**THE STATE COMMITTEE OF COMMUNICATION,
INFORMATIZATION AND TELECOMMUNICATION TECHNOLOGIES
OF THE REPUBLIC OF UZBEKISTAN
TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES**

On the rights of manuscript

ABDURAKHMANOV SHOKHRUKH FURKATOVICH

SIP SIGNALING MANAGEMENT IN IMS

5A311301 - Data transmission equipment's and systems

Thesis
for obtaining academic degree of Master

**Scientific adviser
Hosilov K.Ш**

Tashkent 2014

CONTENT

Introduction

The President of Uzbekistan Islam Karimov outlined tasks for rapid implementation of measures and projects in the field of information and communication technologies. In his report, he said, in particular: "More and more importance is being paid to rapid implementation of measures and projects in the field of information and communication technologies. We must realize that without a cardinal, I would say the explosive progress towards wide implementation in all areas of economy, of modern information and communication systems to our everyday life, it is difficult to see the future [1]. We need in the shortest possible time, not only to eliminate the gap occurring in many kinds of information services, but also to enter into the category of advanced countries with a high level of information and communication technologies" - said the head of the state.

The communication, information, financial, banking and transport services and those on auto and household electronic goods repairing developed with highest rates. It is especially worth noting the dynamic development of services in the sphere of information and communication technologies, which for over the past four years have been increasing annually on average by 50 percent. In the countryside we must have not only the developed communities and modern residential houses, but also the high quality roads, no-break power and drinking water supply, developed network of social facilities such as rural medical centers, schools, children’s sport facilities, telecommunications and postal service, as well as other services and trading facilities etc [2].

In recent years Internet usage and services, accessed through both fixed and mobile networks, have experienced rapid growth. This growth was driven by the capability of the Internet to provide many new services seamlessly to the users at any time. These Internet services continue to grow because the open protocols used are available on the web to any service developer. It is estimated that there are over one billion cellular users worldwide. As the number of cellular users continues to grow, more efforts are made to draw the cellular technology closer to the all-IP telecommunication technologies that offer Quality of Service (QoS) to users, and appropriate charging schemes for multimedia services to network operators. With Internet Protocol (IP) becoming spreading through in the backbone, the challenge of integrating voice and data services in the fixed and mobile environments becomes more formidable. The Internet Protocol Multimedia Subsystem (IMS) is a global, access-independent and standard-based IP connectivity and service control architecture that enables various types of multimedia services to end. Users using common Internet-based protocols The IMS was introduced by the Third Generation Partnership Project (3GPP) standardization body for the 3G networks in Release 5 Technical Specification (TS) (3GPP TS 23.228, 2006). Since its introduction, IMS has been adopted by other major telecommunication standardization bodies in mobile and fixed networks as the basis for the 2 Next Generation Network (NGN).

Topicality of the subject of the Master's thesis. Today modern Internet and communication networks are based on the IMS technologies that allow sending different types of information like voice, data, video and others. Within increasing number of Internet users, different problems are going up on the networks. The main problems on the communication networks are quality of service, network security and traffic management on the today’s point.

Therefore, this work is devoted to Analysis of SIP signaling management in IMS.

The main objective of the Master’s Thesis analysis SIP signaling in IMS management with QoS. Consistent with this objective the following tasks have been put analysis SIP signalin with Qos and without QoS and also lost packet analyses and Attempts of sending packets comparison UDP and SIP.

The subject of research is analyzing SIP signaling and IMS technology system and take characteristics from network.

The object of the research is analyzing packets of IMS multiservice networks such as local area network, access network. For example, input and output packets in local area network are inspected.

Methodological basis of research is analyzing NS-2 and Simulation model of lost packet, experimental analysis.

The scientific novelty is implementing Sip signaling systems on the modern telecommunication networks.

Practical value and introduction of the research results. The content of the present work is focused on analyzing SIP and it can implement for controlling systems of GSM, IP-telephony, and other networks.

Publications of research. According to theme of master dissertation are published two scientific works.

Dissertation structure. The dissertation consists of the introduction, three chapters, and conclusions to every chapter and used literature list with final common conclusion.

The first chapter - "IMS Benefit in ICT Network" consists of theoretical aspects IP-packet networks and analysis of DPI solutions for packet networks security in global telecommunication market.

The second part - "The principle of IMS signaling system in multimedia service" defines SIP network elements, User Agent, Proxy Server, Registrar, Session Border Controller, Redirect server, The IMS Architecture, Call Session Control Function, PSTN/GSM Interworking Functions, IMS Elements, Signaling Management in SIP, SIGTRAN and SS7, SIP Signaling Management, H.323 Signal Management, SS7 Signal Management.

In the third part - "Management signaling load in SIP signaling network" Functions of maintenance signaling management in network, procedure flow control signaling traffic, Messages flow control signaling traffic (FCM), are given and explained. Also, SIP Based QoS Management Framework for IMS Multimedia Services is analyzed.

Chapter I. IMS Benefit in ICT Network

1. Multimedia in telecommunication Network

The aim of the proposal was to provide a communication network that could survive the impact of a nuclear war and employed a new approach to data communication based on packet switching. The Department of Defense (DoD) through the Advanced Research Projects Agency (ARPA) commissioned the ARPANET, in 1969. ARPANET was initially an experimental communication network that consisted of only four nodes: UCLA, UCSB, SRI, and the University of Utah. It's popularity grew very rapidly over the next two decades and by the end of 1989, there were over 100,000 nodes connecting research universities and government organizations around the world. This network later came to be known as the 'Internet' and a layered protocol architecture (i.e. TCP/IP ref. Model) was adopted to facilitate services such as remote connection, file transfer, electronic mail, and news distribution over it. The proliferation of the Internet exploded over the past decade to over 10 million nodes since the release of the World Wide Web. The current Internet infrastructure, however, behaves as a 'Best Effort' delivery system. Simply put, it makes an honest attempt to deliver packets from a source to its destination, but provides no guarantees on the packet either being actually delivered and/or the time it would take to deliver it [7].

While this behavior is appropriate for textual data that requires correct delivery rather than timely delivery, it is not suitable for time. Constraint multimedia data such as video and audio. Recently there has been a tremendous growth in demand for distributed multimedia applications over the Internet, which operate by exchanging 'multimedia' involving a myriad of media types. These applications have shown their value as powerful technologies that can enable remote sharing of resources or interactive work collaborations, thus saving both time and money. Typical applications of distributed multimedia systems include Internet based radio/television broadcast, video conferencing, video telephony, real-time interactive and collaborative work environments, video/audio on demand, multimedia mail, distant learning, etc. The popularity of these applications has highlighted the limitations of the current best effort Internet service model and viability of its associated networking protocol stack (i.e. TCP/IP) for the communication of multimedia data. In networking terminology, such performance guarantees are referred to as Quality of Service (QoS) guarantees, and can be provided only by suitable enhancements to the basic Internet Service model. Circuit.switched networks, like the telephony system, Plain Old Telephone Service (POTS), have been designed from the ground up to support such QoS guarantees. However, this approach suffers from many shortcomings like scalability, resource wastage, high complexity and high overhead. Another approach, known as Asynchronous Transfer Mode (ATM), relies on cell switching to form virtual circuits that provide some of the QoS guarantees of traditional circuit switched networks. Although ATM has become very popular as the backbone of high bandwidth and local networks, it has not been widely accepted as a substitute for the protocol stack used on the Internet.

2. Signaling Architecture and Types

SIP fits within the existing Internet multimedia protocol stack as shown in Figure. 1.1. below. SIP elements can be classified as User Agents (UA), proxies and servers or intermediaries. Though it is possible for UAs to communicate directly without the server, servers are generally used by network administrators and service providers to keep track of traffic in their network, and also to protect their business[3].

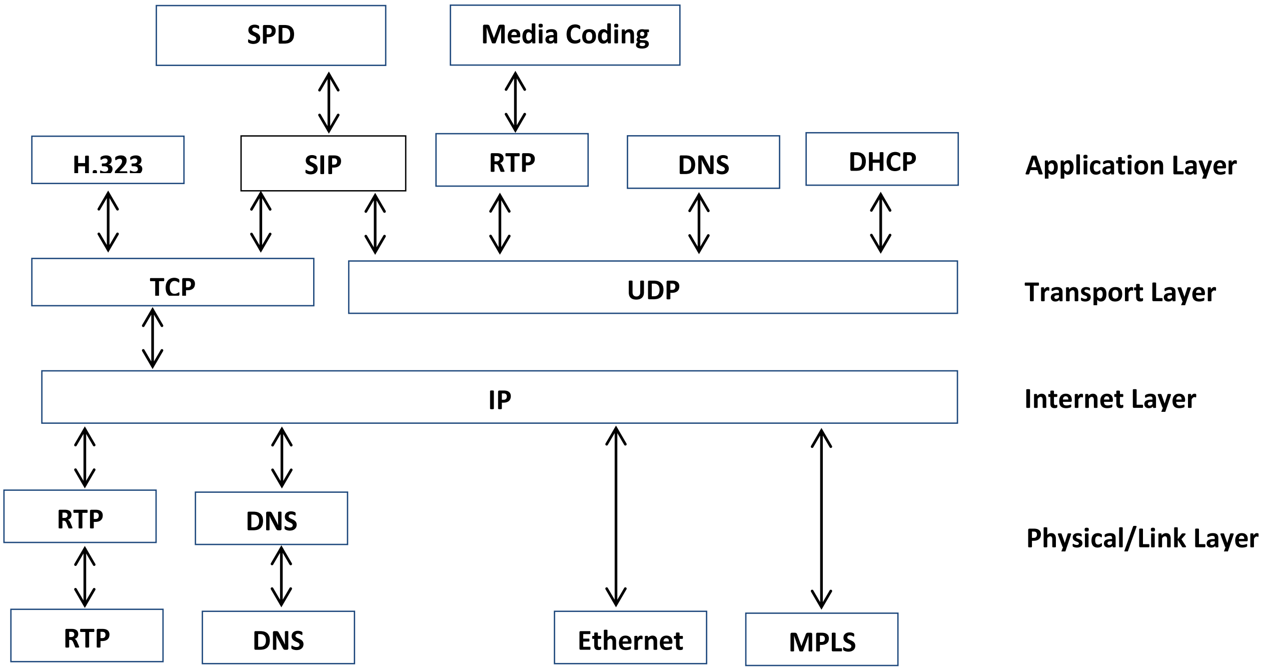

Figure 1.1. The Internet multimedia protocol stack

Shown in Figure 1.1. are the SIP network elements. An SIP UA is the endpoint for dialogs.

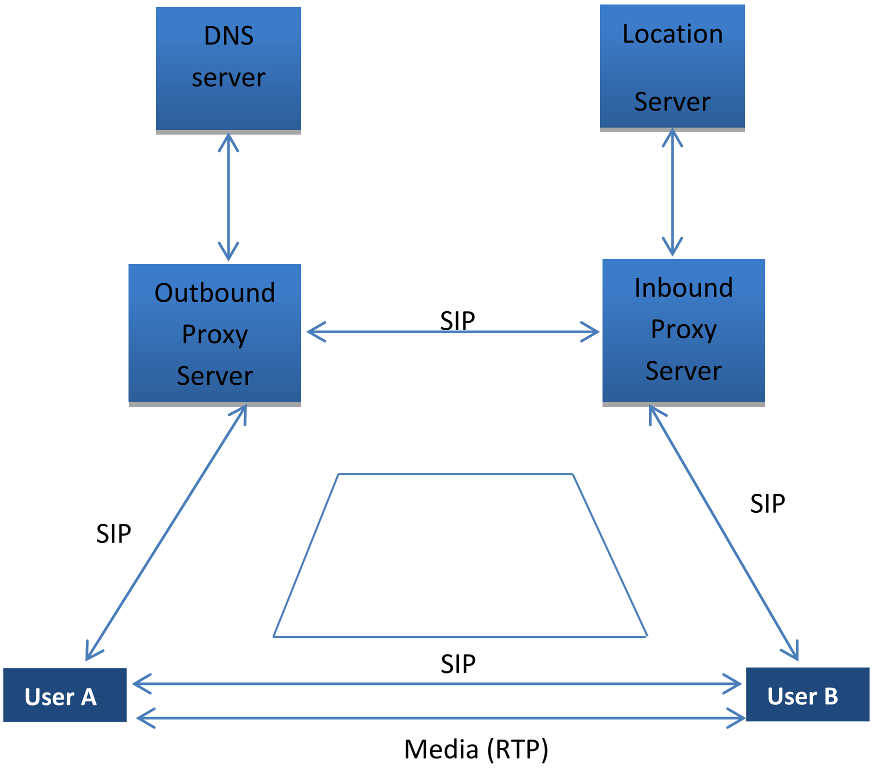

Figure 1.2. SIP Trapezoid

UA runs within a UE and is divided into two parts: UA Client (UAC) and UA Serve (UAS). SIP intermediaries are logic entities through which SIP messages pass on their way to their final destination. They are used to route and redirect the requests. In practice, these entities are owned or housed within the network operator’s premises.

3. Signaling system 7(Ss7)

A worldwide standard for telecommunications defined by the International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU.T). The SS7 standard defines the procedures and protocol by which network elements in the public switched telephone network (PSTN) exchange information over a digital signaling network to enable wireless (cellular) and wireline call setup, routing, and control[4]. American National Standards Institute (ANSI) and Bell Communications Research (Telcordia Technologies) standards used in North America and the European Telecommunications Standards Institute (ETSI) standard used in Europe.

The SS7 network and protocol are used for:

- Basic call setup, management, and tear down.
- Wireless services such as personal communications services (PCS), wireless roaming, and mobile subscriber authentication.
- Local number portability (LNP).
- Toll-free (800/888) and toll (900) wireline services.
- Enhanced call features such as call forwarding, calling party name/number display, and three-way calling.
- Efficient and secure worldwide telecommunications.
- SMS (Short Message Service)**.**

Everything in the telecommunications network is based on signaling—call setup, connection, teardown and billing.

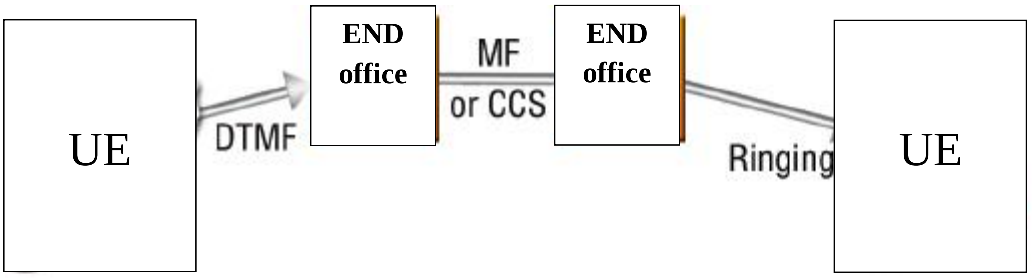

Figure 1.3. CAS: ESF, SF, RBS, MFR2

The two forms of signaling that you are most familiar with used by Patton products are:

- Channel Associated Signaling (CAS) RBS or MFR2 are examples of CAS signaling (see Figure 1.3).
- Common Channel Signaling (CCS) ISDN.PRI

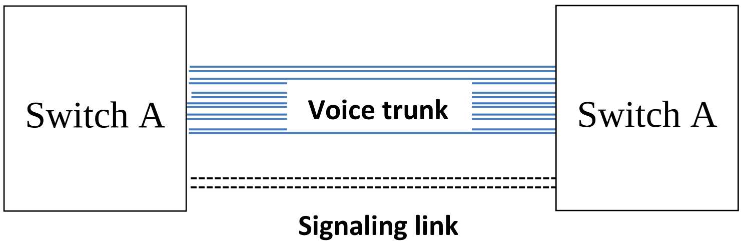

Figure 1.4. CCS: PRI ISDN

While similar to ISDN.PRI, Signaling System Number Seven (SS7) uses different messaging for call setup and teardown. SS7 lets any SS7.enabled node to talk to any other, regardless of whether they have direct trunk connections between them. The preferred mode of signaling for SS7 networks is Quasi Associated, whereas ISDN.PRI uses the Associated Signaling mode[5].

SS7 messages are 56 or 64 kbps bidirectional channels called (signaling links) exchanged between network elements. Signaling occurs out of band on dedicated channels rather than in band on voice channels.

