Technology Review#2001-2

Network Convergence and Voice over IP

Debashish Mitra

March 2001

Contents

1. Introduction

Voice communication has traditionally been carried over dedicated Telephone networks operated by Telecommunication service providers such as the BSNL and MTNL in India or AT&T in USA. These telephone networks have progressively evolved from the initial analog circuits to the current digital networks with bandwidth in excess of 1 Gbps. For reasons of varying bandwidth and networking requirements, different services were provided on separate networks. For example, Telegraph networks, Telex networks, Telephone networks, Facsimile networks, Cable networks and Data networks support different services, as their names would suggest.

These networks possessed characteristics that satisfied the peculiar requirements of the service they provided. For example, the voice network would support bandwidths of 64 Kbps for voice communication and would ensure telco-grade voice communication with little jitter and echo cancellation. Likewise, the cable networks would provide even higher bandwidth and improved quality of service (QoS) for video transmission. On the other hand, the data communication networks' bandwidth and QoS requirements are highly flexible. This means that the data communication requirements could be a Telnet application, requiring minimal data pipe, but reasonably fast network response times. Or it could be a batch transmission application that required a higher throughput, but can tolerate larger inter packet delivery delays. For most types of data communication applications, reliability is critical, which means that the delivery protocols would implement mechanisms for error checking, acknowledgment, re-transmissions and sequencing. On the other hand, for real-time applications such as voice communications, it would make little sense to retransmit a lost packet for play back at the receiving end, if it is out of sequence and is considerably delayed. Essentially, the main point to be noted is that these networks have been designed differently in terms of their underlying architecture and communication protocols.

In the late eighties and early nineties it was realized that integrating these networks into a single integrated network, such that all services would use common facilities, would result in efficiency and cost savings. This was the new mantra that made possible the creation and deployment of ISDN and similar networks, bringing data and voice communication together. However, nearly all these networks were built and operated by major telecommunication equipment manufacturers and service providers. Although, the major international standards bodies such as ITU-T (formerly CCITT), or the ETSI defined a relevant set of standards for implementation and to assure inter-operability between products from different telecom equipment manufacturers, these standards were still inadequate to reduce the proprietary nature of most implementations. It meant that even if the standards assured inter-operability among equipment and networks for existing communication services (which number only in dozens), they fell woefully short, on account of proprietary implementations, for being able to spawn and envisage even greater types of potential communication services. Consider what the Internet has done for conceiving and spawning innumerable types of web-based applications at progressively lower costs.

Subsequently, from the mid-nineties onwards, the Internet has proved to be the major all-encompassing network that demonstrated its prowess in delivering all types of media (data, voice and video) at lowest cost. Data communication equipment manufacturing

companies, such as Cisco, have also been instrumental in driving up the reach of the Internet and Internet protocols. Internet protocols became the preferred protocol for delivering communication payload for all types of networks, mainly for their open and widely accepted interface implementations. Contrast this with ATM, which somehow has been left behind.

However, a major shortcoming in the Internet protocols – TCP, UDP over IP has been their inability to transfer real-time application data such as voice and video. The major issues were jitter, network latency, echo cancellation, quality of service and security. To overcome this shortcoming, newer implementations of IP (e.g. IP version 6) and a flurry of associated protocol specifications (e.g. H.323 or SIP) were defined to plug the gap between the Internet protocols and other telecom application-oriented protocols. These activities of developing and implementing new IP-based protocol definitions for multimedia communications; their underlying network architecture and also integration with existing networks are collectively termed as Voice over IP or VoIP in short.

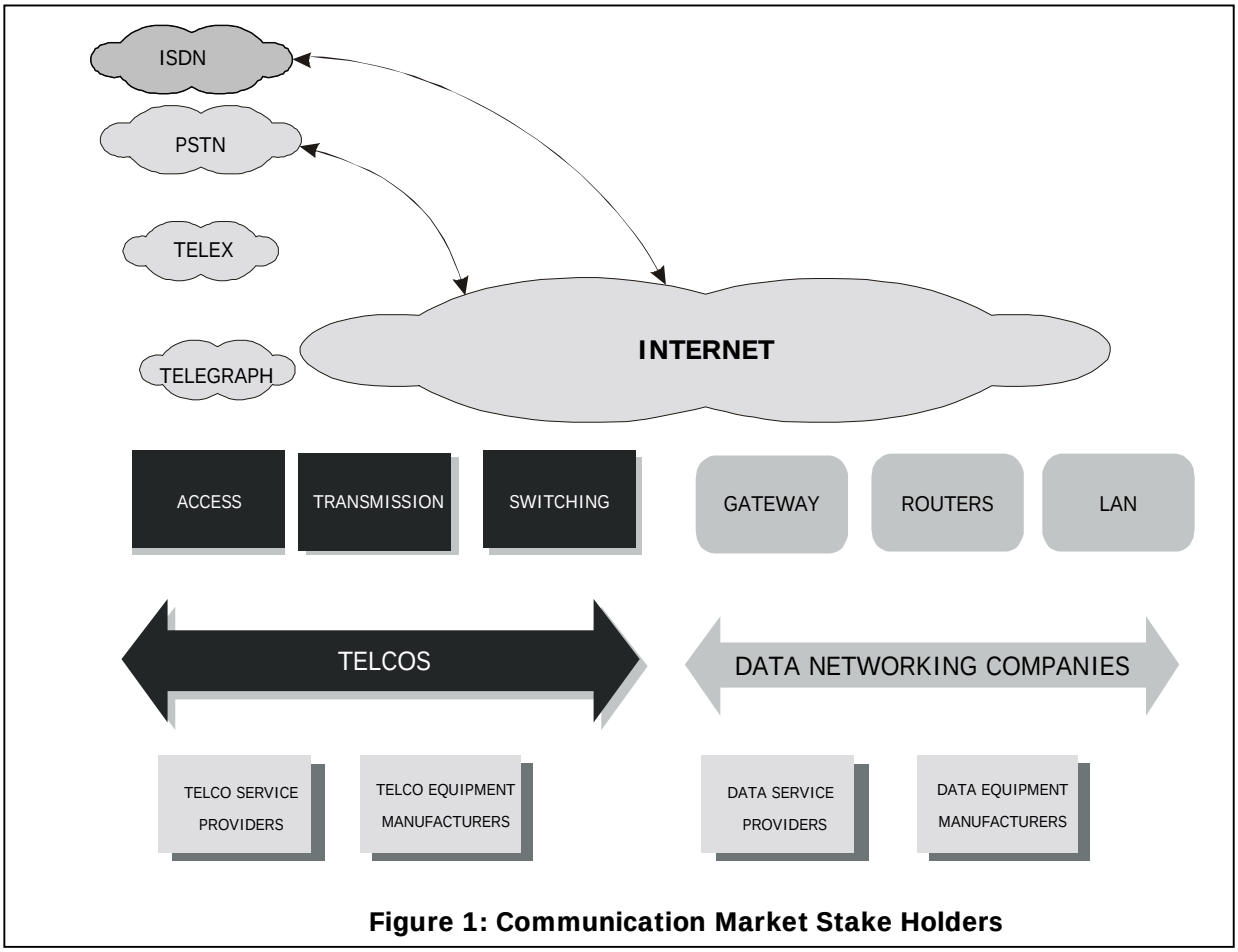

Figure 1: Communication Market Stake Holders

The effort to integrate all communication services over IP is a transition effort on two major fronts. First, the Telecommunication equipment manufacturers were interested in integrating the currently deployed services and network protocols to IP. Second, the Data communication equipment manufacturers, who were already using IP for data communication services were moving upward to provide voice and multimedia services over data networks.

The culmination of the above efforts and various standards making bodies is supposed to achieve the objectives of service portability, network convergence and secured network access. It is hoped that with the transition of voice (multimedia) over to Internet protocols would open the doors to the conceptualization and implementation of numerous services in thousands from the current dozens.

2. Issues in voice communication over networks

As the IP network was primarily designed to carry data, it does not provide real-time guarantees but only provides best effort service, which is inadequate for voice communication. Upper layer protocols were designed to provide such guarantees. Further, as there are several vendors in the market implementing these protocols, conformance to standards and interoperability issues have become important. The major issues governing transfer of a voice stream over the Internet or using Internet protocols are listed below.

Bandwidth requirement

In the analog world, the voice transmission frequency spectrum requirement is 0-3.4 KHz in the base band, and is nominally called a 4 KHz voice channel for convenience. For digital telecommunication, the signal is sampled at twice the rate. The minimum-sampling rate required is thus 8 KHz. If each sample contains 8 bits, the digital bandwidth required works out to be 64 Kbps.

Telco quality voice requires sampling at 8 KHz. The bandwidth then depends on the level of quantization. With Linear quantization at 8 bits/sample or at 16 bits/sample, the bandwidth is either 64 Kbps or 128 Kbps. Further, the quantization (e.g. PCM) is modified by using an A-law or μ-law companding curve.

In order to communicate telco-grade voice (or similarly, other real-time applications such as moving video) two different approaches can be attempted. To transmit information of the highest quality over unrestricted bandwidth or to reduce the bandwidth required for transmitting information (voice) of a given quality. Stated differently, decisions are required regarding what information should be transmitted and how it should be transmitted.

Compression and decompression (CODEC) of digital signals is a means of reducing the required bandwidth or transmission bit rate. Certain source data are highly redundant, particularly digitized images such as video and facsimile. If, for example, a digital signal contains a string of zeroes, it will be economical to transmit a code indicating that a string of zero follows along with the length of the string. Many different algorithms for compression and decompression of digital codes have been constructed.

