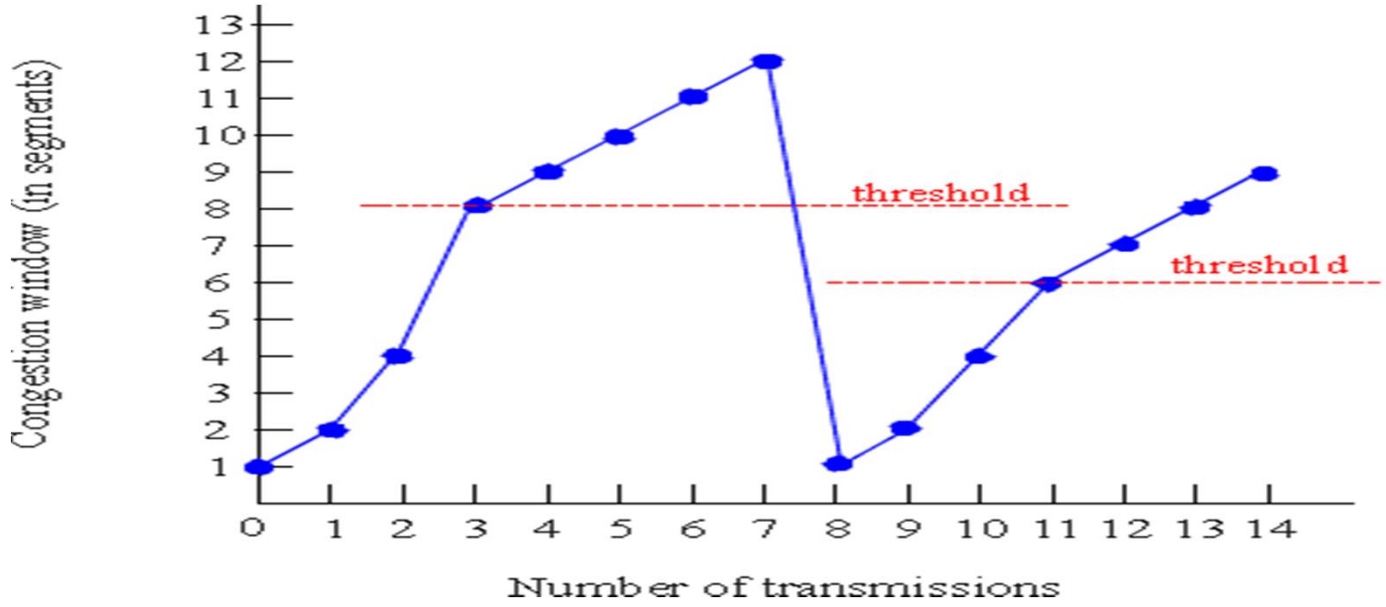
TCP-Congestion control



- If the congestion window is less than the threshold, it expands exponentially.
- If the congestion window exceeds the threshold, it expands in a linear way.
- The threshold is set to one half of the current congestion window whenever a timeout occurs, and the congestion window is then reset to one.