Signaling Points: All nodes in the SS7 network are called Signaling Points (SPs). Each SP is identified by a unique address called a Point Code (PC). SPs have the ability to read a Point Code and determine if the message is for that node and the ability to route SS7 messages to another SP. Each signaling point in the SS7 network is uniquely identified by a numeric point code. Point codes are carried in signaling messages exchanged between signaling points to identify the source and destination of each message. Each signaling point uses a routing table to select the appropriate signaling path for each message. There are three kinds of signaling points in the SS7 network (see Figure 1.5):

- SSP (Service Switching Point or Signal Switching Point)
- STP (Signal Transfer Point)
- SCP (Service Control Point)

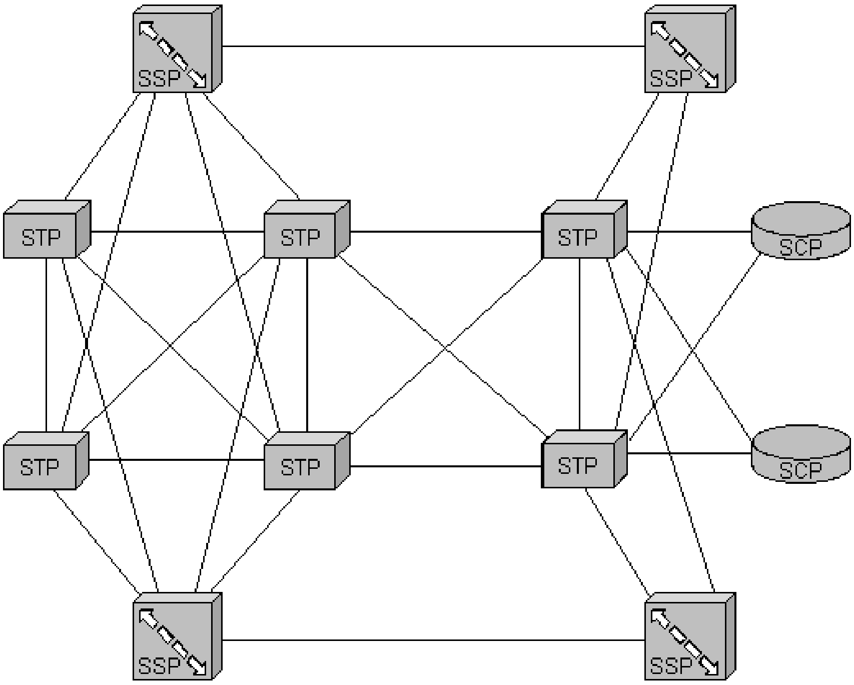

Figure 1.5. SS7 Signaling Points

SS7 Protocol Layers: The SS7 protocol is designed to both facilitate these functions and to maintain the network over which they are provided. Like most modern protocols, the SS7 protocol is layered.

Physical Layer MTP Layer 1: This defines the physical and electrical characteristics of the signaling links of the SS7 network. Signaling links utilize DS–0 channels and carry raw signaling data at a rate of 56 kbps or 64 kbps (56 kbps is the more common implementation).

Data Link Layer MTP: The layer 2 portion provides link.layer functionality. It ensures that the two end points of a signaling link can reliably exchange signaling messages. It incorporates such capabilities as error checking, flow control, and sequence checking.

Network Layer MTP: The layer 3 portion extends the functionality provided by MTP level 2 to provide network layer functionality. It ensures that messages can be delivered between signaling points across the SS7 network regardless of whether they are directly connected. It includes such capabilities as node addressing, routing, alternate routing, and congestion control.

While MTP network management messages and basic call.setup messages are addressed to a node as a whole, other messages are used by separate applications (referred to as subsystems) within a node. Examples of subsystems are 800 call processing, calling card processing, advanced intelligent network (AIN), and custom local.area signaling services (CLASS) services (e.g., repeat dialing and call return). The SCCP allows these subsystems to be addressed explicitly. Enhanced routing is called global title (GT) routing. It keeps SPs from having overly large routing tables that would be difficult to provision and maintain. A GT is a directory number that serves as an alias for a physical network address. A physical address consists of a point code and an application reference called a subsystem number (SSN). GT routing allows SPs to use alias addressing to save them from having to maintain overly large physical address tables. Centralized STPs are then used to convert the GT address into a physical address; this process is called Global Title Translation (GTT). This provides the mapping of traditional telephony addresses (phone numbers) to SS7 addresses (PC and/or SSN) for enhanced services. GTT is typically performed at STPs[5].

4. H.343 Protocol

IP based videoconferencing has grown steadily over the past four to five years as multiple vendors have been piloting proprietary systems on corporate Intranets and the Internet. In 1995, a set of those vendors realized that a standard was necessary for the market to expand and started work on H.323. H.323 was ratified by the ITU.T in May of 1996 and is now the basis for IP conferencing applications ranging from corporate networks to the Internet. The standard was designed with two goals in mind, first, to provide a mechanism for interactive. Multimedia communications on IP packet based networks and second, to define interoperability mechanisms between packet based H.323 endpoints and other H. series standards and traditional telephony. H.323 endpoints can operate over any network that supports the transmission of IP traffic. H.323 includes all of the audio and video algorithms defined for H.320 and H.324 but only mandates G.711 audio and H.261 video[14].

H.323 is built on top of the Internet Engineering Task Force's. IETF Real.time Transport Protocol RTP 24 and. Real.time Transport Control Protocol RTCP specifications that define audio and video transport and control. H.323 call setup is based on an extended Q.931, and its capability exchange mechanisms on H.245. H.323 includes the T.120 series standards for data collaboration and has provisions to allow T.120 terminals to participate in the data portion of a H.323 conference. H.323 includes point to point and multipoint conferences where multipoint conferences have centralized control and either centralized or distributed audio and video. The gatekeeper controls access to the network for terminals, gateways, and MCUs and provides address translation for all H.323 components. A H.323 Gateway provides real-Time, two-Way communications between H.323 terminals on the packet-based network and other ITU.T terminals or telephones on the PSTN or ISDN. A Multipoint Controller MC provides the control services for three or more end points participating in a multipoint conference. A Multipoint Processor MP provides the media services e.g. mixing, switching for three or more endpoints participating in a multipoint conference. Together, the MC and the MP make up a Multipoint Conferencing Unit or MCU.

Figure. 1.6. shows the H.323 components in a typical network deployment. In this Figure 1.6, switched circuit network is abbreviated SCN.

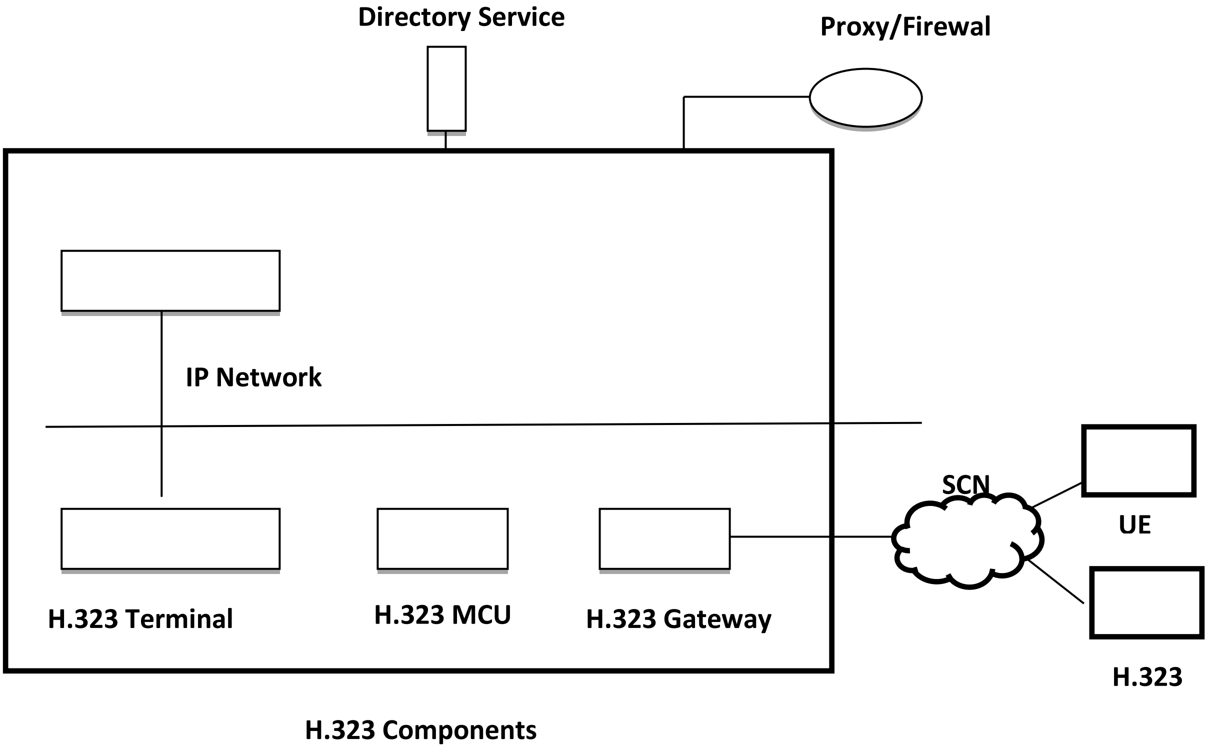

Figure. 1.6. H.323 components.

H.323 terminal: Figure. shows how the generic multimedia terminal architecture has been adapted for H.323 and IP Networks. A H.323 terminal includes the following components[13]:

Call control – H.323 uses an extended Q.931 for its call setup and tear down protocol that was defined specifically for IP network operation. The extended protocol is defined in H.225.0 and uses Q.931 user to user information elements to transfer IP specific information like the H.323 dialing alias.

Connection control – Connection control in H.323 is done by the H.245 protocol. H.245 specifies the commands and procedures for endpoint capability exchange, master slave negotiation, mode switching and mode selection for the various audio, video, and data modes. H.245 uses logical channels to specify what information is being transmitted and contains commands equivalent to those defined in H.242 and H.243. H.245 is more flexible than H.242 or H.243 in that it has advanced capability structures and procedures for signaling multiple media transmission modes. H.245 defines the following services:

- capability definitions with dependencies;
- the ability to request the transmission of a particular audio, video or data mode;
- the ability to manage logical channels;
- the ability to establish a master terminal for the purpose of managing logical channels;
- the ability to control the bit rate of individual logical channels;
- the ability to measure the round trip delay between endpoints.

Audio codec – H.323 includes the same audio algorithms as H.320 and specifies G.711 as mandatory H.323 includes the low bandwidth audio codecs G.723.1 and G.729 for Internet Telephony applications and dial-up links. H.323 specifies how to packetize audio streams based on a whole number of samples or frames depending on the algorithm and allows terminals to stop sending audio when no information _e.g. silence. is detected at the microphone input. audio algorithms that are supported in addition

Video codec – H.323 uses the same video algorithms as H.320 with the additional specification of how to packetize the video streams for transmission on a packet based network. These video algorithms, which were designed to be transmitted in a continuous stream, do not have an elegant method of handling a large piece of missing data e.g. a dropped packet.

Data applications – The same data applications defined in the T.120 protocol suite for use with H.320 are also defined and used for H.323.

Data service’s – Data services in H.323 are provided by the T.120 protocol suite and are run on an IP network specific stack defined in T.123.

Synchronization – Receive Path Delay. In H.323, the transmitter sends timestamps on each audio and video packet which represent the capture time of the data. In this case, the receiver optionally delays the audio to match the video. H.323 terminals differ from H.320 terminals in that they must handle inter packet arrival time jitter. Terminals are typically designed with a packet arrival jitter queue that exceeds the average video to audio codec delay skew by a significant amount. Summarizes the different methods used for media synchronization [14].

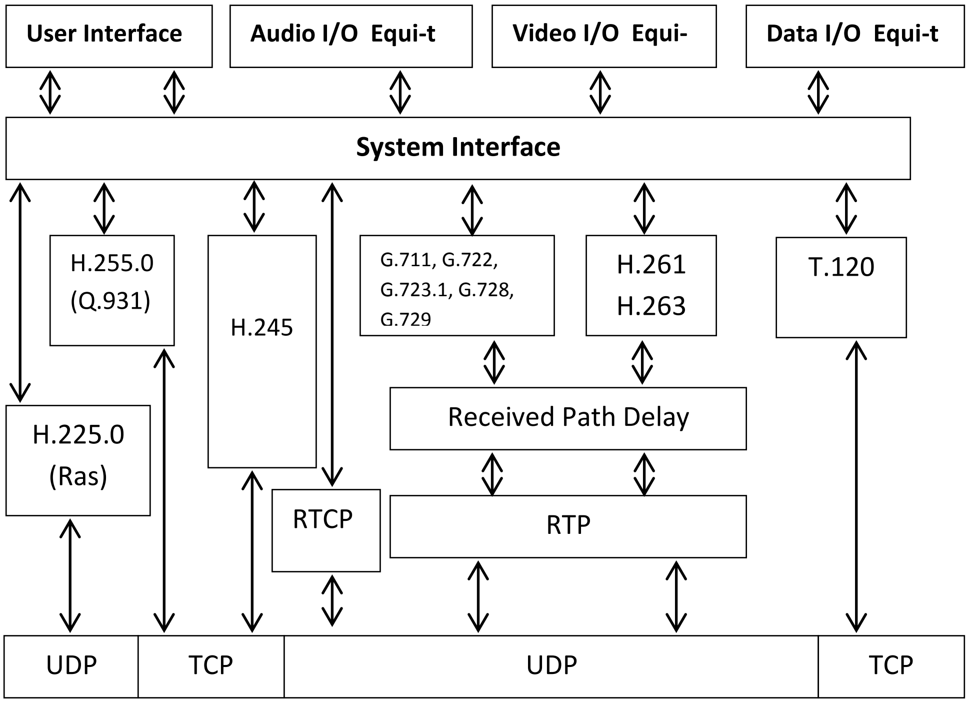

Figure. 1.7. H.323 endpoint architecture

Multiplex – H.323 uses the Real.time Transport Protocol _RTP. for media stream packetization and synchronization. In the case of an IP based network, the UDP port number serves as the multiplex for streams moving across the network. The Real.time Transport Control Protocol RTCP. Provides both transmit and receive statistics between conference endpoints based on the transmission and reception of RTP packets

Gatekeeper: The gatekeeper controls access to the network for terminals, gateways, and MCUs and provides address translation for all H.323 components.

The gatekeeper provides the best opportunity for manufacturers to add standards plus features into their solution. A smartly designed gatekeeper can allow the deployment of multimedia conferencing to be tailored to a specific network configuration. The gatekeeper's key functions include:

Admissions control – Authorizes network access for all endpoints based on a programmed criteria.

Registration and address resolution – The gatekeeper manages terminals, gateways, and MCUs. Gateways and MCUs can be added to a network without the need to configure their location in individual terminals. The gatekeeper acts as an address translation device so users may use aliases such as their email address as their name instead of a network address _e.g. 121.8.4.63. for dialling purposes[6].

Call management – In addition to maintaining lists of ongoing calls, rejected calls, call accounting on the use of WAN links, and the configuration of the other H.323 components, a gatekeeper can provide a call routing function. The call routing function permits endpoints to dial packet or switched based terminals without actually knowing where those terminals are or what network they are connected to. For a typical call, a user will click a name in a phone and then be connected. The details of whether or not the call uses a gateway should be completely invisible to the user of the system.

Gateway: A H.323 Gateway provides real-time, two-way communications between H.323 terminals on the packet based network and other ITU.T terminals or telephones on the public switched telephone network PSTN. or ISDN.

Control processing – Control processing for H.323 is functionally the same as H.320 with the exception that in addition to negotiating the modes of a conference, a MCU also determines how the media in the conference will be distributed.

Media distribution – In H.323, a MCU has multiple options for media distribution. A MCU can conduct a conference using unicast, multicast, or a combination of both transport mechanisms. H.323–H.320 inter working: To properly gateway between a H.323 and H.320 endpoint, H.246 specifies that a gateway must support all of the mandatory functionality specified in the H.320 system specification on its switched circuit network ISDN.

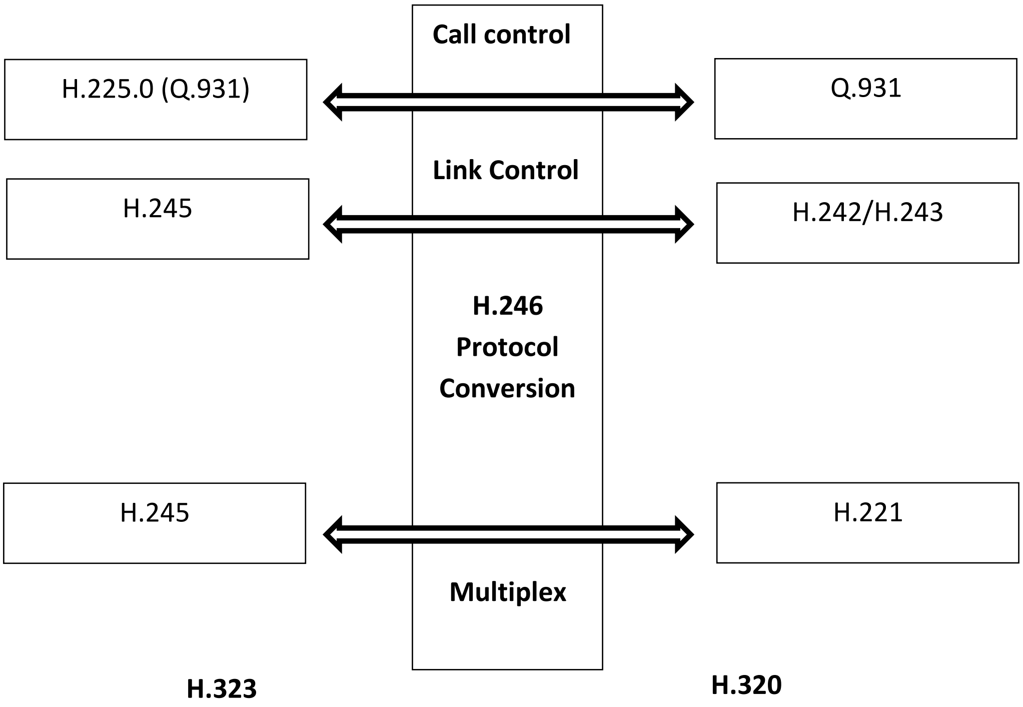

Figure.1.8. H.323 to H.320 protocol conversion defined in H.246

5. Session Initiation Protocol (SIP)

The Session Initiation Protocol (SIP), defined in RFC 3261 is an application level signaling protocol for setting up, modifying, and terminating real time sessions between participants over an IP data network. SIP can support any type of single media or multimedia session, including teleconferencing.

