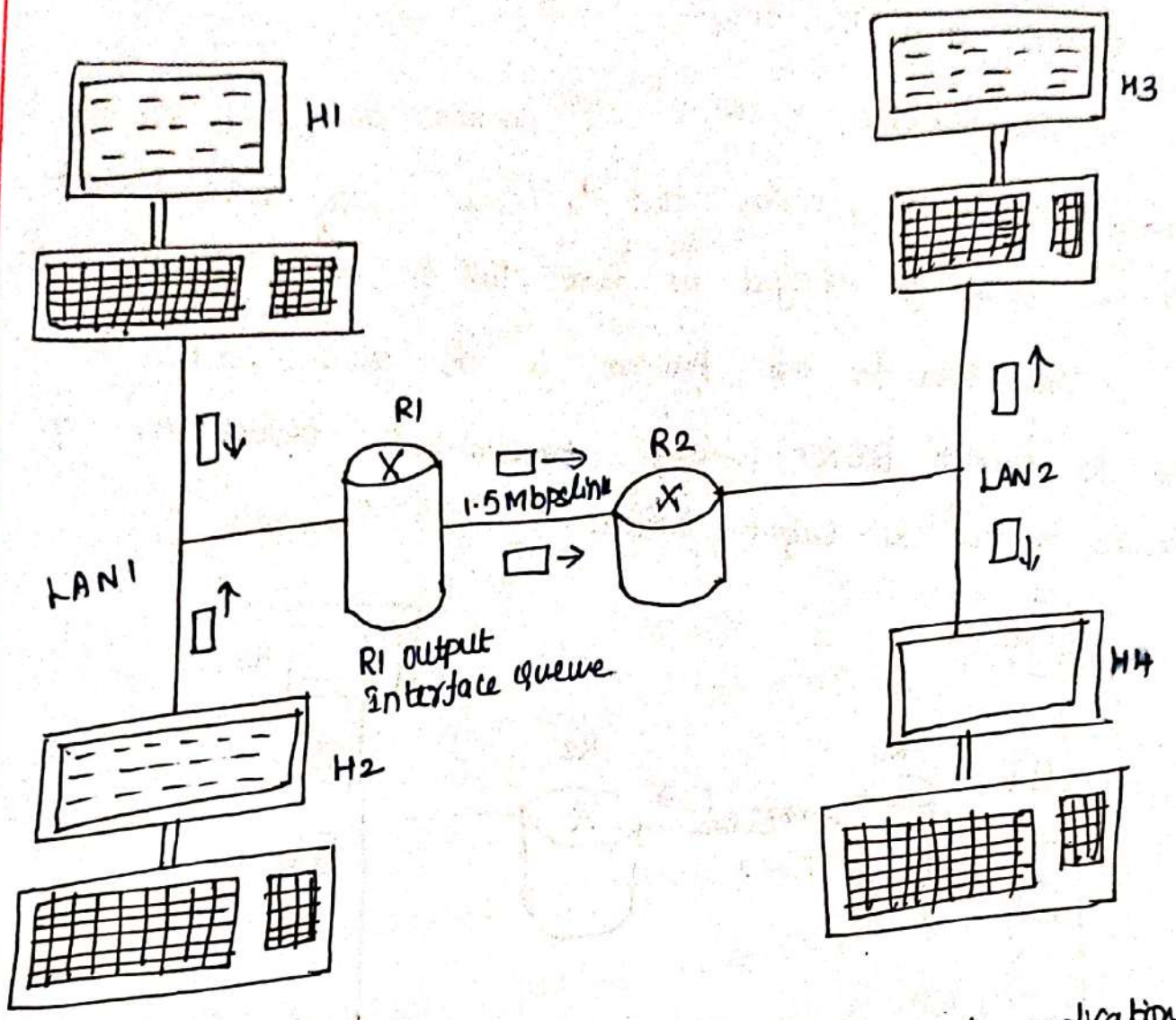
Internet provides a best effort service to all of its appns, but it does not make any Promises about QoS an appln. will receive.

Public Internet does not allow delay sensitive multimedia appns. to request any special treatment. Because every Packet including delay sensitive audio and video packets are treated equally at the routers.

There are two appln. Packet flows originate on Hosts H1 and H2 on LAN1 Connection and those Packets are destined for HOSTS H3 and H4 on another LAN 2 Connection.

The routers on the two LANs are connected by a 1.5mbps link.

If LAN speeds are higher than 1.5mbps means it cause packet delay and packet loss.



Scenarios:

For proving QoS guarantees to multimedia applications

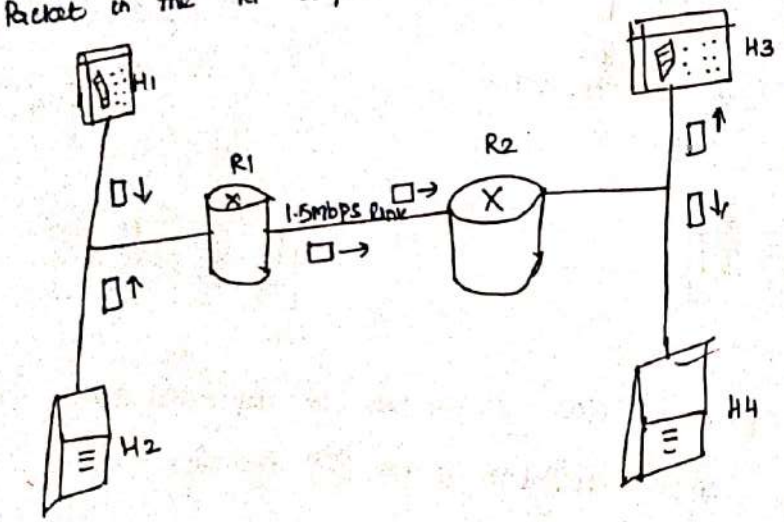
1. 1MBPs Audio Application & A FTP Transfer

A 1Mbps audio appln. shares the 1.5mbps link blw. R1 and R2 with FTP appln. that is transferring a file from H2 to H4.