Real-Time Transport Protocol

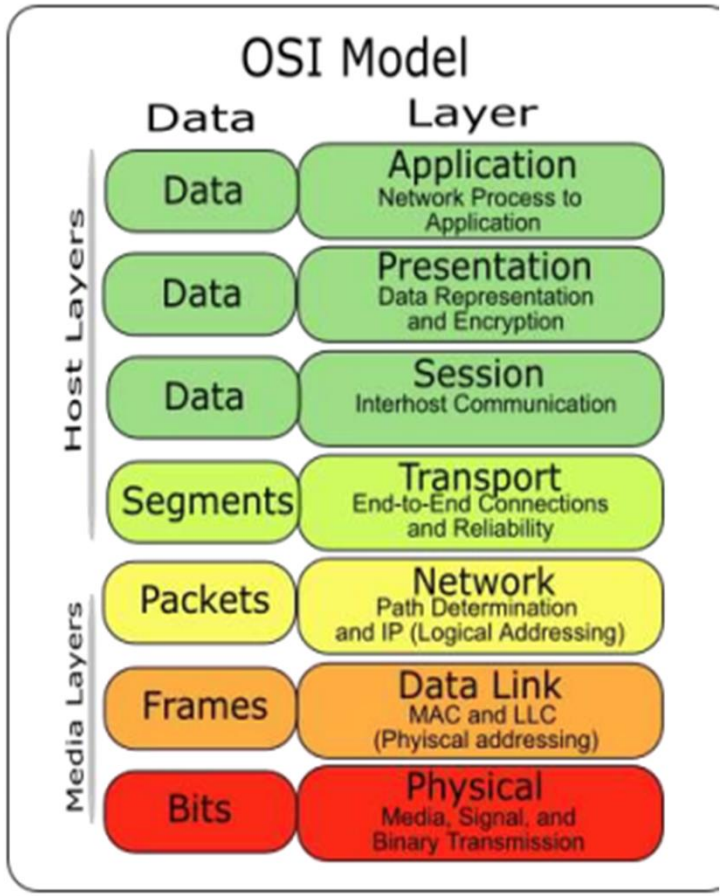
- End-to-end delivery services for applications transmitting real-time data, such as audio and video over multicast and unicast networks.

- Application layer protocol

- Typically used on top of IP and UDP
  - Layer **4** – UDP or TCP
  - Layer **3** – Internet Protocol IP
  - Layer **7** – RTP

- Applications that use RTP are:
  - Less sensitive to packet loss.
  - Very sensitive to packet delays.

  E.x:-
  - Video teleconferencing
  - Internet Telephony (VoIP)
  - Internet audio, video streaming



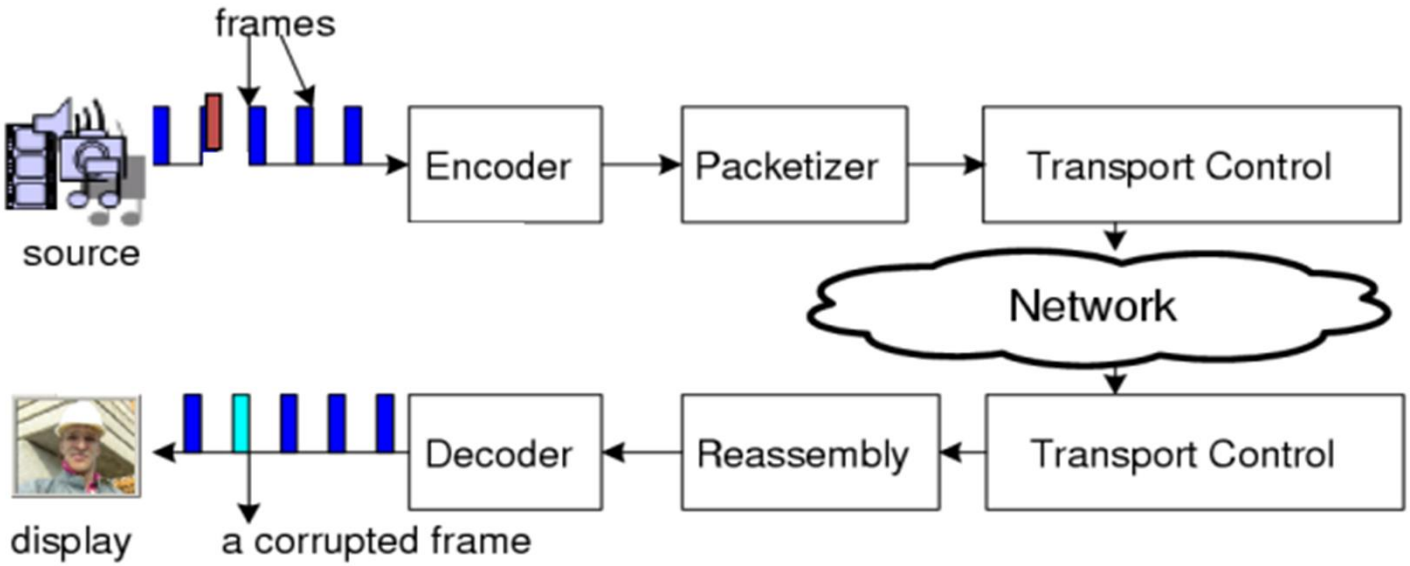
RTP Features

- All RTP and RTCP PDUs are sent to same multicast group (by all participants)