SIP is just one component in the set of protocols and services needed to support multimedia exchanges over the Internet. SIP is the signaling protocol that enables one party to place a call to another party and to negotiate the parameters of a multimedia session[3]. The actual audio, video, or other multimedia content is exchanged between session participants using an appropriate transport protocol. In many cases, the transport protocol to use is the Real-Time Transport Protocol

(RTP). Directory access and lookup protocols are also needed. The key driving force behind SIP is to enable Internet telephony, also referred to as Voice over IP (VoIP). There is wide industry acceptance that SIP will be the standard IP signaling mechanism for voice and multimedia calling services. Further, as older Private Branch Exchanges (PBXs) and network switches are phased out, industry is moving toward a voice networking model that is SIP signaled, IP based, and packet switched, not only in the wide area but also on the customer premises[12].

- User location: Users can move to other locations and access their telephony or other application features from remote locations;
- User availability: This step involves determination of the willingness of the called party to engage in communications;
- User capabilities: In this step, the media and media parameters to be used are determined;
- Session setup point-to-point and multiparty calls are set up, with agreed session parameters;
- Session management this step includes transfer and termination of sessions, modifying session parameters, and invoking services;

SIP employs design elements developed for earlier protocols. SIP is based on an HTTP like request/response transaction model. Each transaction consists of a client request that invokes a particular method, or function, on the server and at least one response. SIP uses most of the header fields, encoding rules, and status codes of HTTP. This provides a readable text. Based format for displaying information. SIP incorporates the use of a Session Description Protocol (SDP), which defines session content using a set of types similar to those used in Multipurpose Internet Mail Extensions (MIME).

SIP Components and Protocols A system using SIP can be viewed as consisting of components defined on two dimensions: client/server and individual network elements. RFC 3261 defines client and server as follows.

Client: A client is any network element that sends SIP requests and receives SIP responses. Clients may or may not interact directly with a human user. User agent clients and proxies are clients.

Server: A server is a network element that receives requests in order to service them and sends back responses to those requests. Examples of servers are proxies, user agent servers, redirect servers, and registrars.

Redirect Server: The redirect server is used during session initiation to determine the address of the called device. The redirect server returns this information to the calling device, directing the UAC to contact an alternate Universal Resource Identifier (URI). A URI is a generic identifier used to name any resource on the Internet. The URL used for Web addresses is a type of URI. See RFC 2396 for more detail.

Proxy Server: The proxy server is an intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. A proxy server primarily plays the role of routing, meaning that its job is to ensure that a request is sent to another entity closer to the targeted user. Proxies are also useful for enforcing policy (for example, making sure a user is allowed to make a call). A proxy interprets, and, if necessary, rewrites specific parts of a request message before forwarding it.

Registrar: A registrar is a server that accepts REGISTER requests and places the information it receives (the SIP address and associated IP address of the registering device) in those requests into the location service for the domain it handles.

Location Service: A location service is used by a SIP redirect or proxy server to obtain information about a caller's possible location(s). For this purpose, the location service maintains a database of SIP.address IP.address mappings.

The various servers are defined in RFC 3261 as logical devices. They may be implemented as separate servers configured on the Internet or they may be combined into a single application that resides in a physical server.

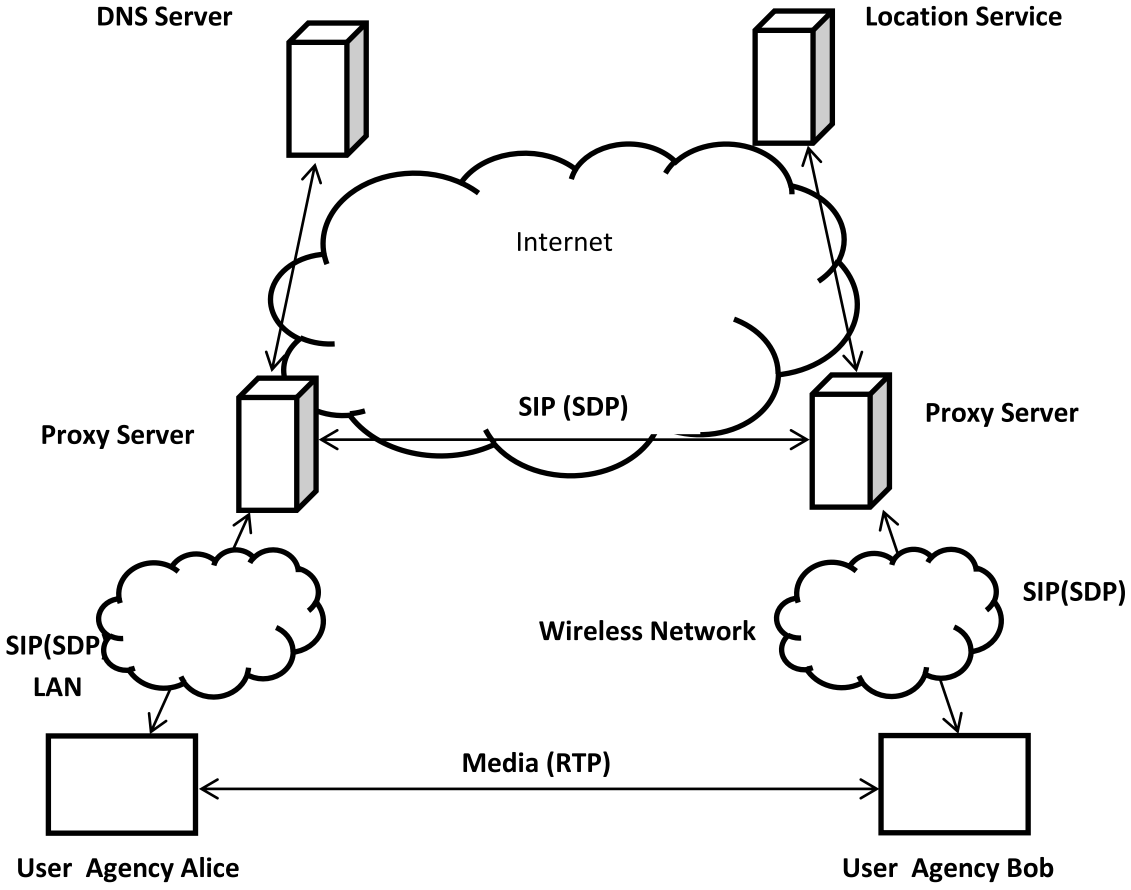

Figure.1.9. SIP components

Figure shows how some of the SIP components relate to one another and the protocols that are employed. A user agent acting as a client (in this case UAC Alice) uses SIP to set up a session with a user agent that acts as a server (in this case UAS Bob). The session initiation dialogue uses SIP and involves one or more proxy servers to forward requests and responses between the two user agents. The user agents also make use of the SDP, which is used to describe the media session.

6. Sigtran

The Signaling Transport (SIGTRAN) working group of the Internet Engineering Task Force (IETF) has designed a new set of protocols to transport SS7 signaling messages over IP. The suite of protocols consists of a new transport protocol and various adaptation protocols and became a standard in 2000 and 2001 and is described in various RFCs on the IETF homepage. Using the SIGTRAN protocols is the first step to merge SS7 networks with IP networks. The primary reason for the use of IP is to off-load the heavily loaded SS7 networks and make them scalable for the increasing amount of telephone and mobile users. The SIGTRAN solution will also be used to connect isolated islands of SS7 networks, which otherwise would have required an expensive SS7 infrastructure[18].

For message delivery over IP on the Internet the transportation protocols Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are used, but for real time signaling they imply certain limitations.

- Ordered, reliable transfer.
- Redundancy in case of link failure.
- Low loss and delay.
- Security against Denial of Service (DoS).

UDP is a connectionless transport protocol that does not intrinsically use acknowledgment (ACK) messages to guarantee reliable and ordered transportation. UDP is useful in situations when high transmission rates are needed, but does not have to fulfill the other performance requirements of signaling messages.

TCP is a byte oriented transport protocol that provides a stream of bytes and guarantees that it is delivered in order. This is ideal for transmitting large amounts of data, such as files or email, but the strictly in-order-delivery is also what makes it unsuitable for signaling messages. TCP is extremely sensitive to delay variance caused by the network or packet loss which often causes retransmissions [13].

The SIGTRAN protocol suite includes the transport protocol SCTP, along with several user adaptation (UA) layer protocols that are necessary for the transport of SS7 messages over IP. The SIGTRAN architecture consists of three layers:

- IP layer;
- Transport layer (SCTP);
- User adaptation layer (e.g. M2PA, M2UA, M3UA, and SUA).

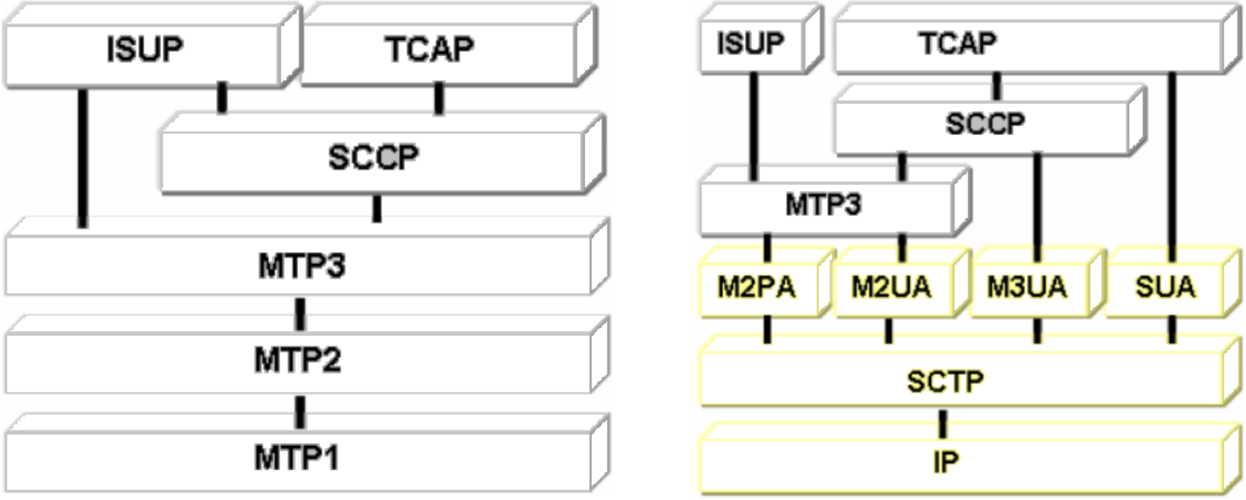

Figure.1.10. The MTP1 and MTP2 layers in the traditional SS7 stack (left) are replaced by SIGTRAN protocols (right) to enable signaling over IP[18]

In Figure 1.10, the three lower layers in the protocol stack show the new SIGTRAN protocols. They replace the lower layers of the SS7 stack (MTP1 and MTP2), enabling transportation over IP. SCTP is a transport protocol similar to TCP, but with a few changes to better suit SS7 signaling. A user adaptation protocol makes its SS7 user (MTP3, SCCP, TCAP, ISUP etc.) unaware of that the original lower SS7 layers have been replaced. In Figure 1.10 the ISUP connection to M3UA is not shown to simplify the figure, but it is also a frequent protocol combination. Depending on the telephone network, different user adaptation protocols can be chosen depending on their characteristic features.

MTP2.user Peer-to-peer Adaptation layer (M2PA) is a SIGTRAN protocol that transports SS7 MTP signaling messages over IP using SCTP. It is an adaptation protocol between MTP3 and SCTP and works between pairs of signaling nodes. Using M2PA makes it possible to maintain the original topology of the SS7 network, i.e. all the network elements such as Signaling Transfer Points (STPs), point codes, etc. The only thing that changes is that transportation of signaling occurs over IP instead of over traditional 64 kbit/s links; see Figure 1.11.

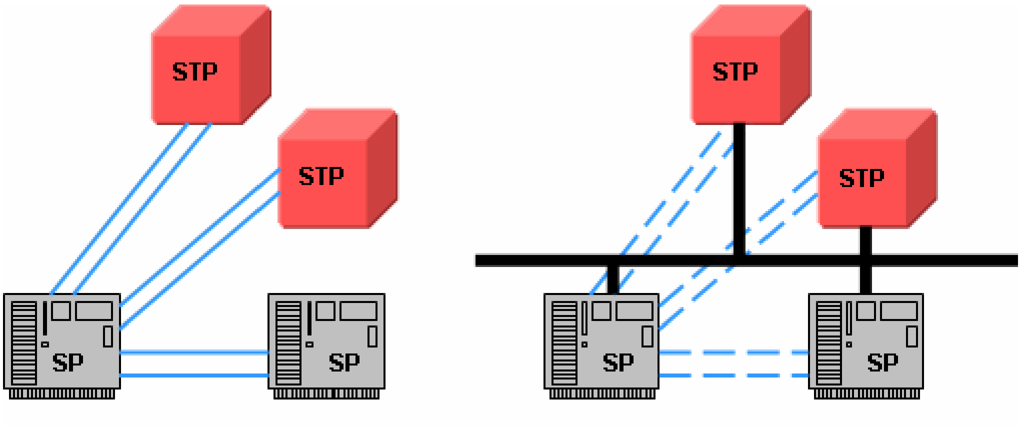

Figure. 1.11. M2PA changes the physical links between nodes[5]

M2PA can be used between two IP signaling nodes in an IP network, or between a Signaling Gateway (SGW) and an IP signaling node, but is most common between two SGWs, e.g. to interconnect two SS7 network islands (PSTN A and PSTN B) through an IP network. Figure 1.12 shows the two distant SS7 networks that are combined together via a less expensive IP network. The IP solution mixes signaling traffic with other IP traffic and therefore reduces the costs of signaling, since a link can be shared among many users[5].

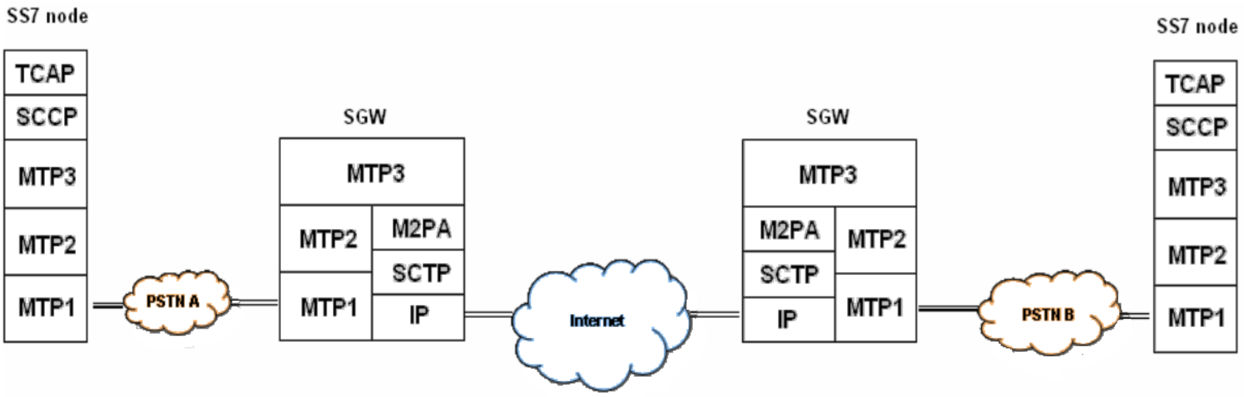

Figure 1.12. Two distant SS7 network islands are connected over Internet through M2PA

Since both SGWs have an MTP3 layer they also have a point code and a SS7 PC must be assigned to each SGW. Because of the peer to peer feature of M2PA, it is possible for the MTP3.peers to communicate directly. The user of M2PA is

MTP3 in both nodes, just as MTP3 is the user of MTP2 in the SS7 stack. This means that M2PA is actually just a replacement for MTP2 and therefore has functions similar to MTP2.

