VoIP TECHNOLOGY

The development of wireless N/w. Involves a migration from circuit switched Networks into packet switched Configuration for both wide Voice and data.

A No. of packet switched N/w. are used such as Asynchronous Transfer Mode (ATM) or Frame Relay.

The ultimate goal of these N/w. is to use the Internet Protocol (IP).

Migration of Global system for mobile communication (GSM) to the universal Mobile Telecommunication Service (UMTS) can be obtained by use of Frame Relay followed by ATM and IP.

The IP transport of voice & a recent development Voice over IP (VOIP) will be used in 3G wireless N/w.

VOIP

IP has a no. of advantages over circuit switching.

Has Advanced Voice Coding techniques such as Adaptive Multi Rate (AMR) coder used in Enhanced Data Rates for Global Evaluation (EDGE) and UMTS N/w.

Ip → Practically implemented in everywhere, not only is it supported by every pc, also supported by handheld computers and personal organizers.

Ip is used to carry both voice and data.

The Basics of Ip Transport

Open system Interconnection (OSI) model developed by ISO.

Seven layers and each layer perform its own task,

Ip (Internet protocol) passes a packet of data from one router to another router through the N/W to the appropriate destination by identifying the destination IP addr. in IP packet header.

IP is inherently unreliable and provides no Protection against a loss of packets.

Packets are transmitted from source to destination using router.

Packets will take different routes through the network so different packets can have different delays and also that packets may arrive at the destination out of sequence.

OSI models & protocol Stacks

Application Layer	Layer 7
Presentation Layer	Layer 6
Session Layer	Layer 5
Transport layer	Layer 4
Network layer	Layer 3
Datalink Layer	Layer 2
Physical Layer	Layer 1

Applications & Services
TCP or UDP
IP
Data link
physical

TCP.

Transmission Control protocol used in Data N/w. in order to ensure an error free and in sequence delivery of packets to the destination application. This protocol resides on the layer above IP.

When a session is to set up b/w. two appln. then the appln. data is first passed to TCP where TCP header is applied after that the data is passed to IP where an IP header is applied finally it is forwarded through the N/w.

TCP header must contain source port number & destination port no. along with other information such as sequence numbers, acknowledgement numbers and checksum.

Source and Destination port nos => Identify the appl" at each end.

Sequence nos. & acknowledgement nos. => Enable the detection of lost packets

Checksum => Enables the detection of corruption packets.

TCP uses these information elements to request the retransmission of lost or corrupted packets and to deliver packets to the destination application in the correct order.

TCP is a connection oriented protocol. So do all the actions first it establishes a connection b/w peer TCP instances at each end.

This involves a sequence of messages b/w. TCP instances prior to the transfer of user data.

UDP

User Datagram protocol

Instead of using TCP at layer 4 the another option is UDP.

UDP is a connection less protocol.

It is simple protocol

It does not support recovery from loss or error and does not ensure an in-sequence delivery of packets.

UDP is only suitable for simple request response types of transactions rather than the sequential transfer of multiple packets.

UDP is used in appln. like Domain Name Service (DNS) and a classic one shot Request Response protocol.

VoIP challenges

Any commercial N/w. must satisfies the requirements such as,

1. Good speech quality
2. Low Transmission Delay
3. Low Delay variation
4. Low Loss Transmission

Good speech quality is a strong requirement of any Commercial, wireless and other Kinds of N/w. It has been achieved through 64Kbps (G.711) voice Coding and the use of Circuit Switching, which

Low loss transmission can be achieved through the use of TCP at layer 4. But TCP causes excess delay of packet to reach the destination

In order to minimize delay in the delivery of the voice packets using TCP we can use UDP at layer 4. But UDP offers no protection against packet loss.

In case of speech, excessive jitters (delays) are more disturbing than occasional packet loss.

Excessive packet loss is unacceptable but a limited amount can be tolerated without noticeable speech quality degradation. when transporting voice UDP is chosen at layer 4 rather than TCP.

In VoIP we need to support more features that are not supported by UDP,

1. The destination appln. needs to know the coding scheme used by the source appln. to decode the voice packets.

2. The appln. also needs timing information so that packets can be played out to the user in a synchronized manner.

3. When packets are lost, so that a previous packet could be replayed to fill the gap if appropriate.

For these needs, Real Time Transport protocol (RTP) has been developed.

This protocol Resides above UDP in the protocol stack.

Whenever a packet of coded voice is to be sent, it is sent as the payload of an RTP Packet.

Packet consists of,

1. RTP Header
2. Sequence number
3. Time stamp
4. Identification.

RTP Header => Provides which voice code scheme is used.

Time stamp -> for the instant at which the voice packet was sampled.

Identification => Source of the voice packet

RTP has a companion protocol known as RTCP (Real time transport Control protocol)

RTCP is a signaling protocol

It does not carry coded voice packets.

It includes a no. of messages which are exchanged b/w. session users.

These messages provide feedback regarding the quality session.

Whenever a RTP session is opened, RTCP session is also implicitly opened.

This means that, when a UDP port no. is assigned to RTP session for the transfer of voice packe a separate port no. is assigned for RTCP messages.

VOIP Protocol layers

Voip application	Layer 6 and 7
RTP, RTCP	Layer 5
UDP	Layer 4
IP	Layer 3
Data link	Layer 2
Physical	Layer 1

RTP port no. will always be even and the corresponding RTCP port no. will be the next highest no. So, it is odd no.

RTP & RTCP donot guarantee minimal delays, low jitter or low packet loss. so in order to do that other protocols are required.

H.323

In all telephony n/w. has a specific signaling protocol.

