Design and Implementation of a Simplified Signalling System for Distributed Communication Networks

A thesis submitted to the
Department of Electrical and Electronic Engineering
of
Bangladesh University of Engineering & Technology
In partial fulfillment of the requirements
for the degree of
M.Sc. Engg. (Electrical and Electronic Engineering)

By

GMA Ehsan ur Rahman

Department of Electrical and Electronic Engineering

Bangladesh University of Engineering & Technology

Dhaka-1000, Bangladesh

December, 2008

APPROVAL CERTIFICATE

The thesis titled "Design and Implementation of a simplified Signalling System for distributed Communication Networks." submitted by GMA Ehsan ur Rahman, Roll No. 040306255F, Session October 2003 to the Department of Electrical and Electronic Engineering of Bangladesh University of Engineering and Technology has been accepted as satisfactory in partial fulfillment of the requirements for the degree of M.Sc. Engg. in Electrical and Electronic Engineering on 28 December 2008.

Board of Examiners

1 SRahman 28/12/2008

Dr. Md. Saifur Rahman
Professor
Department of Electrical and Electronic Engineering
BUET, Dhaka-1000

Chairman (Supervisor)

2 28/12/2008

Prof. Dr. Aminul Hoque
Professor and Head
Department of Electrical and Electronic Engineering
BUET, Dhaka-1000

Member (Ex-Officio)

3

Dr. Newaz Muhammad Sayfur Rahim
Associate Professor
Department of Electrical and Electronic Engineering
BUET, Dhaka-1000

Member

4

Dr. Md. Mostofa Akbar
Associate Professor
Department of Electrical and Electronic Engineering
BUET, Dhaka-1000

Member (External)

DECLARATION

I hereby declare that this thesis or any part of it has not been submitted elsewhere for the award of any degree or diploma.

(GMA Ehsan ur Rahman)

ACKNOWLEDGEMENT

I would like to express my sincere thanks to my supervisor Dr. Md. Saifur Rahman for his guidance, thoughtful suggestions, encouragement and support towards successful completion of the thesis. I would also like to thank my employers of "City Cell & Banglalink", for granting me leave for completion of this thesis. Without their support this work would not have been completed.

It is nearly impossible for me to name each and every person who contributed some way or other to this work, but I would like to thank the members of my family for their encouragement, and everyone else including my colleagues and friends, who participated in fruitful discussions and made my time enjoyable.

ABSTRACT

Signalling System is the most important part of a communication system. Signalling System Seven (SS7) was introduced to enable both analog and digital voice communication, data communication and connectionless communication between diversified communications networks. A huge number of organizations, institutes, manufacturers, service providers are developing and implementing new signalling systems and protocols to meet communications demand for customized products but still keeping the interoperability with the standard signalling systems and protocols. Such initiatives are absent in Bangladesh. This work is an initiative to develop our own customized solutions for special communications products and services in the ever growing diversified field of communications. With this end in view, a novel signalling system named as "Bus Independent Signalling (BIS)" has been proposed and developed as part of the current research work.

The proposed BIS system is an Open System Interconnection (OSI) layer-4 protocol, and can be transferred over very simple physical or transmission layers like RS-232, RS-485 and the popular TCP/IP. Being dynamic in nature, it can also carry the user data as the payload of the BIS messages in the OSI application layer. Thus, using the proposed BIS system, both simple and large distributed communication networks can be built, and a lot of telecommunication products can be developed. Such an application is also developed and implemented in this research work. A future roadmap is also proposed to take the BIS to a useful base for telecommunications products and services in Bangladesh.

The BIS protocol has the advantages of dynamic system configuration for the maximum optimization of resources. It has the capability of self synchronization to be able to transfer data over both synchronous and asynchronous transmission buses. It supports both packed and unpacked data, real-time and offline data for point to point and point to multi-point communications. Thus, the proposed BIS system can be used for a diversified field of applications.

LIST OF ABBREVIATIONS

ANSI	American National Standards Institute
ATM	Asynchronous Transfer Mode
BSSAP	Base Station System Application Part
CAP	Camel Application Part
CAMEL	Customized Application of Mobile Enhanced Logic
CAS	Channel Associated Signalling
CCIS	Common Channel Interoffice Signalling Systems
CCITT	Comité Consultatif International Télégraphique et Téléphonique
CCS	Common Channel Signalling
CIC	Circuit Identification Code
DPC	Destination Point Code
DSS1	Digital Subscriber Signalling system No.1
DTMF	Dual Tone Multi-Frequency
DVB	Digital Video Broadcasting
EIA	Electronic Industries Alliance
EIR	Equipment Information Register
FISU	Fill In Signal Unit
GKRCS	Gatekeeper Routed Call Signalling
GSM	Global System for Mobile Communications
HLR	Home Location Register
HSL	High speed Signalling Link
HTTP	Hypertext Transfer Protocol
BIS	Bus Independent Signalling
IDD	International Direct Dialling
IETF	International Engineering Task Force
INAP	Intelligent Network Application Part
IP	Internet Protocol
ISDN	Integrated Service Digital Network
ISUP	ISDN User Part
ITU	International Telecommunication Union
LE	Local Exchange
LS	Link Set
LSSU	Link Status Signal Unit
MAP	Mobile Application Part
MCU	Micro Controller Unit
MGCP	Media Gateway Control Protocol

MSU	Message Signal Unit
MTP	Message Transfer Part
NGN	Next Generation Network
NI	Network Indicator
NMEA	National Marine Educators Association
OPC	Originating Point Code
OSI	Open System Interconnection
PABX	Private Automatic Branch Exchange
PCM	Pulse Code Modulation
PDA	Personal Digital Assistant
PDSN	Packet Data Switch Network
PLMN	Public Land Mobile Network
POTS	Plain old telephone service
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAS	Registration, Admissions, and Status
RFC	Request for Comments
RSVP	Resource Reservation Protocol
RTCP	RTP Control protocol
RTCP	RTP Control protocol
RTP	Real-Time Transport
RVP	Remote Voice Protocol
SAP	Session Announcement Protocol
SCCP	Signalling Connection Control Part
SCP	Signalling Control Part
SCTP	Stream Control Transmission Protocol SCTP
SDH	Synchronous Digital Hierarchy
SDP	Session Description Protocol
SG	Signalling Gateways
SGCP	Simple Gateway Control Protocol
SI	Service Indicator
SIF	Signalling Information Field
SIGTRAN	Signalling Transport
SIO	Service Information Octet
SIP	Session Initiation Protocol
SLS	Signalling Link Selection

SPC	Signalling Point Code
SS7	Signalling System 7
STP	Signalling Transfer Points
SUA	SCCP User Adaptation
TCAP	Transaction Capabilities Application Part
TCP	Transmission Control Protocol
TIA	Telecommunications Industry Association
TUP	Telephony User Part
UART	Universal Asynchronous Receiver/Transmitter
UAS	User-agent Server
UDP	User Datagram Protocol
USB	Universal Serial Bus
VAS	Value-Added Services
VLR	Visitor Location Register
VOIP	Voice over Internet Protocol

CONTENTS

CHAPTER 1

INTRODUCTION

Signalling system is the most important part for any type of communication network. Keeping this on the top priority all the communication system developers are developing new signalling systems or improving the existing once. In doing so, many developers and industries are developing their own signalling systems or protocols to meet their requirement and make their product usable in the common domain. In the field of telecommunications, a *protocol* is the set of standard rules for data representation, signalling, authentication and error detection required to send information over a communications channel. From small hand-held Personal Digital Assistant (PDA) to large Packet Data Switch Network (PDSN) everywhere manufacturers are introducing standard of their own signalling protocols. In some case they are not publishing their customized protocols, which they are demanding as proprietary protocols. Usages of these equipments have become difficult [1] in the existing common platforms. However, now a days some developers, manufacturers or solution providers want to work in a common platform, and for these reason they are trying to develop some interoperable protocols. All over the world North America, South-America, European Countries, Japan, China, Israel, India, Australia customization is going on everywhere in the field of communication, but still they are trying to connect each other in a common platform.

1.1 Literature Review

The widely used Signalling System No.7 (SS7) passed a long way of development; it has been developed as Common Channel Signalling (CCS) by major telephone companies and the ITU-T since 1975. The first international CCS protocol was defined by the ITU-T as Signalling System No. 6 in 1977. SS7 was defined as an international standard by ITU-T in 1980. SS7 was designed to replace SS6, which had a restricted 28-bit signal unit that was both limited in function and not amendable to digital systems. SS7 has subsequently replaced the old SS6, SS5, R1 and R2, with the exception that R1 and R2 variants are still used in numerous countries [2].

SS5 and its earlier versions made use of in-band signalling, where the call-setup information was sent by playing special multi-frequency tones into the telephone lines (known as bearer channels in the parlance of the telecom industry). However, this led to security problems. Modern designs of telephone equipment that implement out-of-band signalling protocols explicitly keep the end-user's audio path—the so-called speech path—separate from the signalling path to eliminate the possibility that end users may introduce tones that would be mistaken for those used for signalling.

SS6 and SS7 moved to a system in which the signalling information was out-of-band, carried in a separate signalling channel. This avoided the security problems that the earlier systems had, as the end user had no connection to these channels. SS6 and SS7 are referred to as so-called Common Channel Interoffice Signalling Systems (CCIS) or Common Channel Signalling (CCS) due to their hard separation of signalling and bearer channels. This required a separate channel dedicated solely to signalling, but the greater speed of signalling decreased the holding time of the bearer channels, and the number of available channels was rapidly increasing anyway at the time SS7 was implemented.

The common channel signalling paradigm was translated to IP via the SIGTRAN protocols as defined by the IETF. While running on a transport system based upon IP, the SIGTRAN protocols do not act as SS7 variants, rather they act as transports of the existing national and international variants of SS7.

There are two main reasons for carrying out research on the development of a new Signalling System, which are as follows:

- Technical necessity of a new signalling system
- Business demand of the new signalling system

These points are described elaborately in the sections 1.1.1 and 1.1.2.

1.1.1 Technical necessity of a new signalling system

Small System Distributed Network (SSDN) is a network of small devices or functional modules, which are made of small scale microcontrollers or hardware.

These small modules work together in a SSDN, therefore the overall function of the network is distributed over all the modules rather than centralized. This type of network is more fail safe than any centralized system and the overall hardware and network overhead cost is reduced. Existing signalling schemes SS7, SIGTRAN, H.323, SIP etc. for the communication network are not suitable or easy to use for **SSDNs** and the existing signalling scheme of these types are usually proprietary schemes used solely for their own system. Thus the objective of the current research is to develop a signalling (Bus Independent Signalling- **BIS.1**) scheme for Bangladesh which would run on these types of SSDNs. This signalling system will be a highly customizable to meet all class of requirements for any type of communication applications.

1.1.2 Business demand of the new signalling system

In Bangladesh, we do not have any customized solution to develop a common platform to meet our local needs, such as industrial data acquisition, small system telecommunication (PABX), distributed network (PDSN, IP-PBX), industrial and power sector remote monitoring, remote monitoring and controlling of home appliances, automated security system, bio-engineering measurement, power measurement and billing, wireless data communication and many more applications to mention. We have a potential of providing these type of integrated solution both in the local and international markets. It is already too late for us to start Research and Development (R&D) in this field, locally in our country. If this is delayed further no opportunity would be left for us to enter into the world of ever-growing communication technology and it would be difficult for us to be in the global network with our own products and solutions.

1.2. Related work on signalling

Development of various types of signalling system both for data and voice communication is still going on, SIGTRAN is still in the development phase of the as it is not yet fully optimized and portable to all types of network. Signalling system or protocols for small system or small scale communication are also being developed by several manufacturers or groups of developers.

F-Bus (for "Fast Bus") is an ANSI/IEEE data bus oriented towards backplanes and cell phones. The standard specifies a way for various pieces of electronic hardware to communicate, typically with one piece acting as master (sending a request), and another acting as a slave (returning an answer). The F-Bus is a bi-directional full-duplex serial type of bus running at 115,200 bit/s, 8 data bits, no parity, one stop bit. Much like a standard RS-232 serial port, F-Bus connections uses one pin for data transmit and one pin for data receive and another for the ground. Nokia is using this in their mobile phones for transferring SMS to a PC [3, 4].

The M-Bus ("Meter-Bus") is a European standard for remote reading of heat-meters and it is also usable for all other types of consumption meters, and also for various type of sensors and actuators. With its standardization as a galvanic interface for remote readout of heat meters this bus wins a great importance for the energy industry as relevant users. Nokia, Ericsson is using this protocol in their mobile phones for SMS transfer to PC [5-7].

There are other protocols used by several manufacturers in their systems and most of them are similar to the CAS (R2) signalling but customized by them according to their own requirements.

And even the SS7 itself is customized by several countries to meet their local requirements.

1.3 Objective of the present work

The telecommunication signalling system (SS7) is mainly based on point to point connection and the protocols used above the physical layer are also for point to point connectivity. Though presently SS7 is also being adopted over the point to multi point network architecture of TCP-IP, it is still very complex to be implemented in small systems (like small PBX network, Point to Multi-point small data network, etc) using 8/16 bit processors. For this reason a light weight data communication layered system has been proposed to adopt a point-multi-point signalling protocol, which would be independent of the main payload bearer network. This would be called the Bus

Independent Signalling (BIS) system, which may have a separate or an integrated signalling path network. The BIS of the second category, namely, the integrated signalling path uses the RS-232, RS-485, TCP/IP protocols and caries the payload itself.