Pulse code modulation (PCM) and adaptive differential PCM (ADPCM) are examples of "waveform" CODEC techniques. Waveform CODECs are compression techniques that exploit the redundant characteristics of the waveform itself. In addition to waveform CODECs, there are source CODECs that compress speech by sending only simplified parametric information about voice transmission; these CODECs require less bandwidth.

Source CODECs include linear predictive coding (LPC), code-excited linear prediction (CELP) and multipulse-multilevel quantization (MP-MLQ).

Coding techniques for telephony and voice packet are standardized by the ITU-T in its G-series recommendations.

Some algorithms for voice compression and decompression are given in the table below.

Table - Coding Algorithms

Input Range	Transmission Rate	Standard
Linear Predictive Coding algorithm	64 Kbps	LPC-10 G.711
Code Excited Linear Prediction (CELP)	8 Kbps	G.729 G.729 A
32 Kbps Adaptive Differential Pulse Code Modulation (ADPCM)	32 Kbps	G.721

Mean Opinion Score (MOS)

Each CODEC provides a certain quality of speech. The quality of transmitted speech is a subjective response of the listener. A common benchmark used to determine the quality of sound produced by specific CODECs is the mean opinion score (MOS). With MOS, a wide range of listeners judge the quality of a voice sample (corresponding to a particular CODEC) on a scale of 1 (bad) to 5 (excellent). The scores are averaged to provide the MOS for that sample. The table below shows the relationship between CODECs and MOS scores.

Table - Compression Methods and MOS Scores

Compression Method	Bit Rate (Kbps)	Framing Size (ms)	MOS Score
G.711 PCM	64	1.25	4.1
G.729 CS-ACELP	8	10	3.92
G.729 x 2 Encodings	8	10	3.27
G.729 x 3 Encodings	8	10	2.68
G.729a CS-ACELP	8	10	3.7

Although it might seem logical from a resource usage standpoint to convert all calls to low bit-rate CODECs to save on infrastructure costs, there are drawbacks to compressing voice. One of the main drawbacks is signal distortion due to multiple encodings (called tandem encodings). For example, when a G.729 voice signal is tandem-encoded three times, the MOS score drops from 3.92 (very good) to 2.68 (unacceptable).

Telco-grade voice refers to MOS scores of 4 or above.

Delay

A very important design consideration in implementing voice communications networks is minimizing one-way, end-to-end delay. Voice traffic is real-time traffic and if there is too long a delay in voice packet delivery, speech will be unrecognizable. An acceptable delay is less than 200 milliseconds. Delay is inherent in voice networking and is caused by a number of different factors.

There are basically two kinds of delay inherent in today's telephony networks:

- Propagation delay – caused by the characteristics of the speed of light traveling via a fiber-optic-based or copper-based medium of the underlying network.

- Handling delay (also called serialization delay) – caused by the devices that handle voice information and have a significant impact on voice quality in a packet network. This delay includes the time it takes to generate a voice packet. DSPs may take 5ms to 20ms to generate a frame and usually one or more frames are placed in a voice packet. Another component of this delay is the time taken to move the packet to the output queue. Some devices expedite this process by determining packet destination and getting the packet to the output queue quickly. The actual delay at the output queue, in terms of time spent in the queue before being serviced, is yet another component of this handling delay and is normally around 10ms. A CODEC-induced delay is considered a handling delay. The table below shows the delay introduced by different CODECs.

Table CODEC-Induced Delays

CODEC	Bit Rate (Kbps)	Compression Delay (ms)
G.711 PCM	64	5
G.729 CS-ACELP	8	15
G.729a CS-ACELP	8	15

Serialization delay

Serialization delay is the amount of time a router takes to place a packet on a wire for transmission. Fragmentation helps to eliminate serialization delay, but fragmentation, such as FRF.12, doesn't help without a queuing mechanism in place. For example, if a 1000-byte packet enters a router's queue and is fragmented into ten 100-byte packets, without a queuing mechanism in place, a router will still send all 1000-bytes before it starts to send another packet. Conversely, if there is a queuing mechanism in place, but no fragmentation, voice traffic can still fail. If a router receives a 1000-byte packet in its queue and begins sending this packet in an instant before it receives a voice packet, the voice packet will have to wait until all 1000 bytes are sent across the wire, before entering the queue, because once a router starts sending a packet, it will continue to do so until the full packet is processed. Therefore, it is essential that there is a method for a router to break large data packets into smaller ones, and a queuing strategy in place to help voice packets jump to the front of a queue ahead of data packets for transmission.

End-to-End delay

End-to-end delay depends on the end-to-end signal paths/data paths, the CODEC, and the payload size of the packets.

Jitter

Jitter is variation in the delay of arrivals of voice packets at the receiver. This causes a discontinuity of the voice stream. It is usually compensated for by using a play-out buffer for playing out the voice smoothly. Play-out control can be exercised both in adaptive or non-adaptive play-out delay mode.

Echo Cancellation

Echo is hearing your own voice in the telephone receiver while you are talking. When timed properly, echo is reassuring to the speaker. If the echo exceeds approximately 25ms, it can be distracting and cause breaks in the conversation. In a traditional telephony network, echo is normally caused by a mismatch in impedance from the four-wire network switch conversion to the two-wire local loop and is controlled by echo cancellers.

In voice over packet-based networks or VoIP, echo cancellers are built into the low bit-rate CODECs and are operated on each DSP. Echo cancellers are limited by design by the total amount of time they will wait for the reflected speech to be received, which is known as an echo trail. The echo trail is normally 32ms.

Reliability

Traditional data communication strives to provide reliable end-to-end communication between two peers. They use checksum and sequence numbering for error control and some form of negative acknowledgement with a packet retransmission handshake for error recovery. The negative acknowledgement with subsequent re-transmission handshake adds more than a round trip delay to transmission. For time-critical data, the retransmitted message/packet might therefore be entirely useless. Thus, VoIP networks should leave the proper error control and error recovery scheme to higher communication layers. They can thus provide the level of reliability required, taking into account the impact of the delay characteristics. Therefore, UDP is the transport level protocol of choice for voice and like communications. Reliability is built into higher layers.

Audio data is delay-sensitive and requires the transmitted voice packets to reach the destination with minimum delay and minimum delay jitter. Although TCP/IP provides reliable connection, it is at the cost of packet delay or higher network latency. On the other hand, UDP is faster compared to TCP. However, as packet sequencing and some degree of reliability are required over UDP/IP, RTP over UDP/IP is usually used for voice and video communication.

Interoperability

In a public network environment, in order for products from different vendors to inter-operate with each other, they need to conform to standards. These standards are being devised by the ITU-T and the IETF. H.323 from ITU-T is by far the more popular standard. However, SIP/MGCP standards from IETF are rapidly gaining more acceptance as relatively light weight and easily scalable protocols.

Security

On the Internet, since anybody can capture packets meant for someone else, security of voice communication becomes an important issue. Some measure of security can be provided by using encryption and tunneling. Usually, the common tunneling protocol used is Layer 2 Tunneling protocol, and the common encryption mechanism used is Secure Sockets Layer (SSL).

Integration with PSTN and ISDN

IP Telephony needs to co-exist with traditional PSTN for still some more time. It means that both PSTN and IP telephony networks should appear as a single network to users. This is achieved through the use of gateways between the Internet on the one hand and PSTN or ISDN on the other.

Scalability

As succeeding VoIP products strive to provide Telco-grade voice quality over IP as is true for PSTN, but at a progressively lower cost, there is a potential for high growth rates in VoIP systems. In such a scenario, it is essential that these systems be flexible enough to grow into large user markets.

3. Typical voice call handling in a VoIP application

It is useful to understand what happens at an application level when a call is placed using VoIP. The diagram below describes the general flow of a two-party voice call using VoIP.