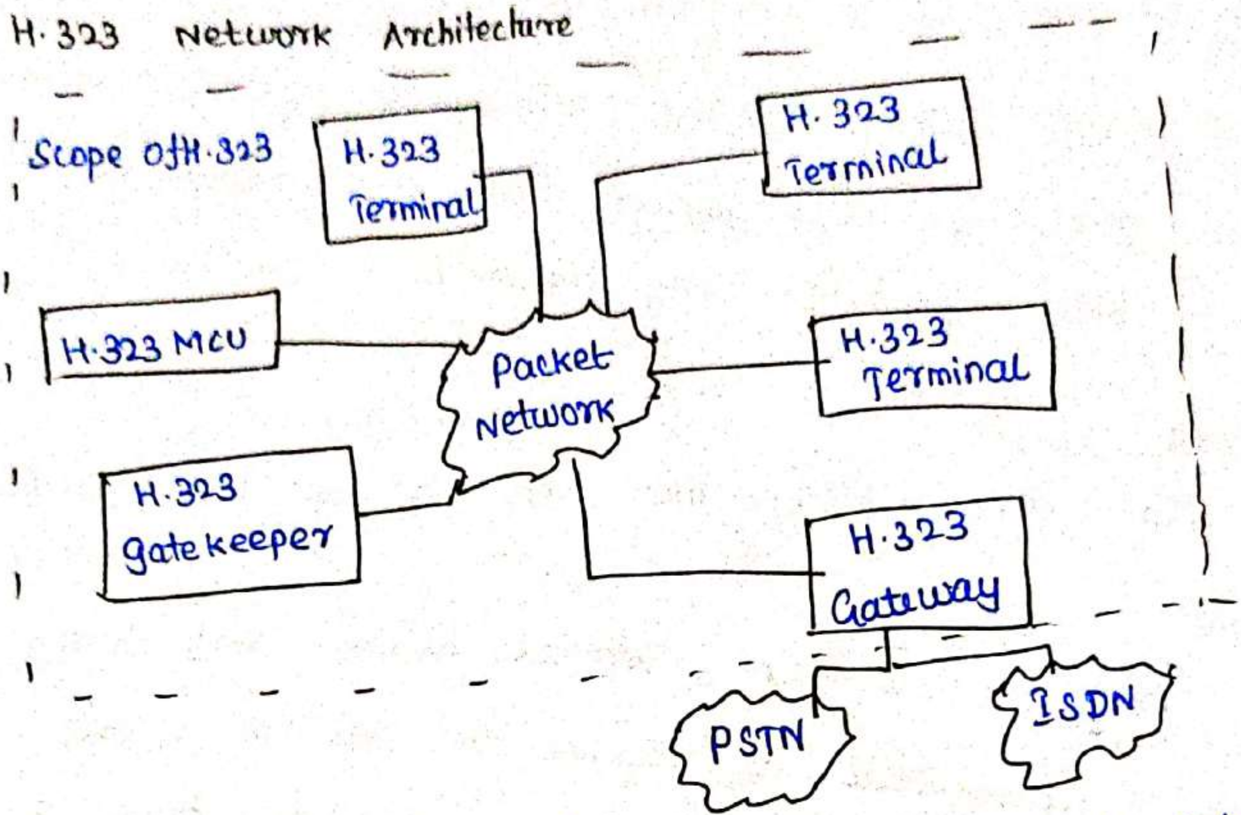
These protocols are invoked before and during a call to communicate a desire to set up a call, to monitor call progress and to gracefully bring a call to a conclusion. Eg: ISDN user port (ISUP)

The first successful set of protocols for VoIP was developed by International TeleCommunication union (ITU). This set is known as H.323.

It is packet-Based Multimedia communication sly. Recently new protocols have been developed is known as Session Initiation protocol (SIP)

SIP & H.323 are two VoIP signaling Protocols used.

H.323 Network Architecture



This architecture involves H.323 terminals, gateways, gate keepers and Multipoint Controller Units (MCUs).

Objective of H.323 => To Enable the exchange of media streams between H.323 endpoints, where an H.323 end point is an H.323 terminal, gateway or a MCU.

H.323 Terminal

H.323 Terminal is an endpoint that offers real time communications with other H.323 end points. Typically an end-user communications device. Supports atleast one audio code and H.323 Gateway video codes.

H.323 Gateway

A gateway is an H.323 endpoint that provides translation services between the H.323 network and another type of n/w. such as Integrated Services Digital Network (ISDN) or public switched Telephone Network (PSTN).

One side of gateway supports H.323 signaling and terminates packet media.

The other side of gateway interfaces to a circuit switched N/w. and supports the transmission characteristics and signaling protocols.

Translation is performed internally within the gateway.

Translation is totally transparent to other nodes in the circuit switched network and in the H.323 n/w.

Communication b/w. terminals needs to pass via an external n/w. such as the PSTN.

H.323 Gatekeeper

A gatekeeper is an optional entity within an H.323 n/w.

It controls a no. of H.323 terminals gateway and multipoint controllers (MCs).

It authorizes n/w. access from one or more endpoints and may choose to permit or deny any given call from an endpoint within its control.

The set of terminals, gateways and MCs controlled by a single gatekeeper is known as a zone.

A zone can span multiple n/w. or subn/w. and it is not necessary that all entities within a zone be contiguous.

Multipoint controller units (MCUs)

MC is a H.323 endpoint that manages multipoint conferences b/w. three or more terminals and gateways.

H.323 Protocols

<table>
<tr><td>Audio / video application</td><td colspan="4">Terminal / Application protocol Control</td></tr>
<tr><td>Audio / video codecs</td><td>RTCP</td><td>H.225.0 RAS signaling</td><td>H.225.0 call signaling</td><td>H.245 Control signaling</td></tr>
<tr><td colspan="3">UDP</td><td colspan="2">TCP</td></tr>
<tr><td colspan="5">IP</td></tr>
<tr><td colspan="5">Layer 2 - Data link</td></tr>
<tr><td colspan="5">Layer 1 - physical</td></tr>
</table>

The exchange of media is performed using RTP over UDP and wherever there is RTP, there is also RTCP.

H.225.0 & H.245 => Define the actual messages that are exchanged between H.323 end points.

Generic protocol

H.225.0 Protocol

Two - port Protocol,

one port => variant of ITU - T recommendation Q - 931, ISDN layer 3 Specification.

used for the establishment and tear-down of Connections b/w. H.323 end points. This type of signaling is known as Call signaling or Q.931 signaling.

Other part of It is known as Registration, Admission and Status (RAS) signaling.

used b/w. end points and gatekeeprs enables a gate keeper to manage the end points with in its zone.

H.245 protocol

Control protocol. used b/w. two or more end points.

To manage the media streams b/w. H.323 session participants

H.245 operates by the establishment of one or more logical channels b/w. end points.

These logical channels carry the media streams b/w. the participants and have a no. of properties like media type, bit rate.