- **RTP** supports several file formats like MPEG and MJPEG but you can add extra formats.

- **RTP** also has jitter compensation, multimedia streaming (tolerates packet loss) and detection of out of sequence arrival in data attributes.

How RTP work?



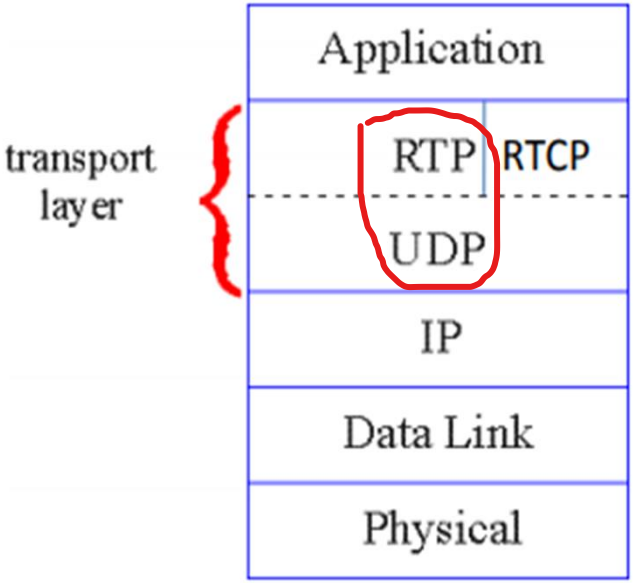
➢ **Why not TCP?**

- TCP does retransmissions → unbounded delays due to (Acks, Flow control, windowing)
- No provision for time stamping
- TCP does not support multicast
- TCP congestion control (slow-start) unsuitable for real-time transport (A-V media)

➢ **Why not UDP?**

- UDP offers datagram-like service
- Connectionless , Unreliable , Unordered
- No Flow , Error , Congestion control
- Port numbers

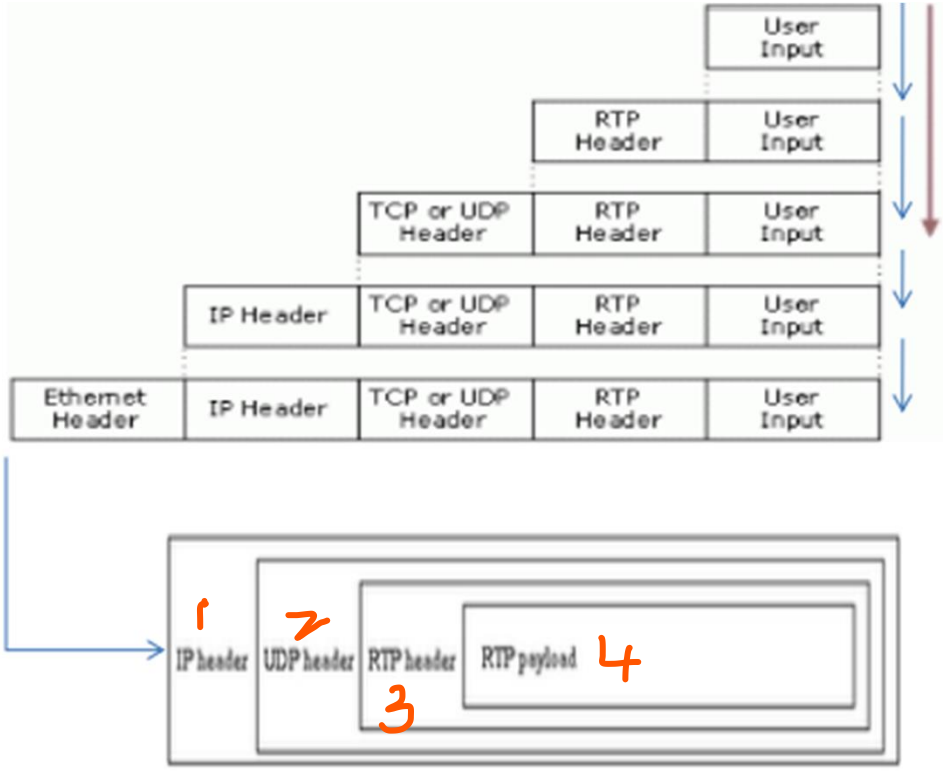
RTP + UDP usually used for multimedia services