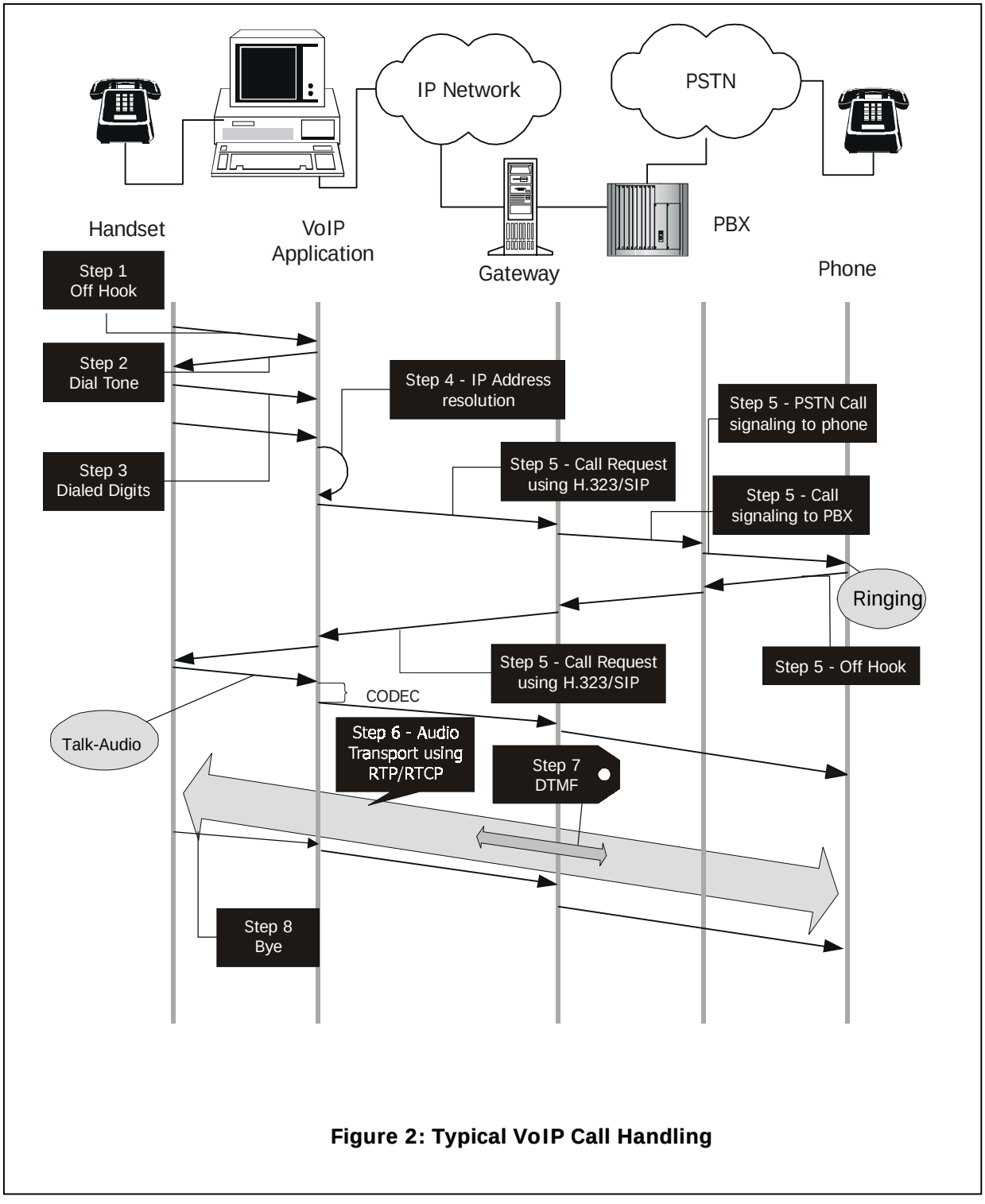

Figure 2: Typical VoIP Call Handling

Table - Typical VoIP Call Handling

Step	Action
Step1.	The user picks up the handset; this signals an off-hook condition to the signaling application part of VoIP.
Step2.	The session application part of VoIP issues a dial tone and waits for the user to dial a telephone number.
Step3.	The user dials the telephone number; those numbers are accumulated and stored by the session application.
Step4.	After enough digits are accumulated to match a configured destination pattern, the telephone number is mapped to an IP host via the dial-plan mapper. The IP host has a direct connection to either the destination telephone number or a PBX that is responsible for completing the call to the configured destination pattern.
Step5.	The session application then runs the session protocol (H.323 or SIP/MGCP) to establish a transmission and a reception channel for each direction over the IP network. If the call is being handled by a Private Branch Exchange (PBX), the PBX forwards the call to the destination telephone. If Resource Reservation Protocol (RSVP) has been configured, the RSVP reservations are put into effect to achieve the desired QoS over the IP network.
Step6.	The coder-decoder compression schemes (CODECs) are enabled for both ends of the connection and the conversation proceeds using Real-time Transport Protocol/User Datagram Protocol/Internet Protocol (RTP/UDP/IP) as the protocol stack.
Step7.	Any call-progress indications (or other signals that can be carried inband) are cut through the voice path as soon as an end-to-end audio channel is established. Signaling that can be detected by the voice ports (for example, inband dual-tone multifrequency (DTMF) digits after the call setup is complete) is also trapped by the session application at either end of the connection. It is carried over the IP network, encapsulated in the Real-time Transport Control Protocol (RTCP) using the RTCP application-defined (APP) extension mechanism.
Step8.	When either end of the call hangs up, the RSVP reservations are torn down (if RSVP is used) and the session ends. Each end becomes idle, waiting for the next off-hook condition to trigger another call setup.

4. H.323 Standard

The H.323 standard has been developed by the ITU-T for equipment manufacturers and vendors who provide Voice over IP service. It provides technical recommendations for voice communication over LANs assuming that no Quality of Service (QoS) is being provided by LANs. It was originally developed for multimedia conferencing on LANs, but was later extended to Voice over IP. The first and second versions of H.323 were released in 1996 and 1998 respectively. Currently, version 4 of H.323 is under consideration.

Components of H.323

The H.323 standard proposes an architecture that is composed of four logical components – Terminal, Gateways, Gatekeepers and Multipoint Control Units (MCUs). The architecture schematic is depicted in the following diagram. The various components are described subsequently.

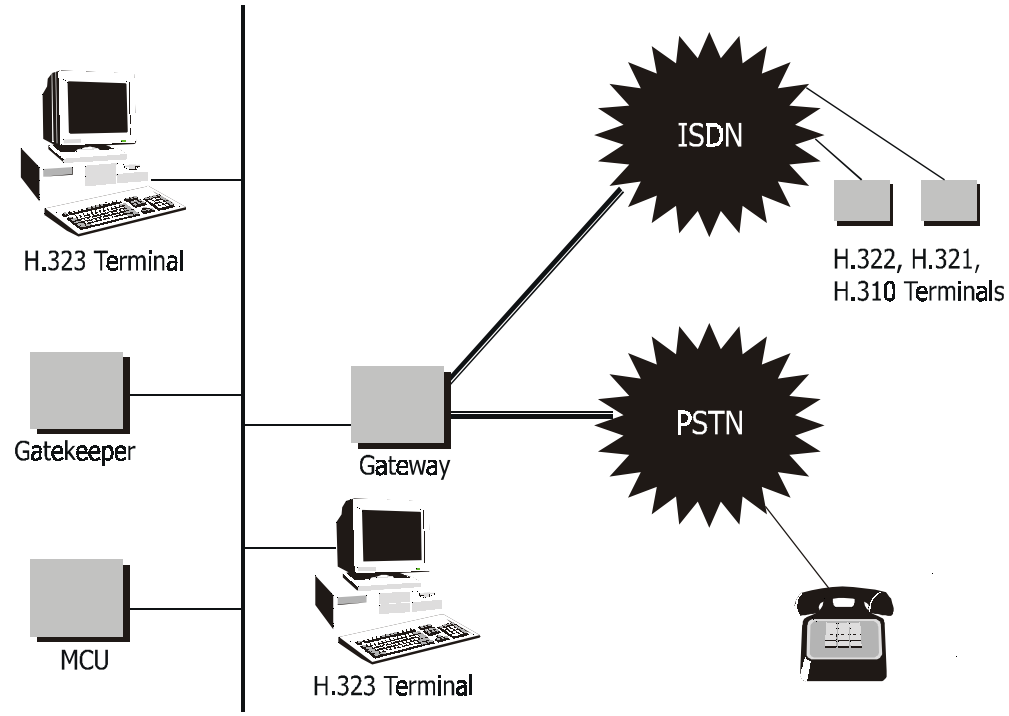

Figure 3: VoIP H.323 Architecture

Terminals

These are LAN client endpoints that provide real-time, two-way communications. All H.323 terminals are required to support H.245, H.225, Q.931, Registration Admission Status (RAS) and real-time transport (RTP) protocols. H.245 is used for controlling channel usage, while H.225 or Q.931 are used for call signaling, call setup and teardown. RTP is used as a media transport protocol that carries the voice traffic. RAS is used by the endpoint for interacting with the gatekeeper. H.323 terminals may also use T.120 data conferencing protocols, video codecs and support for MCU. An H.323 terminal can communicate with either another H.323 terminal, a H.323 gateway or a MCU.

Gateways

An H.323 gateway is an endpoint on the network that provides for real-time, two-way communications between H.323 terminals on the IP network with other ITU terminals on a switch-based network like PSTN or to another H.323 gateway. The gateways handle different transmission formats. Gateways are optional devices in the H.323 architecture because terminals in a single LAN can communicate directly with each other without using a gateway.

Only if the communication needs to span to other networks such as the PSTN, will a gateway be required. In such cases, H.245 and Q.931 protocols are used, by the participating endpoints and the intermediate gateway.

Gatekeepers

This is an important component of the H.323 architecture and functions as its “manager”. It is the central point for all calls within its zone and provides services to the registered endpoints. A zone is the aggregation of the gatekeeper and the registered endpoints.

A gatekeeper performs functions such as address translation, admissions control, call signaling, call authorization, call management and bandwidth management.

Multipoint Control Units (MCU)

The MCU acts as an endpoint on the network for providing capability for three or more terminals and gateways to participate in a multipoint conference. The MCU consists of a mandatory Multipoint Controller (MC) and an optional Multipoint Processor (MP). The MC’s functions are to determine the common capabilities of conferencing terminals, using the H.245 protocol. It however does not perform multiplexing of audio, video and data streams. The multiplexing of these media streams is handled by the MP under control of the MC.

H.323 Protocol Stack

A schematic description of the H.323 protocol stack is given in the following diagram. The unreliable but low latency UDP is used to transport audio, video and registration packets. Whereas the reliable but slow TCP is used for data and control packets in call signaling, the T.120 protocol is used for data conferencing.