Signaling Protocol

3 Signaling Protocol RAS, Q.931 and H.245 may be used in the established, maintenance and tear down of a call.

Actions taken,

1. It may use RAS signaling to obtain permission from a gate keeper.

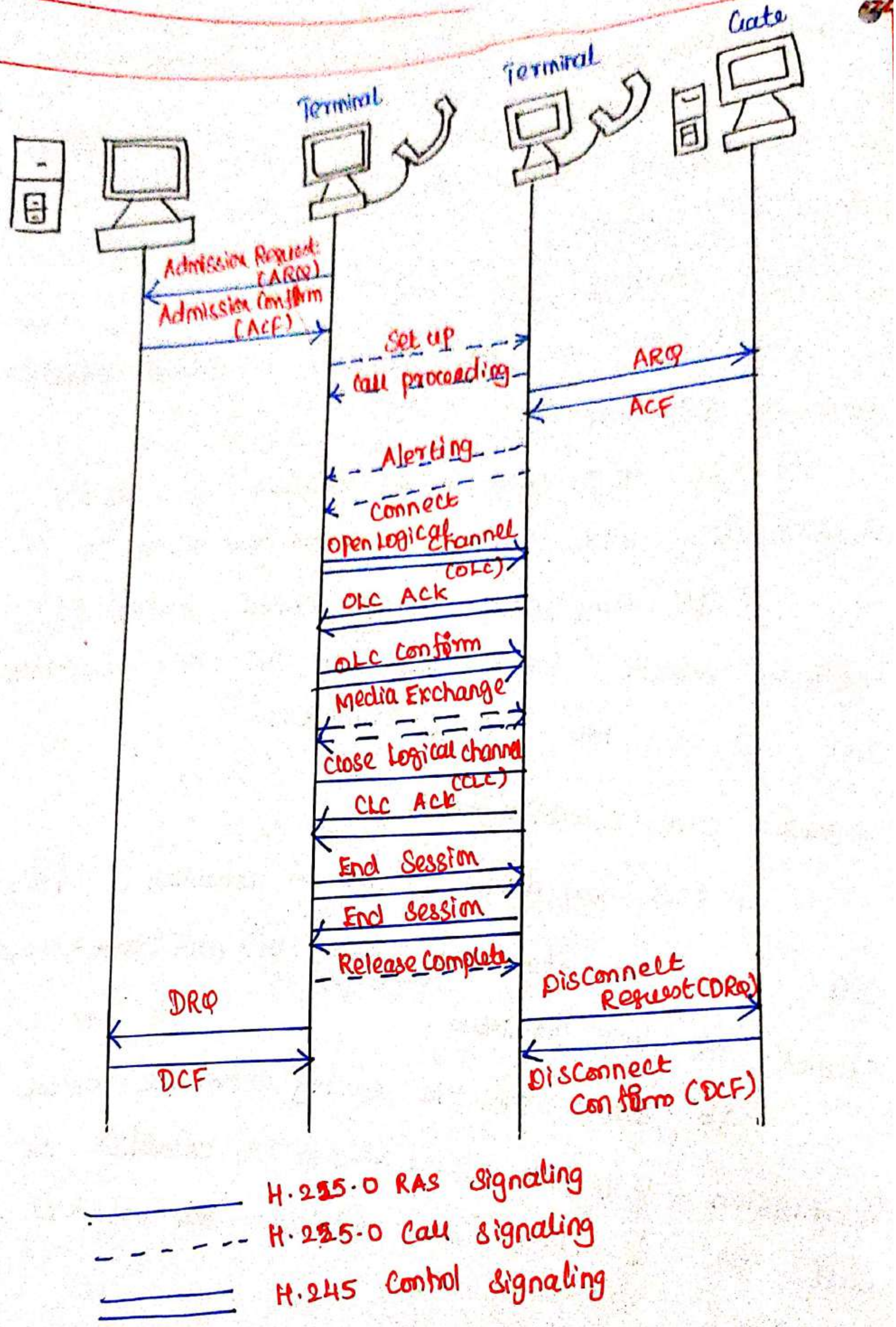
2. It may use Q.931 signaling to establish the call Communication with other call points and set up the call

3. It may use H.245 Control signaling to negotiate media Parameters with the other end points and set up the media transfer.

H.323 Call Establishment

H.323 endpoints need to establish a VoIP call b/w. two terminals and different gate keeper Control the two terminals.

At first step, the calling terminal request Permission from its gate keeper to establish the call. This is done with Admission Request (ARQ) message.


Gate
Terminal
Terminal
Admission Request (ARQ)
Admission Confirm (ACF)
Set up
Call proceeding
ARQ
ACF
Alerting
Connect
Open Logical channel (OLC)
OLC Ack
OLC confirm
Media Exchange
Close Logical channel (CLC)
CLC Ack
End Session
End session
Release Complete
DRQ
DCF
Disconnect Request (DRQ)
Disconnect Confirm (DCF)
H.225.0 RAS signaling
H.225.0 Call signaling
H.245 Control signaling

The terminal indicates the type of call identifier, a call reference value and information regarding the other party or parties to participate in the call.

The information regarding the other party to the call includes one or more aliases and for signaling addresses.

Most important parameter in ARQ is Bandwidth

Bandwidth parameter specifies the amount of BW required in units of 100bps.

If a two party call is needed, with each party sending voice at 64 kbps then the BW required is 128 kbps and value carried in the BW parameter is 1280.

The purpose of BW parameter is to enable the gate keeper to reserve resources for the call.

The gatekeeper indicates a successful admission by responding to the end point with an Admission Confirm (ACF) message.

The difference b/w ARQ & ACF => when a parameter is used in ARQ, it is simply a request from the endpoints, the end point must stay within the BW limitations imposed by the gatekeep

Another parameter which is common in both ARQ and ACF is call model parameter, which is optional in ARQ and mandatory in the ACF.

In ARQ => Call model indicates whether the end points wants to send call signaling directly to the other party or prefers that call signaling be passed via the gatekeeper.

In ACF => call model represents the gatekeepers decision as to whether call signaling is to pass via the gatekeeper or directly between the terminals.

The set up message is the first-call signaling message sent from one terminal to other to establish the call.

The message must contain the Q.931 protocol discriminator, call Reference setup, a Bearer Capability and user-user information content.

Bearer capability information => used in the circuit switching.

It does not map very well on an IP network.

A number of parameters are included within the mandatory user-to-user information element.

The user-to-user information element is included in all H.225.0 call signaling messages.

Alerting message is optional it indicates the called device is ringing.

When the called party answers, the called terminal returns a connect message it must be sent if the call is to be completed. Some of the messages from the called party to calling party is optional such messages are called proceeding and Alerting.

H. 245 is a control protocol that manages the establishment and release of media sessions. This task can be done through logical channels, where it is unidirectional RTP stream from one party to the other.

Logical channel

A logical channel is opened by sending an open logical channel (OLC) request message.

This message has forward logical channel parameters. It consists of type of data to be sent, an RTP session ID, an RTP payload type.

Scanned with CamScanner

If the recipient of the message wants to accept the media to be sent, then it will return an open logical channel ACK message.

H.323 channel is a bidirectional logical channel. Establishing two logical channels, one in each direction.

Upon receipt of open logical channel Ack the originating end point responds with an open logical channel confirm message to indicate that all is well. Now RTP streams and RTCP messages can flow in each direction.

H.323 Call Release

The first step of call release process involves closing the logical channels that have been created by H.245 signaling and closing the RTP streams between the users.

Closing a logical channel involves the sending of a close logical channel message.

In case of a successful closure the far end should send the response message close logical channel ACK.

A logical channel can be closed only by the entity that created it in the first place.

The receiving end point in a unidirectional channel can request the sending end point to close the channel. It can perform by sending the request channel close message.

Once all logical channels in a session are closed the session itself is terminated when an endpoint sends an end session command message.

Each end point uses the Disconnect Request (DRQ) message to request permission from its gatekeeper to disconnect.

The gatekeeper responds with the Disconnect Confirm (DCF) message.

SIP (Session Initiation protocol)

SIP is powerful alternative to H.323 Protocol.

Advantage Compared with H.323 protocol,

More flexible solution

Simpler than H.323

Easier to implement
Better suited to support of intelligent user devices.
Like H.323, SIP is simply a signaling protocol and does not carry the voice packets.