Applications of the proposed BIS systems: separate bearer path (channelized voice communication for PBX) and integrated bearer path data communication using same bearer network DDSN. This work is undertaken to initiate the process to interact with the most commonly used signalling system of telecommunication (SS7 & SIGTRAN), to be able to customize it according to our requirement in a customized network and at the end to be able to develop our own signalling system to meet the present and future demands. Any signalling system and protocol developed for the first time is not bullet-proof at the beginning, and needs a long-term development and modification to be able to fit in the existing system and to survive for long. In this work not only the signalling architecture and its implementation in the standalone system have been described, but also the way of further development, multi-protocol adaptation and applications described. This will help further development of the proposed signalling system for our customized application.

1.4 Organization of the Thesis

This chapter (Chapter 1) has described the objective of the research work, necessity of this research work and the background of the related work.

Chapter 2 describes the following topics in a greater detail: overview of the telecommunication signalling system, introduction to signalling, purpose of signalling, traffic control procedure, communication using database, network management procedure, classification of signalling systems based on architecture and application, channel associated and common channel signalling system have also been described.

In Chapter 3, a detailed description of SS7 and SIGTRAN are enumerated. It includes SS7 network structure, components, protocol layers, ISUP message structure, call setup, Signalling Connection Control Part (SCCP), SS7 over IP, layers of SIGTRAN for a complete understanding of the present telecommunications signalling systems and protocols.

Chapter 4 describes the Non-SS7 signalling protocols. It includes overview of H.323, H.323 elements, protocol suite, RAS signalling, call control signalling (H.225), media control and transport (H.245 and RTP/RTCP), H.323 call-flows and the overview of the Session Initiation Protocol (SIP) also. SIP messages, basic operation of SIP, overview of RS-232 and RS-485 have also been discussed for a better understanding of the next generation communication protocol and the transmission layers to be used in the proposed BIS system.

In Chapter 5, the new signalling system has been proposed and its additional requirements on the existing signalling systems have been explained. The proposed Bus Independent Signalling (BIS) has also been described in this chapter. It also covers the BIS network structure, network type, BIS stack, messages, quality and performance analysis, some application modules. Capacity related calculations are also presented.

Implementation of the BIS system and its application in two basic types of network have been described in a greater detail in Chapter-6. All the required hardware, software modules, firmware and software flowcharts, network dimensioning, interfaces and gateway hardware and software architecture have also been presented in this chapter.

Chapter 7 presents the results and discussion of the current research. A comparative study is provided in this chapter between the proposed protocol and the general purpose standard SS7 protocol I used. The merits of the proposed system are also highlighted.

Chapter 8 includes the conclusions and provides some suggestions for future work that may be continued along the line of the present implementation of the proposed BIS system.

CHAPTER 2

OVERVIEW OF TELECOMMUNICATIONS SIGNALLING SYSTEM

This chapter describes definition of various technical terms, purpose of signalling, classification of the signalling systems based on the applications and architecture.

2.1 Introduction

A *protocol* is a formally prescribed set of rules, or conduct that governs an event. A commonly observed protocol is the handshake of two people meeting for the first time. This says, "I recognize your presence, and you have my attention". At parting, the handshake is repeated, and it implies that the meeting is at an end and each party can resume his/her affairs. Protocols also govern our timing of events.

Control of procedures in communication networks must be based on some additional information provided by users, and generated by network nodes. This additional control information, when passed between network entities (network elements, user devices and databases, etc.), is referred to as *signalling* [8].

The primary need for the signalling came into the scene while making a telecom network. In the old days of telephony, signalling related to a call was provided in the form of dialogues between a subscriber and an operator (or a chain of operators on long distances), where a specification of name and location (or later the telephone number) of the called remote party had to be provided to enable the call set-up. Later, different signalling systems have been developed, which comprised various types of signals like pulses and tones, sent in analogue or digital form over the lines. These systems are still in operation in the existing networks.

Finally, with the rise of digital transmission (bearer signalling), signalling also took its digital form. Several signalling systems have been standardized for different type of applications and have become recognized as international standards.

2.2 Purpose of signalling

Generally, signalling is used to transfer instructions relevant to the following three main groups of networks activities:

- Control of traffic procedures (set-up, supervision, release of connections / services)
- Communication with databases (especially important in mobile networks),
- Network management procedures.

Here is one example of use of the SS7 signalling in the GSM telecom network. The signalling and network activities are shown in Figure 2.1.

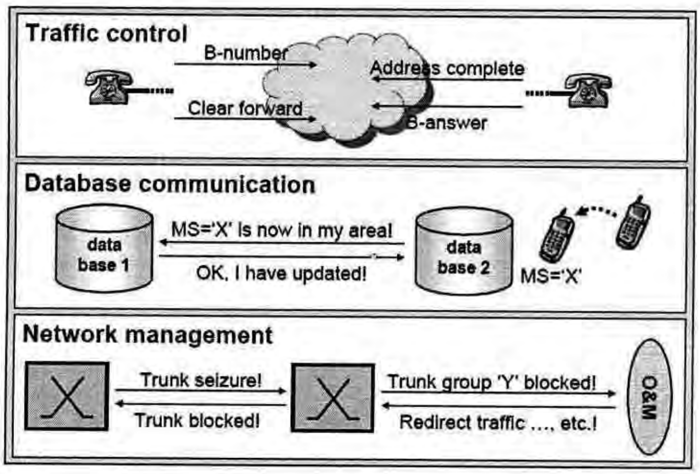


Figure 2.1: Signalling and network activities.

SS7 is used to cover the following three aspects-

- Traffic control
- Database communication
- Network management

2.2.1 Traffic control

This procedure comprises routing and switching of a connection to a recipient, checking the recipient's status and providing backward information to the calling party (ringing tone, busy tone, and announcement), redirecting the connection, choosing appropriate tariffs for billing, activation of supplementary services, and many others [8].

2.2.2 Database communication

It enables the operators to provide services based on the information, which is necessary to complete the connection (like the position of a mobile subscriber in the network, his/her privileges, etc.), which is required to complete an operation (like verifying the validity of a credit card), or which finally may affect the logic of a connection set-up and the ratification of the service itself (like in case of *intelligent network* services).

2.2.3 Network management

This procedures allow the operators to communicate with the network elements (exchanges, databases, routers, cross-connects, etc.), reconfigure the network connections, and control and supervise the network as a whole. These procedures a more and more centralized, and have been standardized under the concept of Telecommunications Management Network [9].

2.3 Classification of signalling system

Signalling system can be classified from different point of views. Mainly we can classify all types of signalling system that exist in various types of network from the following two points of view:

a) Based on the basic application
b) Based on the architecture

a) The applications include how the host and client will be connected, how they will control the signalling procedure, what type of massages will be delivered between them. This type of signalling system can be divided into 3 categories which are
   - Connection Oriented Signalling
   - Connectionless signalling
   - Customized signalling

b) Based on the Network architecture, signalling in a telephone network may be divided into the following two basic categories:

- Access signalling (or subscriber signalling)
- Trunk signalling (or inter-exchange signalling)

2.3.1 Connection oriented signalling

This type of signalling system is mainly used in realtime communication, like voice transfer through the telecommunication network. The mostly used signalling system is the Signalling System No. 7, SS7 for short. In this signalling system, some resources need to be allocated first to enable the connection of the user. Then the signalling starts between the elements [10].

2.3.2 Connectionless signalling

This type of signalling is used for data communication, mobile/wireless voice communication, where fixed connection between the network elements is not required before the actual data/voice transfer begins. In data communication it is not necessary to be a realtime process, so connection between the host and user need not to be fixed or allocated permanently during the data transfer process, for example, the act of file transfer between two PCs, SMS transfer from one user to another. For voice communication in a mobile/wireless network, connection between users or elements are not fixed but dynamically allocated and shared by the users. For proper allocation and proper resource utilization user authentication (mainly database communication) and resource allocation (network management) are necessary for which signalling is not required for any connection before the bearer transmission begins. As an example in mobile communication user database of party A and party B need to be verified to confirm that they have the permission for the requested services (like IDD calls, SMS and others) and for B party's location confirmation no connection is needed before the voice connection setup commences.

2.3.3 Customized signalling

Customized signalling systems are mainly used in communication systems where customized services are required. For example, in mobile communication if we need to route some specific calls originated from a specific location to some other specific network element a modification in the existing standard signalling system may be required. Some manufacturer also use their own proprietary signalling in their system for better security or for rendering special services.

2.3.4 Access signalling systems

Access signalling system is used to allow a subscriber to pass any type of information, which is required for establishment of the connection and/or securing provision for a specific service, to the exchange. This, in most of the cases, includes the dialed number, but may also contain many other information (like, type of transmission resources, specification of service parameters). Since signalling works both ways, it also allows the exchange to inform the user about the possibility, progress or trouble in providing a connection or a service. Access signalling can be divided basically into the followings two types:

- **Subscriber line signalling** (used in PSTN),
- **Digital subscriber signalling** (used in ISDN and PLMN).

The classification of the signalling based on architecture is shown in Figure 2.2..

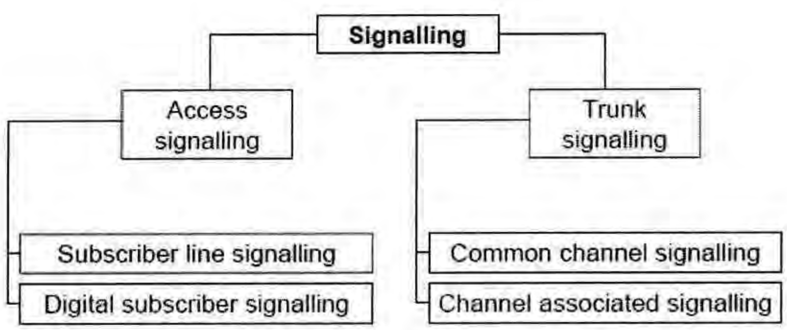


Figure 2.2: Signalling in telecommunication networks.

Subscriber line signalling is used on analogue lines connecting user terminals (telephones or fax machines) to the local exchange. It consists of various elements, such as:

- On/off hook signals
- Dialed digits
- Information tones (dial tone, busy tone etc)

• Recorded announcements,

• Ringing signals.

The digits of a dialed number (the B-number) may be transferred using either the pulse (old-type rotary-dialing) telephones or as a combination of two tones known as Dual Tone Multi-Frequency (DTMF) signals used for modern push-button telephones. The off hook signals can have different meanings, depending on the state of the call or subscriber. When an A-subscriber lifts the handset, the off hook signal means 'call attempt' but when a B-subscriber lifts the handset to answer a call, the same signal means 'B-answer'.

The information tones (dial tone, ringing tone, busy tone, etc.) are audio signals used to keep the calling party (the A-subscriber) informed about what is going on in the network during the set-up of a call.

The establishment and release phases as well as the signals sent, for a normal call between two subscribers connected to the same Local Exchange (LE) is shown in the signalling diagram of Figure 2.3.

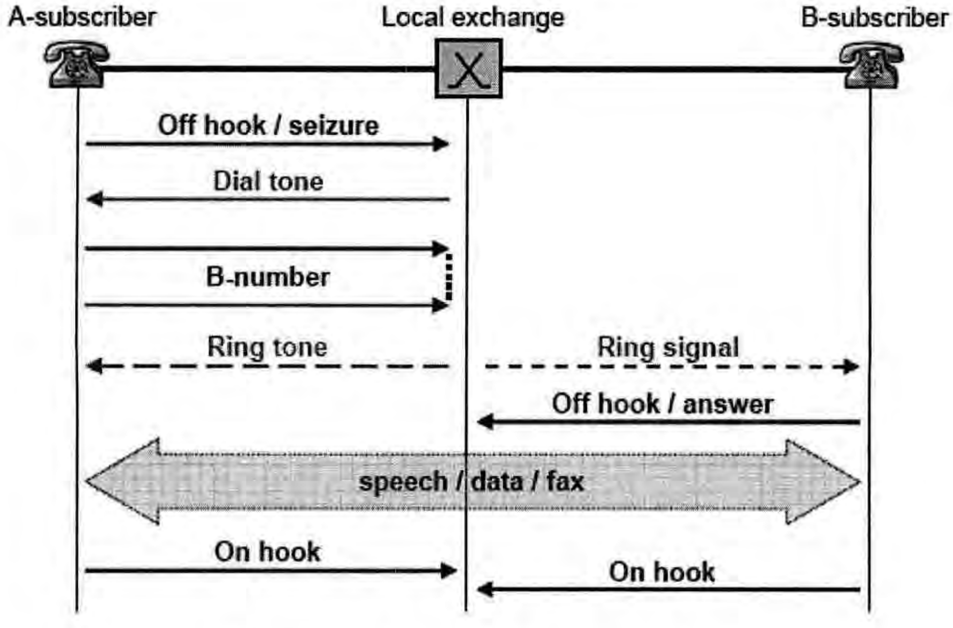


Figure 2.3: Subscriber line signalling

Digital subscriber signalling is used on digital lines connecting ISDN terminals (telephones, fax machines, computers) to the local ISDN exchange. It consists of signalling messages in the form of packets. ISDN access signalling system is called *Digital Subscriber Signalling System No.1* (*DSS1*). It uses a special channel for transmission of signalling, the *D-channel*. The signalling protocols are based on the OSI (Open System Interconnection) reference model, layers 1 to 3. Consequently, the signalling messages are transferred as data packets between the user's terminal and the Local Exchange (LE). Because of the much more complex service environment at the ISDN user's site, the amount of signalling information and the number of variations differ greatly from the arrangement used for the ordinary telephone subscriber signalling described above. This fact is reflected in the number of parameters included in D-channel messages. The ISDN configuration for Basic Access, the related OSI layers and functions, and the parameter structure of the first D-channel message sent at a call request, i.e. a SETUP message is shown in Figure 2.4.