In the best effort Internet, the audio and FTP packets are mixed in the output queue at R1 and transmitted in a FIFO order.

In this scenario, a burst of packets from the FTP source could fill up the queue and it cause IP audio packets to be excessively delayed or lost due to buffer overflow at R1.

The soln. for this problem is an audio packet in the R1 output buffer always transmitted before any FTP packet in the R1 output buffer.



Principle 1: packet marking allows a router to distinguish among packets belonging to different classes of traffic.

2. 1Mbps Audio Application and a High priority FTP transfer

In this case packets are distinguish on the basis of Senders Ip address and routers are classify the packets according to some criteria.

Principle 1 (Modified): Packet classification allows a router to distinguish among packets belonging to different classes of traffic.

3. Misbehaving Audio Application and FTP Transfer

Principle 2: It is desirable to provide a degree of isolation among traffic flows, so that one flow is not adversely affected by another misbehaving flow.

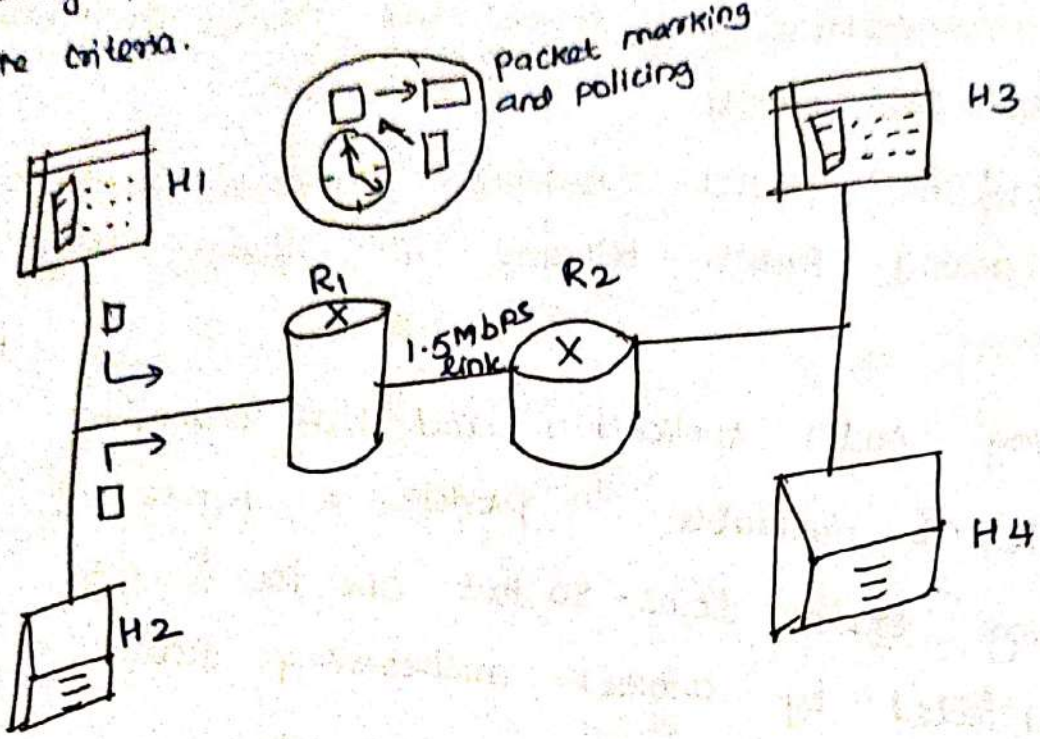
Two approaches used,

1. It is possible to police traffic flows
2. The link level packet scheduling mechanism to explicitly allocate a fixed amount of link bandwidth to each appln. flow.

Approach 1:

A traffic flow must meet certain criteria then only policing mechanism can be ensure that these Criteria are indeed observed.