SIP - Network Architecture
SIP defines two basic classes of n/w. entities like clients and servers.
A client is also known as a user Agent client. it is an application program that sends SIP requests.
A server is an entity that responds to those requests. So SIP is called a client-server protocol.

Client
A client may be found within a user's device. Eg: A SIP phone may also be found with in the same platform as a server.

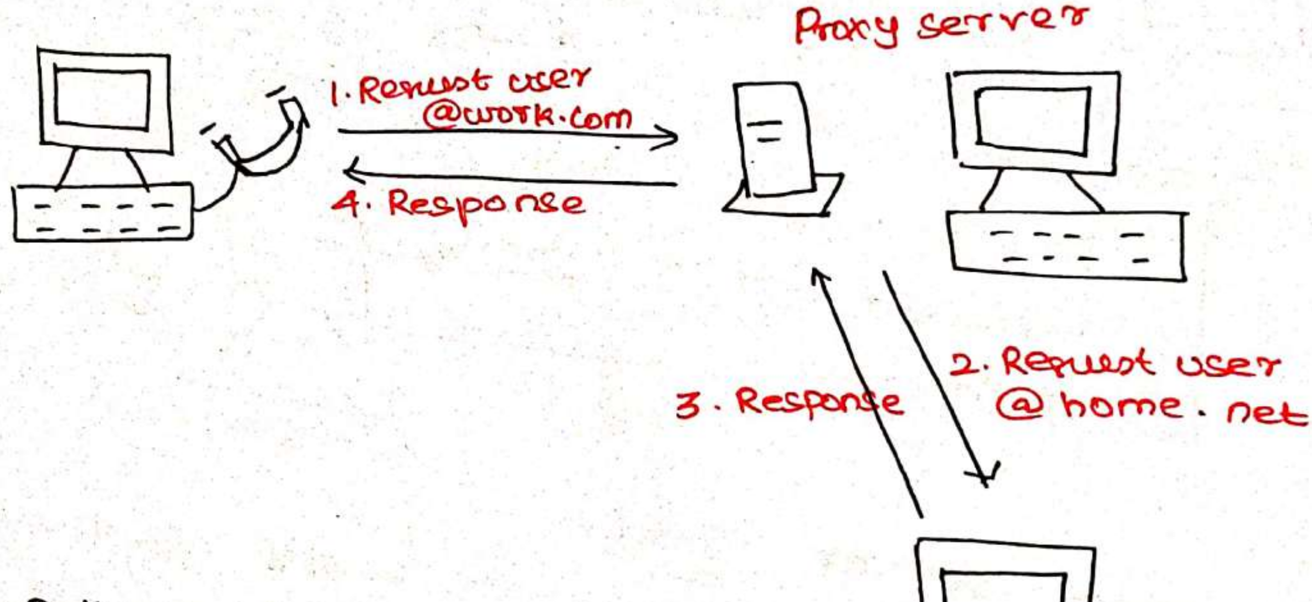
Server
4 types of servers are available,
1. Proxy servers 2. Redirect servers
3. User agent servers 4. Registrars.

1. Proxy Servers

A Proxy Servers acts similarly to a proxy server used for web access from a Corporate LAN.

Clients send requests to the proxy, which either handles those requests itself or forwards them on to other services, perhaps after performing some translation.

Proxy servers perform both receives requests and sends request, which incorporates both server and client functionality.



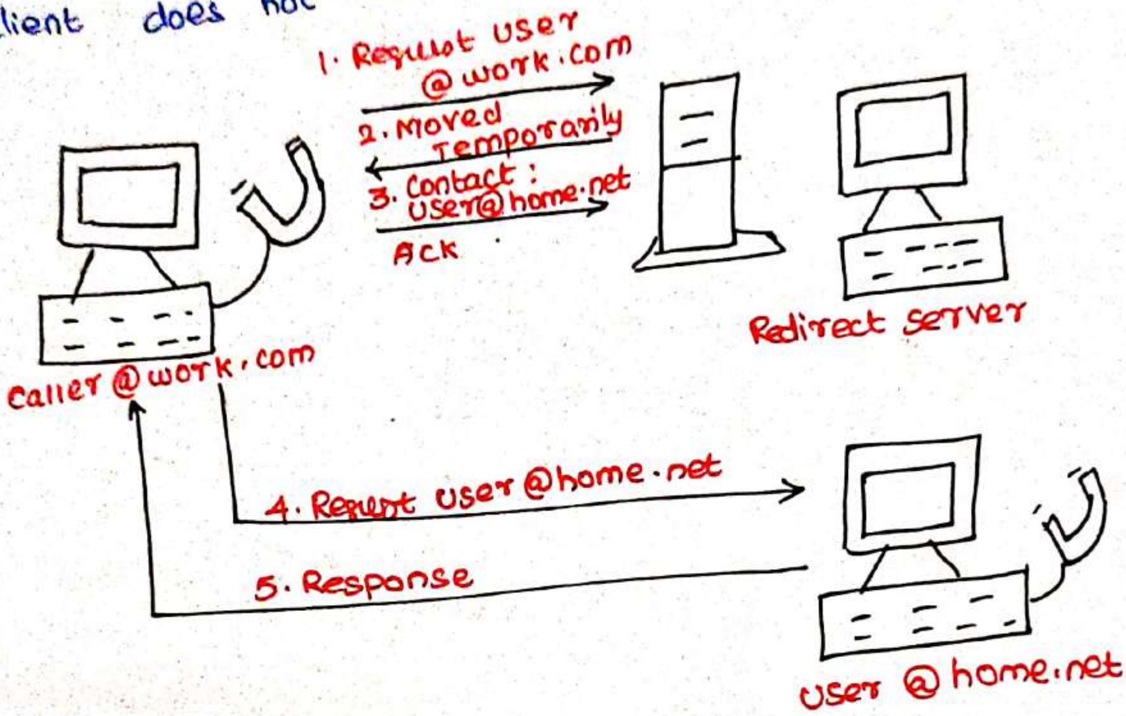
2. Redirect Servers

A redirect server is a server that accepts SIP requests, maps the destination address to zero or more new addresses and returns the translated address to the originator of the request.

The originator of the request may send requests to the address returned by the redirect server.

A redirect server does not initiate any SIP requests of its own.

The difference b/w. proxy and redirect server is that, in case of a Redirect server, the originating client does not actual forwarding of the call.



3. User - Agent server

A user agent server accepts SIP requests and contacts the user. A response from the user to the user-agent server results in a SIP response on behalf of the user.

A SIP device such as SIP enabled phone will function as both a user agent client and a user agent server.

Acting as a user-agent client is able to initiate SIP requests and acting as a user-agent server can receiver and respond to SIP requests.

It can able to initiate a calls & receive calls. It is a client-server protocol to be used for peer-to-peer communication.