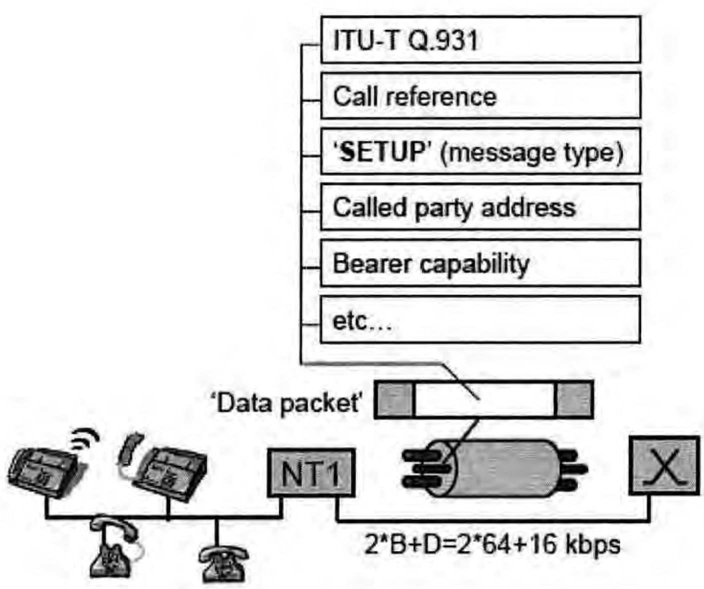


Figure 2.4: ISDN Basic Access (BA)

At the beginning of the call set-up phase, the ISDN user terminal (the A party) must provide the network (initially the LE) with the information needed to establish the call. This information must be precisely defined. For instance, the network does not know beforehand what type of terminal (telephone, data terminal, etc.) or service it will be dealing with. A call is initiated by the calling subscriber sending the address information from an ISDN terminal and, where applicable, by sending additional service information. Pushing the send button will cause the terminal to start transferring the first D-channel message, which is a SETUP message. If the message contains all the data required to establish a call, a CALL PROCEEDING message is returned to the calling subscriber's terminal. This signal confirms that the requested call establishment has been initiated and that no more call establishment information will be accepted (refer to Figure 2.5).

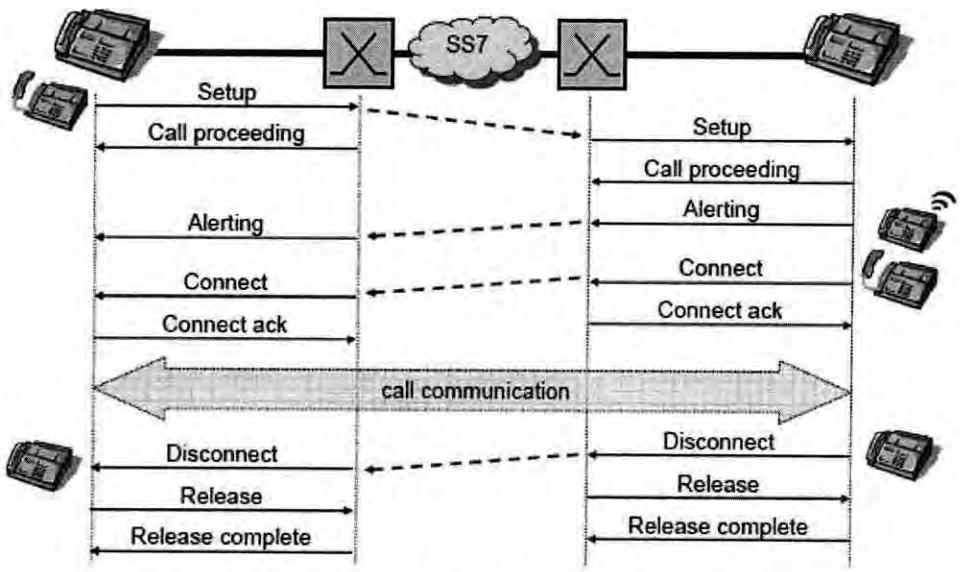


Figure 2.5: Digital subscriber signalling.

After the B-side has received a SETUP message, an ALERT message will be sent through the network to the calling user's terminal (A). This message informs the A-terminal that the B-terminal has been 'alerted' saying that there is an incoming call. We may compare this communication process with that of an ordinary telephone call in PSTN, where the A-subscriber receives ringing tone and the B-subscriber receives ringing signal at the same time.

When the B-terminal accepts the call, a CONNECT message is sent through the network to the A-terminal. After the two sides receiving the CONNECT ACKNOWLEDGEMENT message, the call enters an active state.

The call can be released from both sides. As in the establishment phase, the release of a call involves interchange of messages between the two sides and between each side and its local exchange.

The signalling in the network, i.e. between the two local exchanges, requires SS7 signalling and the corresponding ISUP (ISDN-User Part) signalling protocol, which will be described later in this chapter.

2.3.5 Trunk signalling methods and systems

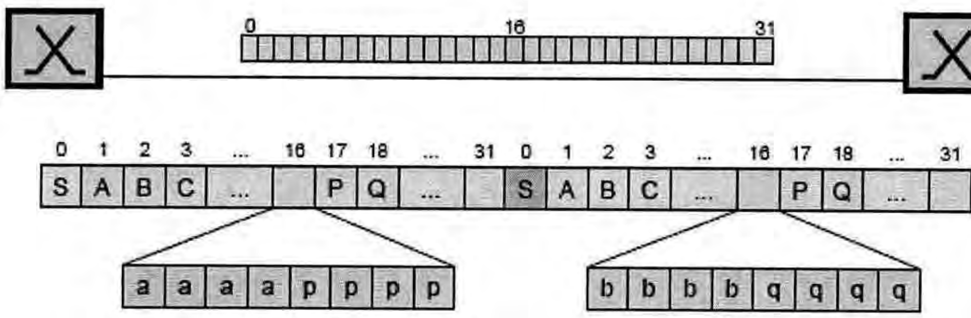
Trunk signalling is the language of network nodes and is concerned primarily with management of network resources and provision of communication path between exchanges (with the use of routing and switching). However, with the development of ISDN, mobile networks and network intelligence, this type of signalling had to provide means also for database queries and network management procedures. In trunk signalling (refer to Figure 2.2) all possible signalling systems fall into one of the following two categories (*signalling methods*):

- Channel Associated Signalling (CAS)
- Common Channel Signalling (CCS)

2.4 Channel Associated Signalling (CAS)

'Channel Associated Signalling' (CAS) is associated with the traditional trunk signalling systems. This is shown in Figure 2.6. Some of these systems are specified by ITU-T (formerly CCITT). Typical examples of such systems, which are still used globally in national as well as in international networks, are systems No. 5, R1 and R2. These systems were originally designed to mainly support ordinary telephony connections and related additional services.

The term 'Channel Associated Signalling' (CAS) indicates that the transfer of signals is very closely associated with the 'channel', which in this context means the traffic communication channel. In other words, signals and traffic 'travel' the same way through the network. A typical feature of these systems is that trunk signals sent over a PCM (Pulse Code Modulated) link with 32 time slots are transferred in time slot 16 as well as on the traffic channels (time slots 1-15 and 17-31). The signals sent in time slot 16 are named 'line signals' and the signals sent in the traffic channels are named 'register signals'.



time slot	used for
0	frame synchronisation
1-15	register signals / traffic channels
16	line signals
17-31	register signals / traffic channels

Figure 2.7: Channel Associated Signalling (CAS)

The USA, Japan and some other countries use a system with 24 time slots per frame. In the 24-channel system one bit in each time slot in every sixth frame is allocated for line signalling. Register signals are transferred in the same way as in the 30/32 PCM system. Line signals can be sent or received during the entire call. Even when a 'line' (traffic channel) is idle, a line signal called 'Idle line' is usually sent continuously for that channel. The line signalling is handled by specific devices and functions in the exchange and must be allocated for each trunk line using a CAS system. Examples of line signals are:

- Idle line
- Seizure of line and seizure acknowledgement
- B-answer
- Clearing the line in the forward / backward direction
- Release guard
- Forced release
- Line blocking
- Charging pulses.

Register signals are used during the call set-up phase and sent on the traffic channel that has been reserved for the call. The following are typical register signal contents:
• B-number,
• Calling party's category (A-subscriber),
• B-status information,
• A-number (in some cases).

In systems like No. 5, R1 or R2, the signals consist of tones or combinations of tones. On PCM links theses tones are, of course, converted into digital form. The call setup process in CAS is depicted in Figure 2.7.

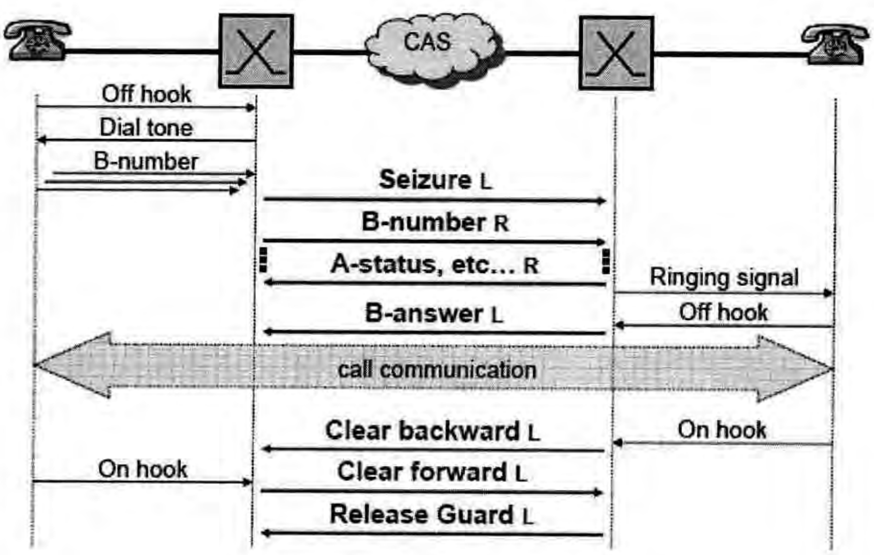


Figure 2.7: Call setup in CAS

The exchanges usually contain dedicated signalling equipment for the handling of register signals. System R2 requires two types of equipment: code senders and code receivers. The names indicate the direction of the transmitted register signals. Nowadays these two devices are often combined to form a single device called 'code-sender- receiver'.

Because the register signalling equipment is only used during the call setup phase, it is usually connected to the traffic communication channel only for a few seconds. This means that the equipment can be shared by many trunk lines. The optimal number of code-sender-receivers is determined when dimensioning the exchange on the basis of current traffic data and other parameters.

2.5 Common Channel Signalling (CCS)

As far back as the middle and late seventies, manufacturers intensified their efforts to design a new, faster and more flexible signalling system (as compared with the existing CAS systems). The result of this development was a new signalling system based on a modern packet data communication concept, i.e. a system intended for 'computer-to-computer' communication.

Further on, the system was designed for use of a common data channel (signalling link) which would exclusively serve as carrier of all signals required by a large number of traffic channels. This is why the system was defined as a 'Common Channel Signalling (CCS)' system to distinguish it from CAS systems. This is shown in Figure 2.8.

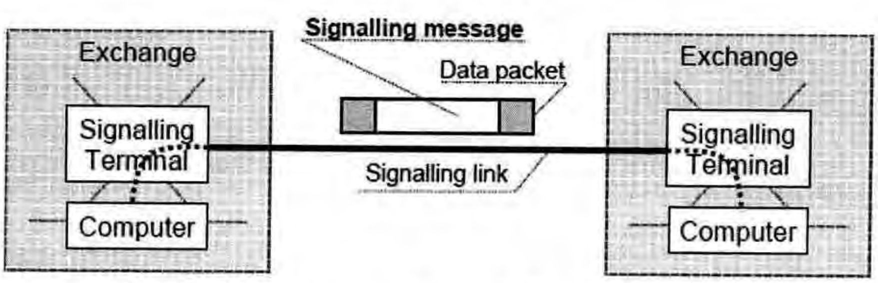


Figure 2.8: Common Channel Signalling (CCS)

The signalling system described above was specified by CCITT in 1980 and given the name 'Signalling System No. 7' (SS7) and was intended for use in the national as well as international digital networks.

The first SS7 version (1980) was designed for telephony and data. During the 80's the demand for new services increased dramatically and the SS7 was therefore developed to meet the signalling requirements specified for all these new services. Today SS7 is used in many different networks and related services, typically within PSTN, ISDN, PLMN and IN, all over the world. It should be noted here that as early as in 1968, CCITT specified a Common Channel Signalling system called CCS system No. 6, which was designed especially for international analog telephony networks. However, very few installations of this system remain today. It has, as mentioned already, been replaced by SS7.

2.6 SS7 features

SS7 is still the most widely used signalling system for the following main features:

- **High flexibility** - SS7 can be used by many different types of telecommunication services. It is used for setting up and releasing connections in traditional telephony and data communication, in mobile telephony and data communication, for the provision of ISDN services, and many other applications. SS7 is also used for interchange of data between databases (e.g. VLR↔HLR in cellular networks).
- **High capacity** - A single signalling 'link' can support several thousand trunk lines.
- **High speed** - Setting up a call through a number of exchanges takes less than a second.
- **High reliability** - The system contains powerful functions for elimination of disturbances in the signalling network. One example is the possibility of choosing alternative links for signalling.
- **Economical** - The fact that one and the same signalling system can be used by a wide range of telecommunication services and connections is an important economical aspect. Besides, system SS7 is much simpler and requires less hardware than older signalling systems. SS7 can handle both the so-called circuit related signalling and non-circuit related signalling. The term 'circuit' in this context means 'traffic channel'. Thus, 'circuit related signalling' means signals sent in order to support a call establishment or release procedure.