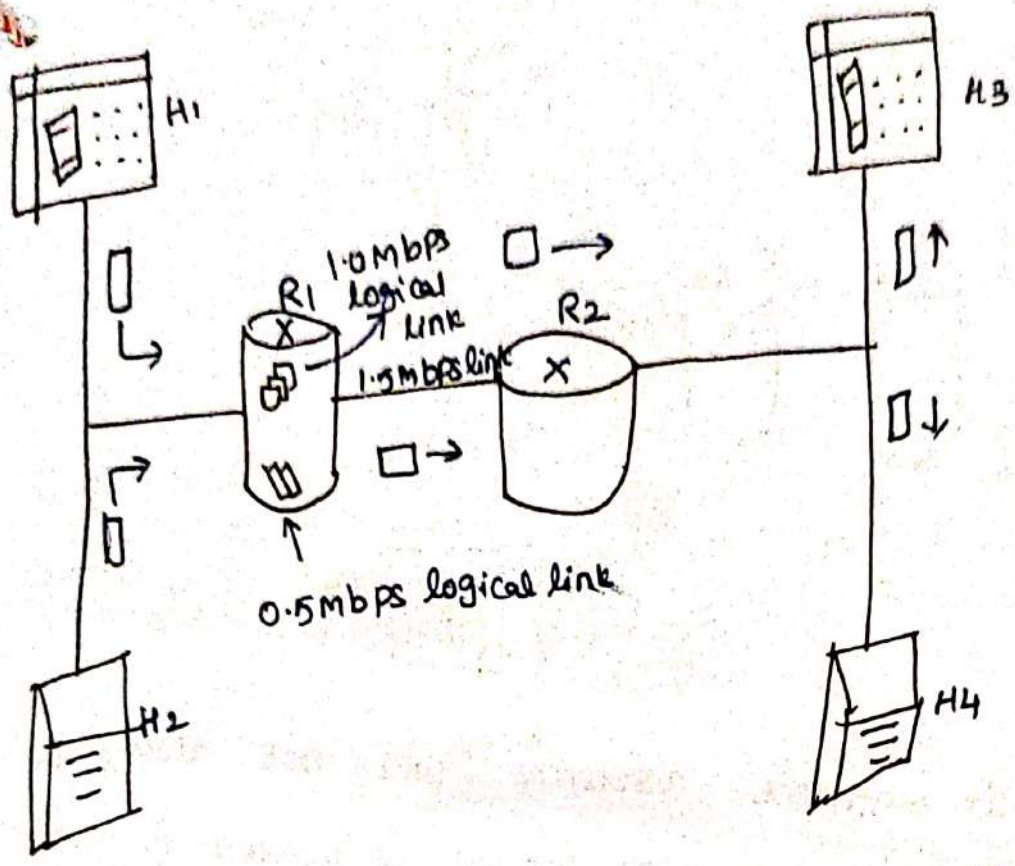
If the policed appln. misbehaves then the policing mechanism will take some action such as drop or delay packets. So the traffic entering the nlw. must confirm the criteria.



Approach 2

A flow can use only the amount of BW that has been allocated to it and it cannot utilize BW that is not currently being used by other appln.

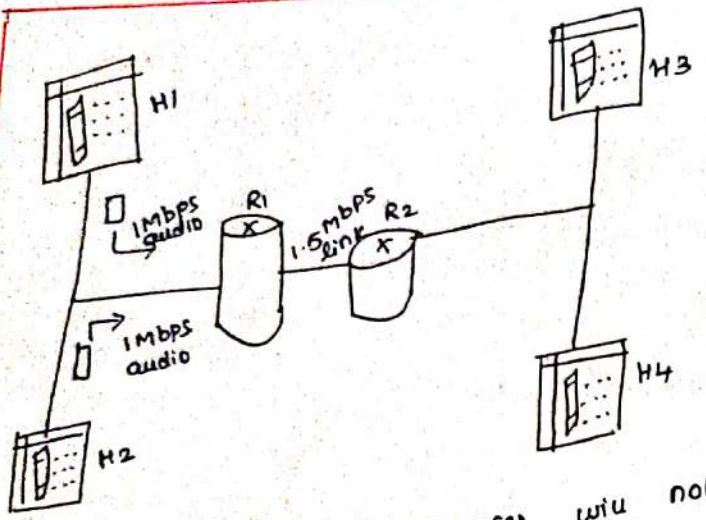
Principle 3: While providing isolation among flows, it is desirable to use resources as efficiently as possible.



4. TWO 1Mbps Audio Applications over an overloaded 1.5Mbps link

The Combined data rate of the two flows exceeds the link capacity. So each appln. can lose 25% of its transmitted packets.

The need of providing QoS to a flow is the need for the flow to declare its QoS requirements. The process of declaring the QoS requirement and having the network either accept the flow or block the flow is referred to as the call admission process.



Principle 4: If sufficient resources will not always be available, a call admission process is needed in which flows declare their QoS requirements and are then either admitted to the network or blocked from the network.

Four principles will provide QoS guarantees for multimedia appln.

Scheduling and policing Mechanisms

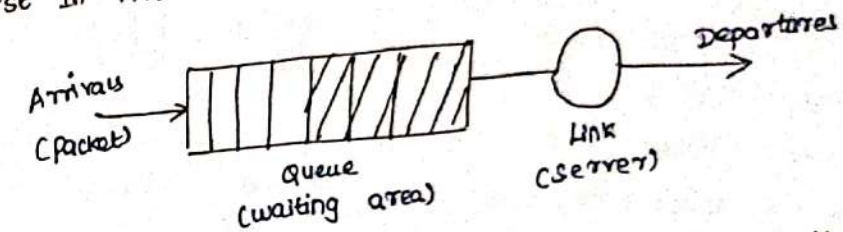
Scheduling Mechanisms

The packets belonging to various network flows are multiplexed and queued for transmission at output buffers associated with a link.

The way how the queued packets are selected for transmission on the link is known as link-scheduling discipline