A. Registrar

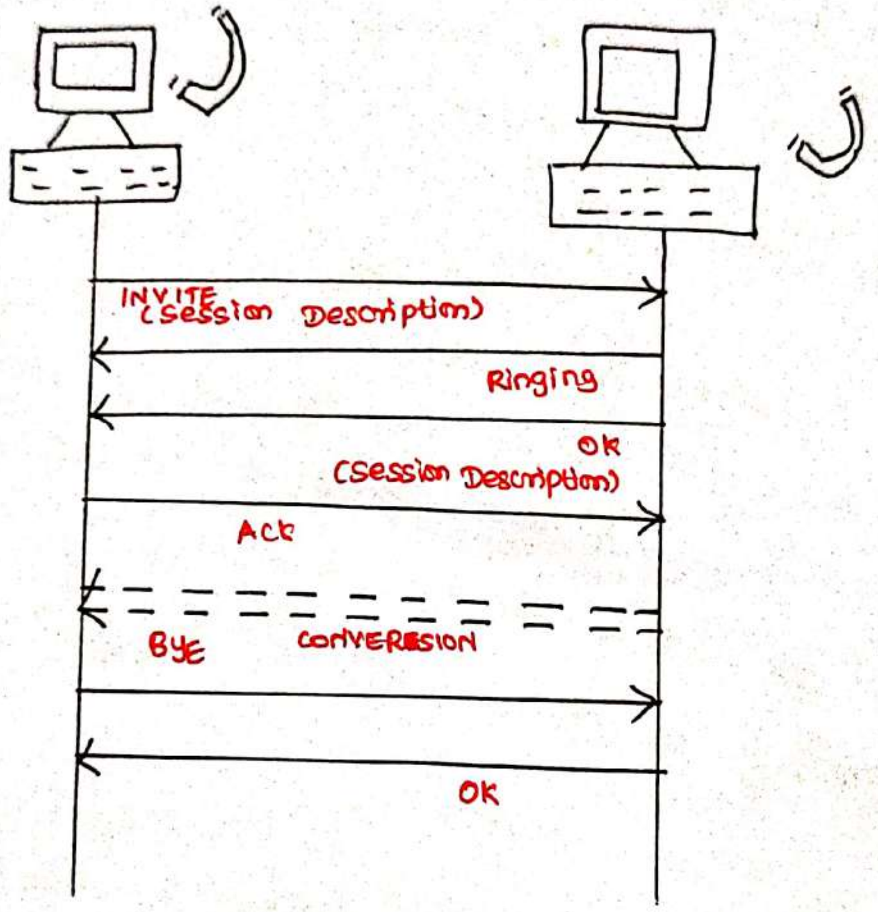
A Registrar is a Server that accepts SIP Register requests. SIP includes the concept of user registration, it means a user signals to the network that is available at a particular address.

Typicaly, a registrar will be Combined with a proxy or redirect Server.

Registration in SIP server a Similar purpose to location updating in a GSM network.

SIP Call Establishment

At a high level, SIP call establishment is very simple. The process starts with a SIP INVITE message, which is used from the calling party to the called party.



This message invites the called party to participate in a session or call, which includes INVITE message a session description also send.

It gives the description of media that the calling party wants to use.

Scanned with CamScanner

This description includes the voice coding schemes, IP address and a port number.

Voice coding schemes are used by caller and port number is used by the called party for sending media back to the caller.

After transmitting INVITE message subsequently the called party answers the call, which generates ok response back to the caller.

The OK response is actually indicated by the status code value of 200 in the response.

The 200 (OK) response contains a session description, IP address and a port no.

Session Description indicating the media that the caller wants to use and port no. to which the caller should send packets.

After receiving the OK response, the caller responds with ACK to confirm that the OK response has been received.

SIP call establishment is a simple process because the signaling pass via one or more proxy servers. SIP call establishment is much simpler than the H.323 process.

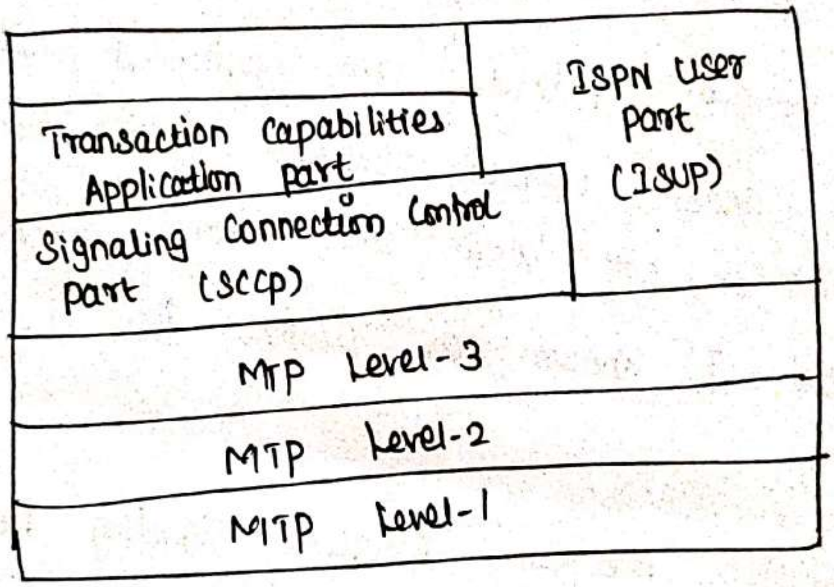
VoIP and SS7

VoIP has H.323 and SIP for support in traditional telephony.

SS7 is mobile networks. So VOIP based network is to communicate with any traditional network as well as inter network with SS7.

To support this, IETF has developed a set of protocols known as sigtran

Signaling System 7 (SS7) protocol stack



The bottom three layers are called the message Transfer part (MTP). This is a set of protocols responsible for getting a particular SS7 message from the source Signaling point to the destination Signaling point.

Isup is used for establishment of regular phone calls and sccp used in the establishments of regular phone calls.

sccp is mostly used for the transport of higher layer applications such as GSM.

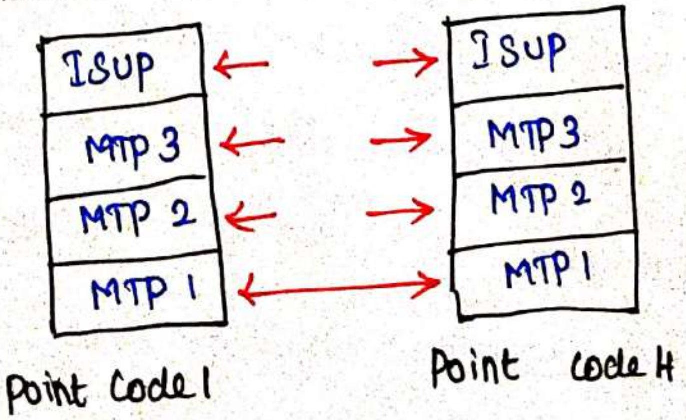
Mobile Application part (MAP) or the Inteligent Network Application part (INAP)

Many network applications use Services of the Transaction capabilities Application part (TCAP) and it uses the Services of sccp.

sccp provides an enhanced addressing mechanism to enable signaling between entities even when those entities do not know each others signaling address. This address is known as Global title addressing.