There is a great need for interchange of data between databases in order to support certain functions related to cellular networks, IN services, etc. Such communication of ‘data’ over the SS7 network is normally not related to any ‘circuit’ (traffic communication channel) and is therefore, in SS7 descriptions, regarded as ‘non-circuit related’ signalling. The original version of SS7 was not designed to support this type of signalling but this facility has been added in its later versions.

SS7 signalling system and the related SS7 over IP (SIGTRAN) will be described in detail in the next chapter.

CHAPTER 3

SS7 AND SIGTRAN

In this chapter Signalling System No.7 (SS7), its network elements, and protocol layers with its detailed message structure will be described. Call setup process in ISUP and other non-ISUP application layers will also be described. Finally the SIGTRAN protocol will be described in detail in order to have a complete and clear understanding of SS7 and SS7 related signalling systems and protocols.

3.1 SS7 network components

An SS7 network is independent from the transmission network. It consists of the Signalling Points (SPs), Signalling Transfer Points (STPs) and Signalling Links (SLs). Physically SP and STP are located in the nodes of a telephony network. STP can also be a stand-alone node [10]. The signalling network components are shown in Figure 3.1.

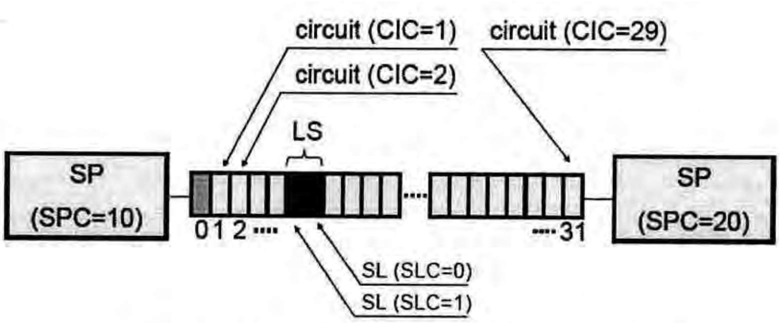


Figure 3.1: Signalling network components

Signalling Link (SL) is a basic component in a signalling network that connects two Signalling Points (SPs). It provides mechanisms for reliable message transfer (error and sequence control). It is identified by the **Signalling Link Code (SLC).**

Link Set (LS) is a set of SLs connecting directly two SPs. The maximum number of SLs within an LS is 16 (16 time slots of 64kbps).

Signalling Point (SP) is a node where the originator or recipient of the signalling message resides. Each SP is identified by the **Signalling Point Code (SPC).** SPC uniquely identifies SP within national or international signalling network. In order to discriminate between national and international signalling network nodes an extra parameter, called **Network Indicator (NI)** is used. The examples of national and international point codes are shown in Figure 3.2.

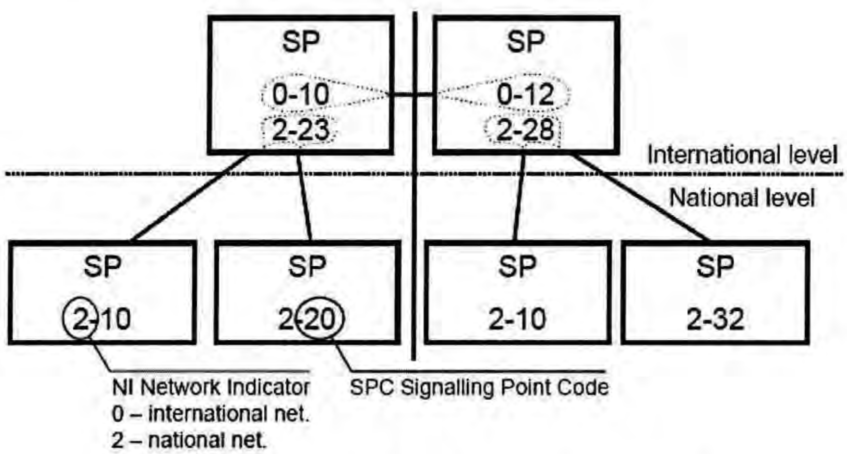


Figure 3-2: National and international SPCs

Originating Point (OP) is an SP at which a particular signalling message is generated. Each signalling message carries inside a routing label **Originating Point Code (OPC)**, which identifies the originating point for that message.

Destination Point (DP) is the SP to which a particular signalling message is destined. Each signalling message carries inside a routing label **Destination Point Code (DPC)**, which identifies the destination point for that message.

Signalling Transfer Point (STP) is the node that transfers messages in the network like a router in X.25 or TCP/IP network without analysis of their content (accept routing label).

Signalling Route (SR) is a predetermined path a message takes through the signalling network between the originating point and the destination point. A Signalling route is defined as LS, which is assigned to carry traffic to a particular destination. LS may carry several signalling routes and hence convey traffic to several destinations.

Signalling Route Set (SRS) is a group of all Signalling Routes (SRs) that may be used for message traversing between an originating point and destination point.

STP Pair is a pair of STPs that work together. In normal use, the signalling traffic is divided between the two STPs on load-sharing basis. In case of failure in one STP, the other STP must have a capacity to handle all the signalling traffic of the failed STP. The signalling route and route set are shown in Figure 3.3.

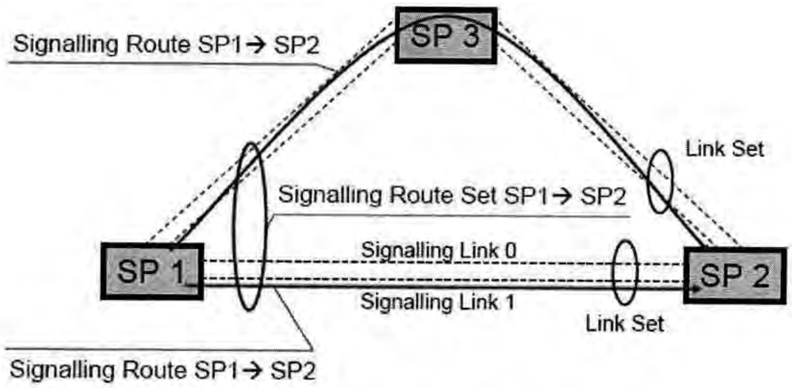


Figure 3.3: The signalling route and route set

3.2 SS7 network structure

The SS7 network structure covers network hierarchy, and network links which are described in the following subsections.

3.2.1 SS7 network hierarchy

A complex network generally has a hierarchical structure of STPs. One example of an STP hierarchy is when international exchanges constitute the higher level and national exchanges the lower level. This may be continued to the local exchanges constituting the lowest level [11].

ITU-T suggests the following guidelines for network structure design:

• Each SP that is not an STP is connected to at least two STPs of the lower level,

• Each STP of the lower level is connected to at least two STPs of the higher level,

• STPs in the higher level are fully meshed (all STPs have direct link to each other).

The SS7 structure hierarchy is shown in Figure 3.4.

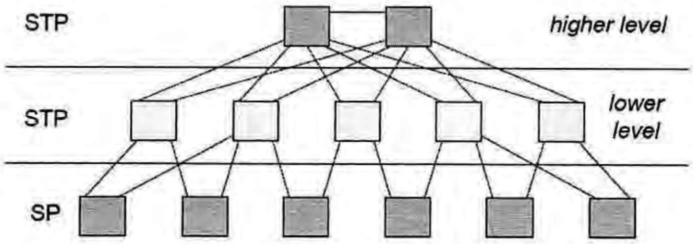


Figure 3.4: SS7 structure hierarchy

3.2.2 Network links

SS7 Signalling Network links are characterized by their usage and grouped into the following classes [12] (refer to Figure 3.5).

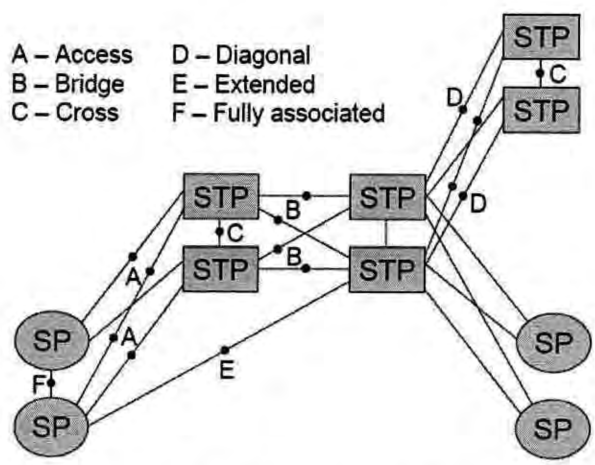


Figure 3.5: SS7 Network links

• **A** - Access link connects an SP to an STP. Only messages originating from or destined to the signalling end point are transmitted on an A-link.

• **B** - Bridge link connects to STP pairs at the same hierarchical level (local-local, regional-regional).

• **C** - Cross link connects STPs performing identical functions into a mated pair. A C-link is used only when an STP has no other route available to a destination signalling point due to link failure(s).

• **D** – Diagonal link connects a local STP pair to a higher level STP pair.

• **E** - Extended link connects an SP to an alternate STP. E-links provide an alternate signalling path if an SP's 'home' STP cannot be reached via an A-link. E-links are not usually provisioned unless the benefit of a marginally higher degree of reliability justifies the added expense.

• **F** - Fully associated link connects two SP. F-links are not usually used in networks with STPs. In networks without STPs, F-links directly connect SPs.

3.3 The SS7 Signalling

SS7, similar to other packet data networks, comprises a number of protocols that operate on different levels [11]. The stack of the most popular SS7 protocols is shown in Figure 3.6.

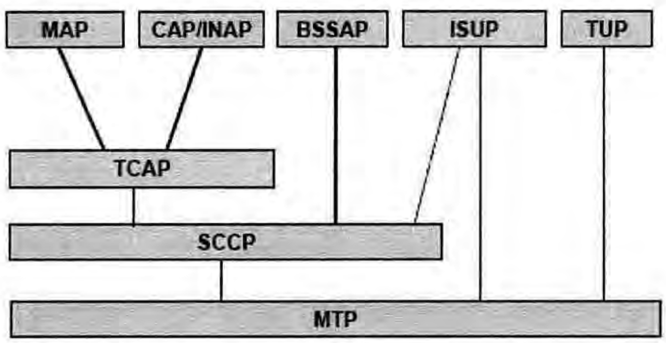


Figure 3.6: SS7 protocol stack

MTP – Message Transfer Part provides bearer services in an SS7 network. It is used to transfer messages of all upper layer protocols (MTP users) and has to be implemented in all SS7 nodes. MTP is divided into 3 levels:

• MTP Level 1 defines the requirements to be met by the physical circuit, usually a 64 kbits/s PCM channel.

• MTP Level 2 has functions for reliable transfer of data over physical connection, e.g. separation of messages, error detection and error correction.

• MTP Level 3 has functions for signalling message handling (distribution to the proper MTP user and routing) and network management (supervision of quality and capacity, rerouting in case of failure or congestion).

The structure of SS7 with the MTP is shown in Figure 3.7.

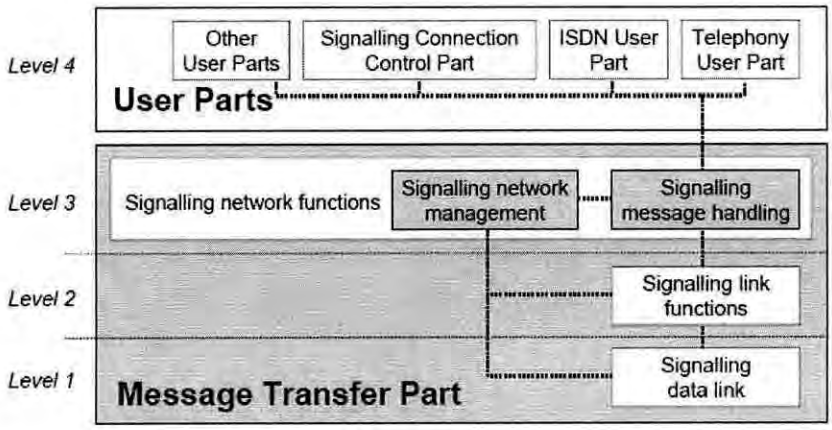


Figure 3.7: SS7 structure with MTP

SCCP – Signalling Connection Control Part is giving extra addressing possibilities used for non circuit-related signalling. It is implemented in all PLMN's SS7 nodes and in all international STPs.

TUP – Telephony User Part is used to establish and release traffic connections to and from PSTN exchanges. It is, however, constantly being replaced by ISUP in highly digitized telephony networks.

ISUP – ISDN User Part is used to establish and release traffic connections to ISDN exchanges and also between PLMN exchanges, like MSC and GMSC.

BSSAP – Base Station System Application Part is used in PLMN for communication between the BSS and the Core Network (A interface).

CAP – CAMEL Application Part and **INAP - Intelligent Network Application Part** are protocols used for signalling related to Intelligent Network (IN) and Mobile IN (MIN) services.

MAP - Mobile Application Part is used for communication between all nodes within the PLMN Core Network, for example, during mobile terminating call set-up when a GMSC is asking an HLR where to route the call or during location updating when an HLR sends all the data about the subscriber to the new MSC/VLR.

TCAP - Transaction Capabilities Application Part makes it possible to run simultaneous dialogues concerning different processes or subscribers between the core network nodes.