1. First-In-First out (FIFO)
2. Priority queuing
3. Round Robin and weighed Fair Queuing (WFQ)

1. First In First out (FIFO)



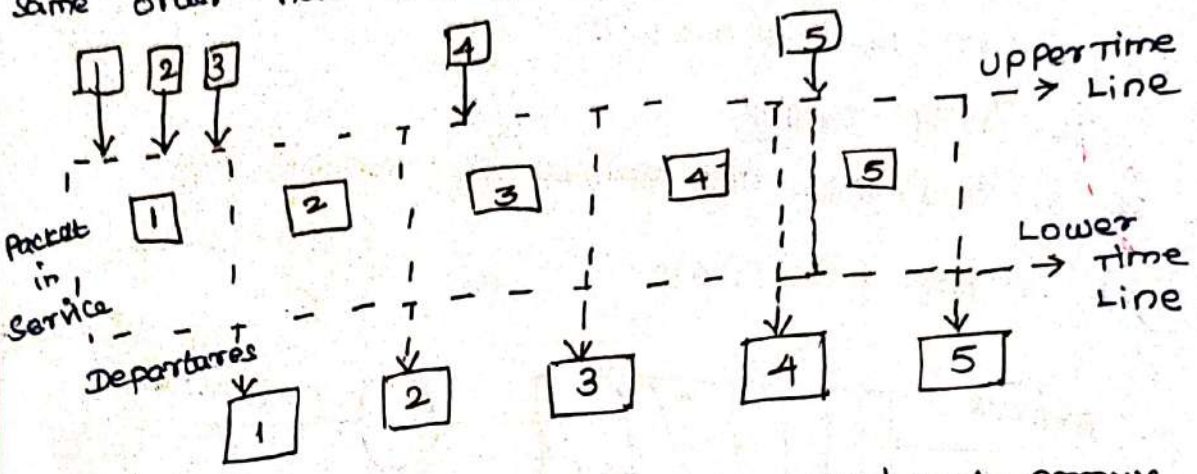
Packets arriving at the link output queue wait for transmission if the link is currently busy and transmitting another packet.

If there is not sufficient buffering space to hold the arriving packet then,

1. The queue's packet discarding policy determines whether the packet will be dropped.
2. Whether other packets will be removed from the queue to make space for the arriving packet.

When a packet is completely transmitted over the outgoing link it is removed from the queue. The FIFO

Scheduling selects packets for link transmission in the same order how they arrived at the output link queue.



Packet arrivals are indicated by numbered arrows above the upper time line and the no. indicating the order in which the packet arrived.

Individual packet departures are shown above the lower timeline. The time that a packet spends in service is indicated by the shaded rectangle between the two timelines.

In FIFO discipline, packets leave in the same order in which they arrived. After the departure of packet 4 the link remains idle until the arrival of packet 5.

2. Priority Queuing

The packets arriving at the output link are classified into priority classes at the output queue.

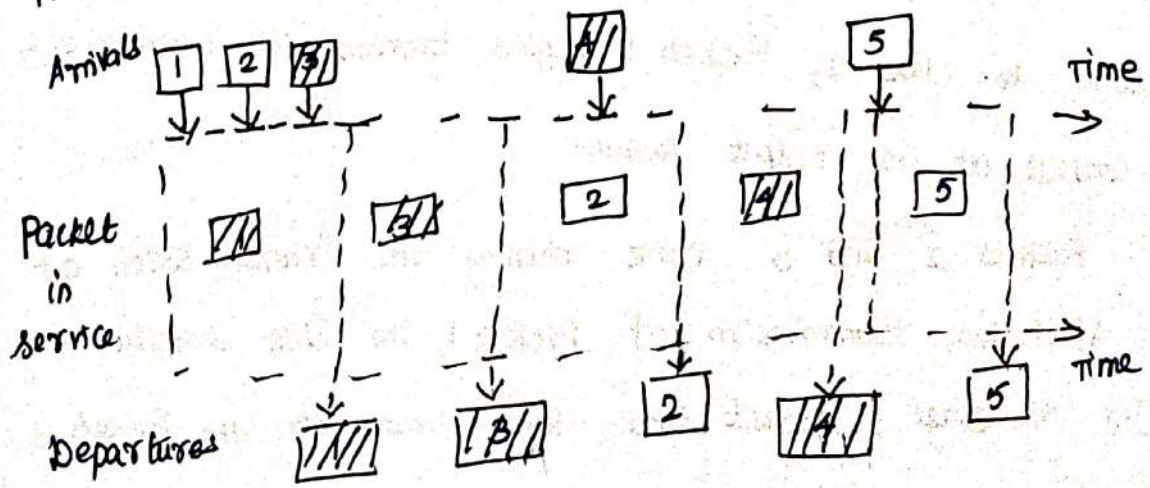
Functions such as,

1. Explicit marking
2. Packet Header
3. Source Ip address
4. Destination Ip address
5. Destination Port number

Each Priority class has its own queue. When transmitting a packet, a highest Priority Packet will transmit first. If more than one Packet has a same priority means packets are done in a FIFO manner.

Packets 1, 3 and 4 belong to the high priority class & Packets 2, 5 belong to low priority class.

Packet 1 arrives and its finding the link is idle after that it begins transmission. During the transmission of Packet 1, Packets 2 and 3 arrive and they are queued in low & high Priority queues respectively.



After Packet 1 was transmitted, Packet 3 is selected for transmission over Packet 2 because Packet 2 has low Priority than packet 3.

At the end of the transmission of Packet 3, Packet 2 begins transmission. Packet 4 arrives during the transmission of Packet 2.

3. Round Robin and Weighted Fair Queuing (WFQ)

Packets are ordered into classes.

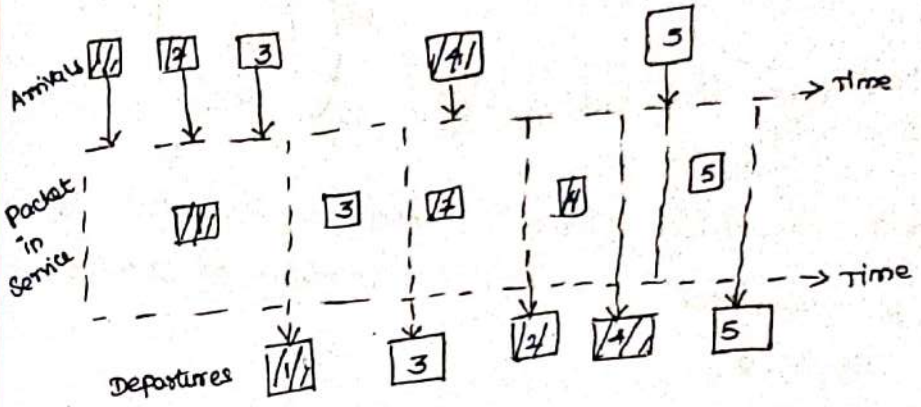
In this queuing a class 1 Packet is transmitted followed by a class 2 packet and so on. work conserving queuing discipline will never allow the link to remain idle whenever there are packets for transmission.