3 scenarios.

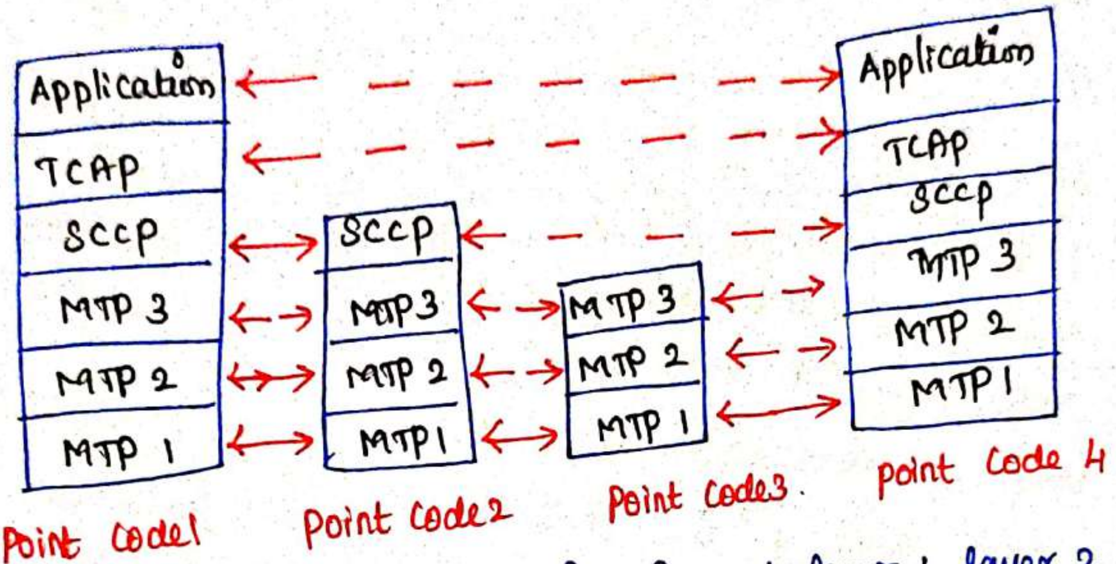
A. Communication between Adjacent signaling points



The Two entities represent by Point code 1 and point Cod 4. Communicate at layer 1

At this layer, a peer-to-peer relationship exists between the two entities. point Code is another name of Signaling addresses.

B. Communication between Non-Adjacent signaling points



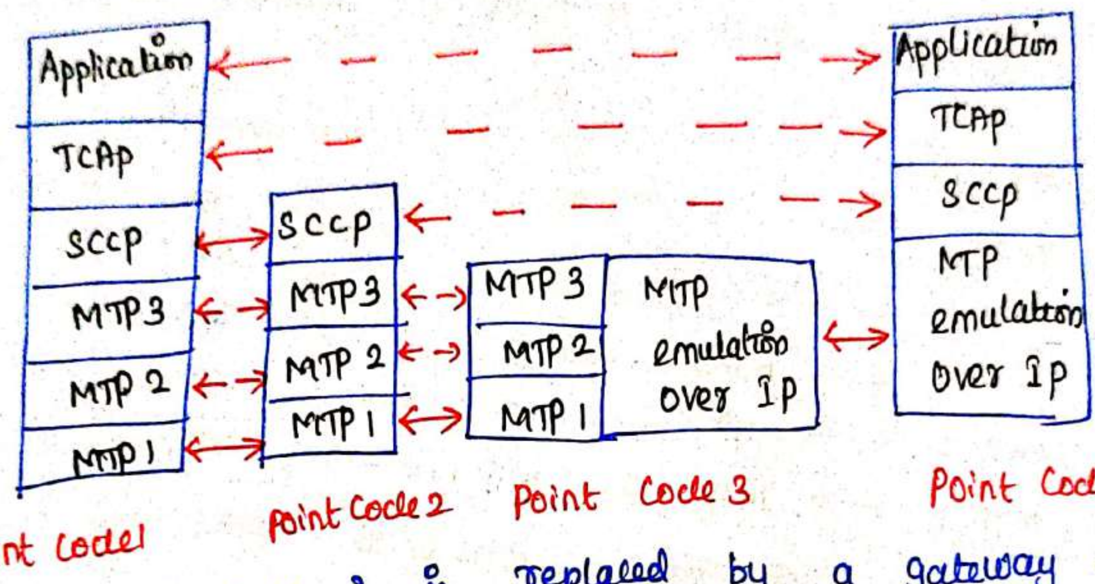
A peer-to-peer relationship at layer 1, layer 2 and layer 3 between point codes 1 and 2, 2 and 3, 3 and 4.

At the sccp layer, a peer-to-peer relationship exists between point codes 1 and 2 and 2 and 4.

At TCAP and application layers, a peer-to-peer relationship Can only take between point codes 1 and 4.

Communication between code point 2 and 4 takes place means the sccp layer at each point code knows only about the layer above (TCAP) the layer below it (MTP3) and corresponding sccp peer.

C. Communication between SS7- based & IP- based Applications



Here, Point Code 3 is replaced by a gateway that Supports standard SS7 on one side & IP- based MTP emulation on other side.

point code 4 does not support the lower SS7 layers at all it can support MTP emulation over IP

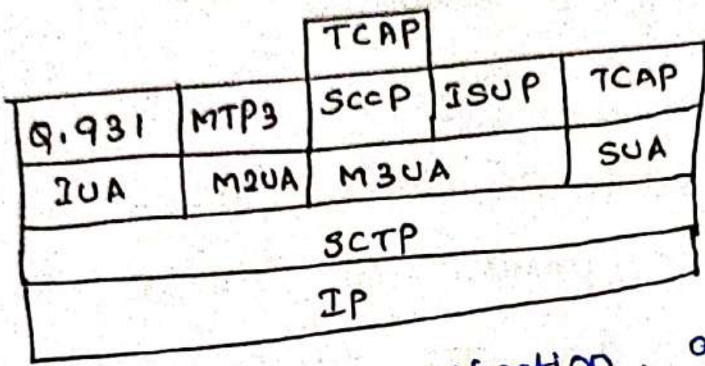
The MTP emulation at point code 4 appears to the SCCP layer as standard MTP then the layer SCCP does not care any layers above SCCP.

The SCCP layers at point code 1 & 2 do not care so it is possible to implement SS7 based appln. at Point code 4 without implementing whole SS7 stack.

Sigtran Protocol Suite

Above IP we have protocol known as the stream control transmission protocol (SCTP).

To obtain the function of neither UDP nor TCP offer both the speed and reliability required of a transport protocol used to carry signaling.



In the SCTP specification, a user is known as an upper layer protocol (ULP).

A ULP can be any of the protocols above the SCTP layer. Each of the protocols above SCTP is an adaptation layer.

In adaptation layer we have IUA, M2UA, M3UA and SUA. Each of the adaptation layers uses the same primitives to and from the layer above. These are used by equivalent SS7 layer.