MTP2.User Adaptation layer (M2UA) also adapts MTP3 to SCTP, and is a protocol that sends signaling messages between the MTP3 layer on a media gateway controller (MGC) and the MTP2 layer on a SGW, e.g. in a VoIP network. Instead of being a peer.to.peer protocol like M2PA, it operates on a client.server basis, where the MGC (IP node) is the client and the SGW acts as the server. This way the MTP3 layer on the MGC is the user of the MTP2 layer on the SGW, and neither of them is aware that they actually are remote. This phenomenon when signaling messages are transported over IP from the top of one SS7 layer to the bottom of another is called backhauling. Since the SGW does not have an MTP3 layer, only the MGC has a point code, see Figure. 1.13.

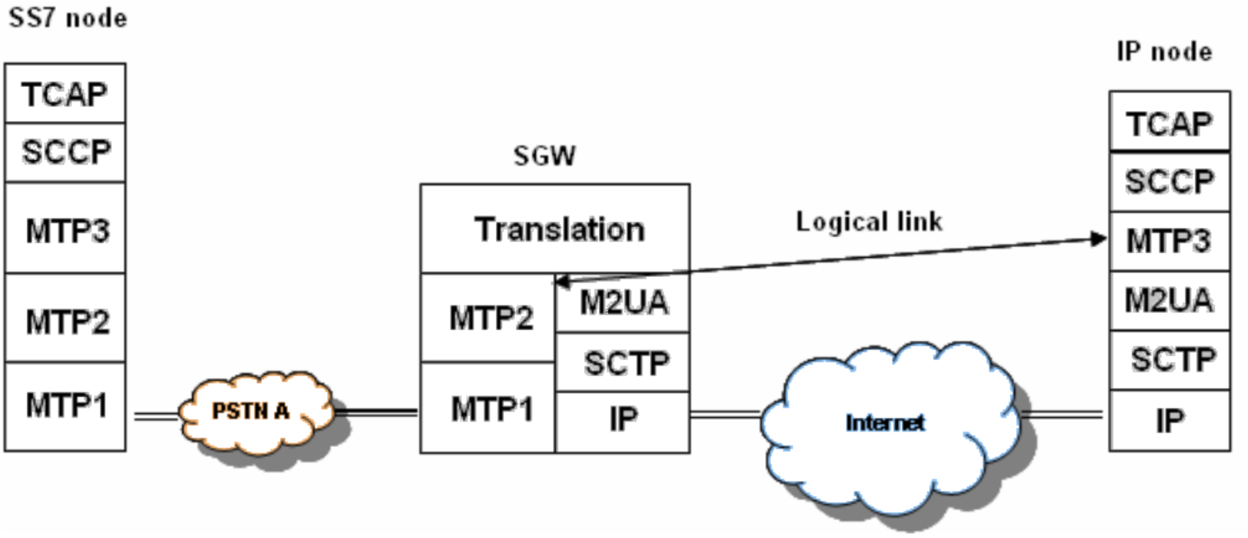

Figure.1.13. Back hauling with M2UA in two distant nodes. The SGW and the MGC are not aware that they are remote and each node thinks that MTP3 is directly communicating with MTP2

M2UA is frequently used when there is a low density of physical SS7 links in some particular part of the network, or if the SGWs are at a great distance from each other. In this case backhauling can connect several of these signaling nodes to one centralized network element, thus allowing these distant nodes to share a single SGW. Since this is done over the IP network, it is much cheaper than SS7 links, hence M2UA is a cost saving alternative. Another advantage is the fact that each SGW, that connects a remote signaling point to a MGC, does not have a point code. The point code is assigned to the MGC, which saves many SS7 PCs that would otherwise have been required by each SGW (as when using M2PA)[5].

The MTP3 User Adaptation (M3UA) layer operates on a client.server basis, just as M2UA, to provide remote connection between two SS7 layers in a SGW and a MGC (IP node). However, in this case, the SGW has a MTP3 layer (and a point code) that communicates with the ISUP/SCCP layer of the MGC, see Figure. Even in this case, the nodes are not aware of each other; the MTP3 in the SGW does not know that its user (ISUP or SCCP) is remote and similarly the ISUP/SCCP layer at the MGC does not know that the SGW´s MTP3 layer is not its own. This is another example of backhauling.

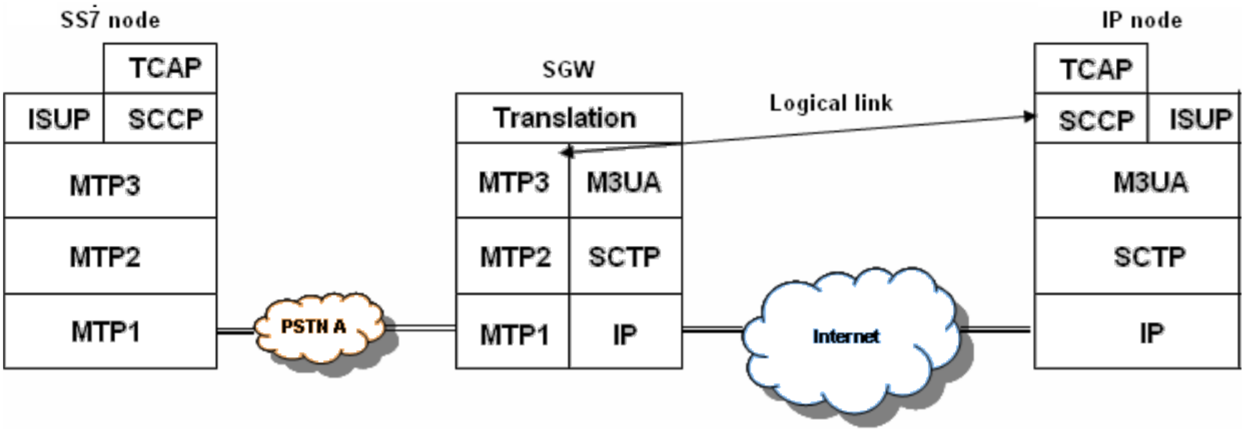

Figure. 1.14. Backhauling using M3UA[18]

As with M2UA, M3UA does not process any signaling packets; it simply forwards them to their destination. This means that the M3UA in the IP node does not have routing tables and does not execute any other functions of the corresponding MTP3 layer. If M3UA is used in an all-IP network with no pure SS7 nodes, it replaces the MTP3 layers of the both IP nodes and operates in a point to point manner that is known as IP Signaling Point (IPSP) behavior. M3UA is one of the user adaptation layer protocols that remove most SS7 layers from the signaling points and that change the topology of the network to a more IP-like one. In an all-IP network, M3UA is not restricted to the SS7 requirements of maximum message size of 272 bytes, but can use the larger bandwidth of available via the IP network. The flexibility of M3UA and its ability to better use the IP network and its advantages have lead to it being chosen as the standard protocol for UMTS networks.

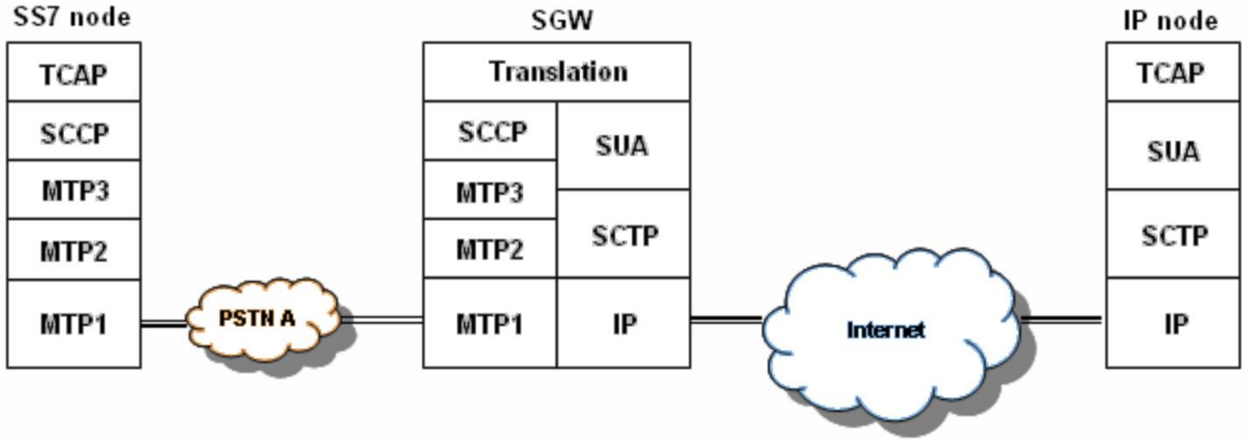

Figure 1.15. Backhauling with SUA

The SUA layer’s main tasks are to transfer SCCP user data between a SGW and a MGC (client. Server model) and to map between SCCP addresses and IP addresses in the SGW. However, because of SUA´s inability to transport ISUP messages (see Figure, 1.15), 3GPP has chosen to use M3UA as the standard signaling protocol in the central parts of the UMTS networks while using SUA as a complement for nodes with databases, e.g. home location registers (HLRs).

Conclusion on chapter I

The development of ims has taken many years, and the rate of its take-up has perhaps been slower than its proponents had first envisioned. however, in recent years it has become clear that ims really will make a significant impact on the industry. In a world looking towards widespread coverage and declining traditional wireline usage, a network architecture that focuses on services, not access, is something all carriers should be interested in. the promise of ims to converge fixed and mobile networks onto an ims core supporting a common set of services has to be attractive to those who currently face the operational costs of running two separate networks in parallel. from a long term view ims offers not only reduced network operational costs, but also lower barriers to entry for innovative services to be deployed rapidly. In a world with declining traditional

Network architecture that focuses on services, not access, has to be an attractive solution. For traditional wireline carriers, although IMS formally only defines a method for native SIP endpoints within a network, there has been much work to address how to incorporate legacy endpoints into the architecture, while minimizing the cost and impact of the transition. To understand the IMS architecture in more detail. And has a broad product portfolio that can be deployed today to enhance an existing IMS network, or can be deployed to manage a seamless phased migration from the existing network toward an IMS future.

Chapter II. The principle of IMS signaling system in multimedia service

1. SIP network elements

Although in the simplest configuration it is possible to use just two user agents that send SIP messages directly to each other, a typical SIP network will contain more than one type of SIP elements[3]. Basic SIP elements are user agents, proxies, registrars, and redirect servers. We will briefly describe them in this section[7].

Note that the elements, as presented in this section, are often only logical entities. It is often profitable to co.locate them together, for instance, to increase the speed of processing, but that depends on a particular implementation and configuration.

2. User Agents

Internet end points that use SIP to find each other and to negotiate a session characteristics are called user agents. User agents usually, but not necessarily, reside on a user's computer in form of an application. This is currently the most widely used approach, but user agents can be also cellular phones, PSTN gateways, PDAs, automated IVR systems and so on.

User agents are often referred to as User Agent Server (UAS) and User Agent Client (UAC). UAS and UAC are logical entities only, each user agent contains a UAC and UAS. UAC is the part of the user agent that sends requests and receives responses. UAS is the part of the user agent that receives requests and sends responses. For instance, caller's user agent behaves like UAC when it sends an INVITE requests and receives responses to the request. Caller's user agent behaves like a UAS when it receives the INVITE and sends responses[8].

Three user agents and one statefull forking proxy. Each user agent contains UAC and UAS. The part of the proxy that receives the INVITE from the caller in fact acts as a UAS. When forwarding the request statefully the proxy creates two UACs, each of them is responsible for one branch. In our example caller B picked up and later when he wants to tear down the call it sends a BYE. At this time the user agent that was previously UAS becomes a UAC and vice versa.

3. Proxy Servers

In addition to that SIP allows creation of an infrastructure of network hosts called proxy servers. User agents can send messages to a proxy server. Proxy servers are very important entities in the SIP infrastructure. They perform routing of a session invitations according to invitee's current location, authentication, accounting and many other important functions.

The most important task of a proxy server is to route session invitations "closer" to caller. The session invitation will usually traverse a set of proxies until it finds one which knows the actual location of the called. Such a proxy will forward the session invitation directly to the called and the caller will then accept or decline the session invitation. There are two basic types of SIP proxy servers stateless and stateful[11].

4. Registrar

We mentioned that the SIP proxy at proxy.b.com knows current Bob's location but haven't mentioned yet how a proxy can learn current location of a user. Bob's user agent (SIP phone) must register with a registrar.

The registrar is a special SIP entity that receives registrations from users, extracts information about their current location (IP address, port and username in this case) and stores the information into location database. Purpose of the location database is to map sip:bob@b.com to something like sip:bob@1.2.3.4:5060. The location database is then used by B’s proxy server. When the proxy receives an invitation for sip:bob@b.com it will search the location database. It finds sip:bob@1.2.3.4:5060 and will send the invitation there. A registrar is very often a logical entity only. Because of their tight coupling with proxies registrars, are usually co. Located with proxy servers. A REGISTER message containing Address of Record ip:jan@iptel.org and contact address sip:jan@1.2.3.4:5060 where 1.2.3.4 is IP address of the phone, is sent to the registrar. The registrar extracts this information and stores it into the location database[13].

Each registration has a limited lifespan. Expires header field or expires parameter of Contact header field determines for how long is the registration valid. The user agent must refresh the registration within the lifespan otherwise it will expire and the user will become unavailable.

5. Session Border Controller

A session border controller is a device used in some Voice over Internet Protocol (VoIP) networks to exert control over the signaling and usually also the media streams involved in setting up, conducting, and tearing down telephone calls or other interactive media communications. Within the context of VoIP, the term session refers to a call. Each call consists of one or more call signaling message exchanges that control the call, and one or more call media streams which carry the call's audio, video, or other data along with information of call statistics and quality. Together, these streams make up a session. It is the job of a session border controller to exert influence over the data flows of sessions.

The term border refers to a point of demarcation between one part of a network and another. As a simple example, at the edge of a corporate network, a firewall demarcates the local network (inside the corporation) from the rest of the Internet (outside the corporation). A more complex example is that of a large corporation where different departments have security needs for each location and perhaps for each kind of data. In this case, filtering routers or other network elements are used to control the flow of data streams. It is the job of a session border controller to assist policy administrators in managing the flow of session data across these borders[6].

The term controller **r**efers to the influence that session border controllers have on the data streams that comprise Sessions, as they traverse borders between one part of a network and another. Additionally, session border controllers often provide measurement, access control, and data conversion facilities for the calls they control.

6. Redirect Server

The SIP Redirect feature allows the IMG to respond to the 3xx class of SIP messages returned from a redirect server. The 3xx responses provide information about a user's new location, or alternative services that may be able to satisfy the call. This feature is based on RFC 3261 section 8.1.3.4 and RFC 2543.

In a SIP network it is very common to have a redirect server which determines where to route the call. The redirect server may reply to the 2020 IMG with a 300 response which has a list of contacts to try to connect with. The 2020 IMG will try each one of those contacts one at a time, until the call is completed, to a maximum of 10 attempts. The 2020 IMG only accepts a redirect to another endpoint in the SIP network and the SIP endpoint does not have to be one of the configured as an external gateway within WebUI [6].

7. IMS Architecture

IMS, introduced in 3GPP Rel.5, has been built around a collection of core components with distinctive functionality (Figure 2.1). SIP, which is the main traffic control protocol in IMS, was developed by the Internet Engineering Task Force (IETF) and adopted by 3GPP for IMS. A quick look under the hood shows that IMS applies many proven and trusted concepts from GSM, such as the core network architecture, service triggering, and mobility. IMS enforces strict separation between control plane and user plane [11]. The control plane consists of network entities that are primarily involved in controlling establishment, usage, charging, and termination aspects for communication services. The user plane, by contrast, consists of network entities that process and transport media. This separation makes it possible to transport media between participants along an optimized path and with defined quality of service. The individual components in a communication service are made up of a mix of media – for example, voice and streaming video – and might even follow separate paths. Unlike traditional circuit. Switched networks, IMS does not establish the media path (“circuit”) when a call or session is established.

That is, the capacity for transporting media is not allocated until a media transport session is actually needed and established. Therefore, media transport, which includes actions like call forwarding and call transfer, can be optimized for an established call.

The establishment of an IMS based communication session involves the negotiation of media capabilities between the calling and called parties. In addition, these parties as well as the IMS application servers involved in an IMS based communication session may renegotiate media capabilities or add a multimedia component at any time during a call.

The IMS architecture as defined by the 3GPP standards is an all. Packet core network that creates an access. Agnostic environment to deliver a wide range of multimedia services that a user can access using any device or network connection. Leveraging the SIP protocol, IMS supports IP to IP sessions over any wireline connection (e.g., DSL, cable) or wireless network protocol (e.g., Wi.Fi, GSM or CDMA). The IMS infrastructure allows a carrier to interwork between the TDM and IP networks to provide a seamless service experience. Access layer: IMS is access independent. In case of mobile, it can be GPRS, EDGE (also called enhanced GPRS), UMTS or Wireless LAN. 3GPP UMTS R5 focuses on EDGE and UMTS accesses. 3GPP UMTS R6 adds WLAN. 3GPP2 assumes cdma2000 accesses. Fixed service providers will apply IMS to ADSL and cable network accesses [10].