3.3.1 MTP Level 1

MTP Level 1 or signalling data link level defines the electrical connections between two SPs. A signalling data link is a bi-directional transmission path for signalling, that is, two data channels are working together in opposite directions at the same bit rate. This path is usually is digital, however the analog connection is also possible [13].

Digital signalling data link: Usually, one channel of the 2Mbits/s PCM line is used as a signalling data link. ITU-T recommends time slot 16, but states that if the time slot 16 is unavailable, any of the channels 1-31 may be used. The bit rate of the transmission is thus 64 kbits/s. Recently, ITU-T has specified a new type of digital signalling data link, called **High speed Signalling Link (HSL)**, where the bit rate of the signalling link is 2 Mbits/s.

Analogue Signalling Data Link: In exceptional cases an analogue signalling data link may be used, for example, when a PCM system is not available in some part of a signalling network. For telephone call control applications, the signalling bit rate over the analogue signalling data link should be at least 4.8 kbits/s.

High speed signalling Link: In mobile networks, due to high signalling load, there is a need for high capacity signalling links, for example between STP nodes and the

HLR. The HSL has almost 2 Mbits/s capacity compared to the standard 64 kbits/s signalling link.

SS7 hardware in a telephone exchange: Figure 3.8 presents the basic hardware blocks of a PSTN/ISDN exchange.

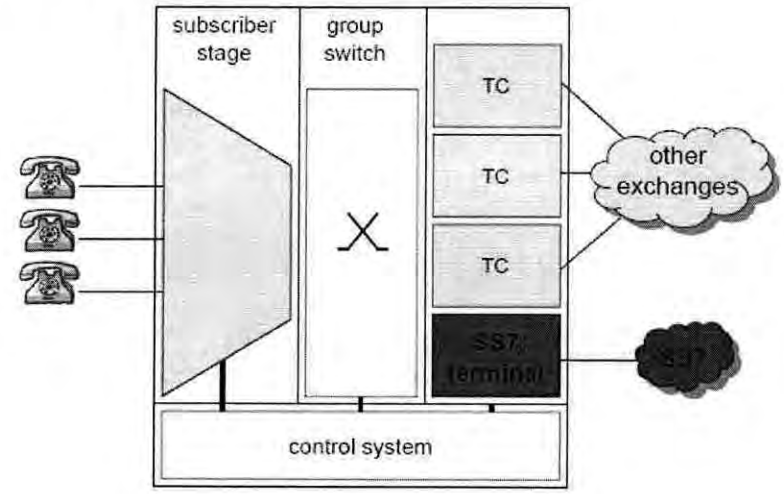


Figure 3.8: PSTN local exchange

Today's local exchange contains two switching points. The first one is the central group switch. The second is a less complex switch in the subscriber stage to allow common equipment to be located there and to concentrate traffic to the central group switch. The subscriber stage and the lines of other exchanges are connected to the central group switch, as is other equipment that should be connectable, such as signalling terminals. Termination Circuits (TC) interfaces the PCM trunk lines to other exchanges. The SS7 connection in a telephone exchange is shown in Figure 3.9.

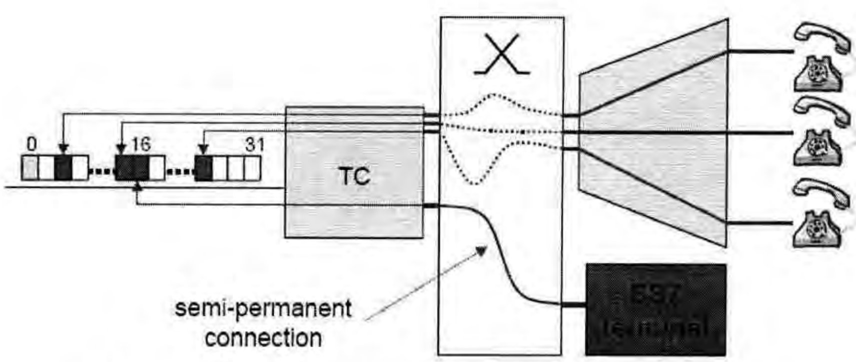


Figure 3.9: SS7 connection in telephone exchange

Modern exchanges have a modular design, i.e. all the parts of the exchange can be dimensioned according to the operator needs. The same technological platform can be used for a local exchange as well as for international exchange. For example the international exchange contains a larger group switch, more lines to other exchanges and more signalling terminals than the local exchange. The local exchange however, contains the subscriber stages that are not present in the international switch. The 64 kbits/s semi-permanent connection is defined in the Group Switch to interconnect an SS7 terminal with the trunk line to another signalling point.

The functions of MTP 1 and MTP 2 are usually implemented inside the signalling terminal, whereas the functions of MTP 3 and User Parts (UPs) are implemented in control system software. It means that there is a separate MTP 1 and MTP 2 entity per each interface which is signalling link and there is only one MTP 3 entity common for the entire node, able to communicate with multiple MTP 2 entities and able to route the packets between them. The relations between MTP entities and signalling links are shown in Figure 3.10.

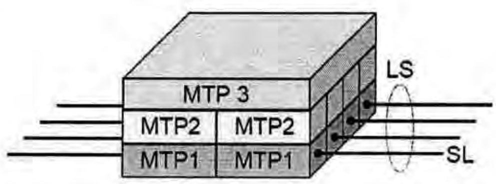
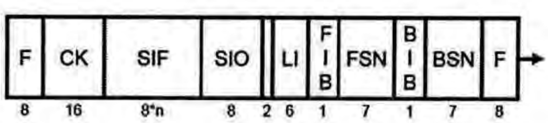


Figure 3.10: *Relations between MTP entities and signalling links*

3.3.2 MTP Level 2

Signal Unit: A signalling message, delivered by the higher levels, is transferred over the SL by means of variable length Signal Units (SU). The Message Signal Unit (MSU) is presented in Figure 3.11.



F-flag=7E hex, 01111110 bin
BSN- Backward Sequence Number
BIB-Backward Indicator Bit
FSN-Forward Sequence Number

FIB-Forward Indicator Bit
LI-Length Indicator
SIF-Service Information Field
CK-Check Bits

Figure 3.11: MSU Message Signal Unit

The **Flags (F)** indicate the beginning and the end of the signal unit. A bit stuffing functions are used to eliminate this pattern appearing within the SU. Every SU has 16 **Check Bits (CK)** for error detection. The check bits are generated by the transmitting signalling terminal by applying a specific algorithm to the bits of the SU. The receiving terminal uses the same formula to check the correspondence of the bits and the remaining part of the SU. If the complete correspondence is not found, the SU is discarded. The fields **FSN**, **BSN**, **FIB** and **BIB** are used to give the positive acknowledgements or to ask for retransmission if the SU was not received correctly.

Backward Sequence Number (BSN) is the 7 bits long field reserved for sequence numbers from 0 to 127. These are used to acknowledge the correct transmission of a signal unit.

Backward Indicator Bit (BIB) marks the SU as:
- Positive acknowledged, if the logical value of the BIB bit is the same as that received in the latest SU.
- Negative acknowledged, if the value of BIB is not equal to the value in the latest received SU.

Forward Sequence Number (FSN) is the 7 bits long field for sequence numbers from 0 to 127. The FSN is used to recognize the SU, which has been received out of sequence. If the logical value of the **Forward Indicator Bit (FIB)** is equal to the one in the previous SU, the receiver is informed that the SU is sent for the first time. If the logical value of FIB is not equal to the one in the previous SU, the receiver is informed that it is a repetition of a previously sent SU. Another method of error correction, called the *preventive cyclic retransmission* applies for intercontinental SLs, where the one-way propagation delay is greater than or equal to 15 ms and for all SLs established via satellite. In this method, during the period when there are no new SUs to be transmitted, all the SUs which have not yet been positively acknowledged are retransmitted cyclically. The FSN, BSN, FIB and BIB usage are shown in Figure 3.12.

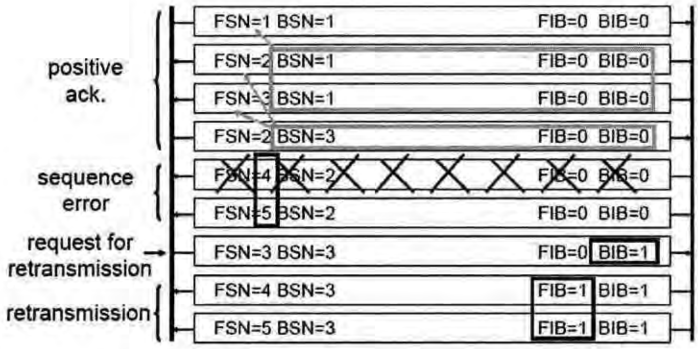


Figure 3.12: MTP L2- FSN, BSN, FIB and BIB usage

The **Length Indicator (LI)** indicates the number of octets between the LI octet and the CK field if number of octets is less than 63. The LI value equal to 63 indicates that the number of octets between LI and CK is 63 or more. Please note that maximum length of SIF and SIO that are between LI and CK is 272bits. LI also points out the type of the SU. The possible types of the SU are shown in the Figure 3.13.

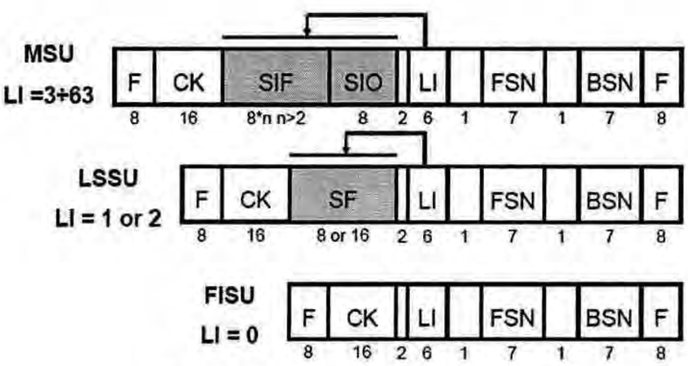


Figure 3.13: Length indicator

• **MSU - Message Signal Unit** (LI = 3 - 63) is used to carry upper layer messages protocol messages.

• **LSSU - Link Status Signal Unit (LSSU)** is identified by an LI value equal to 1 or 2. If the LI has a value of 1 then the status field consists of one octet; if the LI has a value of 2 then the status field consists of two octets. When a terminal, which is able to process only a one-octet status field, receives an LSSU with a two-octet status field, the terminal ignores the second octet for compatibility reasons, but process the first octet as specified in the standard. Figure 3.14 lists the length indicator values.

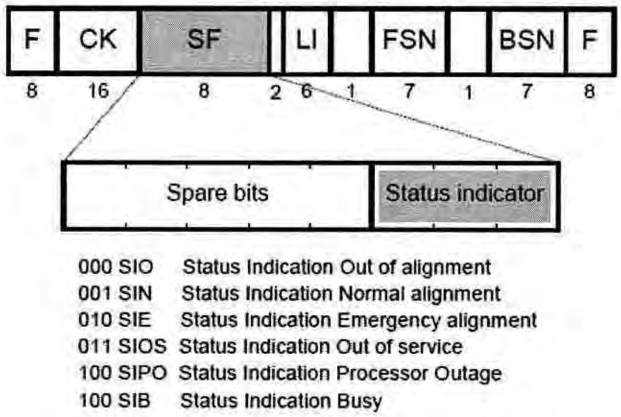


Figure 3.14: Status Field in an LSSU

• **FISU - Fill-In Signal Unit** (LI = 0) is used for error supervision (it carries only error correction fields). To keep the link running, it is sent when there is nothing else in the transmission buffer to be sent.

The **Service Information Octet (SIO)** is divided into the following three components (refer to Figure 3.15):

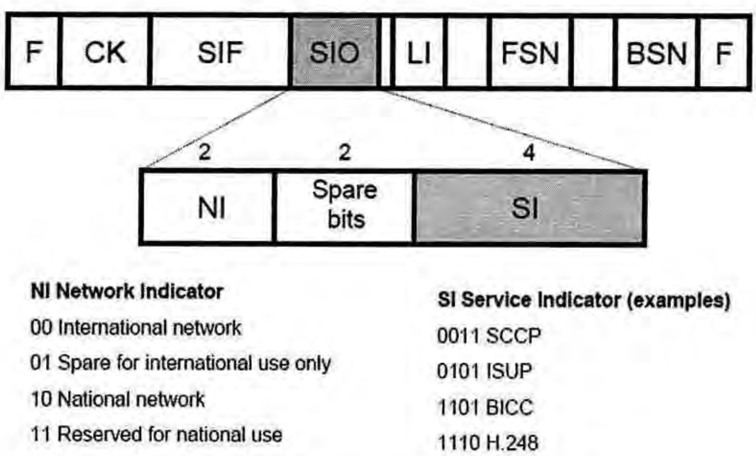


Figure 3.15: Service Information Octet

• **Service Indicator (SI)** specifies to which upper layer protocol (MTP user) the signalling message should be delivered,

• **Network Indicator (NI)** determines whether it is a national or an international network.

• **Spare bits** are not used in the ETSI version of the SS7. In ANSI version these spare bits are used to code the priority of the MSU. The **SI** codes are allocated as follows:

• 0000 - Signalling network management messages,

• 0001 - Signalling network testing and maintenance messages,

• 0011 - SCCP,

• 0100 - TUP,

• 0101 - ISUP,

• 0110 - DUP (call and circuit related messages),

• 0111 - DUP (facility registration and cancellation messages),

• 1000 - MTP Testing User Part,

• 1001 - B-ISUP,

• 1010 - S-ISUP,

• 1100 - Q.2630,

• 1101 -BICC,

• 1110 - H.248.