A work conserving round robin discipline looks for a packet of a given class but finds none will immediately check the next class in the round robin sequence.

Packets 1, 2 and 4 belong to class 1 & Packets 3 and 5 belong to class 2, Packet 1 begins transmission immediately upon arrival at the output queue.

Packets 2 and 3 arrive during the transmission of Packet 1. After the transmission of Packet 1, the link scheduler looks for a class 2 packet and thus transmits the Packet 3.

After the transmission of Packet 3, the scheduler looks for a class 1 packet and thus transmits Packet 2. Like that round robin scheduling will transmits the Packets.



Weighted Fair queuing (WFQ) Discipline,

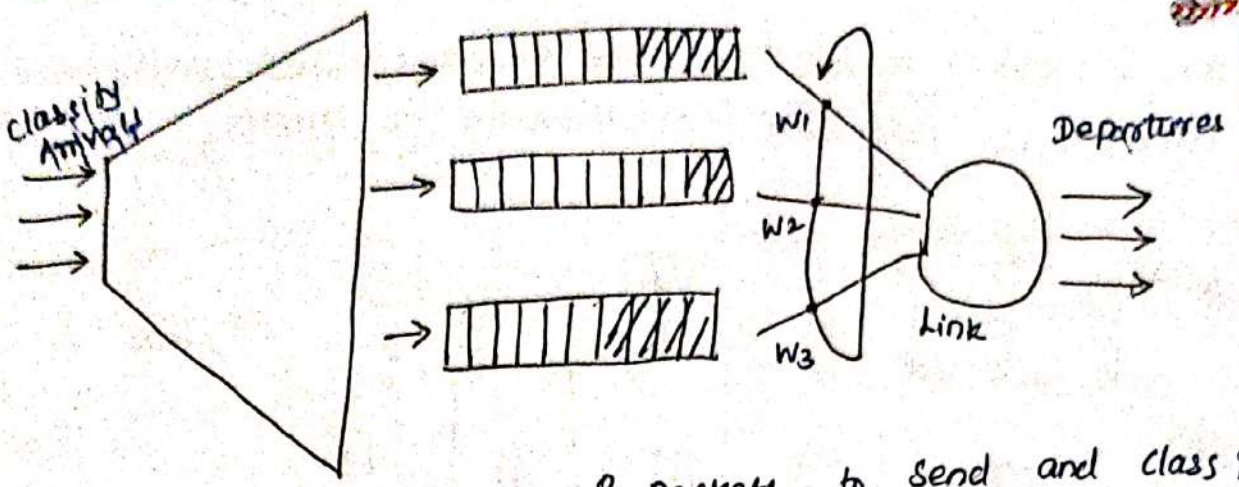
Arriving Packets are classified and queued in the appropriate per-class waiting area. As in round robin scheduling, a WFQ scheduler will serve classes in a circular manner.

First it serving class 1, then serving class 2 then serving class 3 and then repeating the service pattern.

WFQ is also a work conserving queuing discipline & thus immediately move on to the next class in the service sequence when it finds an empty class queue.

WFQ differs from round robin queuing.

Let's Consider class i has a weight of W_i,



under WFQ, during class i packets to send and class i will be guaranteed to receive a fraction of service equal to $w_i / (\Sigma w_j)$

where class has weight of (w_i)

Fraction of service = $\frac{w_i}{\Sigma w_j}$

w_j ⇒ overall class weight

A link has transmission rate R then class i will always achieve a through out of $R \cdot w_i / w_j$

where

R ⇒ Transmission Rate

Throughout ⇒ $R \cdot \frac{w_i}{\Sigma w_j}$

Policing : The Leaky Bucket

Policing is the regulation of the rate at which a flow is allowed to inject packets into the N/w.

1. Average Rate

It limits the amount of traffic that can be sent into the N/w. over a relatively long period of time.

$$\text{Average Rate} = \frac{\text{No. of packets transmitted}}{\text{Time Interval}}$$

2. Peak Rate

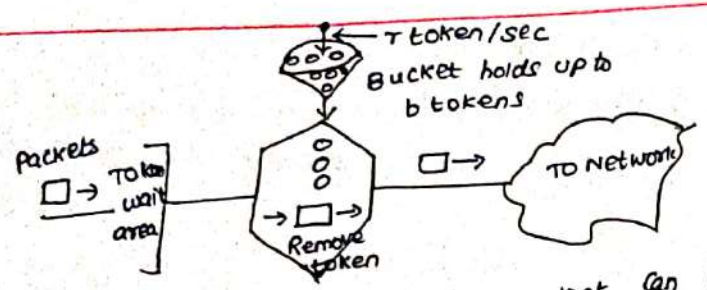
Peak Rate Constraint limits the maximum no. of packets that can be sent over a shorter period of time.

3. Burst Size

The N/w. may also limit the max. no. of packets that can be sent into the n/w. over an extremely short interval of time.