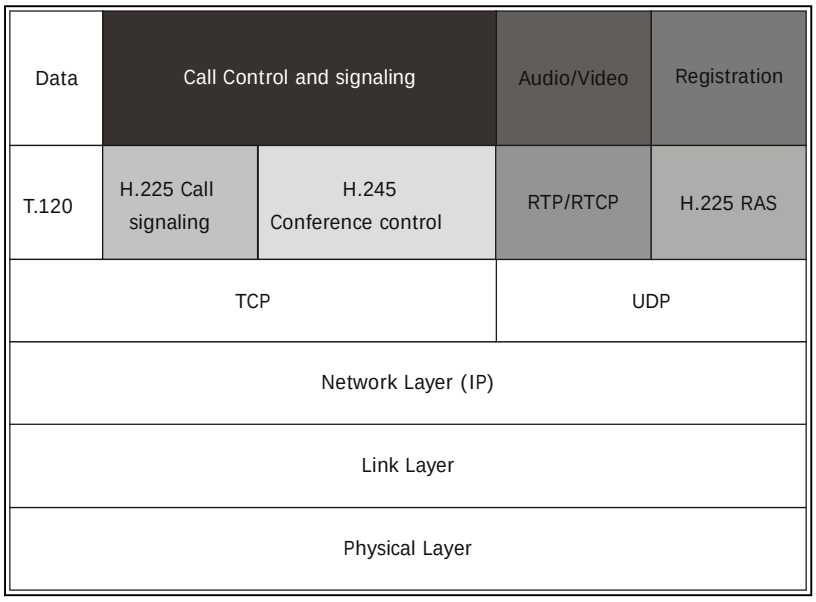

Figure 4: H.323 Protocol Stack

Control and signaling in H.323 system

H.323 provides three control protocols – H.225/Q.931 call signaling, H.225/RAS call signaling and H.245 Media control. The H.225/Q.931 is used for call signaling control. The H.225/RAS channel is used for establishing a call from the source to the receiving host. After the call is established, H.245 is finally used to negotiate the media streams.

H.225/RAS

This RAS (Registration, Admission and Signaling) channel is used between the endpoints and the gatekeeper. RAS uses unreliable UDP and hence also implements timeouts and retry count mechanisms for incorporating reliability.

RAS procedures used by endpoints encompass Gateway discovery, Endpoint registration, Endpoint location, admission, bandwidth negotiation and status change.

H.225/Call Signaling

This channel is used to carry H.225 control messages. In networks that do not contain a gatekeeper, call signaling messages are exchanged directly between endpoints using the Call Signaling Transport Address. In this case, it is assumed that the calling endpoint knows the called endpoints. However, in networks containing gatekeepers, the initial admission message can take place between the calling endpoint and the gatekeeper, using the gatekeeper's RAS channel Transport Address. This call signaling is done over TCP.

H.245 Media and Conference Control

After establishment of a call, the H.323 systems use the H.245 media control protocol to negotiate and establish all the media channels to be carried by RTP/RTCP.

This protocol is used to perform functions such as determination of master and slave in a multi-party conference, capability exchange, media channel control and conference control.

H.323 Call Setup

Given below is a set of steps required for setting up a H.323 call.

- Discover a gatekeeper that would manage the endpoint
- Register the endpoint with the gatekeeper
- Endpoint enters the call setup phase
- Capability exchange between the endpoints
- Call is established
- After calling, the call can be terminated by either party

H.323 Implementations

One of the most popular H.323 implementation available in the market is from Radvision. Its H.323 stack is widely used by service providers. Some of the other H.323 implementations available in the market are from Elemedia, Cisco, Micom, Nortel, Vocaltec, Neura Solutions and Ericsson. A description of their products is given in the *Industry products* section of this document.

5. Session Initiation Protocol

Session Initiation Protocol or SIP is the IETF standard for voice or multimedia session establishment over the Internet. It was proposed as a standard (RFC 2543) in Feb. 1999. Its original author was Henning Schulzrinne. SIP is an application level protocol used for call setup management and teardown. SIP is used in association with its other IETF sister protocols like the SAP, SDP and MGCP (MEGACO) to provide a broader range of VoIP services. The SIP architecture is similar to HTTP (client-server protocol) architecture. It comprises requests that are sent from the SIP user client to the SIP Server. The Server processes the request and responds to the client. A request message, together with the associated response messages makes a SIP transaction.

SIP makes minimal assumptions about the underlying transport protocol and itself provides reliability and does not depend on the underlying protocol's characteristics. SIP depends on Session Description Protocol (SDP) for negotiation of session parameters such as codec identification and media. It supports user mobility through proxy servers and redirecting requests to the user's currently registered location. The SIP specifications are provided in RFC2543 of IETF.

Some major SIP features are as follows:

Feature	Description
Call Setup	Session Establishment with agreed call parameters between the two endpoints.
Renegotiate call parameters	Renegotiate session parameters while the call is in progress.
User Location	Determination of the end system to be used for communication, given the user's email style address.
User Availability	Determination of the willingness of the called party to engage in a conversation.
User Capabilities	Determination and negotiation of the media and call parameters to be used in the session.
Call Handling	Transfer and termination of the call.

SIP Components

The SIP architecture specifies two components as given below.

User Agents

A SIP User Agent is an end system (end point) acting on behalf of the user. It consists of two parts:

User Agent Client (UAC): This is the user client portion, which is used to initiate a SIP request to the SIP servers or the UAS.

User Agent Server (UAS): This is the user server portion that listens and responds to SIP requests

Note: User = UAC+UAS

SIP Servers

The SIP architecture describes the following types of network servers to help in the SIP call setup and services.

Registration Server: This server receives registration requests from SIP users and updates their current location with itself.

Proxy Server: This server receives SIP requests and forwards them to the next-hop server, which has more information of the called party.

Redirect Server: This server on receipt of the SIP request, determines the next-hop server and returns the address of the next-hop server to the client instead of forwarding the request to the next-hop server itself (as in the case of SIP proxy).

SIP Messages

SIP defines the following major messages between the client and server.

INVITE	Request to invite a user (called party) to a call
ACK	Acknowledgment to start reliable exchange of invitation messages
BYE	To terminate (or transfer) the call between the two endpoints
OPTIONS	Request to get information about the capabilities of a call
REGISTER	To register information of current location with a SIP registration server
CANCEL	Request to terminate search of a user or “ringing”
INFO	Mid-call information (e.g. ISUP, DTMF)
PRACK	Provisional Acknowledgement
COMET	Pre-condition met
SUBSCRIBE	Request to subscribe to an event
NOTIFY	Notify subscribers

Typical SIP Call setup

The following diagram describes a typical voice call session setup over the Internet using SIP.

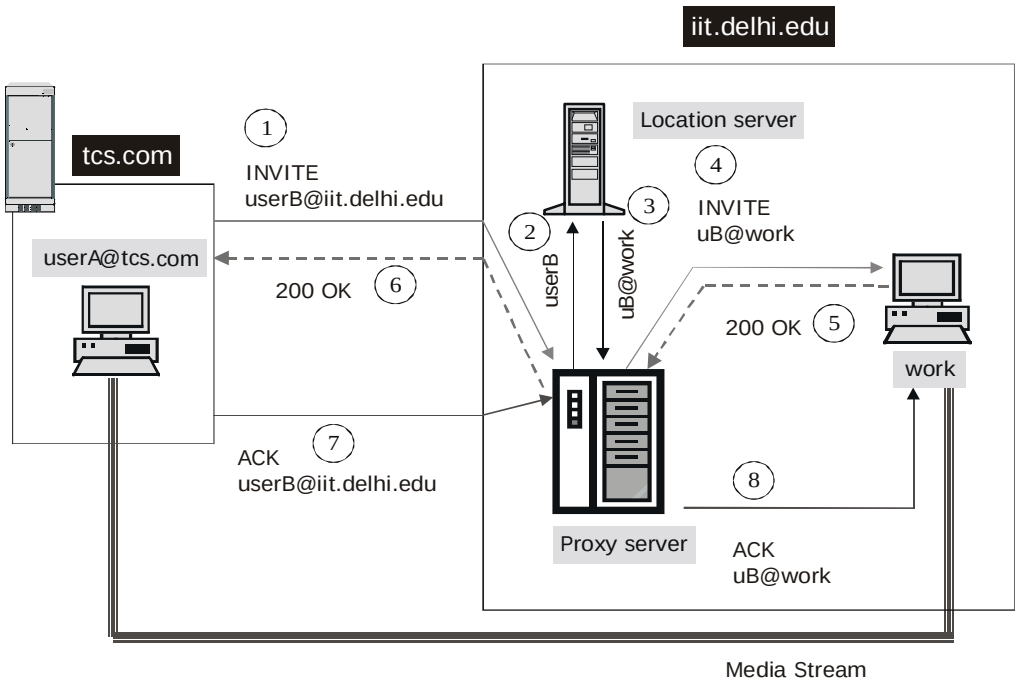

Figure 5: SIP – Basic Operation

In this diagram am SIP client "userA@tcs.com" creates an INVITE message for "userB@iit.delhi.edu" to invite the latter to a voice call. Given below is a step- by-step description.

1. UserA (userA@tcs.com) sends an INVITE message meant for UserB (userB@iit.delhi.edu) to the SIP Proxy server of iit.delhi.edu domain. Alternately, this message would have been sent to the SIP Proxy server of tcs.com domain, which in turn would have forwarded this to the SIP Proxy server of the iit.delhi.edu domain. The Proxy server tries to obtain the IP address of the SIP server that will handle the requests for the requested domain.

2. The Proxy server of iit.delhi.edu domain consults the Location server to determine the current address of UserB.

3. The Location server returns the current address of UserB, which is uB@work.

4. The Proxy server then sends INVITE to uB@work. The proxy server inserts its address in the via field of the Invite message.