The **Signalling Information Field (SIF)** carries the upper layer protocol information. It includes the **routing label**, which is used by the MTP Level 3 to route the message through the signalling network to the proper destination. The components of SIF is shown in Figure 3.16.

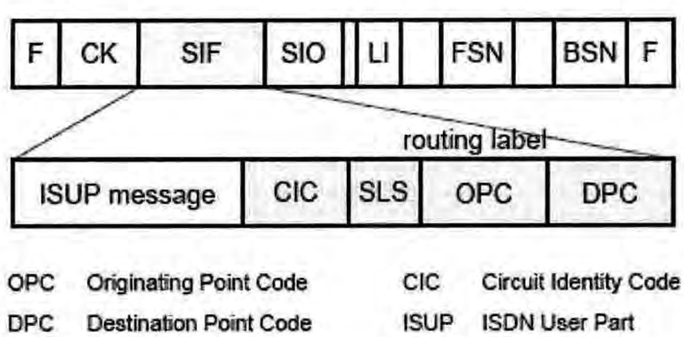


Figure 3-16: Service Information Field (ISUP)

The examples of the routing labels for other SS7 protocols are shown in Fig. 3.17.

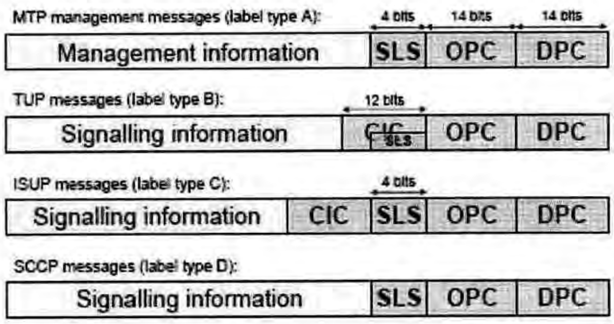


Figure 3.17: MTP routing labels

The **Signalling Link Selection (SLS)** field is used in performing load sharing. This field exists in the same position in all types of messages.
In the case of circuit related messages of the TUP, the field contains the least significant bits of the CIC, and these bits are not repeated elsewhere. In the case of all other User Parts, the SLS is an independent field.

In the case of MTP level 3 messages, the SLS field exactly corresponds to the SLC which indicates the SL between the destination point and originating point to which the message refers.

3.3.3 MTP Level 3

The main purpose of MTP Level 3 is to ensure reliable handling of incoming or outgoing signalling messages sent from one SP – via interconnected SLs – to other SPs. Functions and procedures must also be provided to cope with failures or disturbances in the signalling network. The functions of Level 3 are divided into two major categories:

- Signalling Message Handling,
- Signalling Network Management.

3.4 ISDN User Part

The early telephone network consisted of a pure analog system that connected telephone users directly by a mechanical interconnection of wires. This system was very inefficient, was very prone to breakdown and noise, and did not lend itself easily to long-distance connections. Beginning in the 1960s, the telephone system gradually began converting its internal connections to digital switching system. Today, nearly all voice switching is digital within the telephone network. Still, the final connection from the local exchange to the customer equipment was, and still largely is, an analog Plain-Old Telephone Service (POTS) line.

A standards movement was started by the International Telephone and Telegraph Consultative Committee (CCITT), now known as the International Telecommunications Union (ITU). The ITU is a United Nations organization that coordinates and standardizes international telecommunications. Original recommendations of ISDN were in CCITT Recommendation I.120 (1984), which described some initial guidelines for implementing ISDN. ISDN is an abbreviation of Integrated Service Digital Network. 'Digital network' means that the user is given access to a telecom network ensuring high quality voice connections and high-speed data transmission via digital circuits, while 'integrated services' imply that a whole gamut of facilities can be provided through a single standard telephone socket. These facilities include ISDN telephony, group 4 fax, data transmission between computers with an ISDN card, video telephony and other digital equipment, such as routers, bridges etc. [14].

ISDN transmission takes place via a digital network from one subscriber to another. Various forms of information (such as voice, images, etc.) are transformed into digital signals at the input and are transmitted along digital channels at a speed of 64 kbits/s. ISDN User Part (ISUP) defines the protocol and procedures used to set-up, manage and release trunk circuits that carry voice and data calls over the public switched telephone network. ISUP is used for both ISDN and non-ISDN calls. Calls that originate and terminate at the same switch do not use ISUP signalling.

3.4.1 Message Structure

ISDN User Part messages are carried on the SL by means of MTP MSUs. The SIO field of each MSU containing an ISUP message consists of an integral number of octets and encompasses the following parts (refer to Figure 3.18):

Routing label
Circuit Identification Code (CIC)
Message Type Code
Mandatory Fixed Part
Mandatory Variable Part
Optional Part

Figure 3.18: ISUP message structure

Routing label: The format and codes used for the routing label are described in the MTP standard. For each individual circuit connection, the same routing label must be used for each message that is transmitted for that connection. Signalling information **CIC, SLS, OPC, DPC** are shown in the graph of Figure 3.19.

Signalling information	CIC	SLS	OPC	DPC

Figure 3.19: Routing label

The SLS bits are set to the four least significant bits of the CIC as shown in Figure 3.20. ISUP by doing so ensures the in-sequence delivery of all messages related to a particular connection (refer to the example shown in Figure 3.21).

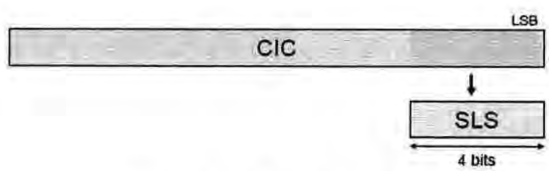


Figure 3.20: CIC and SLS

In the example shown in Figure 3.21, all the messages related to the connection represented by the CIC=0x1010 between exchanges 2-20 and 2-50 are exchanged under normal conditions over the same SLs and LSs.

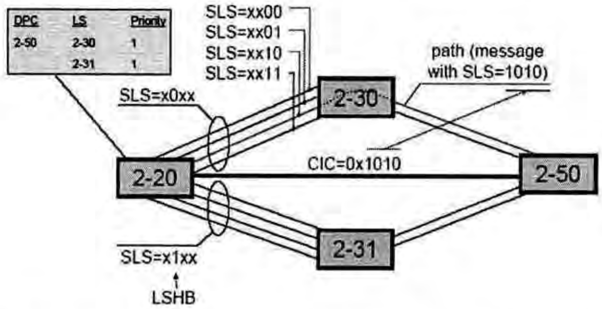


Figure 3.21: Interaction between ISUP and MTP load sharing

Circuit Identification Code: The format of the Circuit Identification Code (CIC) is shown in Figure 3.22.

Bit	8	7	6	5	4	3	2	1
octet 1	CIC (least significant bits)							
octet 2	Spare				CIC (most sig. bits)			

Figure 3.22: Circuit Identity Code (CIC) format

For international applications, the four spare bits of the CIC field are reserved for CIC extension, provided that bilateral agreement is obtained before any increase in size is performed. For national applications, the four spare bits can be used as required.

Message type code: The message type code consists of a one-octet field and is mandatory for all messages. The message type code uniquely defines the function and format of each ISUP message. The message types that are defined for ISUP are shown in Table 3.1.

Table 3.1: ISUP Messages.

ACM	Address complete	COT	Continuity
ANM	Answer	CPG	Call progress
BLA	Blocking ack.	CQM	Circuit group query
BLO	Blocking	CQR	Circuit group query response
CCR	Continuity check request	CRG	Charge information
CFN	Confusion	FAA	Facility accepted
CGB	Circuit group blocking	FAC	Facility
CGBA	Circuit group blocking ack.	FAR	Facility request
CGU	Circuit group unblocking	FRJ	Facility reject
CGUA	Circuit group unblocking ack.	GRA	Circuit group reset ack.
CON	Connect	GRS	Circuit group reset
IAM	Initial address	ROT	Forward transfer
IDR	Identification request	RSC	Reset circuit
INF	Information	SAM	Subsequent address
INR	Information request	SGM	Segmentation
IRS	Identification response	SUS	Suspend
LPA	Loopback ack.	UBA	Unblocking Ack
NRM	Network resource management	UBL	Unblocking
OLM	Overload	UCIC	Unequipped CIC
PAM	Pass along	UPA	User part available
REL	Release	UPT	User part test
RES	Resume	USR	User to user information
RLC	Release complete		

Formatting principles: Each message consists of a number of parameters. Each parameter has a name, which is coded as a single octet. The length of a parameter may be fixed or variable, and a length indicator of one octet for each parameter may be included. The detailed format is uniquely defined for each message type. A general format diagram is shown in Figure 3.23.

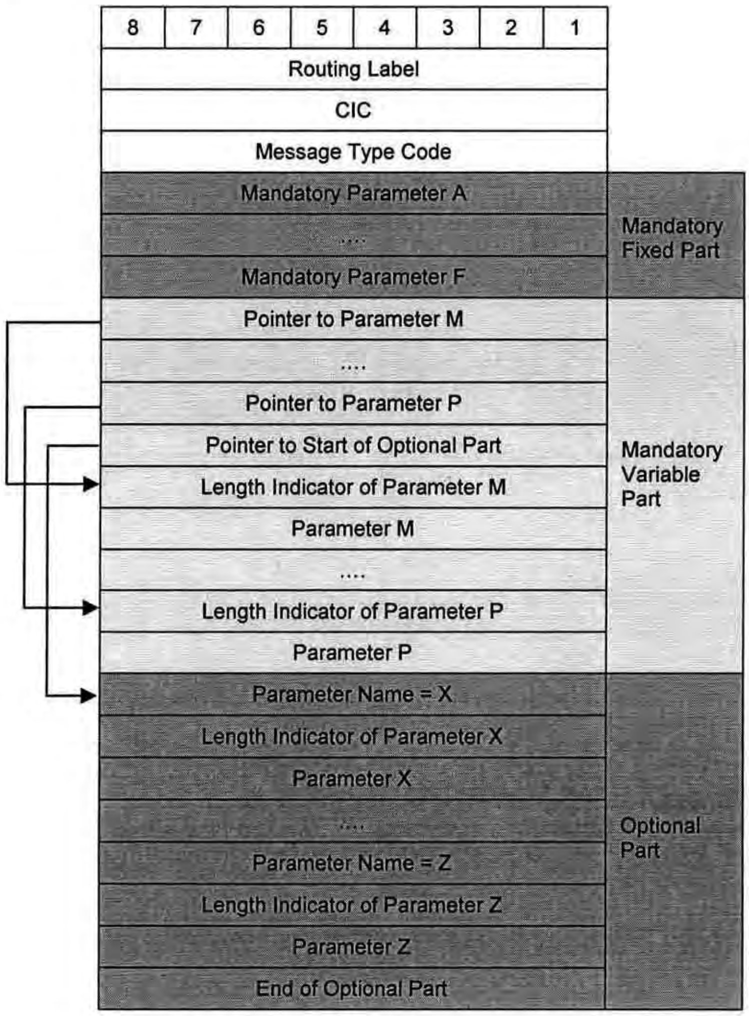


Figure 3.23: General message format.

Mandatory fixed part: Those parameters that are mandatory and of fixed length for a particular message type will be contained in the mandatory fixed part. The position, length and order of the parameters are uniquely defined by the message type, thus the names of the parameters and the length indicators are not included in the message.

Mandatory variable part: Mandatory parameters of variable length will be included in the mandatory variable part. Pointers are used to indicate the beginning of each parameter. Each pointer is encoded as a single octet. The name of each parameter and the order in which the pointers are sent is implicit in the message type. Parameter names are, therefore, not included in the message. The number of parameters, and thus the number of pointers is uniquely defined by the message type.

A pointer is also included to indicate the beginning of the optional part. If the message type indicates that no optional part is allowed, then this pointer will not be present. If the message type indicates that an optional part is possible (reflected by the presence of an 'end of optional parameter', but there is no optional part included in this particular message, then a pointer field containing all zeros is used. All the pointers are sent consecutively at the beginning of the mandatory variable part. Each parameter contains the parameter length indicator followed by the contents of the parameters. If there are no mandatory variable parameters, but optional parameters are possible, the start of optional parameters pointer (coded all '0's if no optional parameter is present and coded '00000001' if any optional parameter is present) is included.

Optional part: The optional part consists of parameters that may or may not occur in any particular message type. Both fixed length and variable length parameters may be included. Optional parameters may be transmitted in any order. Each optional parameter will include the parameter name (one octet) and the length indicator (one octet) followed by the parameter contents.

End of optional parameters octet: If optional parameters are present and after all optional parameters have been sent, an 'end of optional parameters' octet containing all zeros is transmitted. If no optional parameter is present an 'end of optional parameter' octet is not transmitted.

Coding of the length indicator: The length indicator field is binary coded to indicate the number of octets in the parameter content field. The length indicated does not include the parameter name octet or the length indicator octet.

Coding of the pointers: The pointer value (in binary) gives the number of octets between the pointer itself (included) and the first octet (not included) of the parameter associated with that pointer. The pointer value all zeros is used to indicate that, in the case of optional parameters, no optional parameter is present.

3.5 Call set-up

The call setup procedure is described in sections 3.5.1 to 3.5.5 that follow.

3.5.1 IAM and SAM messages

Originating exchange: When the originating gateway exchange has received the complete selection information from the calling party, and has determined that the call is to be routed to another exchange, selection of a suitable, free, inter-exchange circuit takes place and an Initial Address Message (IAM) is sent to the succeeding exchange [14]. This is shown in Figure 3.24.