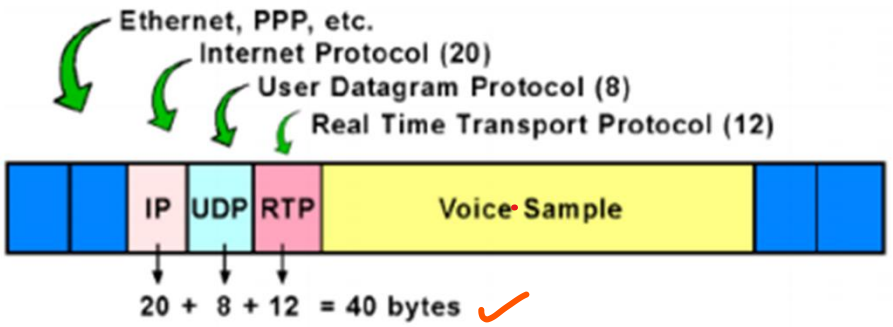


RTP Packets

Protocol architecture

Applications	
RTP & RTCP	
Other transport and network protocols	UDP
	IP

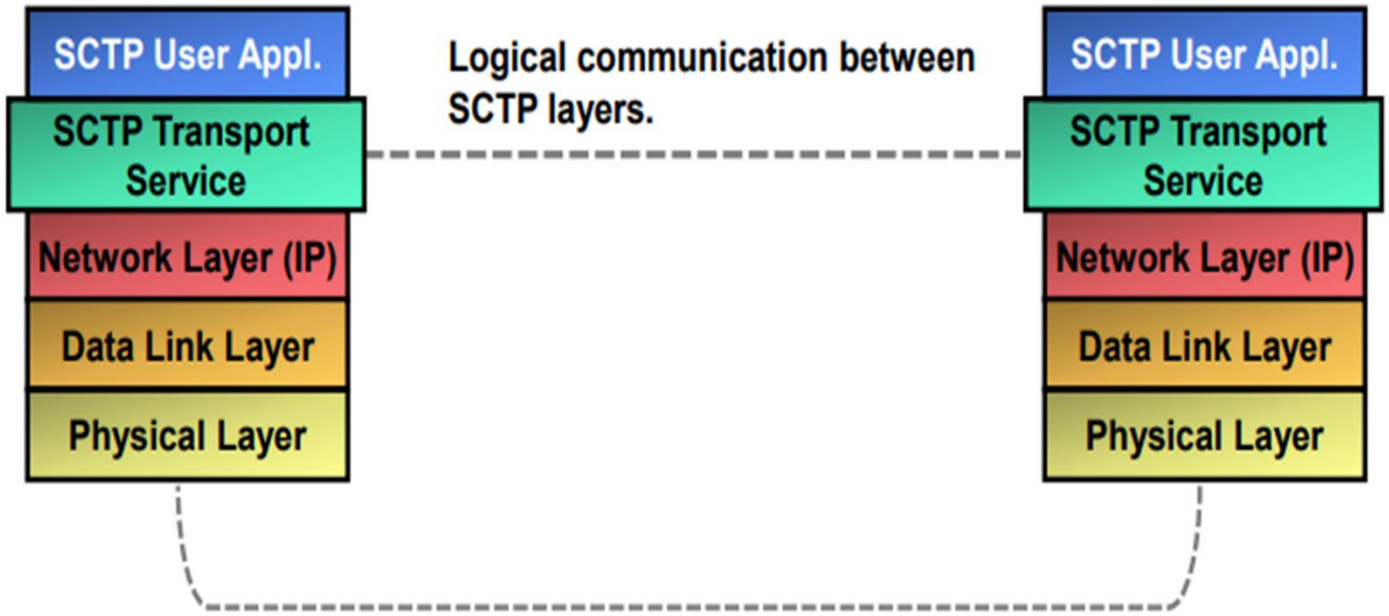




1. What is SCTP?

SCTP (Stream Control Transmission Protocol, RFC4960) is a transport protocol on OSI layer 4 (like TCP or UDP).
SCTP was specifically designed as a transport protocol for public telephony network signalling message transport. However, SCTP is generic and may supersede TCP in other applications as well.

Simplified OSI stack (session and presentation layers omitted):



2. Why use SCTP? (1/2)

SCTP has similar characteristics and applications as TCP (RFC0793), but includes some important improvements:

1. No head-of-line blocking:

TCP imposes a strict data ordering. However, if a user data message is lost during transit, all subsequent user data messages are delayed until the lost message has been retransmitted (= head-of-line blocking).
Some applications do not require a strict ordering of messages. E.g. applications that exchange unrelated application messages could cope with out-of-order messages (messages are simply processed as they arrive at the receiver). But TCP does not allow messages to pass each other.

2. No stream-oriented data transfer:

TCP is stream-oriented. This means that TCP treats data chunks transmitted by an application as an ordered stream of bytes (=octets in network speak). While this concept supports a wide range of applications (message oriented like email, character oriented like TELNET, stream oriented like video), it is unsuited in most applications because these exchange application level messages.
SCTP preserves application level message boundaries, thus liberating applications from implementing a framing protocol on top of TCP for delineating messages. SCTP simply maps application messages to chunks on the transmit path and back to application messages on the receive path.

2. Why use SCTP? (2/2)