In the limit, as the interval length approaches zero, the burst size limits the no. of packets that can be instantaneously sent into the n/w.

The leaky bucket mechanism is an abstraction that can be used to characterize these policing limits.



A leaky bucket has a bucket that can hold up to b tokens,

1. New tokens are added to the bucket, are always generated at a rate of r tokens per second.

2. If the bucket is filled with less than b tokens when a token is generated, the newly generated token is added to the bucket otherwise the newly generated token is ignored and the token bucket remains full with b tokens.

Bucket filled $< b$ - add new token

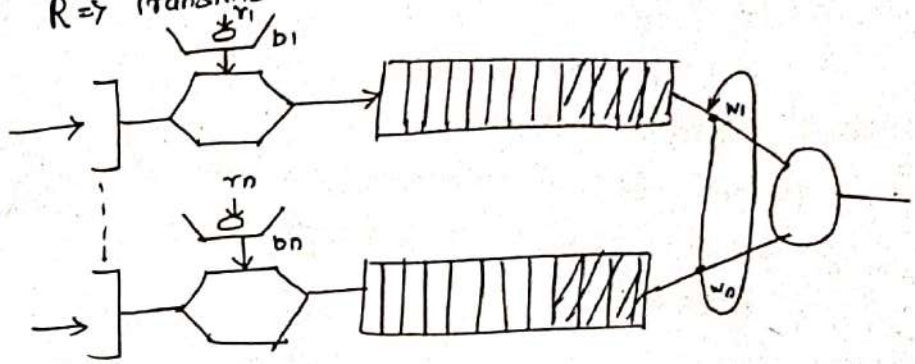
Bucket filled $> b$ - Ignore token

Leaky Bucket + weighted fair queing $\Rightarrow$ provable maximum delay in a queue

n multiplexed leaky bucket flows with WFQ scheduling. Router's output will link 12 mux flows. Flow i is the set of packets that are not distinguished from each other by the scheduler.

In WFQ each flow i is generated to receive a share of the link BW equal to $R \cdot w_i / \sum w_j$.

R => Transmission rate of the link in packets/sec.



If flow i's token bucket is initially full. A burst of b_i packets then arrives to the leaky bucket policer flow i. These packets remove all of the tokens (w/o wait) from the leaky bucket and then join the WFQ waiting area for flow i.

These b_i packets has $R \cdot w_i / (\sum w_j)$ packet/sec and the last of these packets will have a max. delay d_{max} until its transmission is completed.

$$\text{Maximum delay, } d_{max} = \frac{b_i}{R \cdot w_i / \sum w_j}$$

The amount of time until the last bit of the last packet is transmitted cannot be more than

$$\frac{b_i}{R \cdot W_i / \sum W_j}$$

Integrated Services (Intserv)

Intserv is a framework developed within the IETF to provide individualized QoS guarantees to individual application sessions.

1. Reserved Resources

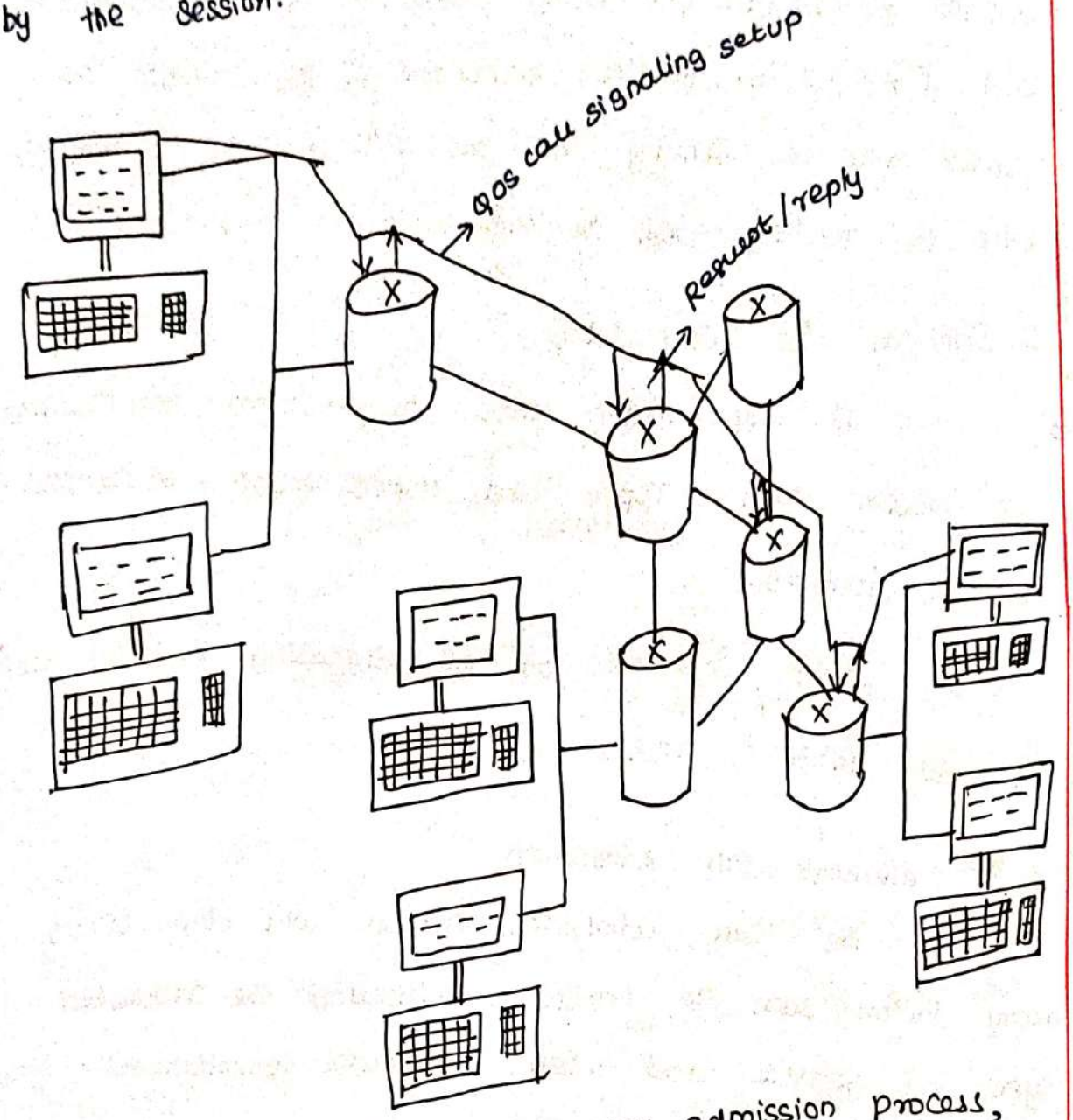
A router is required to know what amounts of its resources are already reserved for ongoing sessions.