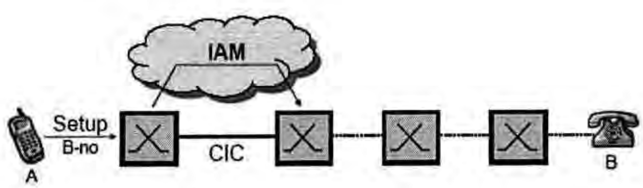


Figure 3.24: Call set-up (originating exchange).

Parameters in IAM: In addition, in the case of a subscriber with digital access, the set-up message contains bearer capability information which is analyzed by the originating exchange to determine the correct transmission medium requirement and network signalling capability (ISDN user part preference indicator). The bearer capability information will be mapped into the user service information parameter of the IAM.

The information used to determine the routing of the call by the originating exchange will be included in the IAM (as transmission medium requirement and forward call indicators) to enable correct routing at intermediate exchanges. The IAM service information is shown in Figure 3.25.

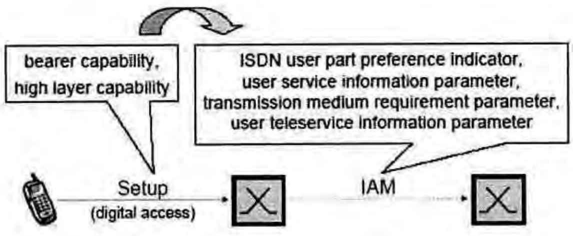


Figure 3.25: IAM – service information.

The IAM in principle contains all the information that is required to route the call to the destination exchange and connect the call to the called party. The following values are used in the forward call indicators parameter field:

• National/international call indicator:

o call to be treated as a national call.

o call to be treated as an international call.

• Interworking indicator:

o no interworking encountered (No.7 signalling all the way).

o interworking encountered.

• ISDN user part indicator:

o ISDN user part not used all the way.

o ISDN user part used all the way.

• ISDN user part preference indicator:

o ISDN user part preferred all the way.

o ISDN user part not required all the way.

o ISDN user part required all the way.

• ISDN access indicator:

o originating access non-ISDN.

o originating access ISDN.

National/international call indicator can be set to any value in the country of origin. In the international network this bit is not checked. In the destination country, calls from the international network will have this bit set to 1. The national / international call indicator is shown in Figure 3.26.

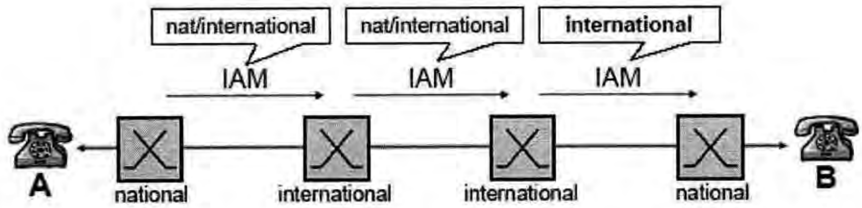


Figure 3.26: National/international call indicator.

The ISDN-User Part preference indicator is set according to the bearer service, teleservice and supplementary service(s) requested. The exact setting depends on the service demand conditions and may differ on individual cases. In principle, if the service demand requires ISDN-User Part to be essential then the indicator is set to 'required', if the service required is optional but preferred it is set to 'preferred', otherwise it is set to 'not required'. The indicator is set to either 'required' or 'preferred', or 'not required', according to the most stringent condition required by one or more of the parameters in the initial address message. The transmission medium requirement parameter contains the connection type required information. The following values are used in transmission medium requirement parameter:

- speech,
- 3.1 kHz audio,
- 64 kbit/s unrestricted,
- 64 kbit/s unrestricted preferred,
- 2 × 64 kbit/s unrestricted (multirate connection type),
- 384 kbit/s unrestricted (multirate connection type),
- 1536 kbit/s unrestricted (multirate connection type),
- 1920 kbit/s unrestricted (multirate connection type).

Within a network if the intermediate exchange does not route the call using just the connection type specified in the transmission medium requirement parameter, the exchange may also examine the user service information containing the bearer capability information and/or the user tele-service information containing the high layer capability information, if available, to determine if a suitable route can be selected. In this case if a new connection type is provided the transmission medium requirement parameter is modified to the new connection type. The parameters within an IAM are shown in Figure 3.27 and those in the IAM message are shown in the example of Figure 3.28 [14].

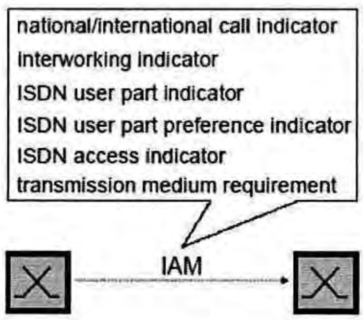


Figure 3.27: Some parameters in IAM.

----0101 Service Indicator	ISDN User Part
--00---- Sub-Service: Priority	Spare/priority 0 (U.S.A. only)
11------ Sub-Service: Network Ind	National message 1
******** Destination Point Code	9472
******** Originating Point Code	2049
******** Signalling Link Selection	3
******** Circuit Ident Code	3 (PCM: 0 Channel:3)
0000---- Spare	
00000001 Message Type	0x1 (IAM)
------00 Satellite Indicator	No satellite circuit
----00-- Continuity Chk Indicator	Cont Check not required
---0---- Echo Control Device Ind	O/G half echo ctrl not incl
000----- Spare	
-------0 Nat./Internat. Indicator	Treat as a national call
-----00- End-to-End Method Ind	No end-to-end method available
----1--- Interworking Indicator	Interworking encountered
---0---- End/End Information Ind	No end-to-end info available
--0----- ISDN User Part Indicator	ISDN-UP not used all the way
01------ ISDN-UP Preference Ind	ISDN-UP not reqd all the way
-------0 ISDN Access Indicator	Originating access non-ISDN
-----00- SCCP Method Indicator	No indication
Called party number	
00001000 Parameter Length	8
-0000011 Nature of Address	National (significant) number
1------- Odd/Even Indicator	Odd number of address signals
----0000 Spare -001---- Numbering Plan Indicator	ISDN Nr.plan (E.164)
1------- Internal Network No. Ind	Routing to INN not allowed
******** Called Address Signals	1725179741F
0000---- Filler	
Propagation delay counter	
00110001 Parameter Name	Propagation delay counter
00000010 Parameter Length	2
******** Propagation delay value	0
Parameter compatibility inform	
00111001 Parameter Name	Parameter compatibility
00000010 Parameter Length	2
00110001 1st upgraded parameter	49

Figure 3.28: Examples of IAM message.

The sending sequence of address information on international calls will be the country code followed by the national (significant) number. On national connections, the address information may be the subscriber number or the national (significant) number as required by the administration concerned. The end-of-pulsing (Sending Finished - ST) signal is used whenever the originating exchange is in a position to know by digit analysis that the final digit has been sent. The end of pulsing signal is shown in Figure 3.29.

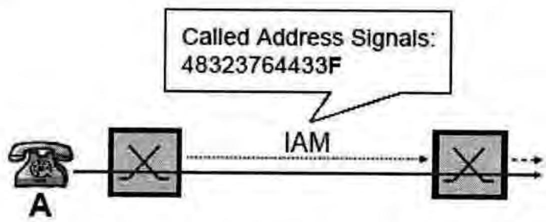


Figure 3.29: End-of-pulsing signal.

The nature of connection indicators are set appropriately based on the characteristics of the selected outgoing circuit. The originating exchange may also include in the IAM:

• a call reference (including the point code of the originating exchange) to enable the destination exchange to establish an end-to-end connection,

• the calling party number if this is to be passed forward without being requested,

• other information related to supplementary services and network utilities.

A list of the messages has already been shown in Table 3.1.

SAM message: In the *overlap* call set-up all the digits are not sent in IAM. The remaining digits are sent in Subsequent Address Messages (SAM). This can make a call set-up faster, for example, when, due to interworking, dialed digits are delivered slowly, but the first digits are sufficient for the intermediate exchange to route the call.

The remaining digits of the number may be sent in SAMs containing one or several digits as they are received. Efficiency can be gained by grouping together as many digits as possible. However, to prevent an increase in post sending delay in those cases where overlap operation with subscribers' dialing is used, it may be desirable to send the last few digits individually. If the number of digits in the called party number received by the intermediate exchange is not sufficient to route the call, the routing will be carried out when the intermediate exchange has received additional digits in SAM(s).

Any address digits received in SAM(s) during the circuit selection process may be included in this IAM. Any SAM(s) received after the IAM has been sent, are forwarded to the succeeding exchange as SAM(s).

In case of the outgoing international exchange, all digits required for routing the call through the international network are sent in the IAM. On calls with a country code in the number, the IAM contains a minimum of 4 digits and should contain as many digits as are available. The SAM message is shown Figure 3.30.

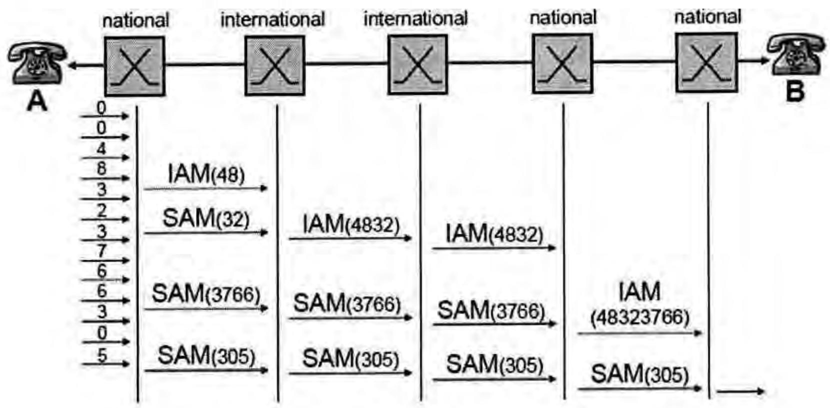


Figure 3.30: SAM message.

3.5.2 ACM and CON message

Before going to describe the ACM and CON messages, the following two terms will be explained first.

Destination exchange: An ACM will be sent from the destination exchange as soon as it has been determined that the complete called party number has been received, or an indication received from the called party that an inband tone is being connected. However, there is no direct mapping from alerting, received from the access signalling system, to ACM in the network. In the case where the continuity check is performed, the destination exchange will withhold sending the address complete message until a successful continuity indication has been received.

Terminating Access for non-ISDN: In the case where the terminating access is non-ISDN, the following action takes place at the destination exchange:

• In all cases an ACM is sent as soon as it has been determined that the complete called party number has been received, and the destination exchange established that the called subscriber is free. Indicators in the address complete message will be set to indicate:

o called line status: 'Subscriber free'

o ISDN access indicator: 'Non ISDN'

• In the case of a PBX, an ACM is sent as soon as it has been determined that the called party number has been received. Indicators in the ACM will be set to indicate:

o called line status: 'No indication'

o ISDN access indicator: 'Non-ISDN'

The ACM message flow for non-ISDN termination is shown in Figure 3.31.

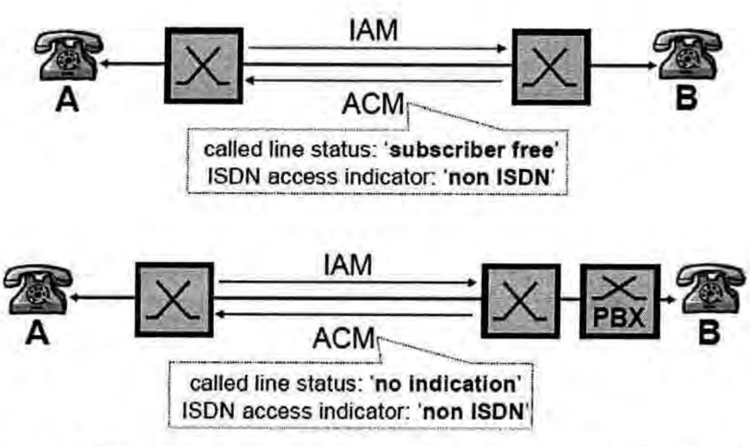


Figure 3.31: ACM message (non ISDN terminating access).

Terminating Access ISDN: In the case where the terminating access is ISDN, the following conditions can apply:

• If an indication that the address is complete or no status indication has been received from the ISDN access prior to the destination exchange determining that the complete called party number has been received, the indicators in the ACM will be set as follows:

o called line status: 'No indication'

o ISDN access indicator: 'ISDN'

In that case the indication that the destination user is being alerted is transferred in a CPG.

• The destination exchange concludes from the receipt of an indication from the ISDN access that the complete called party number has been received. In this case the indicators in the ACM will be set as follows:

o called line status: 'Subscriber free',

o ISDN access indicator: 'ISDN'.

The ACM message flow for an ISDN termination is shown in Figure 3.32.

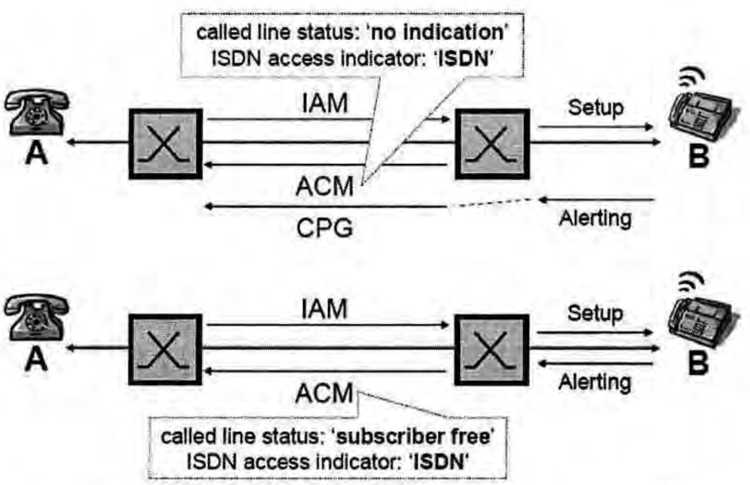


Figure 3.32: ACM message (terminating access ISDN)

If a connect indication is received from the ISDN access under the following conditions:

• no alerting indication received from the ISDN access; and
• an ACM has not yet been sent by the destination exchange,
• a CON message is sent by the destination exchange. This CON message signifies both address complete and answer conditions. Indicators in the CON will indicate:

• called line status: 'Subscriber free',

• ISDN access indicator: 'ISDN'.