3. Multihoming:

Since a TCP connection is defined by the quadruple source IP, destination IP, source port and destination port, TCP does not support multihoming (use of multiple IP addresses on either side of the connection to allow multiple transmission paths through the network thus increasing reliability).

SCTP has built-in support for multihoming which offloads high-availability applications from implementing this feature.

4. Certain protection against denial of service attacks:

The connection setup of TCP allows denial of service attacks, particularly SYN attacks. Each time the TCP layer receives a SYN packet for setting up a new connection, it allocates a data structure for storing connection parameters (called Transport Control Block). Flooding with a high number of such SYN packets may lead to memory exhaustion.

SCTP implements a procedure to avoid or at least make it more difficult for an attacker to launch a connection denial of service attack (4-way connection setup with state cookie).

TCP ⇒ 3-way

SCTP ⇒ 4-way

3. Main features of SCTP

1) **Multiple data stream support:**
Support for multiple logical streams of application messages. Ordering of messages within a stream. Avoidance of head-of-line blocking.

2) **Message oriented data transfer:**
Transport of user data as messages, preservation of application level message boundaries.

3) **Multihoming for network redundancy:**
Use of multiple IP addresses per SCTP endpoint to allow transmission of data chunks through different network paths.

4) **Denial of service attack protection:**
Some measures to protect against denial of service attacks such as connection setup flooding.

5) **Fragmentation:**
Detection of path MTU and fragmentation of data chunks to fit into the available path MTU.

6) **Error correction:**
Acknowledged error-free, non-duplicated data transfer.

7) **Congestion avoidance:**
Similar functionality as in TCP to avoid congestion to build up in the network.