5. UAS of UserB responds to the proxy server with 200 OK message.

6. The Proxy server in turn sends a 200 OK response back to userA@tcs.com.

7. UserA@tcs.com then sends an ACK message destined for UserB via the proxy server.

8. The Proxy server forwards the ACK message to uB@work.

9. After both the parties agree to participate in the call, an RTP/RTCP channel (media stream) is opened between the two endpoints for transporting voice.

10. After transmission is complete, the session is torn down, using the BYE and ACK messages between the two participating endpoints.

SIP Implementations

Although SIP is relatively new, it has already been implemented by several companies. The implementations encompass SIP proxy and redirect servers; User agents on MS Windows, Linux, etc.; Ethernet Phones; Softswitches; firewalls, SIP-H.323 translators and unified messaging systems.

Some of the current ongoing implementations are being done by companies such as dynamicsoft, Hughes Software Systems, Cisco, Ericsson, Hewlett Packard, Lucent, Nokia, Nortel, Siemens, Telogy, Iwatsu Electric and Vovida. Universities such as Carnegie-Mellon University and Columbia University are actively developing the standard through their implementations. The SIP stack can also be found as Open Source software. Companies such as Vovida or dynamicsoft have SIP stacks in the Open Source arena.

6. Comparison between H.323 and SIP

SIP is a relatively new protocol as compared to H.323 and hence, has been able to avoid all the problems associated with H.323. Because H.323 had been initially designed, keeping ATM and ISDN in mind, it was not suited to control voice traffic over IP networks. The earlier version of H.323 is inherently complex with large overheads and is thus inefficient for IP networks, where bandwidth is a premium commodity.

On the other hand, as SIP has been designed keeping the Internet in mind, it has been able to better address and circumvent the complexity and extensibility issues. SIP is "HTTP-*ish",* i.e. it reuses most of the HTTP header fields, encoding rules, error codes and authentication mechanisms. SIP uses only 37 header fields as compared to hundreds of elements in the H.323 header. This "HTTP-*ish"* characteristic of SIP enables it to be lightweight and also gives it the potential of becoming a more popular protocol, such as HTTP, over the Internet.

H.323 uses a binary representation for its messages. This is based on ASN.1 syntax. The SIP however, is a text-based protocol such as HTTP. SIP is more scalable, whereas H.323 has limited scalability, as it was initially designed for use within a single LAN. The newer versions of H.323 have, however, managed to address this issue. Loop detection techniques in complex multi-domain searches in H.323 are limited and not very scalable. This is done in a limited manner in H.323 by maintaining message states. However, in SIP this is done efficiently by checking the path history stored in the message header and thus it can be done in a stateless manner.

Given below is a table listing the differences between the two protocols.

Feature	**H.323**	**SIP**
Architecture	Stack Implementation	Element Implementation
Complexity	Complex	Simple
Standards body	ITU	IETF
Protocol	Mostly TCP	Mostly UDP
Protocol Encoding	Binary (ASN.1, Q.931)	Text (HTTP-ish)
Server processing	State-full	State-less, Transaction oriented
Addressing	Flat alias, E.164, email	SIP, E.164, URLs
Call Setup delay	V1: 6-7x RTT to V3: 1.5-2.5x RTT	1.5x RTT
Mid-call failure	Fail	Live
Loop Detection	V1:No, v3: Path Value	Yes – “via” field, time, hops
Manageability	Yes	No
Call control	Yes	Yes

7. Related VoIP Protocols

The following diagram depicts the relationship of SIP, H.323 and other related protocols.

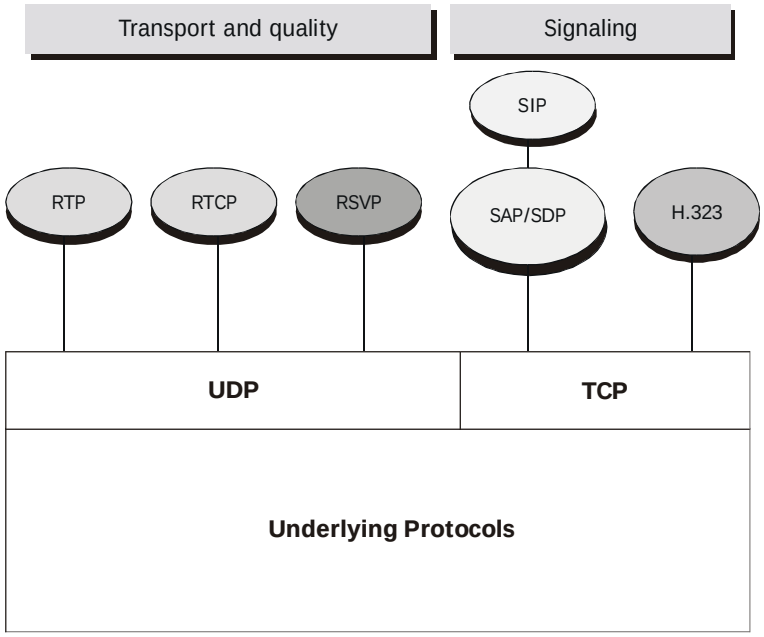

Figure 6: SIP, H.323 and Other protocols

Session Description Protocol (SDP)

SDP is an IETF specified protocol (RFC2327) that helps in describing multimedia sessions. It is used for session announcements, session invitation, etc. For example, the SDP payload gets included in the SIP INVITE packet to convey information about the sender to the recipient and vice versa, before participating in the session. This allows media information to be similarly shared between the parties. An SDP payload includes the following information:

- Session name and purpose
- Address and port number
- Start and stop times
- Media information
- Bandwidth requirement
- Contact information

The above information is conveyed in text format. In general, SDP must convey sufficient information to enable a party to join a session and also to announce the resources to be used

in a multiparty conference. The media information that SDP sends is: type of media (audio or video), transport protocol (RTP, UDP, etc.) and media format (MPEG video, H.263 video, etc.).

Session Announcement Protocol (SAP)

The SAP protocol is used for advertising multicast conferences and multicast sessions. A SAP announcer periodically multicasts announcement packets to a well known multicast address and port (port number: 9875). The SAP listener listens to the well known SAP address and port and learns of the multicast scopes using the Multicast Scope Zone Announcement Protocol. A SAP announcer is unaware of the presence or absence of SAP listeners. A SAP announcement is multicast with the same scope as the session it is announcing, thus ensuring that the recipients of the announcement can also be potential recipients of the session being advertised. If a session uses addresses in multiple administrative scope ranges, it is necessary for the announcer to send identical copies of the announcement to each administrative scope range. It is alright for multiple announcers to announce a single session, thus ensuring robustness of the protocol.

The intervening time period between announcements is decided such that the total bandwidth used by all the announcements in a single SAP group is less than a pre-configured limit. Each announcer is required to listen to all the announcements in its group in order to determine the total number of sessions being announced in the group. One of the protocol's objectives is to announce the existence of long-lived wide area multicast sessions and involves a large startup delay before a complete set of announcements is heard by a listener.

SAP Proxy caches can also be deployed to reduce the inherent delays in SAP. A SAP proxy is expected to listen to all SAP groups in its scope and maintain an upto date list of all announced sessions along with the last receipt time of each announcement.

SAP also contains mechanisms to ensure the integrity of session announcements, announcement encryption and also to authenticate the origin of an announcement.

Media Gateway Control Protocol (MGCP)

MGCP defines the communication between "Call Agents" (call control elements) and gateways. It is an IETF specification. Call Agents are also called Media Gateway Controllers. It is a control protocol that monitors the events on IP phones and gateways and instructs them to send media to specified addresses. MGCP has evolved from two earlier protocols – the Simple Gateway Control Protocol and the Internet Protocol Device Control.

As per recommendations, the call control intelligence is located outside the gateway in the Call Agents. These Call agents are assumed to have synchronized with each other and they issue coherent commands to the gateways under their control. The issued commands are executed by the gateways in a master/slave manner. MGCP defines the concepts of "Endpoints" and "Connections" to describe and establish voice paths between two participants. Similarly, it has defined "Events" and "Signals" to describe set-up or teardown of

sessions. MGCP is intended to be a simple protocol for enabling development of reliable and cheap local access systems. Accordingly, the programming complexity is concentrated into the Call Agent.

Creating Connections

Call agents create connections at each endpoint that will participate in a call. If the endpoints are located on different gateways managed by the same call agent, then the creation of a connection is done using the following steps.

- The Call agent asks the first gateway to create a connection on the first endpoint. The response sent by the gateway includes the session description that contains relevant information required by other parties to be able to send packets to the newly created connection.

- The Call agent then sends the session description of the first connection to the second gateway and requests it to create a connection on the second endpoint. The second endpoint and subsequently the second gateway responds and includes its own session description.

- The Call Agent then uses a modify-connection command to provide this second session description to the first endpoint.

Communication can now occur between the two endpoints.

On the other hand, if the two gateways are controlled by different call agents, then MGCP requires that the two call agents synchronize by exchanging information between themselves, using the agent signaling protocol. This will enable the call agents to issue synchronous commands to the different gateways.

Commands

The media gateway control interface is implemented as a set of transactions. These transactions are composed of a pair consisting of a command and an associated mandatory response.

There are eight types of MGCP commands. These commands are used to create, modify and delete connections, audit endpoints and connections, to send notification requests or to notify and finally reset or restart connections.