Session Control layer: Comprises network control servers for managing calls or establishing sessions and modifications. The two main elements of this layer are the CSCF (call session control function) and the HSS (home subscriber server). Sometimes called the SIP server, the CSCF performs end.point registration and routing of the SIP signaling messages to the application server related to a particular service. In addition, the CSCF interworks with the access and transport layers to guarantee QoS for all services. The HSS database maintains each end user’s service profile.

Application layer: Utilizes application and content servers to provide various value. Added services. At the heart of this layer are the AS (application server), MRFC (multimedia resource function controller), and the MRFP (multimedia resource function processor). The AS is responsible for the execution of service. Specific logic, for example call flows and user interface interactions with subscribers, while the MRFP—more commonly known as the IP media server—provides adjunct media processing for the application layer.

Underlying Concepts of the IMS Architecture A set of requirements has been introduced for the design of IMS.

IP connectivity A fundamental requirement is that a client has to have IP connectivity to access IMS services. In addition, it is required that IPv6 is used.

Access Independence The IMS is designed to be access.independent so that IMS Services can be provided over any IP connectivity networks (e.g., GPRS, WLAN, broadband access xDSL, etc). IMS specifications contain some GPRS.specific features. (e.g., GPRS) access specific issues are separated from the core IMS description.

Ensures Quality of Service from IP Multimedia Services Via the IMS, the terminal negotiates its capabilities and expresses its QoS requirements during a Session Initiation Protocol (SIP) session set.up or session modification procedure.

The terminal is able to negotiate such parameters as: Media type, Media type bit rate, packet size, packet transport frequency, bandwidth, etc. After negotiating the parameters at the application level, the terminals reserve suitable resources from the access network.

IP Policy control for ensuring correct usage of media resources IP policy control means the capability to authorize and control the usage of bearer traffic intended for IMS media, based on the signaling parameters at the IMS session. This requires interaction between the IP connectivity access network and the IMS. Charging arrangements The IMS architecture allows different charging capabilities to be used, particularly, off.line (postpaid) and on.line (prepaid) charging.

Interworking with other networks To be a new, successful communication network technology and architecture, the IMS has to be able to connect to as many users as possible. Therefore, the IMS supports communication with PSTN, ISDN, mobile and Internet users. Additionally, it will be possible to support sessions with Internet applications that have been developed outside the 3GPP community.

Service control IMS provides all the network with all the information about the services the user has subscribed to, so that standardized mechanisms are used to enable the network invoking the user’s services.

8. Call session control Function

In GSM, a user can roam on to visited networks provided that the visited network can access the home HLR and an agreement exists between the two operators. The same kind of roaming is supported for R5 multimedia services. In GSM roaming, call control always takes place in the visited network, the only connection to the home network being access to the HLR[15].

In IMS, there was a long and complicated discussion about whether IP multimedia call control for roamers should take place in the visited or home network. Those who said it should take place in the home network pushed the argument that the user would have signed for a range of services, and many of these would not be available or would work differently in a visited network. Those who favored visited network control were concerned about the long delays and signaling traffic created by having all services controlled from the home network that might be located on a different continent. In the end, it was decided that IMS control would be controlled from the home network. This complication gives rise to three flavors of CSCF (Proxy CSCF, Interrogating, Serving CSCF).

CSCF = Call Statefull Control Function. A P.CSCF (Proxy CSCF) is a mobile's first contact point inside a local (or visited) IMS It acts as a SIP Proxy Server. In other words, the P.CSCF accepts SIP requests from the mobiles and then either serves these requests internally or forwards them to other servers.

The P.CSCF includes a Policy Control Function (PCF) that controls the policy regarding how bearers in the GGSN should be used. The P.CSCF performs the following specific functions :

- Forward SIP REGISTER request from a mobile to the mobile 's home network.
- Forward other SIP messages from a mobile to a SIP server (e.g., the mobile's S.CSCF in the mobile's home network).
- Forward SIP messages from the network to a mobile.
- Perform necessary modifications to the SIP requests before forwarding them to other network entities.
- Maintain a security association with the mobile.
- Detect emergency session.
- Create CDRs.

An I.CSCF (Interrogating CSCF) is a contact point within an operator's network for all connections destined to a subscriber of that network operator. There may be multiple ICSCFs within an operator's network.

An S.CSCF (Serving CSCF) provides session control services for a user. It maintains session states for a registered user 's on.going sessions and performs the following main tasks :

9. PSTN/GSM Interworking Functions

The IMS networks need to interact with PSTN so that IMS users can establish services to PSTN users. The architecture for supporting PSTN and legacy mobile networks is shown in The interworking between IMS networks and PSTN/legacy networks occur at two levels: One is the user plane level and the other is the signaling plane level. In the user plane, interworking elements are required to convert IP based media streams on the IMS side to TDM based media streams on the PSTN side. The IMS Media Gateway (IMS.MGW) element is responsible for this function. The IS.MGW elements are controlled by the Media Gateway Control Function (MGCF) through the Megaco protocol. On the signaling plane level, the SIP signaling needs to be converted to legacy signaling such as ISDN Signaling User Part (ISUP)[15]. The MGCF is responsible for converting SIP signaling to legacy signaling such as ISUP. The MGCF is responsible for transporting ISUP signaling messages to a Trunking Signaling Gateway (T.SGW) over IP transport bearer. The T.SGW transports these ISUP messages over the SS7 bearer to either the PSTN or the legacy wireless networks.

The PSTN switch reserves a voice circuit among those it shares with the IMS.MGW and sends an ISUP IAM message over SS7 to a T.SGW (Trunking Signaling Gateway). The TSGW is responsible for signaling transport conversion. It forwards the ISUP IAM message to the MGCF entity over SIGTRAN (Signaling Transport over IP). The MGCF creates a context in the IMS.MGW using the MEGACO/H.248 protocol. This context consists of an association between a TDM termination and an RTP termination. The TDM termination terminates the voice circuit the IMS.MGW shares with the PSTN switch. The RTP termination terminates the RTP channels between the IMS.MGW and the IMS terminal.

10. IMS Elements

The IMS overlay architecture is widely abstracted from the air interfaces, hence IMS can be used for any mobile access network technology, as well as for fixed.line access technology, as currently promoted by TISPAN within the NGN reference architecture definition (Magedanz, Witaszek & Knuettel, 2005). The 3GPP IMS introduces some new elements which require the network operators to upgrade their Core Network (CN) to provide IMS services. Some of the IMS network elements are shown in Figure 2.4, below.

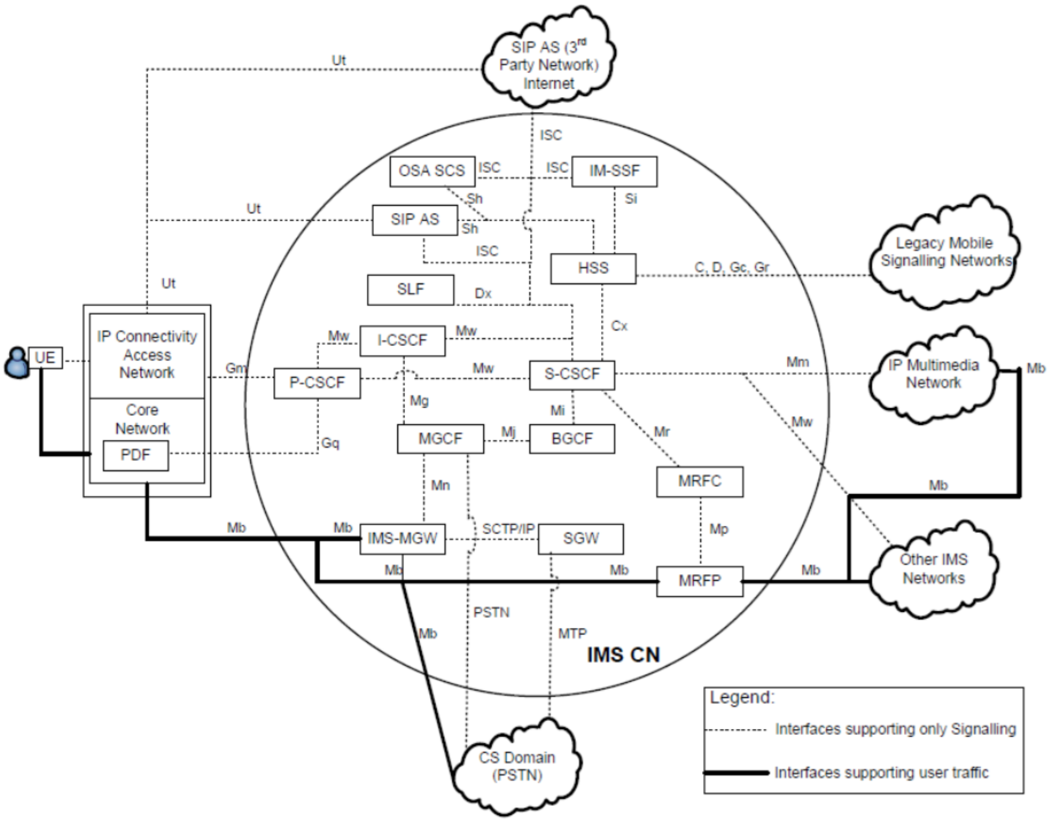

Fig 2.4. The 3GPP IMS Architectural Elements[9]

User Equipment (UE):The UE is the IMS.capable terminal used by the subscriber to access IMS services. It contains the SIP UA that generates and terminates the exchange of SIP messages on the user’s behalf. Once an IP address has been allocated for registration, the UE cannot change it while engaged in an active dialog[9].

Proxy CSCF (P.CSCF):The P.CSCF is the first contact point within the IMS network by the User Equipment (UE). It accepts requests and services them internally or forwards them. The P.CSCF does not modify the request URI in the SIP INVITE message. It can sometimes behave like a UA by terminating and independently generating SIP transactions. The P.CSCF can also generate Charging Data Records (CDR), emergency session detection and also maintain a security association between itself and each UE.

Interrogating CSCF (I.CSCF) I.CSCF is responsible for querying the HSS to determine the S.CSCF for the user. It is the contact point within an operator's network. It is also responsible for establishing the interface between two different IMS networks such as the home and visitor network. An I.CSCF has the Topology Hiding Inter.network Gateway (THIG) which can be used by the network operator to hide network configuration and topology. This function hides the addresses of operator network entities from being passed outside the operator's network.

Serving – CSCF (S.CSCF) The S.CSCF is the heart of the IMS network. It is responsible for processing registrations, for recording the location of each user and also for performing the user authentication, calls processing and routing of calls to the ASs. The S.CSCF performs session control services for the UE. A network operator may have multiple S.CSCFs with each S.CSCF handling different functions. Other S.CSCF functions includes the interaction with AS for the support of services, forwarding SIP request/response to a BGCF for call routing to the PSTN or CS domain and also generating the CDR.

Media Resource Function Processor/ Controller The Media Resource
Function Controller (MRFC) is responsible for the control of media stream resources in the Media Resource Function Processor (MRFP) and the generation of CDR. It also screens the information coming in from the AS and S.CSCF and then controls the MRFP accordingly. The MRFP is responsible for the control of bearer on the Mb interface and providing the resources to the MRFC.

Breaking Gateway Control Function The Breaking Gateway Control Function (BGCF) is used to dial the CS domain users from the IMS network. It selects the network in which PSTN breakout should occur and receives such requests from the S.CSCF. When a user in the IMS network wishes to communicate with other users in the CS domain, the BGCF forwards the session signalling to the called user. The BGCF also generates the CDR[8].

Home Subscriber Server (HSS) The IMS architecture contains two main databases: HSS and the Subscription Locator Function (SLF). While the GSM systems use the Home Locator Register (HLR) to store the user profile, HSS provides the main data storage for all subscriber and service.related data of IMS. The data stored in the HSS includes public and private user identities, registration information, access parameters, service triggering information, and user specific requirements for S.CSCF capabilities. The SLF is used in the network operators who have multiple HSS as a resolution mechanism that enables the I.CSCF, S.CSCF and the AS to find the address of the HSS that holds the subscriber data for a given user identity.

Application Server (AS) Service provisioning in IMS is achieved by the AS, which are contacted on the basis of initial filter criteria. Filter criteria are downloaded by the S.CSCF from the HSS during registration and are part of IMS subscribers' service profile. An AS is a special server and a unique service network entity that fulfils a fixed specific role. It is also responsible for detecting the subscriber presence for IM and presence application. The Service Delivery Platform is a server that extends the AS, therefore it can provide more than a specific service. It enables the creation of service on demand.

Policy Decision Function Policy Decision Function (PDF) takes a service level policy request from the application layer (for example P.CSCF) and translates it into IP QoS parameters. In General Packet Radio Service (GPRS) networks, the PDF uses the 'Go' interface to set the policy for sessions in the Gateway GPRS Support Node (GGSN). In TISPAN.based networks, the PDF contacts the Border Gateway Function (BGF) to enforce the policy. PDF and P.CSCF were combined inRelease 5 (3GPP TS 24.228, 2006) specification of the 3GPP IMS, but the PDF was separated, as a stand-alone element, from P.CSCF starting from Release 6 specification of the IMS.

11. Signaling Management in SIP, SIGTRAN and SS7

Signaling network management provides the functions necessary to maintain signaling service during failures and congestion, and restore normal signaling service after recovery from these conditions. MTP 3 supports all required ANSI and ITU.T network management procedures without intervention from the user parts or applications. MTP 3 notifies applications of significant network events that might impact their operation, such as changes in the accessibility status of remote signaling points, the onset and abatement of congestion, and signaling point restarts[5].

MTP 3 automatically initiates changeover procedures whenever a link fails, is deactivated, is remotely blocked, or is inhibited. No user part or application action is required. MTP 3 does not notify the user part or application when the changeover occurs.

When a signaling link is restored, unblocked, or uninhibited, MTP 3 automatically performs the change back function without interacting with the user parts or applications. Forced and controlled rerouting

MTP 3 also handles forced and controlled rerouting upon receipt of the transfer prohibited and transfer allowed or transfer restricted messages. On receipt of a transfer prohibited (TFP) message, MTP 3 attempts to redirect all traffic for the prohibited destination to an alternate route. If no alternate routes are available, the destination is declared inaccessible and each user part or application is notified with a StatPaused status indication for the concerned destination. Destinations can also be declared inaccessible for other reasons such as signaling link or signaling point failures, which result in similar StatPaused indications to the user parts.

If configured to do so, MTP 3 performs the restart function when the first signaling link becomes active (such as at system startup or after a total failure affecting all links), or on command from a management primitive. At the beginning of an MTP restart, each user part or application is notified with a StatRestart indication. Any new traffic requests generated by user parts during the restart are discarded. When the restart is complete and the MTP 3 layer is ready for traffic, each user part or application receives a StatRestartEnds indication.

Signaling link management MTP 3 provides the basic link management functions and optionally the signaling link management procedures based on automatic allocation of signaling terminals described in the ANSI and ITU.T MTP standards.

MTP 3 requires a successful signaling link test (SLTM generated and SLTA response expected) as part of link activation before considering a signaling link active. Then the signaling link test is performed periodically on each active signaling link, at a configurable period. Signaling link testing is performed with no user part or application interaction.

The SLTM/SLTA exchange is not used in Japanese variants. In this case, successful alignment at MTP layer 2 is considered successful alignment at MTP layer 3.

Signaling route management When configured as an STP, MTP 3 implements the signaling route management procedures transfer prohibited, transfer allowed, transfer restricted, signaling route set test, and signaling route set congestion test described in the ANSI and ITU.T MTP standards. MTP 3 performs these procedures without interacting with the user parts or applications.

12. SIP signaling management

Signaling Management Infrastructure In order to resolve the challenge discussed in previous sections, we are proposing a signaling management infrastructure as in figure. Similar to policy Resource Admission and Control (RAC) on bearer stratum, IMS signaling management adopts policy based approach to satisfy the dynamic, flexible and versatile signaling management requirements. All the policies regarding to signaling management are stored in a centralized database that are accessed[12]. There are two types policy engine network based PE (NBPE) as the default one for all subscribers and subscriber based PE (SBPE) that enables individual preference setting. PE is the core element in the signaling management, which is in charge of generating the policy information from the database, collecting the signaling usage status report from those enforcement elements, and resolving the conflict to align among different signaling handling policies. Here we define five policy types for signaling management.

1. Message validation, which should be applied on the UNI (P.CSCF) to minimize the impact of invalid messages to the IMS CN. Such kind of policy information may include invalid SIP message handling, the allowed maximum length associated with message type, treatment applied when received message length exceeded, such as returning the 513 response code, or discarding less important SIP headers, etc.

2. Signaling screening, which is to be applied on the UNI (P.CSCF) and NNI boundaries (IBCF). It includes the signaling screening criteria, screening treatment, and schedule, etc. Such signaling screening policy drives enforcement entities to screen the unauthorized SIP signaling.

3. Request prioritization, which is to be applied to the entities directly involved with request handling and service interaction, i.e., S.CSCF and AS. Request prioritization policy may include request priority list (request type, target URI, etc.), lifetime, and resource reservation mechanism. Therefore, IMS CN entities can be utilized for the most needed services, especially when the system is under or close to be overloaded.