SS7 MTP2 - User Adaptation layer (M2UA)

This layer provides adaptation between MTP3 and SCTP.

It provides an ~~into~~ interface between MTP3 and SCTP such that standard MTP3 may be used in the IP network without MTP3 appln. S/w realizing that messages are being transported over SCTP & IP instead of MTP2.

SS7 MTP3 - User Adaptation Layer (M3UA)

This layer provides an interface between SCTP and those appln. ~~the~~ that typically use the services of MTP3. M3UA and SCTP enable seamless peer-to-peer communication between MTP3 user appln. in SS7 n/w. the IP n/w. and identical appln. in SS7 n/w.

SS7 SCCP - User Adaptation Layer (SUA)

This layer provides an interface b/w. SCCP user appln. and SCTP.

Appln. such as TCAP use the service of SCCP in the same way that they use the service SUA in the SS7 n/w.

Scanned with CamScanner

ISDN Q.921- User Adaptation layer (IUA)

This layer is the sigtran equivalent of Q.921 Data Link layer which is used to carry Q.931 ISDN Signaling.

Stream Control Transmission Protocol (SCTP)

SCTP provides the reliable and fast delivery of Signaling messages.

Reliable because it is used for detection and recovery of lost of corrupted messages.

SCTP is faster than TCP because it avoids head of line blocking and it has more efficient ~~retrans~~ retransmission mechanisms than TCP.

one-way highway between endpoints then the individual streams are analogues to the individual traffic lanes on that highway.

Advantages of stream

Resources or Queues are allocated individualy to each stream.

A message from one stream does not have to wait in a queue behind a message from another stream.

Scanned with CamScanner

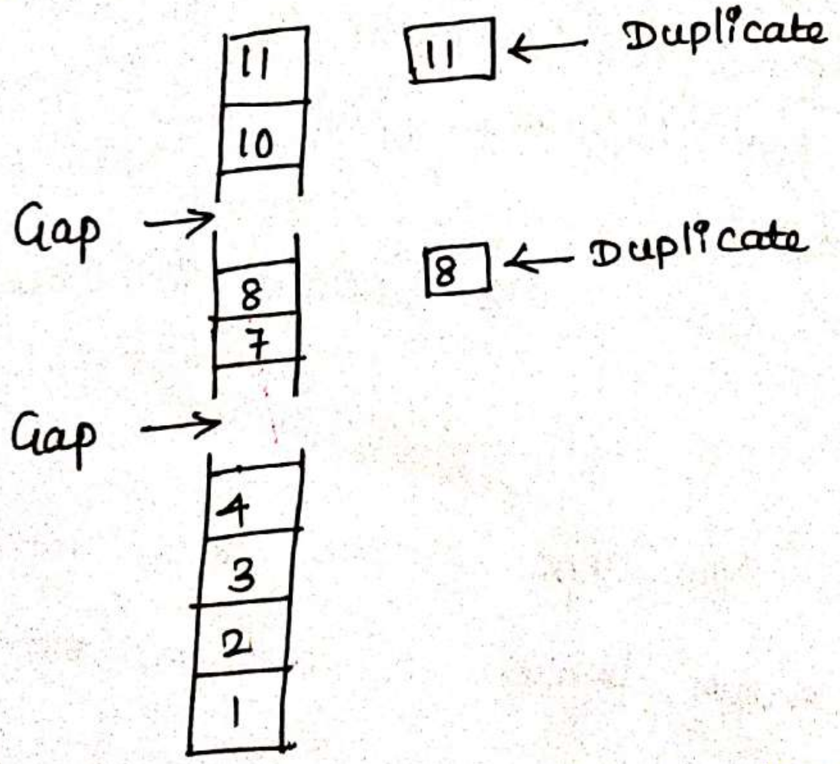
Retransmission

Retransmission in SCTP is based on the SCTP Packets carrying user data (chunks)

chunks include a Transmission Sequence Number (TSN).

The receiver of the chunks to make sure that all chunks have been received by ensuring that no gap exists in TSN.

If a gap is found, then SCTP enables the receiver to specify which TSNs are missing and only those TSNs need to be retransmitted, which is more efficient than TCP.



Chunks with TSNS 1 to 4 have been received correctly, the Chunk with TSNS 5 and 9 is missing. But chunks with 8 and 11 have been received twice.

In case of TCP, all chunks from 5 onwards would be retransmitted but in case of STCP, the receiver has to clearly specify to the sender what is missing and what is duplicated so that the minimum retransmission take place.

STCP supports Congestion avoidance and network level redundancy.

Congestion Avoidance

It is achieved through the use of a parameter in SCTP messages called the Advertised Receiver Credit window

Redundancy

Redundancy is achieved through the given end point can be logically distributed across multiple platforms with multiple IP addresses.

If a given platform fails, then another platform can take over.

Quality of Service - VOIP

The biggest issue with VOIP is ensuring that the quality of service (QOS) & comparable to the QoS achieved in traditional circuit switched telephony.

IP and UDP provide no quality guarantees

RTP, RTCP provide QoS related information. But they do not provide any assurance of quality. So VOIP has to implemented specific solutions to obtain good QoS in the n/w.