Real-time Transport Protocol (RTP)

RTP is used to transfer real-time media, such as audio and video, over packet switched networks. It is used by both SIP and H.323 protocols. The protocol provides timing information to the receiver so that it can correctly compensate for delay jitter. It also allows the receiver to detect packet loss and take appropriate measures. The RTP header contains information that assists the receiver to reconstruct the media and also the information about how the CODEC bitstreams are fragmented into packets. RTP provides enough information to the receiver so that it can recover, in the event of packet loss or jitter. RTP is specified by IETF in RFC1889 and provides functions such as sequencing, payload and source

identification, frame indication and intra-media synchronization. Intra-media synchronization is normally implemented as a play-out buffer to compensate for delay jitter.

Real-time Transport Control Protocol (RTCP)

RTCP is a control protocol that works in conjunction with RTP. In an RTP session, the endpoints periodically send RTCP packets to disseminate useful information about the QoS, etc. The endpoints can then take appropriate measures to efficiently transport the media over the RTP session.

Some of the functions that RTCP provides are QoS Feedback, Session control, User Identification and Inter media synchronization, to synchronize between the audio and video streams. For example, to synchronize the lip movement (in video) with the speech (in audio) streams.

Real-time Streaming Protocol (RTSP)

IETF has defined the RTSP as RFC2326 as a client/server protocol that provides control over the delivery of real-time media streams. It is akin to a “VCR-style” remote control for audio and video streams. Functions such as pause, fast forward, reverse and absolute positioning are provided to the user. It also allows the user to choose the RTP-based delivery mechanisms and also a delivery channel such as UDP, multicast UDP and TCP over IP.

The RTSP functions between the media servers and its clients and establishes and controls the connecting audio and video media streams. The media server provides playback and recording of the media streams to the client, whereas the client can request such services from the media server.

RTSP is an application level protocol similar to HTTP but is meant for audio and video. It requires maintenance of states and allows bi-directional requests between client and server. Further, RTSP requests are used by the client to retrieve media, or invite a server to a conference or add a new media to an existing presentation at the server.

8. Numbering Scheme

The VoIP network has to resolve the dialed destination number to an IP host address by using a dial-plan mapper, which takes inputs from the ITU-T numbering scheme.

The standard PSTN uses a specific numbering scheme, which complies with the ITU-T international public telecommunications numbering plan (E.164) recommendations. For example, in North America, the North American Numbering Plan (NANP) is used, which consists of an area code, an office code, and a station code. Area codes are assigned geographically, office codes are assigned to specific switches, and station codes identify a specific port on that switch. The format in North America is 1Nxx-Nxx-xxxx, with N = digits 2 through 9 and x = digits 0 through 9. Internationally, each country is assigned a one- to three-digit country code; the country's dialing plan follows the country code.

9. Quality of Service

The main goal of quality of service (QoS) is to help reduce or eliminate delay of voice packets including packet loss that travels across a network. It can be defined as the capability of a network to provide better service to selected network traffic over various underlying technologies such as Frame Relay, ATM, and IP. This network feature helps in differentiating different classes of traffic and treats them differently. The various formal measurements of QoS are:

Measurement	Description
Service Availability	The availability of the users' network connection and depends on the connected network device.
Throughput	The packet delivery rate at the endpoints.
Delay	The end- to- end packet delay, while traversing the network.
Delay jitter	The delay variation among similar packets traversing the same path in the network.
Packet loss rate	The rate of packet loss, because of packet dropping and corruption.

QoS of networks should attempt to maximize service availability and throughput, while at the same time minimizing the remaining measurements.

Need for QoS

In the current network scenario, different types of traffic (such as real-time and data) need to share the same network link. These different kinds of traffic require different treatment from the network. This is similar to a first class passenger of an airplane demanding preferential treatment over other passengers. Just as, apart from providing special treatment, a separate airplane cannot be made available to the first class passenger, similarly a separate link or a network connection cannot be given to different customers, though the treatment given can be different. The entire bandwidth has to be shared between priority traffic and regular traffic, and only at places where the traffic flows through active network elements like routers, can these flows be differentiated and treated differently.

The different types of traffic can be grouped as:

- **Non Real-time or Data**: These applications only care about reliable packet delivery like that guaranteed in TCP. They are immune to delays or bandwidth requirements. Examples are web browsing, email, distributed computing, etc.

- **Real-time**: These applications require timely delivery along with reliability. Some of these applications can tolerate an upper bound in delay, whereas others are totally intolerant. This range of expectations is used to further classify real-time applications by QoS models.

QoS Service Models

There are three major architectures or service models for implementing QoS in packet networks. These are:

QoS Service Model	Description
Best Effort Service	In this model there are no QoS guarantees given to the application, except that a best effort to deliver will be made.
Integrated Service	It is also called IntServ. This is an earlier model (1995) devised for integrated service networks such as ISDN or ATM. It believed to have end-to-end QoS strategies implemented at the network elements for all classes of traffic flows.
Differentiated Service	Also called DiffServ. This model was developed later (around 1998), wherein unlike the IntServ, it implements QoS strategies on per hop basis as Per Hop Behavior (PHB), and avoids signaling mechanisms. It tries to differentiate individual packets and responds with a different behavior to the same.

Best Effort Service

This model allows the application to send any amount of data at will and without any authorization. The network elements in turn will try their best to deliver the packets to their destinations without any constraints of maximum delay, latency or jitter, etc. They also give up trying to deliver after attempting for a number of times, in case acknowledgments from the receiver are not received. The network will also not inform the sender that the attempt to deliver has been abandoned. Thus, the end points have to take care and incorporate reliability features within themselves. The IP network is an example of a Best Effort service model.

Integrated Service

The Integrated service model is defined by a set of standards laid down by IETF. This model assures different QoS-profile treatment, dictated by the network elements, to the multiple classes of traffic. In this model, the applications are aware of the traffic characteristics that they would put on the network and accordingly signal the network elements to reserve required resources before sending their data. The network elements in turn acknowledge the signal positively if they are able to reserve the resources or else send a negative acknowledgement.

This model categorizes applications, in terms of their network traffic requirements, into three classes. Real-time Tolerant (RTT), where some delays can be tolerated within a small range as in video or audio playback applications. Real-time Intolerant (RTI), which requires minimal or absolutely no delays, as in video conferencing. And finally, Elastic applications, where as

long as the packets are delivered reliably no delay constraints are imposed, as in web browsing or email. Accordingly, the model provides for the following classes of service:

Guaranteed service: This service guarantees bandwidth and provides a deterministic upper bound on delay. It is used for RTI applications.

Controlled Load service: This service guarantees an average delay, but the specific end-to-end delay by some arbitrary packet cannot be specifically determined.

The Integrated service network implements the following mechanisms to guarantee QoS levels.

Mechanism	**Description**
Admission Control	This allows the network (network elements) to refuse a new traffic flow request from an application, depending upon resource availability. This is usually a policy-based decision taken by the router. Policy Enforcement Points (PEP) and Policy Decision Points (PDP) are components of this mechanism. PEPs and PDPs use a simple request response protocol called Common Open Policy Service (COPS) to communicate between themselves.
Traffic Shaping and Policing	Traffic shaping ensures that the traffic entering the network conforms to the agreed flow characteristic. An example of traffic shaping is the metered expressways in the US, where each vehicle is made to stop and wait for a green light at the ramp before entering the expressway. The frequency of entry is governed by the congestion on the expressway. Traffic policing ensures that applications are sending data into the network as per the agreed traffic QoS profile.
Congestion Management	This is implemented in core routers in which different queuing techniques are used to create and manage different queues for different traffic; algorithms to help classify packets belonging to the various queues are enforced and finally, queued packets are scheduled for transmission. Some of the major types of queuing techniques used by routers are the First In First Out (FIFO) queue and Weighted Fair Queuing (WFQ).

Mechanism	Description
Congestion Avoidance	Unlike congestion management, which deals with the post-congestion situation, congestion avoidance implements strategies to anticipate and avoid congestion. Some strategies, popularly used for congestion avoidance are Tail Drop, Random Early Dropping (RED) and Weighted Random Early Dropping (WRED). All these strategies determine when to drop packets at an active node (router) in anticipation of congestion in the network.
Link Efficiency	This mechanism improves link efficiency by helping to deal with situations wherein jumbograms (large packets from ftp- like applications) with lower priority congest and prevent smaller, but higher priority packets, to go through. It is implemented by router vendors as Link Fragmentation and Interleaving (LFI) strategies. An example of LFI usage is the Multilink point to point protocol (MLP - RFC 1717), wherein datagrams are split, sequenced and recombined over multiple links. MLP uses LFI to break jumbograms into smaller packets and interleave them with smaller packets of higher priority. LFI adds multilink headers to the datagrams to ensure correct transmission and reassembly. Compressed Real-time Protocol Header (CPTR) is another link efficiency improvement mechanism for real-time traffic. CPTR compresses the header of an RTP packet from 40 bytes to 2-5 bytes before transmission.
Flow-wise Soft state management	The QoS- capable active network elements need to maintain the state information of all traffic flows. This information is, however, maintained for a limited time (soft) or until explicitly unreserved, unless it is refreshed by the communicating endpoints. RSVP requests using PATH and RESV have to be periodically sent by the endpoints to reserve the allocated resources.

Resource Reservation Protocol (RSVP)

RSVP protocol specified by IETF in RFC2205 helps in providing quality of service in networks. It can prioritize traffic and helps in giving latency guarantees to specific IP traffic streams. Using RSVP, a packet-switched network can be made to give a more deterministic quality of service as in a circuit-switched network.