4. Overload control, which is preferred to all the IMS signaling entities. It takes care of the overload related treatment, from overload threshold with different congestion level to proper traffic reduction mechanism selection upon receiving of the notification from those overloaded nodes, etc.

5. Regulatory service support, which helps to provide the equivalent regulatory service in IMS as PSTN does. Emergency call is one typical regulatory service that defines the rule of service detection, and resource reservation

mechanism. Policy enforcement may be implemented across all IMS CN entities. Based on network operator's preference, policy enforcement entity should execute some or all of the signaling management functionalities. These entities communicate with corresponding PEs to retrieve policy information, install, enforce them, and provide result report per requests from the policy engine. To satisfy the needs from individual subscribers, SBPE is introduced to define individual screening, message validation and request prioritization policy, along with network based ones.

13. H.323 signal Management

H.323 defines four major components for a network.based communication system: Terminals, Gateways, Gatekeepers and Multipoint Control Units (MCUs).

Terminals are client endpoints on IP-based networks that provide real-time, two-way communications with other H.323 entities. H.323 terminals are required to support the following three functional parts[14]:

Signaling and Control: H.323 must support H.245, a complex standard for channel usage and capabilities, in addition to a Q.931.like protocol defined in H.225 for call signaling and establishment, as well as Registration/Administration/Status (RAS) protocol defined in H.225 for communication with gatekeepers. All of these protocols use ASN.1 encoding for their messages.

Codecs: Codecs are pieces of software that compress audio/video before transmission and decompress them back after receiving compressed packets. For interoperability purposes, every H.323 terminal is required to support the G.711

audio codec. Other audio and video codecs are optional. Gateways provide the connection path between the packet. Switched network and the Switched Circuit Network (SCN, which can be either public or private). The gateway is not required when there is no connection to other networks. In general, a gateway deflects the characteristics of a LAN endpoint to a SCN endpoint, and vice versa. Gateways perform call setup and control on both the packet switched network and on the SCN, and they translate between transmission formats and between communication procedures. Some gateways can also translate between different codec standards for audio and/or video (referred to as transcoding), with the purpose of reducing the bandwidth of the audio/video flow if the SCN bandwidth is limited.

Multipoint Control Units (MCU) support conferencing between three or more endpoints. The MCU typically consists of a Multipoint Controller (MC) and zero or more Multipoint Processors (MP). MC provides the control functions such as negotiation between terminals and determination of common capabilities for processing audio and video. MP performs the necessary processing on the media streams for a conference. Such processing typically involves audio mixing and audio/video switching.

Channels Defined in H.323 uses the concept of channels to structure the information exchange between communication entities. A channel
is a transport.layer connection, which can be either unidirectional or bi.directional. In particular, H.323 defines the following types of channels[13]:

RAS Channel: This channel provides a mechanism for communication between an endpoint and its gatekeeper. The RAS (Registration, Admission, and Status) protocol is specified in H.225.0. Through the RAS channel, an endpoint
registers with the gatekeeper, and requests permission to place a call to another endpoint. If permission is granted, the gatekeeper returns the transport address for the call signaling channel of the called endpoint.

Call Signaling Channel: This channel carries information for call control and supplementary service control. The Q.931.like protocol used over this channel is specified in H.225.0 and H.450.x. When the call is established, the transport address for H.245 Control Channel is indicated on this channel.

H.245 Control Channel: This channel carries the H.245 protocol messages for media control with capability exchange support. After the call participants exchange their capabilities, logical channels for media are opened through the H.245 control channel.

Logical Channel for Media: These channels carry the audio, video, and other media information. Each media type is carried in a separate pair of uni.directional channels, one for each direction, using RTP and RTCP.

H.323 specifies that the RAS channel and the logical channels for media are carried over an unreliable transport protocol, such as UDP. The H.245 control channel is specified to be carried over a reliable transport protocol, such as

TCP. H.323 versions 1 and 2 specify that the call signaling channel is carried over a reliable transport protocol. In version 3, this channel can optionally be carried over an unreliable transport protocol.

14. SS7 Signal management

Failures in the SS7 network have potentially devastating effects on the communications infrastructure. The loss of all SS7 signaling capabilities at an SP isolates it from the rest of the network. The SS7 networks in existence today are known for their reliability, primarily due to the robustness of the SS7 protocol in the area of network management. Of course, this reliability must be accompanied by good network design to provide sufficient network capacity and redundancy. MTP3 Network Management is comprised of a set of messages and procedures that are used to ensure a healthy signaling transport infrastructure. This involves automatically invoking actions based on network events, such as link or route failures and reporting network status to other nodes. Traffic management is responsible for dealing with signaling traffic, which are the messages generated by MTP3 users, such as ISUP and SCCP[4]. The goal of Traffic management is to keep traffic moving toward its destination, even in the event of network failures and congestion, with as little message loss or miss sequencing as possible. This movement often involves rerouting traffic onto an alternate network path and, in some situations, might require message retransmission.

Route management exchanges information about routing status between nodes. As events occur that affect route availability, route management sends messages to notify other nodes about the change in routing states. Route management supplies information to traffic management, allowing it to adjust traffic patterns and flow accordingly.

Link management activates, deactivates, and restores signaling links. This involves notifying MTP users of the availability of signaling links and invoking procedures to restore service when a disruption has occurred. This level of network management is most closely associated with the physical hardware.

The following section discusses a number of the timers used for Signaling Network Management. It enhances the description of the procedure but is not intended to be a complete reference for every timer used. A complete list of timers can be found in Appendix G, "MTP Timers in ITU.T/ETSI/ANSI Applications." All network management messages contain a routing label and an identifier known as an H0/H1 code. Additional message fields are often included based on the particular message type. The general format of a Network Management message is shown in Figure 2.6.

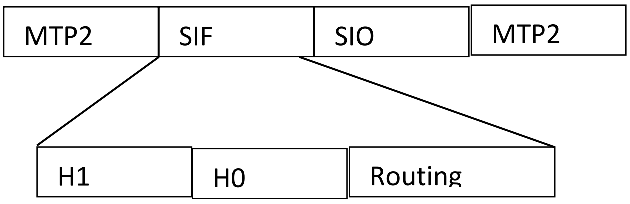

Figure. 2.6. Basic Network Management Message

The "H0/H1" codes, or "Heading" codes, are simply the message type identifiers. There are two Heading Codes for each message: H0 for the family of messages, and H1 for the specific message type within the family. Table 7.4 lists the H0/H1 codes for each message type. The family (H0 code) is listed on the left of the chart. All messages in a row belong to the same message family. For example, the H0/H1 code for a COA message is 12 and it belongs to the CHM (Changeover Message) family[6].

Link Management: Links are physical entities that are made available to MTP3 users when they have proven worthy of carrying messages. If a link fails, it has a direct impact on the two nodes the link connects. It is link management's responsibility to detect any communication loss and attempt to restore it. Both nodes connected to the link invoke procedures for restoration in an attempt to restore communication.

Activation is the process of making a link available to carry MTP3 user traffic. Maintenance personnel typically perform it by invoking commands from an OAM interface to request that the link be activated for use. When a link is aligned at level 2 and passes the proving period, the link is declared available to traffic management.

MTP3 sends an SLTM (Signaling Link Test Message) over the link with the node's DPC at the far end of the linkset. The SLC code in the routing label identifies the link on which the message is sent. The test is performed only if the SLC matches the link on which the message is sent, and if the OPC in the routing label matches the far end Point Code of the receiving node. The message's user data is a simple test pattern of bytes and is typically user configurable. The receiving node responds with a Signaling Link Test Acknowledgement (SLTA) containing the test pattern received in the SLTM message. The SLTA test pattern must match what was sent in the SLTM or the test is considered a failure. In addition, the DPC, network indicator, and SLC in the SLTM are checked to ensure that they match the information at the node on the receiving end of the link over which the message was sent The SLTC ensures that the two connected nodes can communicate at level 3 before placing a link into service for user traffic. At this point the SLTC can detect problems, such as an incorrectly provisioned Point Code or network indicator, in link activation. Route Management: Signaling route management communicates the availability of routes between SS7 nodes. Failures such as the loss of a linkset affect the ability to route messages to their intended destination. A failure can also affect more than just locally connected nodes. For example, the linkset between STP1 and SSP B has failed in Figure . As a result, SSP A should only route messages to SSP B through STP1 as a last resort because STP1 no longer has an associated route. Even though none of the links belonging to SSP A have failed, its ability to route messages to SSP B is affected. Signaling route management provides the means to communicate these types of changes in route availability using Signaling Network Management messages.

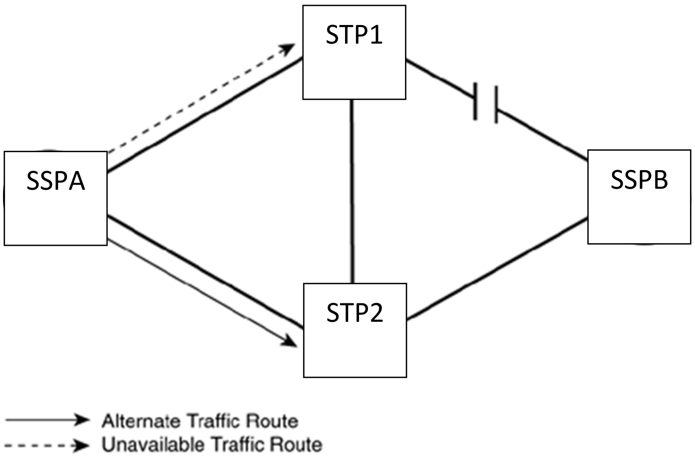

Figure. 2.7. How Loss of Linkset Affects Routes[4].

Conclusions to chapter II

With the maturity and deployment of IMS, more challenges are revealed regarding to the SIP, H.323, SS7 signaling usage. More applications are tight-coupled with the SIP, H.323, SS7 signaling, especially using XML for application data encapsulation. This will change the signaling traffic model and hence dramatically increases the number of SIP, H.323, SS7 signaling messages together with their sizes. Lack of signaling screening will put the system under great risk considering client intelligence and holes in SIP, H.323, SS7 extensibility. Although there are a few draft RFCs to address the weakness of overload control with the signaling protocol, the complexity of IMS solution has put more requirements on it. Both operator and subscriber require a flexible, dynamic and versatile signaling management mechanism, which is beyond the signaling protocol’s capability. Signaling management infrastructure is proposed to effectively manage the IMS signaling and efficiently utilize precise IMS CN entities. PE is responsible to generate and modify the policy information via policy database and signaling usage report from policy enforcement entities. Signaling management may consume more system resource when it performs deep inspection.

Chapter III. Management signaling load in SIP signaling network

Communication between stored program controlled exchanges requires a fast reliable high.capacity signaling system, capable of operating in a digital transmission environment. SS7 is such a signaling system. The modular nature of SS7 makes it flexible and adaptable for a number of uses, but no matter what use is made of the signaling information carried, the MTP is always required. The MTP provides the functions that enable information that is significant for the user parts, passed to the MTP to be transferred across the SS7 signaling network in Message Signal Units (MSU) to the required destination. Mechanisms are provided in the MTP that ensure MSUs are received in the correct sequence and without errors[16].

Whenever an error is detected, the corrupted MSU will be retransmitted. In addition, further procedures ensure that the impact of network or system failures have minimal effect on the ability of the MTP to transfer MSUs.

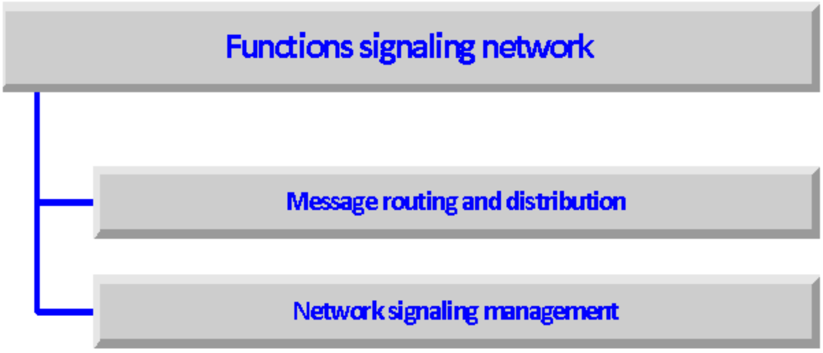
Functions signaling network
Message routing and distribution
Network signaling management

Figure. 3.1. Functions signaling network

1. Basic Functional Blocks

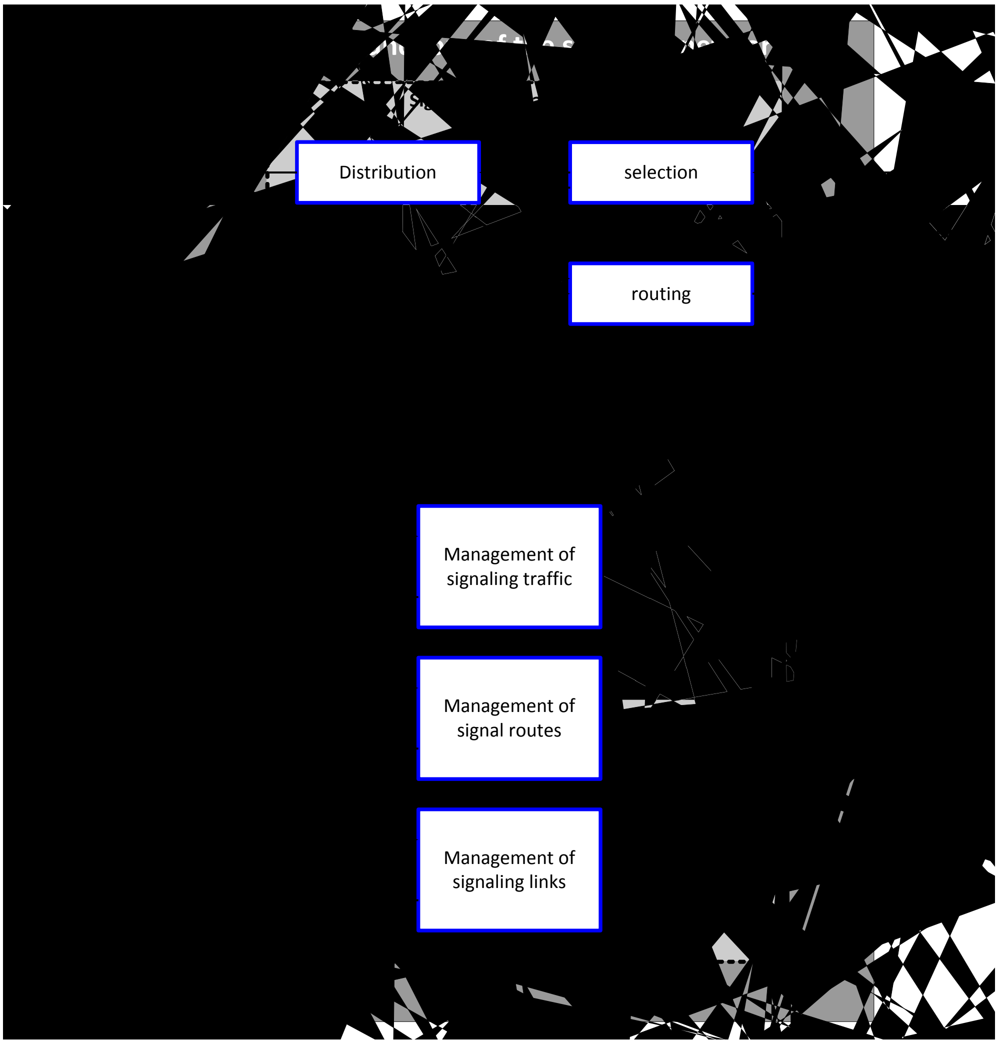
Distribution
selection
routing
Management of signaling traffic
Management of signal routes
Management of signaling links

Fig 3.1. Basic Functional Blocks

Management of signaling network includes management of signaling traffic, signaling routes and signaling links. These functions need to reconfigure the signaling network in the event of failure of links or signaling points, as well as to control traffic during overload or locks. This ensures timely delivery of messages to destinations in the correct sequence, without loss of repetitions or unacceptable delays[17].

2. Functions of maintenance signaling management in network

Signaling network management functions provide the actions and procedures required to maintain the operation of the system and signaling to restore normal conditions in case of failure in the network, links or signaling points[15]:

- Ensuring network performance as incurred failure, if possible;
- Restore the initial configuration after fault elimination.

Signaling network management messages transmitted over the signaling links in significant signal units.