2. Call setup

If any session requiring QoS guarantees it must be able to reserve sufficient resources at each network router on its source to destination path to ensure that its end-to-end QoS requirement is met.

This call setup process also known as call admission. It requires the participation of each router on the path.

Each router must determine the local resources required by the session.



Steps involved in call setup or call admission process,

1. Traffic characterization and specification of Desired QOS

Each session must declare its QOS requirement as well as characterize the traffic that it will be sending into the network.

In the Intserv architecture Rspec (R for reservation) defines the specific QoS being requested by a connection and Tspec (T for traffic) characterizes the traffic the sender will be sending into the network or the receiver will be receiving from the network.

2. Signaling for call setup

If any router wants to reserve any resources for session then Tspec and Rspec must be carried to the routers.

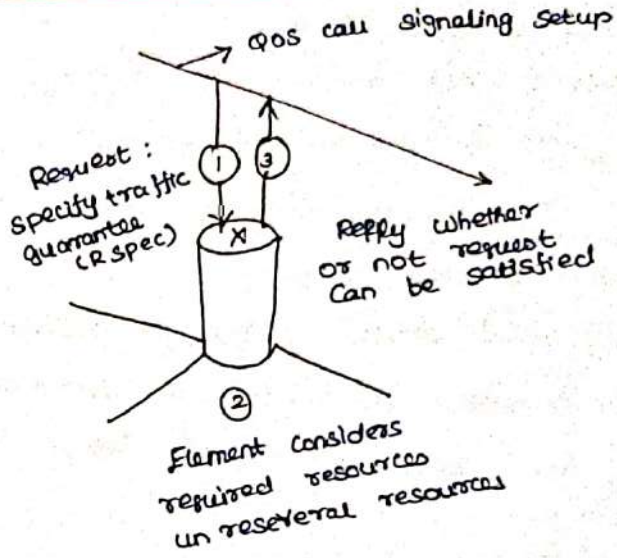
RSVP is one of the signaling protocol used in the Intserv architecture

3. Per-element call Admission

The call admission process will depends on many factors such as traffic specification the requested type of service and existing resource commitments already made by the router to ongoing sessions.

The Intserv architecture has two major classes of service

1. Guaranteed quality of service
2. Controlled load Network service



1. Guaranteed Quality of Service

It provides mathematically provable bounds on the queuing delays that a packet will experience in a router.

A source's traffic characterization is given by a leaky bucket with Parameters (r, b) and the requested service is characterized by a transmitted rate R.

Guaranteed quality of service makes guarantees about performance.

A session requesting guaranteed service is requiring that the bits in its packet be guaranteed a forwarding rate of R bits/sec.

2. Controlled-load Network Service

The session may assume a very high percentage of its packets will successfully pass through the router without dropped and will experience a queuing delay in the router that is close to zero.

Controlled load service makes no quantitative guarantees about Performance. It targets real time multimedia applications that have been developed for today Internet.

Differentiated Services (Diffserv)

The goal of Diffserv is to provide the ability to handle different classes of traffic in different ways within the Internet.

The Intserv model & Per-flow reservation of resources will have two kinds of difficulties,

1. Scalability
2. flexible Service models

1. Scalability

Per flow Resource Reservation Poplies the need for a router to process resource reservations and to

maintain per-flow state for each flow passing through the router.

2. Flexible Service Models

The Intserv framework provides for a small no. of pre-specified service classes. This particular set of service classes does not allow for more qualitative or relative definitions of service distinctions.

The Diffserv architecture aims to provide scalable and flexible service differentiation.

The need for flexibility arises from the fact that new service classes may arise and old service classes may become obsolete.

The diffserv architecture is flexible that means it does not define specific services or service classes. But diffserv provides the functional components that are pieces of network architecture.