RSVP provides mechanisms or requests to reserve resources at each node along the data path. RSVP makes a distinction between the sender and receiver meaning that requests can be sent/applied in only one direction. An application process would normally have both a sender and receiver component. However, because of the above distinction, it is always the

receiver component that makes the QoS request to all the nodes in the reverse path. Although, RSVP is not a routing protocol, it is designed to work with both unicast and multicast routing protocols. As the receiver is responsible for making the RSVP request, it allows larger groups with heterogeneous receiver capabilities/requirements to be accommodated. Dynamic group membership is also possible because of this characteristic. RSVP has the following essential attributes:

- Maintains soft state in routers and host, enabling graceful support for dynamic membership changes
- Is Receiver-oriented
- Provides unicast and multicast support
- Provides Transparent operation through non-RSVP routers

Some of the relevant RFCs supporting RSVP are listed at the end of the document.

Differentiated Service

This model classifies and conditions network traffic at the entry to a network into different behavior aggregates. Each such behavior aggregate is assigned a DS code point. This differentiated service code point is defined by markups using DF bits. Packets at the core routers are given differential treatment while forwarding, based on Per Hop Behaviors (PHB) that are in turn based on the above DS code points.

DiffServ breaks the whole network into DiffServ domains. A domain is a continuous set of nodes, which supports a common resource provisioning and PHB policy. A DS domain is usually controlled by a single entity, such as an ISP or an organization's Intranet. DiffServ is extended across domains by Service Level Agreements (SLAs) between domains. SLAs specify rules, such as those for traffic, and also remarks, such as actions, for out of profile traffic. Traffic Conditioning Agreements (TCAs) are derived from these SLAs. The domain has a well-defined boundary with two types of nodes, as mentioned below:

- **Boundary nodes**: Boundary nodes are located at the boundary of the DiffServ cloud with other domains. These nodes classify and appropriately mark incoming ingress traffic, so that the packets can be forwarded as per the PHB groups supported within the domain. They also enforce TCAs between their own domains and other domains.
- **Interior nodes**: Interior nodes are connected to other interior nodes, or to boundary nodes, but they remain within the boundary.

A DS node can be the ingress or egress node, depending upon the traffic flow. Traffic enters the DS cloud through an ingress node, and leaves through the egress node. The ingress node is responsible for enforcing the TCA with the sender's domain and the egress node shapes the outgoing traffic in compliance with the TCA of the receiver's domain.

The DiffServ minimizes the signaling requirement by using aggregation and PHB. Flows are classified by predetermined rules, so that they fit into a limited set of class flows. This helps in easing congestion in the backbone.

Edge routers use the 8 bit ToS field of the packet header (also called the DS field in DiffServ domain) to mark the packet for preferential treatment by the core routers. The last 6 bits of the ToS field are used for the DS code and the remaining 2 are reserved for future use. Only the edge routers are required to maintain the per-flow states and perform the shaping and policing. Traffic shaping and policing are computation intensive and as the edge routers are usually placed next to slower access links, they are best suited to perform the same. Whereas inside the core network, packets need to be routed very fast and hence, minimum computation is desirable at the core routers and switches.

Per Hop Behaviors is the description of externally observable forwarding behavior demonstrated by a DS node (routers). PHBs can be defined in terms of their resources (buffer and bandwidth) or in terms of their properties (delay and packet loss), or in terms of their priorities relative to other PHBs. PHBs are implemented using buffer and scheduling mechanisms. Multiple PHBs are aggregated together as PHB groups. Given below is the description of two popular PHBs in use.

PHB	Description
Expedited Forwarding (EF PHB)	EF PHB is used to provide premium service to the customer. It is a low-delay, low jitter service providing near constant bit rate. Its SLA specifies a peak bit rate which customer applications will receive. It is the customer's responsibility not to exceed the rate. Packets are dropped on exceeding this rate. EF PHB is defined as a forwarding treatment for a particular DiffServ aggregate, where the departure rate of the aggregate's packets from any DiffServ node must equal or exceed a configurable rate.
Assured Forwarding (AF PHB)	AF PHB is used to provide assured service to a customer, meaning that he/she will get reliable service even in times of network congestion. The customer will be provided with a fixed bandwidth at all times, as per the SLA.

Traffic Classification

This identifies the subset of network traffic which may receive a differentiated service by being conditioned and/or mapped to one or more behavior aggregates. Packet Classifiers use information in the packet header to select appropriate classes. The two types of classifiers are as follows:

- *Behavioral Aggregate Classifiers* - which select packets on the basis of DS codepoints.
- *Multi Field Classifiers* - which select packets based on values of multiple header fields.

Traffic Conditioning

Traffic conditioning ensures that the traffic entering a DS domain at any point complies with the TCA, between the sender's and receiver's domains and the domain's service provisioning policy. It involves traffic shaping, metering, policing and /or remarking as described here.

Meters

The conditioner receives the packets from the classifier and uses a "meter" to measure the "temporal properties" of the stream against the appropriate traffic profile from the TCA. This information is passed along with the packet. Further processing is done by markers, shapers and policers based on whether the packet is in or out of profile.

Markers

The marker marks or remarks a packet with a DS value corresponding to a correct PHB codepoint. The marker may be configured according to policies.

Shapers

It buffers the traffic stream and increases the delay of a stream to make it compliant with a particular traffic profile. Packets may be discarded if the buffer is full.

Droppers

They drop packets of a stream to make it compliant with a particular traffic profile. Droppers can be considered as special cases of shapers with buffer size set to zero.

An example of traffic conditioning and shaping is the metered expressways in the US, where each vehicle is made to stop and wait for a green light at the ramp before entering the expressway. The frequency of entry of vehicles is governed by the congestion on the expressway.

Multi Protocol Label Switching (MPLS)

MPLS is a hybrid technology model, which enables very fast forwarding at the core and slower conventional routing at the edges of a network. It combines the best of ATM's circuit-switching and IP's packet-routing. Packets are assigned a label at the entry to a MPLS domain and are switched inside the domain by a simple look-up table. The MPLS domain is usually the core backbone of a provider's network. These labels determine the quality of service rendered to the packet. At the egress router at the domain's edge, the packets are stripped off their labels and are routed in a conventional manner to their destination.

In MPLS, packets are mapped to Forwarding Equivalence Classes (FECs) only once at the ingress router, and the FEC's corresponding "label" is assigned to the packet and is sent along with it. This label is of fixed length and is only locally significant. At later hops at routers within the MPLS domain,this label is used as an index into the routing

tables to determine the next hop, as well as the new value for the label. Unlike conventional IP routing, there is no complex processing of the packet header involved in MPLS. Compare this to conventional IP routing, where the next hop is determined on the basis of the packet's header, and also by running a network layer routing algorithm. The conventional routing is done using two main functions, partitioning the complete set of possible packets into Forwarding Equivalence classes and mapping each FEC to the next hop. This mapping of packets to FECs is done at every router in conventional IP routing and is a costly operation.

MPLS is multi-protocol because this label assignment and label based switching can be used over any underlying network protocol. An MPLS based router is also called "Label-Switched Router" (LSR), and the path taken by a packet, after being switched by LSRs through an MPLS domain, is called "Label-Switched Path" (LSP).

A labeled packet usually carries multiple labels organized as a Last In First Out (LIFO) label stack. These labels are present as encapsulation or as markup inside the packet header. At a router, forwarding decisions are always based in the stack's topmost label, independent of the underlying labels. This label stack is useful to implement tunneling and hierarchy.

The advantages of MPLS over conventional routing are evident in some situations, as given here.

- MPLS forwarding can be done by ASIC-based switches, because only a simple table look-up and label replacement is involved. A computation-intensive large prefix search, as in conventional routing, is gainfully avoided.

- Incoming packets from different ports, or typified by any other header-independent criteria, can be distinguished by the ingress router by assigning them to different FECs. This scores over conventional IP routing, where only the header information can be used for making routing decisions.

- MPLS allows packets to be differentiated on the basis of the ingress router used for entering the MPLS domain. This is difficult in IP routing as the intermediate router addresses are not included in the packet's header.

- Since the mapping of labels to FECs at the ingress LSRs is a one time activity, these mapping algorithms can be made as complex as desired.

- Unlike conventional IP-based source routing, where an extra set of address information is carried, the MPLS needs to only carry a label to specify fixed paths.

Constraint-based Routing

This is a type of QoS-based routing, in which the viability of a route with respect to meeting specific QoS requirements and also meeting other network constraints, like policy, is determined. This type of routing has two major objectives:

- Select routes that meet QoS requirements.
- Increase network utilization and load distribution. A longer and less congested path may be better for QoS-demanding traffic as compared to the shortest, highly congested path.

In this model, routers are required to exchange various kinds of link state information and dynamically compute routes based on this information. To distribute link state information, most implementers of this model extend the link state information contained in the advertisements of OSPF. However, this increases congestion, because of the need for sending frequent advertisements. This is overcome to an extent by transmitting, only when a significant change to network parameters has occurred, e.g. a sharp fall in network bandwidth, etc. The algorithm to calculate routing tables is based on hop count and bandwidth. In constraint- based routing, the routing tables have to be computed more frequently than in dynamic routing, as the computations can be easily triggered by a plethora of factors such as bandwidth changes, congestion, etc.

Although constraint-based routing does a better job of meeting QoS requirements and provides better network utilization, its major disadvantage is the high computation overhead and large sized routing tables. Also, the selected long paths may consume more resources than a shorter path. In addition, the routes may be unstable and are transient most of the time, as the routing tables are being updated too frequently, which may also lead to race conditions.