Any change in the status of signaling links or routes signaling points entails application of three different groups of signaling network management functions:

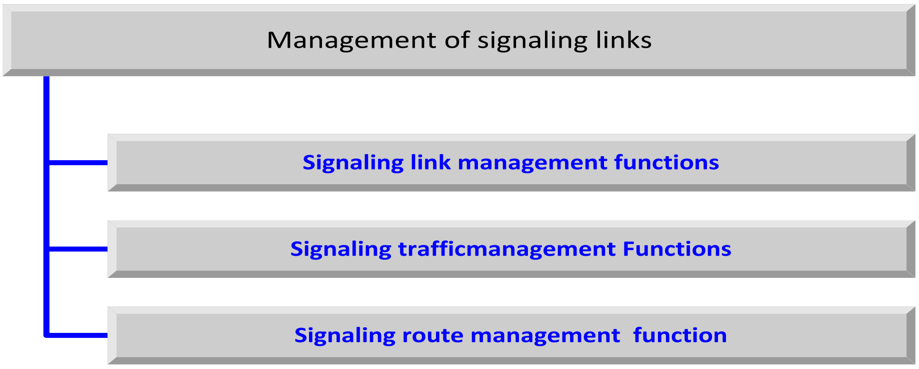
Management of signaling links
Signaling link management functions
Signaling trafficmanagement Functions
Signaling route management function

Figure. 3.3. Management of signaling links

Signaling route management communicates the availability of routes between SS7 nodes. Failures such as the loss of a linkset affect the ability to route messages to their intended destination. A failure can also affect more than just locally connected nodes. For example, the linkset between STP1 and SSP B has failed in Figure 3.3. As a result, SSP A should only route messages to SSP B through STP1 as a last resort because STP1 no longer has an associated route. Even though none of the links belonging to SSP A have failed, its ability to route messages to SSP B is affected. Signaling route management provides the means to communicate these types of changes in route availability using Signaling Network Management messages.

Route management uses the following messages to convey routing status to other network nodes:

- Transfer Prohibited (TFP);
- Transfer Restricted (TFR);
- Transfer Allowed (TFA);
- Transfer Controlled (TFC);

The following additional messages are used for conveying the routing status of clusters. They are only used in ANSI networks:

- Transfer Cluster Prohibited (TCP);
- Transfer Cluster Restricted (TCR);

Each node maintains a state for every destination route. As route management messages are received, the state is updated based on the status conveyed by the message. This allows nodes to make appropriate routing choices when sending messages. Routes can have one of three different states:

- Allowed;
- Prohibited;

- Restricted.

The following sections discuss each of these states and the messages and procedures that are associated with them.

As shown in the messages used by route management all have a common format consisting of a standard routing label, an H0/H1 code identifying the type of network management message and a destination. The destination is the Point Code of the node for which routing status is being conveyed. Traffic Management traffic management is the nucleus of the MTP network management layer that coordinates between the MTP users' communication needs and the available routing resources. It is somewhat of a traffic cop in stopping, starting, redirecting, and throttling traffic. Traffic is diverted away from unavailable links and linksets, stopped in the case of unavailable route sets, and reduced where congestion exists. Traffic management depends on the information provided by link management and route management to direct user traffic [10]. For example, when a TFP is received for a destination, traffic management must determine whether an alternate route is available and shift traffic to this alternate route. During this action, it determines what messages the unavailable destination has not acknowledged so those messages can be retransmitted on the alternate route. This section discusses the following procedures that are employed by traffic management to accomplish such tasks:

- Hangeover;
- Emergency changeover;
- Time.controlled changeover ;
- Changeback ;
- Time.controlled diversion;
- Forced rerouting;
- Controlled rerouting;
- MTP restart;
- Management inhibiting;

3. Procedure Flow Control Signaling Traffic

The purpose of the procedure flow control signaling traffic . traffic shaping on the side of its source, when the signaling network is not able to convey the amount of traffic coming from the user due to subsystem failures of network elements or temporary overload. OKS Network Management does not control the traffic, the problem of this procedure. Informing UP level network congestion. Operation flow control can be used for the following events:

1. Failures in the signaling network (in the links or points) that caused the unavailability beam signaling routes. If no available routes to the same destination from SP MTP subsystem subsystem informs the user about non.delivery of its message. Subsystem user stops the generation of signaling traffic towards unattainable SP. After the route is available to previously inaccessible destination subsystem subsystem MTP inform the user about the possibility of traffic, which then takes the necessary steps to start generating the signal information addressed to the now reachable signaling point.

2. Overload link or point led to a situation in which the exercise of the reconfiguration is not advisable. If the beam signal routes goes into overload, the overload indicator on the internal interface returned from subsystem to subsystem MTP user when receiving from her eighth each message sent by the beam congested routes. STP notifies outbound SP overload beam routes sending a message transmission control (TFC, Transfer control) to receive messages every eight to SP destination, reachable on congested routes, or the incoming beam in a congested beam unit or units.

Links are physical entities that are made available to MTP3 users when they have proven worthy of carrying messages. If a link fails, it has a direct impact on the two nodes the link connects. It is link management’s responsibility to detect any communication loss and attempt to restore it. Both nodes connected to the link invoke procedures for restoration in an attempt to restore communication. Link management can be divided into three processes:

Activation is the process of making a link available to carry MTP3 user traffic. Maintenance personnel typically perform it by invoking commands from an OAM interface to request that the link be activated for use. When a link is aligned at level 2 and passes the proving period, the link is declared available to traffic management.

Deactivation removes a link from service, making it unavailable for carrying traffic. Like activation, this process is typically initiated by invoking commands from an OAM interface. The link is declared unavailable to traffic management when it is deactivated. Restoration is an automated attempt to restore the link to service after a failure, making it available for traffic management use. The link alignment procedure is initiated when level 2 has detected a link failure. When the link is aligned and has passed the proving period, a signaling link test is performed. After the signaling link test has successfully completed, traffic management makes the link available for use.

Signaling Link Test Control When a signaling link is activated, it must undergo initial alignment at MTP2. The SLC code in the routing label identifies the link on which the message is sent. The test is performed only if the SLC matches the link on which the message is sent, and if the OPC in the routing label matches the far end Point Code of the receiving node. The message's user data is a simple test pattern of bytes and is typically user configurable. The receiving node responds with a Signaling Link Test Acknowledgement (SLTA) containing the test pattern received in the SLTM message. The SLTA test pattern must match what was sent in the SLTM or the test is considered a failure. In addition, the DPC, network indicator, and SLC in the SLTM are checked to ensure that they match the information at the node on the receiving end of the link over which the message was sent. The SLTC ensures that the two connected nodes can communicate at level 3 before placing a link into service for user traffic. At this point the SLTC can detect problems, such as an incorrectly provisioned Point Code or network indicator, in link activation. If alignment or the signaling link test fails, the procedure is restarted after a period of time designated by T17. In ANSI networks, a link failure timer (T19) is used to guard the amount of time the link remains out of service. Upon its expiration, a notification is raised to system maintenance, where the restoration procedure can be restarted or the link can optionally be declared as “failed” until manual intervention occurs. acknowledgment, at the distant SP to time out; however, timer T7 restarts each time an SIB is received. Therefore, timer T7 does not time out as long as the distant SP receives SIBs.

4. Messages flow control signaling traffic (FCM)

Flow control allows incoming traffic to be throttled when the MTP2 receive buffer becomes congested. When an SP detects that the number of received MSUs in its input buffer exceeds a particular value—for example, because MTP3 has fallen behind in processing these MSUs—it begins sending out LSSUs with the status indicator set to busy (SIB). These LSSUs are transmitted at an interval set by timer T5, sending SIB (80 to 120 ms), until the congestion abates. The congested SP continues sending outgoing MSUs and FISUs but discards incoming MSUs. It also “freezes” the value of BSN and the BIB in the SUs it sends out to the values that were last transmitted in an SU before the congestion was recognized [10]. This acknowledgment delay would normally cause timer T7, excessive delay of acknowledgment, at the distant SP to time out; however, timer T7 restarts each time an SIB is received. Therefore, timer T7 does not time out as long as the distant SP receives SIBs.

Timer T6, remote congestion, is started when the initial SIB is received. If timer T6 expires, it is considered a fault, and the link is removed from service. Timer T6 ensures that the link does not remain in the congested state for an excessive period of time. When congestion abates, acknowledgments of all incoming MSUs are resumed, and periodic transmission of the SIB indication is discontinued. When the distant SP receives an SU that contains a negative or positive acknowledgment whose backward sequence number acknowledges an MSU in the RTB, timer T6 is stopped, and normal operation at both ends ensues.

5. The message "controlled transmission" (TFC)

The Transfer Controlled message is used to indicate congestion for a route to a particular destination. The TFC message implies “transmit” congestion, in contrast to the “receive” buffer congestion handled by MTP2. Figure shows a typical example in which an STP receives messages from a number of nodes for the same destination. This queues a large number of messages in the transmit buffer for the destination, putting the destination route into a congested state. The STP sends a TFC message to the SPs that generate the traffic, informing them that the STP 1 route to the destination is congested. In the international network and ITU.T networks that do not implement the option of multiple congestion levels, the TFC simply indicates that the destination is in a congested state. In ANSI networks, the TFC includes a congestion level to indicate the severity of the congestion[15].

The congestion level is used in conjunction with the message priority level to throttle messages during periods of congestion. The TFC message contains the H0/H1 code that identifies the message as a TFC message, the Point Code of the affected destination.

The ITU.T defines an option for national networks to allow the use of multiple congestion levels to throttle traffic during periods of congestion. ANSI networks implement this option.

When an STP receives a message for a congested routeset, the priority field in the SIO is compared with the congestion level of the congested routeset. If the priority of the message is lower than the congestion level, a TFC message is sent to the message originator indicating the current congestion level. The originating node updates the congestion status of the route set and notifies its MTP users with an MTP congestion primitive so they can take the appropriate action to reduce traffic generation. The “MTP3/User Part Communication” section discusses MTP primitives further.

6. The message "Testing overload routes beam test (RCT)

The Routeset Congestion Test message tests the congestion level of a network destination. It poses the question, “Is the Routeset still at congestion level x, the RCT message contains the H0/H1 code that identifies the message as a RCT message and the Point Code of the affected destination. As discussed in the previous section, the RCT message is sent in response to a TFC. The priority of the RCT message is set to one less than the congestion level identified in the TFC message. The node sending the RCT can determine whether to resume traffic transmission of a given priority based on whether a TFC is received in response to the RCT. If no TFC is received within T16, the sending node marks the routeset with the new congestion level, which is based on the priority of the transmitted RCT message. Refer to section “Multiple Congestion Levels” for a complete discussion of how the RCT message is used in the transfer controlled procedure[15].

7. Analysis SIP Based QoS Management Framework for IMS Multimedia Services

The aim of this simulation is to evaluate the QoS management architecture over IP Multimedia Subsystems to provide desired QoS for the IMS multimedia traffic over IP access network so that the SIP.based QoS routing modules can achieve predictable QoS results. The environment consists of ns.2 network simulation software in Linux operating system. The results obtains from simulated model are being compared with the existing QoS architecture. Two common multimedia applications (Data, voice) are being used to simulate the architecture.

Simulation Experiments: In this section, the simulation experiments are described, used with MPLS and DiffServ QoS mechanisms and to compare the simulation scenarios with simple network without SIP QoS Modules. Moreover, we present results that depict the improvement in network efficiency due to improved bandwidth sharing in SIP QoS Modules compared to general QoS Models in IMS. We conduct a set of experiments and compare the QoS results and the total bandwidth utilization under various scenarios. These statistics depict a realistic representation of an IP Multimedia Subsystem’s goal of providing best QoS, keeping in view the applicable rules for multimedia traffic and bandwidth utilization. Moreover, it is important to consider the bandwidth associated with the accepted multimedia requests since it is possible for a less efficient scheme to accept a large number of small bandwidth requests compared to a more efficient scheme which accepts fewer requests which comprise a greater amount of bandwidth. QoS routing algorithm proposed in is used for simulations; the algorithm proposed therein for the computation of bandwidth and utilization of paths is integrated with these QoS modules. The simulation experiments are conducted on a SIP network topology for IMS.

The computation of primary and QoS routes for a multimedia request depends on the simulation scenario. In case of SIP, for each request, if it is possible to route the requisite according to the QoS requirements, then the request is immediately accepted; otherwise another attempt is made to place the request by calculating the other routes, failure of which results in the rejection of QoS request.

Scenario1*:* In this Scenario, the Access network contains the nine routers to process the network traffic and data. The Links between theses routers are expressed in three bandwidths i.e. 1MB, 2MB and 3MB. When source sends SIP data to destination, the route established between these routers are different in all the three times according to the available paths and resources. IMS SIP traffic is processed through the SIP LSPs. These SIP LSPs implements the QoS Module and process the SIP traffic for best QoS. The LSP routers establish different paths for traffic but after applying the QoS on these LSPs efficient and effective utilization of resources is achieved. After SIP QoS negotiation, SIP Modules Performs the Marking, Policing and Shaping on the incoming SIP packets. QoS Modules calculate unreserved and available Bandwidth between nodes in established path.

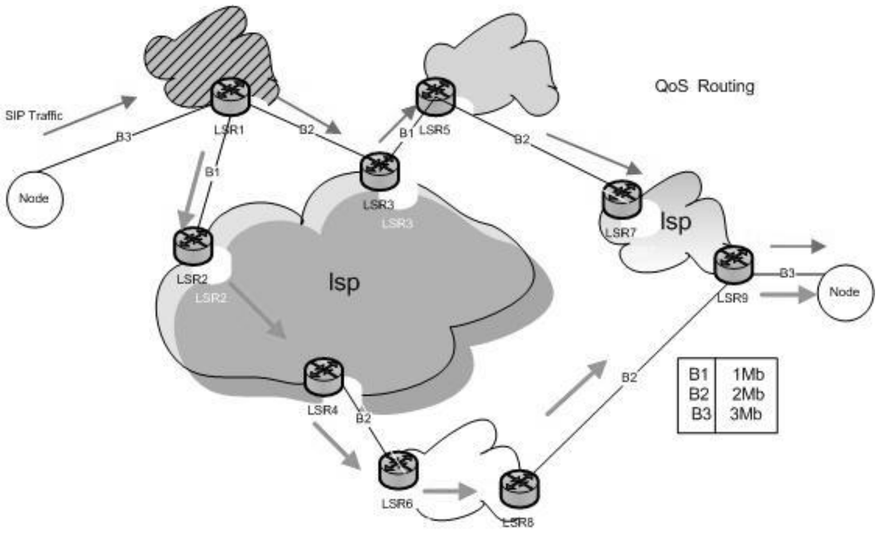

Figure. 3.4. Simulation Scenario1

Route establishment: First route established for SIP Traffic is 1_3_5_7_9 for traffic1. The link bandwidths are B2, B1, B2 and B3. The second path established for SIP traffic 2 is 1_2_4_6_8_9 for traffic 2 after calculating the available bandwidth and 2nd route is established. Similarly 3rd route is established 1_3_4_6_5_7_8_9 for traffic 3.

Observations: It is observed that when the links are available for processing traffic, the route is established in minimum time and it processed data efficiently. After resource reservations the other paths takes more time to establish routes. 1st route establish the shortest path for packet traversing but after that it also traverses the SIP packets for unreserved path and available bandwidth.

Analysis of Scenario1: The Table 1 shows the simulation results for the scenario 1. The totals Number of SIP packets sent by the source and received by the destination include the session establishment packets and also data packets. The Average throughput for SIP data is 87% and link utilization is 99.64%. This shows that the number of packets lost in this case are minimum as resources are available for data.

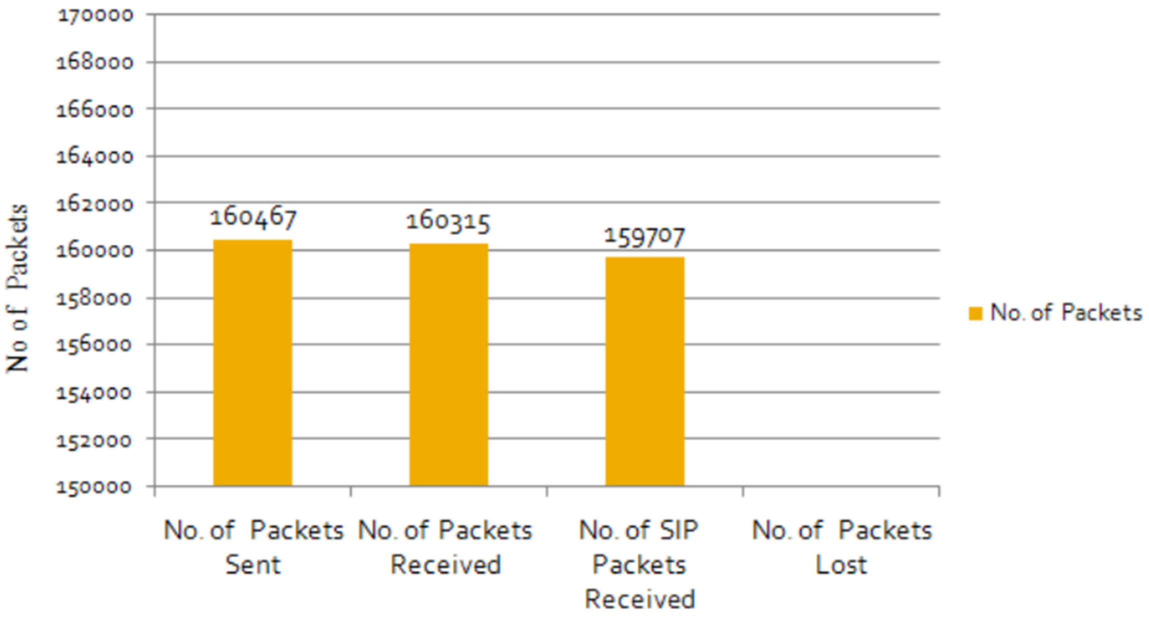

Figure 3.5 Analysis of Scenario 1

Scenario2: Simulation Scenario 2 contains the two SIP Servers that receive the SIP data from IMS core Network. The aim of this simulation is to send SIP data from IMS core to Other IMS core network through SIP QoS Modules implemented on access networks. The network contains the four routers to process data on network. On these routers we enable the QoS Modules for SIP traffic. Both SIP Servers start sending traffic at time 1.06. This setup also contains the other sources for sending UDP data on same link.