Differential Services: Scenario

Two sets of functional components such as

1. Edge functions
2. Core functions

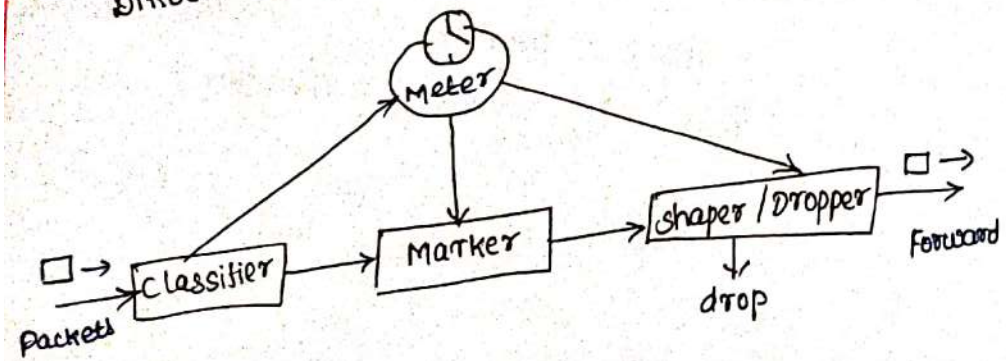
1. Edge functions: packet classification & Traffic conditioning

At the incoming edge of the n/w, arriving packets are marked. The differentiated service field of the packet header is set to some value.

2. Core function: Forwarding

When a differential service marked packet arrives at a Diffserv-capable router the packet is forwarded onto its next hop according to the per-hop behavior associated with that packet's class.

Diffserv Traffic classification & conditioning



Packets arriving to the edge router are first classified. The classifier selects packets based on the values of one or more packet header fields and steers the packet to the appropriate marking fn.

A packet mark is carried within the differentiated service field in IPv4 and IPv6 packet header.

In some cases an end user may have agreed to limit its packet-sending rate to conform to a declared traffic profile.

If the traffic profile is violated, out of profile packets are marked differently, it may be shaped or dropped at the network edge.

Per-Hop Behaviors

The second key component of the Diffserv architecture involves the per-Hop Behaviors (PHB) performed by Diffserv capable routers.

PHB is defined as "a description of the externally observable forwarding behavior of a Diffserv node applied to a particular Diffserv behavior aggregate"

1. A PHB can result in different classes of traffic receiving different performance.

2. PHB defines differences in performance among classes and it does not mandate any particular mechanism for achieving these behaviors.

3. Differences in performance must be observable and Measurable.

Types of PHB

1. Expedited Forwarding (EF) PHB
2. Assured Forwarding (AF) PHB

1. Expedited Forwarding PHB

It specifies the departure rate of a class of traffic from a router must equal or exceed a configured rate.

Provides minimum guaranteed link BW.

Assured Forwarding PHB

AF divides traffic into four classes & each AF class is guaranteed to provide with some minimum amount of BW and Buffering.

Rsvp (Resource Reservation protocol)

Rsvp is a Signaling protocol that allows appns. running in hosts to reserve resources in the Internet.

The Essence of Rsvp

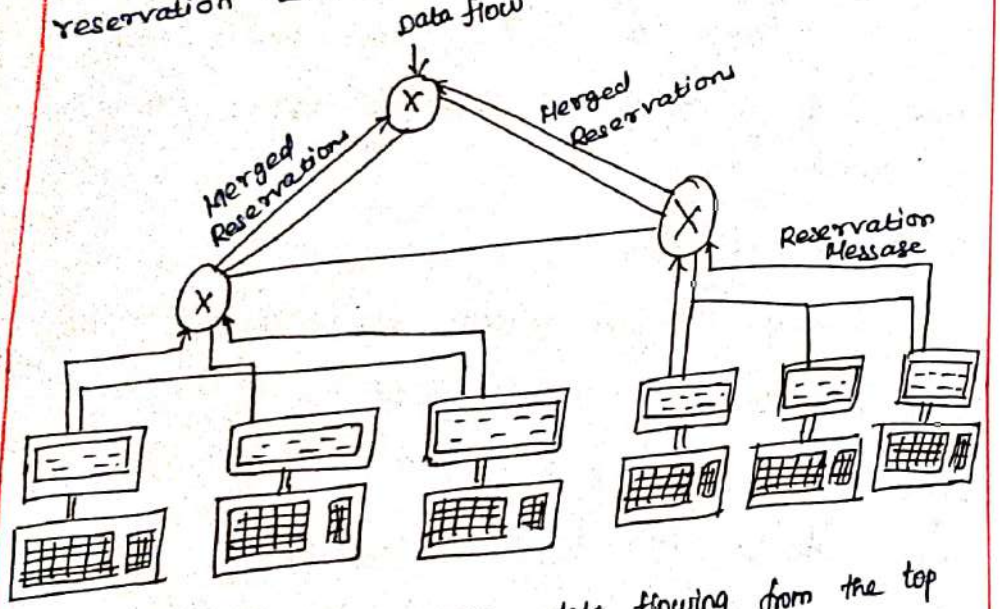
Rsvp protocol allows appns. to reserve BW for their data flows. It is used by a host, on the behalf of an appln. data flow to request a specific amount of BW from the n/w.

Rsvp is also used by the routers to forward BW reservation requests. To implement RSVP th receivers, senders and routers must be install the Rsvp Software.

Characteristics Of RSVP

It provides reservations for BW in multicast trees.

It is receiver-oriented that is receiver of a data flow initiates and maintains the resource reservation used for the flow.



A Multicast tree with data flowing from the top of the tree to hosts at the bottom of the tree. Data originates from the Sender and the reservation message originates from the receivers.

When a router forwards a reservation message upstream towards the Sender then the router may merge the reservation msg. with other reservation msg. arriving from downstream.

RSVP standard does not specify how the nlw. provides reserved BW to the data flow.

Once the reservations are in place and the routers in the Internet will provide the reserved BW to the data flows.

RSVP is not a routing protocol It does not determine the links in which the reservation are to be made.

Once the reservations are in place, the routers packet schedulers must provide the reserved BW to the data flows.