QoS Techniques,

1. Resource Reservation protocol
2. Differentiated Services
3. Multiprotocol label switching (MPLS)

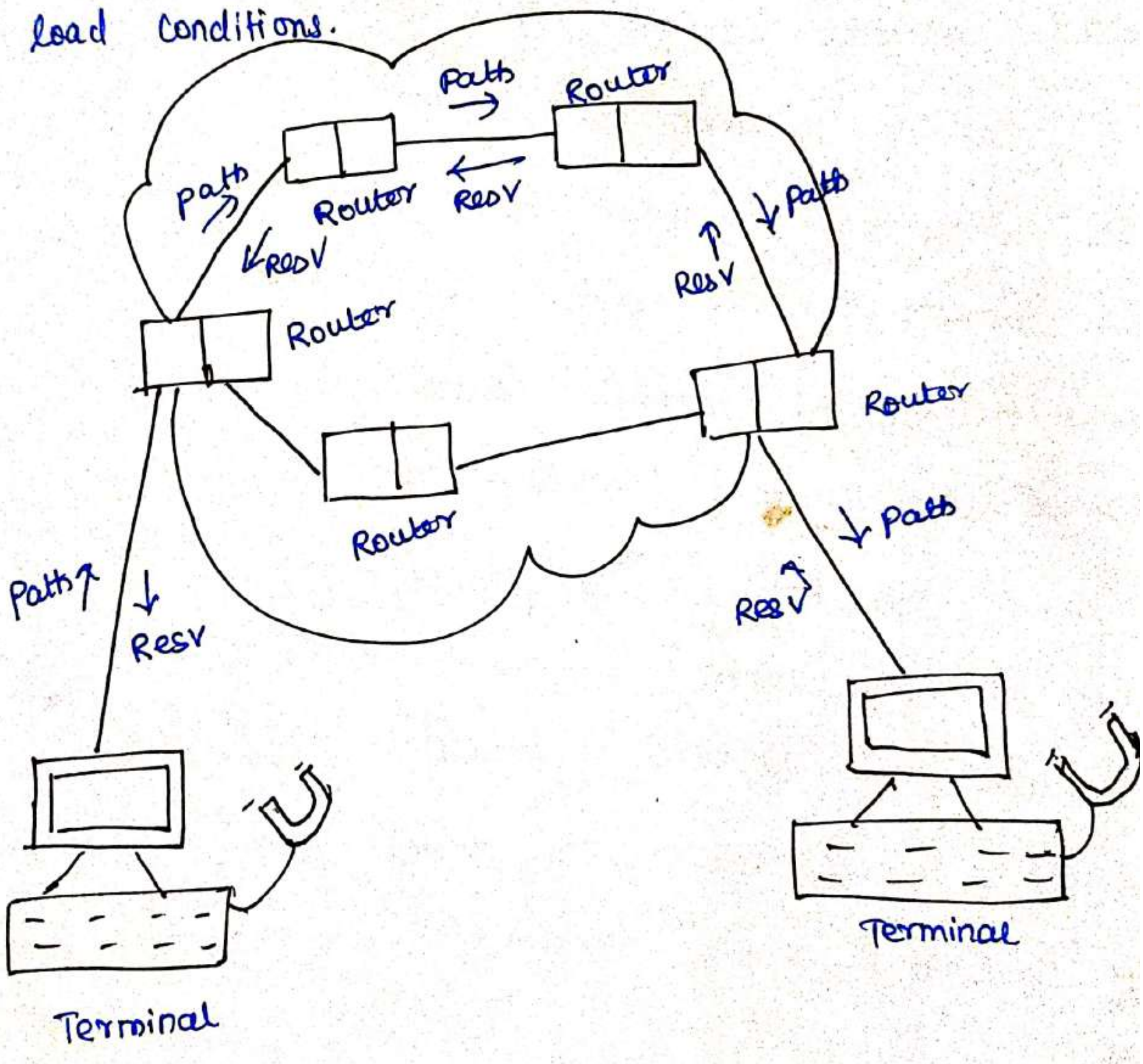
1. Resource Reservation protocol (RSVP) techniques for IP n/w are specified in Resource Reservation RSVP RFC 2205 and RSVP is part of the IETF Integrated Services Suite.

It is a protocol that enables resources to be reserved for a given session or sessions prior to any attempt to exchange media between the participants

It Provides strong qos guarantees, a significant granularity of resource allocation and significant feedback to applications and users.

RSVP currently offers two levels of service.

First is guaranteed which comes as close as possible to circuit emulation. The second is controlled load, which is equivalent to service that would be provided in a best-effort n/w under no load conditions.



Principle,

A Sender first issues a PATH message to the far end via a no. of routers. The Path message contains a traffic Specification which provides details of the data that the sender expects to send.

The Sender data may be in terms of the BW requirement and packet size.

Each RSVP enabled router along the way establishes a 'PATH STATE' that includes the previous Source address of the PATH message.

The receiver of the PATH message responds with a reservation request that includes a flowspec. The flowspec includes traffic Specification and information about the type of reservation Service requested such as controlled load Service or guaranteed service.

The RESV message travels back to the Sender along the Same route that the PATH message took. At each router the requested resources are allocated. Finally the RESV message reaches the Sender with a confirmation that resource has been reserved.

Scanned with CamScanner

The RSVP reservations are made by the receiver not by the Sender of data. This is done in order to accomodate multicast transports.

Multicast transports means there may be large no. of receivers and only one Sender.

RSVP is a control protocol that doesnot Carry user data. The user data (voice) is transported later using RTP. This occurs only after the reservation Procedure have been Performed.

2. Differentiated Service (Diff serv)

Differentiated Service is relatively simple means for Priority different types of traffic. This Protocol is described in RFC 2475, architecture for differentiated services.

It makes use of IPV4 type of Service (TOS) field, Contained in the IPV4 header & equivalent IPV6 traffic Class field. The portion of the TOS field used by Diffserv is Known as DS field.

The DS field require particular type of forwarding. The types of forwarding to be applied are known as Per-HoP Behavior (PHB).

Two types of forwarding,

1. Expected Forwarding
2. Assured Forwarding

1. Expected Forwarding (EF)

EF is specified in RFC 2598. It is a service in that a given traffic stream is assigned a minimum departure rate from a given node, one is greater than the arrival rate at the same node.

The arrival rate doesnot exceed a pre-agreed maximum. This ensures that queing delays are removed. Because queuing delays are major cause of end-to-end delay and jitter.

2. Assumed Forwarding

AF is defined in RFC 2597. This is a service in that packets from a given Source are forwarded with a high probability and traffic from that source doesnot exceed some pre-agreed maximum.

AF defines four classes, with each class allocated a certain amount of resources within a router. within each class, a given packet may have one of three drop rates.

Scanned with CamScanner

3. Multiprotocol Label Switching (MPLS)

Label switching is used in Internet Community and it defines a protocol called MPLS.

It is similar to Diffserv and it marks the traffic at the entrance to the n/w.

MPLS does not allocate a priority within a router but it determines the next router in the path from source to destination. MPLS involves the attachment of a short label to a packet infront of the IP header.

The label contains all the information that a router needs to forward a packet. The value of a label may be used to look up the next hop in the path & forward to the next router.

The difference between Label Switching and standard IP switching is that the match is an exact one it doesnot looking for the longest match. This enables faster routing decisions within routers.

The label identified Forward Equivalence Class (FEC). All Packets of FEC are treated equally for the purpose of forwarding.

MPLS is called as traffic engineering protocol or QoS protocol. It is used to provide QoS by helping to better manage traffic. It is analogous to the establishment of virtual circuits in ATM and can lead to similar QoS benefits.

CODEC methods

There are wide range of voice CODECs (coder / Decoder or Compression/Decompression) protocols available for VoIP phone implementation.

The most common Voice CODECs are G.711, G.723, G.726, G.728 & G.729.

G.711

It converts voice into 64Kbps voice streams.
Same CODEC used in traditional TDM T1 voice
Considered the highest quality

G.723.1

Two different types of G.723.1 compression exist.

one type uses a Code Excited Linear prediction (CELP) algorithm and has a bit rate 5.3 kbps.

The other type uses a multipurpose- Maximum

Likelihood Quantizer (MP-MLQ) algorithm
Provides better quality sound
Bit rate 6.3kbps

G.726
It allows for several different bit rates including 40, 32, 24 and 16kbps.
It works well with packet to private Branch Exchange (PBX) Interconnections.
Most commonly deployed to 32kbps.

G.728
It Provides good voice quality
Specifically designed for low latency appln.
Compresses voice into a 16kbps stream.

G.729
It is one of the better voice quality CODECs
Converts voice into an 8kbps stream.
Two versions :- G.729 & G.729a
G.729a => It has more simplified algorithm over G.729, allowing the end phones to have less processing power for the same level of quality