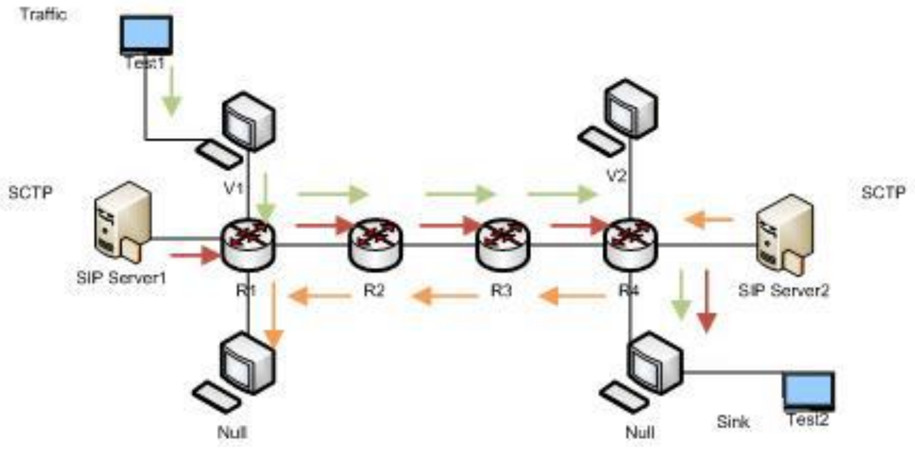

Figure. 3.6. Sample Simulation Topology

Route establishment*:* Both SIP servers start sending data to sink at 1.09ms through the access network [IP Backbone], and the UDP server starts its traffic at time 0 ms. Route establishment for SIP Traffic is shown by figure 6. The link bandwidths are 255MB for each router. The traffic flow for UDP traffic path established is also shown in figure.

Observations: It has been observed that when the links are available for processing traffic, the route is established in minimum time and it processed UDP data efficiently. But when SIP servers start sending data the QoS Modules prioritized the SIP traffic as compared to the UDP data. QoS Module also manages the bandwidth for SIP data traffic so it provides the best QoS for IMS services. Average throughput for bandwidth utilizations for SIP traffic is 92.39Kbps.

Analysis of Scenario*:* The Figure 3.7 also shows the simulation results for the scenario 2. The Total Number of SIP packets send by the source and received by the destination includes data packets for IMS Multimedia voice services and also UDP data traffic. The Average throughput for SIP traffic is 99.52% and link utilization is 99.90%.

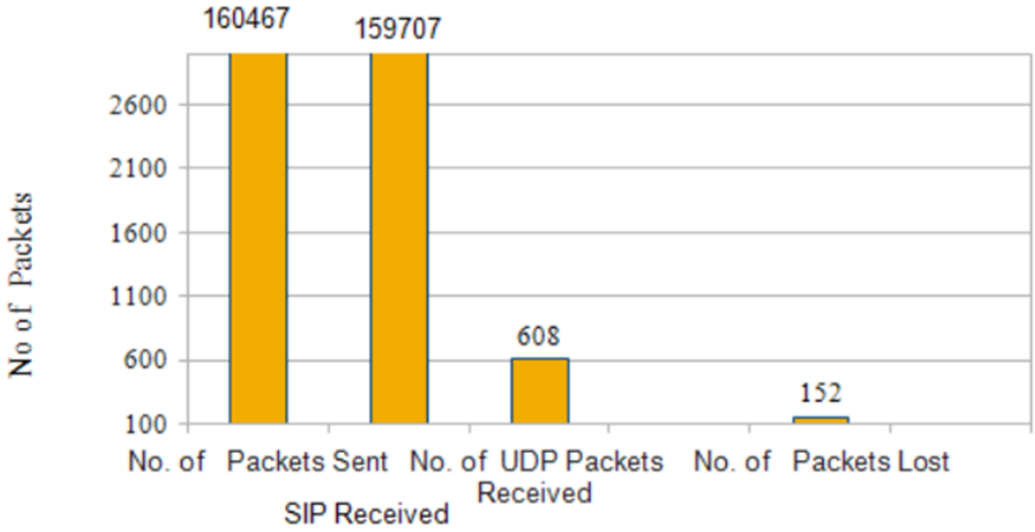

Figure 3.7 Analysis of Scenario2

Figure 3.7 shows the total number of packets sent, received, lost and SIP data packets reached to destination. This graph also represents the Total number of UDP packets processed by the network. The results show that these modules can provide better QoS services to the IMS SIP traffic as compared to the UDP traffic over MPLS and Diffserv network. Multimedia services require more resources as compared to the simple data traffic. Numbers of SIP packets traversed are more than the UDP packets. So the results show that SIP based QoS Modules are more efficient for transmission of multimedia traffic of IMS over IP Access Networks.

Table 1.

Comparison Analysis Data

Packet output	Scenario 1	Scenario 2	Comparison Data
Packet Received	10249	160315	1817
SIP Packet Received	9000	159707	153478
Packet lost	37	152	200
Average throughput	99.64%	99.90%	98.70%
Average throughput of SIP Data	87.50%	99.52%	97.71%

Comparative Analysis: In this section we will compare our approach with simple QoS mechanism over Access networks. Table2 represents the results of SIP data processing over Access networks with SIP.Based Modules disabled and enabled. Simulation results of simple QoS scenario show that the total number of UDP packets traversed by the network is more than the QoS enabled scenario. The average throughput of link is 97.71%. The Total number of packet lost is more as compared to the SIP. Based QoS scenario where packet lost are just 152.

Observations: It has been observed that the simple QoS provides the same services to all the traffic but multimedia traffic requires more resources for the efficient delivery of application. After implementation of QoS SIP modules, multimedia services acquire priority. By comparing the both scenarios we conclude that the overall performance of SIP Data sent through QoS SIP Module provides better utilization of bandwidth and paths. These Modules not only use the available links but also utilize unreserved links. IMS traffic through SIP Module is now more valuable and well organized.

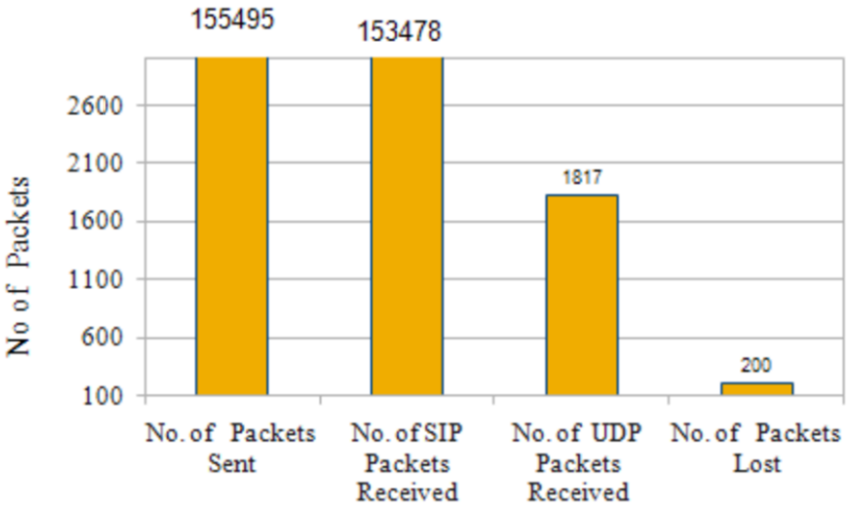

Figure 3.8 SIP Traffic Analysis without QoS

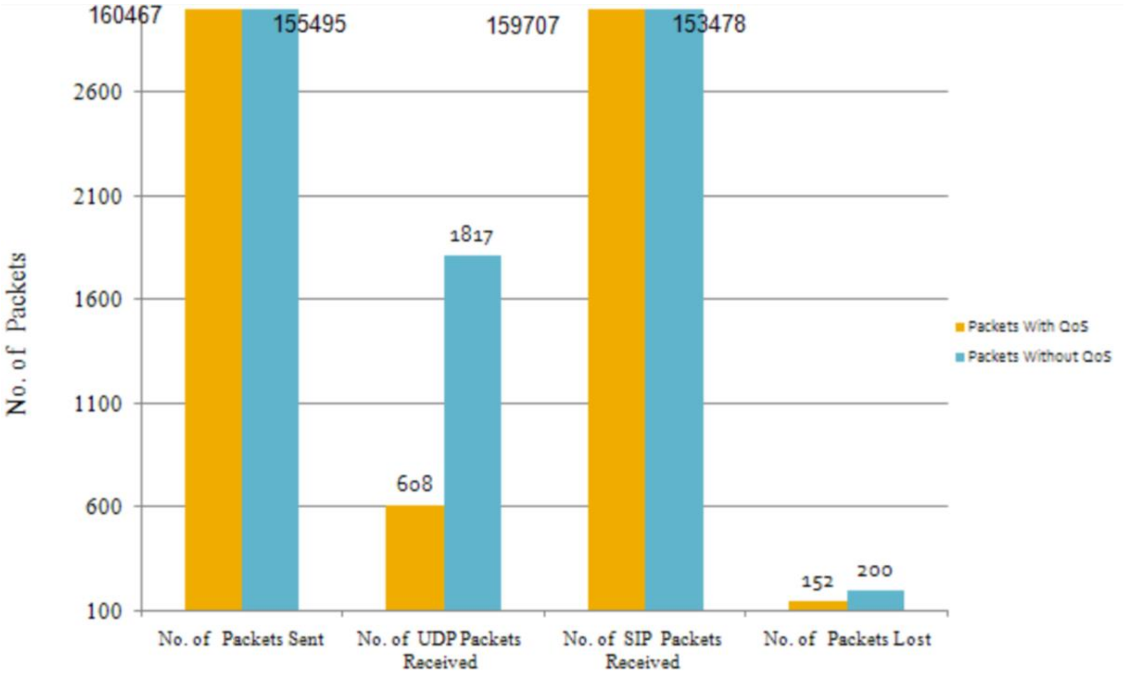

Figure 3.9 Simulation Results

Simulation Results: Scenario1 shows a case where only SIP traffic is present in the network from source to node destination and figure of sceanrio2 shows a case where UDP traffic and SIP traffic is present in the network from source to destination. The bandwidth used for network traffic is measured from the source to destination. It has been observed that UDP is getting negatively affected on a significant increase in SIP traffic. The overall performance of SIP Modules shows that SIP traffic with SIP modules provides the better performance as compared to the QoS disabled scenario. It has been observed that SIP module provides the best path and reduces congestion over access networks. The proposed architecture efficiently utilizes the available bandwidth over link.

Table 6 shows the overall performance of SIP modules over different defined scenarios. The results show that the SIP QoS modules provide better performance in all the given scenarios. The modules give best results MPLS and DiffServ QoS mechanism.

Conclusion on chapter III

QoS Modules have been proposed for handling IMS data traffic with integration of Diffserv & MPLS in this. The performance of SIP modules has been checked using two different network Scenarios. The simulation results have shown that the performance of the proposed architecture is better in both scenarios due to implementation of SIP QoS modules. The Comparison of different architectures shows that the proposed architecture has provided better results as compared to existing architecture. Based on Simulation experiments, it has been observed that SIP module provides the best path and reduces congestion over access networks. The proposed architecture efficiently utilizes the available bandwidth on various links.SIP based QoS Module can be further improved by the use of integration of

Integrated Services, Multi-Protocol Label Switching, Resource Reservation Protocol and Differentiated Services mechanisms

Conclusion

The development of IMS has taken many years, and the rate of its take-up has perhaps been slower than its proponents had first envisioned. however, in recent years it has become clear that IMS really will make a significant impact on the industry. In a world looking towards widespread coverage and declining traditional wireline usage, a network architecture that focuses on services, not access, is something all carriers should be interested in. the promise of IMS to converge fixed and mobile networks onto an IMS core supporting a common set of services has to be attractive to those who currently face the operational costs of running two separate networks in parallel. from a long term view IMS offers not only reduced network operational costs, but also lower barriers to entry for innovative services to be deployed rapidly. In a world with declining traditional

For traditional wireline carriers, although IMS formally only defines a method for native SIP endpoints within a network, there has been much work to address how to incorporate legacy endpoints into the architecture, while minimizing the cost and impact of the transition. To understand the IMS architecture in more detail. And has a broad product portfolio that can be deployed today to enhance an existing IMS network, or can be deployed to manage a seamless phased migration from the existing network toward an IMS future. With the maturity and deployment of IMS, more challenges are revealed regarding to the SIP, H.323, SS7 signaling usage. More applications are tight-coupled with the SIP, H.323, SS7 signaling, especially using XML for application data encapsulation.

Both operator and subscriber require a flexible, dynamic and versatile signaling management mechanism, which is beyond the signaling protocol’s capability. signaling management infrastructure is proposed to effectively manage the IMS signaling and efficiently utilize precise IMS CN entities. PE is responsible to generate and modify the policy information via policy database and signaling usage report from policy enforcement entities. Signaling management may consume more system resource when it performs deep inspection.

QoS Modules have been proposed for handling IMS data traffic with integration of Diffserv & MPLS in this. The performance of SIP modules has been checked using two different network Scenarios. The simulation results have shown that the performance of the proposed architecture is better in both scenarios due to implementation of SIP QoS modules. The Comparison of different architectures shows that the proposed architecture has provided better results as compared to existing architecture. Based on Simulation experiments, it has been observed that SIP module provides the best path and reduces congestion over access networks. The proposed architecture efficiently utilizes the available bandwidth on various links.SIP based QoS Module can be further improved by the use of integration of Integrated Services, Multi-Protocol Label Switching, Resource Reservation Protocol and Differentiated Services mechanisms

List of references

Works by President of Republic of Uzbekistan I.A.Karimov:

1. On January 18 a session of the Cabinet of Ministers of the Republic of Uzbekistan dedicated to the results of socio-economic development in the republic in 2012 and the main priorities of economic program for the year 2013.
2. I.A. Karimov "The global financial-economic crisis, ways and measures to overcome it in the conditions of Uzbekistan" Uzbekistan. T: 2009, pp. 44.M.

Special references:

3. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg, SIP:Session Initiation Protocol, IETF RFC-2543, March 1999
4. Lawrence Harte, Richard Dreher, Dave Bowler, Details of Signalling System 7 basics,3rd edition, Althos Publisher, ISBN 0972805370, Pp 21-97
5. Dryburgh, Lee , Hewitt, Jeff , "Signaling System No. 7 (SS7/C7): Protocol, Architecture, and Services", Publisher: Cisco Press, ISBN: 1587050404, 2004,Pp 31-102.
6. H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, "RTP: a transport protocol for real-time applications," RFC 1889, Internet Engineering Task Force, Jan. 1996.
7. Zhu Bei, Analysis of SIP in UMTS IP Multimedia Subsystem, MSc. Thesis, Computer engineering, North Carolina State University, 2003
8. "IMS – IP Multimedia Subsystem" Ericsson White Paper, 2004.
9. IMS Service Architecture",White Paper , Lucent Tehcnologies, 2005. Jorg Ott,
10. "SIP and Mobility: IP Multimedia Subsystem in 3G Release 5", 11 November 2002, Presentation at Bremen
11. Thomas Magedanz, "IP Multimedia System (IMS) Principles, Architecture and Applications", Tutorial, Technical University of Berlin / Fraunhofer FOKUS, 2006.

12.. Rosenberg et al., “SIP: Session Initiation Protocol,”IETF RFC 3261, June 2002.

13. Packetizer http://www.packetizer.com/

14. H.323 Forum http://www.h323forum.org/

15. Umber Iqbal, Shaleeza sohail, Younas javed., “SIP-Based QoS Management Architecture for IP Multimedia Subsystems over IP Access Networks”,ICCNSS 2010.

16.Muhammad Shoaib Siddiqui, Syed Obaid Amin, nonmembers and Choong Seon Hong, Member “A Set-top Box for End-to-end QoS Management and Home Network Gateway in IMS”,IEEE, 978-1-4244-2559-4/09 ©2009 IEEE

17.Dragos Vingarzan, Peter Weik, Fraunhofer FOKUS, “IMS signaling over current wireless networks: Experiments using the Open IMS Core”.

18.http://www.protocols/pbook/sigtran