Subnet Bandwidth Manager (SBM)

Subnet Bandwidth Manager standard has been defined by IEEE to provide QoS on LANs. SBM provides a signaling mechanism to help reserve resources on a LAN. It enables the standard “best effort” LAN to support RSVP flows. This SBM protocol has been retrofitted into Layer 2 LAN protocols to provide better end-to-end QoS for real-time applications over switched or shared broadcast medium Ethernet. The IEEE 802.1p, 802.1Q and 802.1D standards define how Ethernet switches can classify frames in order to expedite delivery of real-time traffic. IETF’s Integrated Services over Specific Link Layers (ISSLL) working group is in charge of defining the mapping of upper-layer QoS protocols and services with those of layer 2 protocols, such as Ethernet. This has resulted in the development of the Subnet Bandwidth Manager for shared or switched 802 Ethernet LAN.

10. Products and Applications

Industry products

Products belonging to important categories of the Voice over IP market, and their typical features are described in the following table.

Category	Products	Category-wise typical features
Gateways	➢ 3COM Gateway ➢ Cisco systems DE-30+ Gateway ➢ Lucent Technologies ➢ MICOM V/IP Gateway ➢ Neura Solutions Access Plus F200 IP ➢ Nortel Networks CVX SS7 Gateway ➢ Pathstar Access Server ➢ Radvision H.323 stack ➢ VocalTec Series 2000 Gateway	▪ LAN- based gateways, which can be installed on a LAN without re-provisioning of network resources ▪ Multiple O/S support ▪ Analog / Digital (T1/E1) link support ▪ Interfaces to existing communications equipment like PABXs and telephones and no need for network re-provisioning ▪ QoS Support ▪ Billing and Account Record processing ▪ Security e.g. PGP ▪ SS7 signaling ▪ Codec support ▪ Interoperability, Bellcore's NEBS compliance ▪ H.323 support ▪ SIP/MGCP support ▪ Network manageable e.g. SNMP ▪ Web based remote management ▪ Scalable ▪ High Availability
Gatekeepers	➢ Elemedia H.323 Gatekeeper GK2000S ➢ Ericsson H.323 Gatekeeper ➢ Nortel Network's IP connect ➢ Radvision H.323 Gatekeeper ➢ VocalTec Gatekeeper	▪ Admissions control and RAS ▪ H.323 support ▪ Dial Plan management ▪ Centralized accounting and billing ▪ Network security ▪ Web based service management ▪ Web based network management ▪ SNMP support ▪ Scalability
Softswitches	➢ Lucent Softswitch	▪ Multi-signal interoperability between SS7, Q.931, H.323, SIP ▪ PSTN/ISDN to IP gateway ▪ Scalable ▪ Multiple-User style configurable ▪ Programmable ▪ Java based portable application

Category	Products	Category-wise typical features
IP Telephones	➢ Cisco IP Phones ➢ Selsius IP Phones	▪ IP enabled ▪ Configurable IP address ▪ LAN enabled ▪ Programmable features ▪ Audio quality voice ▪ Speakerphone ▪ LCD displays ▪ Caller identification ▪ Line status ▪ Directory ▪ Compatible with other H.323 devices ▪ Supports MS NetMeeting-like conferencing solutions
PC based Soft Phones	➢ Microsoft NetMeeting ➢ Netscape CoolTalk ➢ VocalTec Iphone ➢ White Pine CU-SeeMe Pro	▪ PC to phone capability – requires ITSP authorization ▪ Video capability ▪ Audio / video conferencing using conferencing servers ▪ Data collaboration – e.g. white boarding to share documents ▪ Chat ▪ Auto call handling and answering ▪ Directory service

Voice over IP services

Some typical Voice over IP services available in the market are listed below.

Category	Services	Description and Typical Features
PC to Phone Services	➢ VocalTec Surf&Call ➢ Dialpad.com	This service uses gateways to convert signals and voice to IP. ▪ "Click to Talk" / "Click to Fax" types of service ▪ Call center application support for e-commerce ▪ Nearly free long distance call tariffs ▪ Free downloadable software from the Internet

Category	Services	Description and Typical Features
PC to PC Services	➢ Microsoft NetMeeting ➢ VocalTec Iphone ➢ TaoTalk.com	▪ Can be provided without gateways ▪ Audio and video multi conferencing capabilities ▪ Data collaboration facilities ▪ Application share services
Phone to Phone services	➢ America Online at ~x cents/min long distance over IP ➢ AT&T at ~x cents / min long distance over IP ➢ IDT Corporation at ~x cents / min	▪ Local access remains the same as PSTN ▪ Trunk routes are IP networks ▪ Reduced rates ▪ Same PSTN customers are retained
Prepaid calling card based services	➢ AcculinQ at ~x cents / min ➢ USATEL VIA ONE prepaid calling card	▪ Prepaid calling card based ▪ Call from anywhere
Unified Messaging Services	➢ Glenayre Unified Messaging service ➢ Cisco AVVID	▪ All types of messages – email, voice mail, video mail, paging, SMS, are integrated into one browser-based user interface
Network Services	➢ Level 3's IP Crossroad Service ➢ Qwest Virtual Network Service	▪ These provide quality of service over IP networks ▪ Dedicated network trunks and resources, akin to company's Intranet ▪ Large geographical reach ▪ Multimedia capability ▪ Low cost ▪ Intended for corporate use
Services for service providers	➢ ITXC ➢ Delta Three IP Telephony for carriers ➢ Ericsson IP Telephony for carriers ➢ Cisco/ VocalTec hybrid end-to-end services for carriers and service providers ➢ Cisco AVVID	▪ Intended for Telephone carriers and Internet service providers, prepaid calling card companies, call back companies and ITSPs ▪ Billing ▪ Scaleable service ▪ Manageable service

11. Conclusions

The market place is rapidly moving towards convergence of services onto a single user- end device. In doing so, it is moving away from circuit-switched to packet networks. Service providers have already realized the cost benefits of integrating media over the same packet network devices. They are aggressively defining and implementing standards enabling delivery of multimedia over packet-based networks. These cost benefits are being gradually passed over to the user, albeit a trifle slowly, because of telecom regulatory issues and enormous investments in old technology by telecom monopolies across the world.

The Internet has revolutionized the nature of business and societal behavior with an exponentially increasing Internet penetration. The ubiquitous multimedia terminal, whose current avatars are the multimedia desktops, wireless handsets, and Internet- enabled TVs, are increasingly being seen as the indispensable tool to conduct business and social engagements. User expectations of converged multimedia applications have multiplied manifold.

To meet these requirements, service providers need to quickly transition from circuit-switched technologies to packet networks and implement protocols and standards, as discussed in this paper. This transition is still in the nascent stage, as the major issues of Quality of Service, scalability and security of packet networks need to be substantially enhanced to the level of circuit-switched networks.

Major telecommunications companies who have enormous investments in traditional networks have been slow, but are increasingly committed to making this transition. However, Data network service providers and router manufacturers who were already committed to this transition have to scale up and extend the capabilities of their equipment. Cisco and other similar companies, who belong to the data world, have been exceedingly successful in driving this convergence and in increasing user expectations. Traditional Telcos, however, have been pushed to recognize the eventuality of converged networks because of decreasing returns from traditional networks and applications. A host of other new wave companies have also joined this convergence market place with innovative new applications or by providing efficient mechanisms for implementing convergence.

Some of the newer breed of service-providers are increasingly looking into IP networks to deliver quality video and voice to their subscribers. A case in point are the Cable Network operators who are leveraging their wide subscriber base and packaging voice conferencing, video on demand and Internet connectivity along with their traditional video broadcast services. They are providing broadband optical fiber access to the curb or to the users home and using IP as the network layer.

Most of the protocols that have been discussed in this paper, currently have host based implementations. This is mainly because the protocols are evolving. However, with increasing popularity and acceptance, very soon an increasing percentage of their implementations would be in the embedded domain. End user devices including active network nodes will use these protocols as implemented on chips.

At this point, it has become increasingly necessary for the IT industry to understand, master and further the mechanics of convergence and integrate with it. In the near future, we are going to witness the emergence of native Internet HTTP-ish protocols, which will be more efficient, scalable, secured and which will guarantee quality similar to traditional networks. Application architectures will increasingly accommodate these new protocols and deliver a wider range of innovative services, for which organizations would need to plan accordingly.

Acronyms

ACELP	Algebraic Code Excited Linear Predictor
ADPCM	Adaptive Pulse Code Modulation
ATM	Asynchronous Transfer Mode
BSNL	Bharat Sanchar Nigam Ltd. (formerly DOT of India)
ITSP	Internet Telephone Service Providers
LSP	Label Switch Path
LSR	Label Switch Router
MPLS	Multi-Protocol Label Switching
NEBS	Network Equipment Building Standards from Bellcore
OSPF	Open Shortest Path First – A Routing mechanism to decide path
PAM	Pulse Amplitude Modulation
PCM	Pulse Code Modulation
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RTT	Round Trip Turnaround Delay
TCA	Traffic Conditioning Agreement
ToS	Type of Service field in IP header used to differentiate traffic flows
WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Detection

References

RFC	Description
1707	Multi Link Point-to-Point Protocol
1889	RTP — Real-time Transport Protocol
2205	RSVP – Ver 1. Functional Specification
2206	RSVP Management Information Base using SMIv2
2207	RSVP Extensions for IPSEC Data Flows
2209	RSVP — Ver 1. Message Processing Rules
2326	RTSP — Real-time Streaming Protocol
2327	SDP — Session Description Protocol
2543	SIP — Session Initiation Protocol
2745	RSVP Diagnostic Messages
2746	RSVP Operation over IP Tunnels
2747	RSVP Cryptographic Authentication