The destination exchange will through-connect before the connect message is sent. The CON message flow for an ISDN Termination is shown in Figure 3.33.

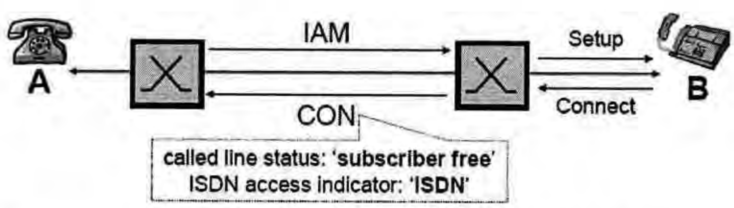


Figure 3.33: CON message (terminating access ISDN).

Ring tone: The sending of the awaiting answer indication (e.g. ring tone) at the destination exchange depends on the type of call. On speech and 3.1 kHz calls and call to an analog called party, the awaiting answer indication is applied to the transmission path to the calling party from the destination exchange on receipt of an alerting indication from the called party or from information contained within the destination exchange that the called party will not or is prohibited from providing in-band tone.

Regardless of whether tones are to be provided or not, the destination exchange will through-connect after the reception of the connection indication from the called party and before sending the ANM/CON message to the preceding exchange.

If the destination exchange does not send the awaiting answer indication because the destination user provides for the sending of tones, then the destination exchange will through-connect the transmission path in the backward direction on receipt of the progress indication. The ring tone flow is shown in Figure 3.34.

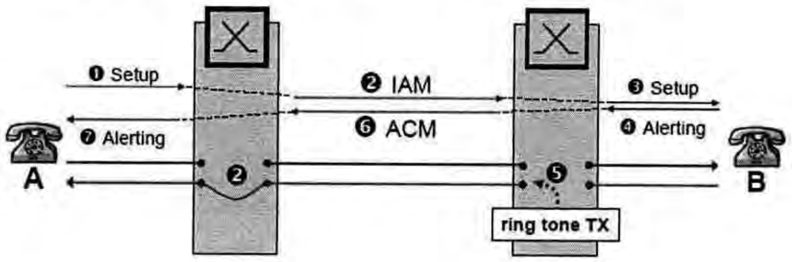


Figure 3.34: Ring tone

3.5.3 CPG message

The CPG message is sent (only after the ACM) from an exchange in the backward direction indicating that an event has occurred during call set-up which should be relayed to the calling party [14].

3.5.4 ANM message

When the called party answers, the destination exchange connects through the transmission path and the ringing tone is removed if applicable. An ANM to the preceding exchange is sent. If the destination exchange is the exchange controlling charging, then charging may begin.

When connections are set-up to terminals having an automatic answer feature, the alerting indication may not be received from the called party. If a destination exchange receives an answer indication, an ANM is sent provided that an ACM has been sent, otherwise the CON message is sent.

Upon receipt of an ANM, an intermediate exchange sends the corresponding ANM to the preceding exchange and, if this is the exchange controlling charging, charging may begin, and timer (T9) is stopped.

When the originating exchange receives an ANM indicating the required connection has been completed, the transmission path is connected-through in the forward direction, if not already connected. The awaiting answer timer (T9) is stopped. If the originating exchange is the exchange controlling charging, charging may begin if applicable. The calling party is informed. The message flow for a successful call setup is shown in Figure 3.35 for a non-blocking method.

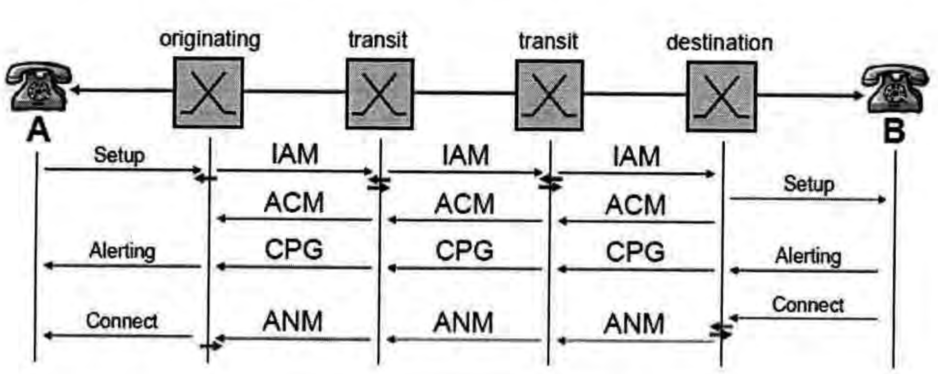


Figure 3.35: Successful call set-up (non blocking method)

The message flow for a successful call setup when overlaps of messages occur is shown in Figure 3.36.

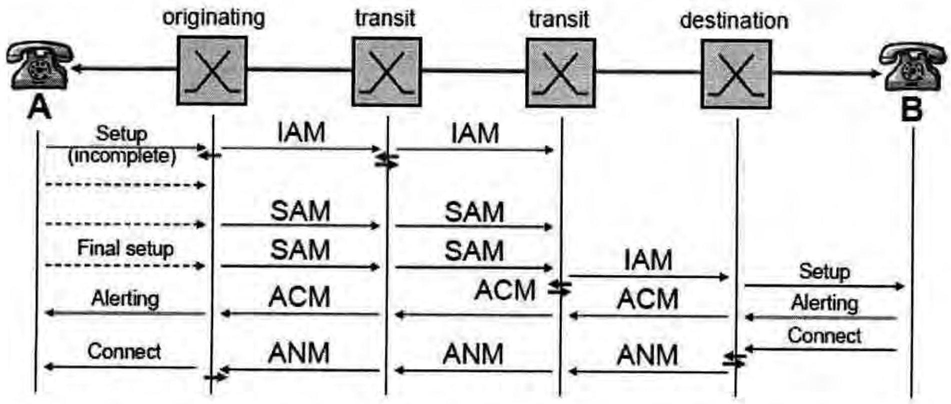


Figure 3.36: Successful call set-up (overlap method)

3.5.5 Unsuccessful call set-up

If at any time in the call set-up the connection cannot be completed, the exchange will (if applicable):

• return an indication (in band or out band) to the calling party; or

• attempt to re-route the call set-up; or

• initiate release procedures to the preceding and/or succeeding exchange.

Exchange initiating a REL message: The initiating exchange immediately starts the release of the switched path (if established). The exchange sends a REL message to the preceding and/or succeeding exchange and timers T1 and T5 are started to ensure that an RLC is received from the preceding and/or succeeding exchange. If a release complete message is not received in response to a release message before expiry of timer (T1), the exchange will retransmit the REL. On transmitting the initial REL message, a 5-15 minute timer (T5) is started. If no release complete message is received on the expiry of this timer (T5), the exchange:

• send a RSC (Reset Circuit) message;

• alert the maintenance system;

• remove the circuit from service;

• continue the sending of the RSC message at 5-15 minute intervals until maintenance action occurs.

Procedure of unsuccessful call set-up, where the destination exchange before sending ACM makes a decision to release the connection and the originating exchange plays the tone/announcement toward the calling subscriber, is presented in Figure 3.37.

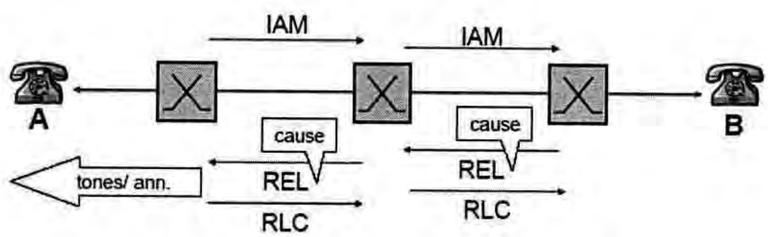


Figure 3.37: Unsuccessful set-up

3.5.6 Normal call release

The release procedures are based on a two message (REL, RLC) approach where by the REL message initiates release of the circuit switched connection. The same procedures are used in the network irrespective of whether they are initiated by the calling party, the called party or the network.

3.6 Signalling Connection Control Part (SCCP)

SCCP supports the non-call related signalling in a telephony networks. The non-call related signalling is mainly used in the mobile networks where a significant signalling load is generated by mobility management functions that keep track of the subscriber location within the network. The location updating, supplementary services activation/ deactivation, intelligent network invocation are the examples of the call non-related signalling [15]. In addition, SCCP supports two modes of operation, namely connection oriented and connection less. SCCP provides transport layer services for the upper layer protocols: TCAP, BSSAP and ISUP (refer to Figure 3.38).

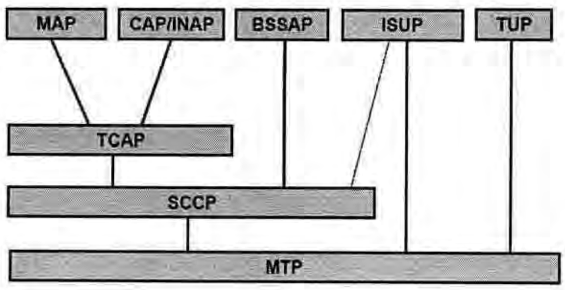


Figure 3.38: SS7 protocol stack

BSSAP – Base Station System Application Part is used in GSM for communication between BSS and CSS (A interface).

CAP (CAMEL Application Part) and **INAP** (Intelligent Network Application Part) are protocols used for signalling concerning IN (Intelligent Network) and MIN (Mobile IN) services.

MAP (Mobile Application Part) is used for communication between all nodes within GSM CSS for example during mobile terminating call set-up when GMSC is asking HLR where to route the call or during location updating when HLR sends all the data about subscriber to the new MSC/VLR.

TCAP (Transaction Capabilities Application Part) makes it possible to run simultaneous dialogues concerning different processes or subscribers between signalling nodes.

3.7 SS7 over IP

SIGTRAN stands for Signalling Transport and it is a new set of standards defined by the *International Engineering Task Force (IETF)*. This set of protocols has been defined in order to provide the architectural model of signalling transport over IP networks [16].

The communication industry is going through a period of explosive change that is both enabling and driving the convergence of services. Data is becoming more significant as a proportion of traffic compared to voice. Operators are seeking ways to consolidate voice and data traffic, platforms and services in order to reduce the operational, maintenance, and initial cost of the network. With the number of technological solutions to choose from, Internet Protocol (IP) is now considered the most promising media on which to build the new integrated services. There is an on-going integration of circuit switched networks and IP networks. Fixed and mobile telephone network operators are designing all-IP architecture, which includes support for *Signalling System No.7 (SS7)* protocols. IP provides an effective way to transport user data and for operators to expand their networks and build new services. Mass popularization of communication services, including Short Message Service (SMS) contribute to the rapid growth of signalling networks. As such, more scalable and flexible networks, such as the Internet and its technologies, are needed. The benefits of using an IP network in comparison to a legacy Time Division Multiplex (TDM)-based network include:

• **Ease of deployment** – When using Signalling Gateways (SG), there is no need to disrupt the existing SS7 network, and future enhancements are transparent.

• **Less costly equipment** – There is no need for further expensive investments in the legacy signalling elements.

• **Better efficiency** – SIGTRAN over an IP network does not require the physical E1/T1 over Synchronous Digital Hierarchy (SDH) rings. Using new technologies like IP over SDH and IP over fibre, for instance, can achieve much higher throughput.

• **Higher bandwidth** – SIGTRAN information over IP does not constrains to link capacity as it does in SS7 network. The IP network is much more flexible than the TDM-based legacy network.

• **Enhanced Services** – Implementing a core IP network facilities a variety of new solutions and Value-Added Services (VAD).

A sample implementation scheme for SS7 over IP is shown in Figure 3.39 [16].

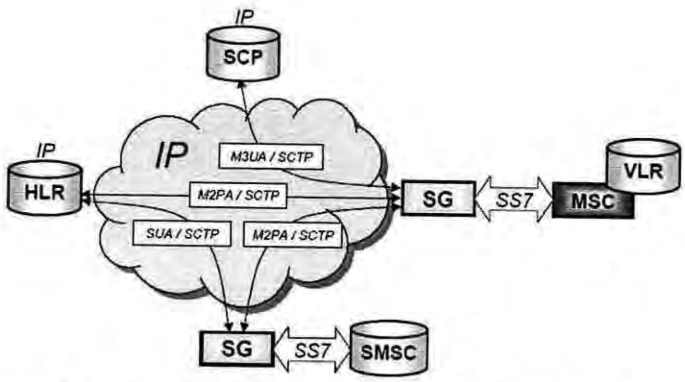


Figure 3.39: Sample implementation scheme for SS7 over IP

Figure 3.39 depicts the diversity of solutions achieved by using signalling transport protocols. Using SIGTRAN protocols such as an MTP3 User Adaptation (M3UA) and an SCCP User Adaptation (SUA), the application vendor (i.e. Short Message Service Centre – SMSC, IP Home Location Register – IP-HLR, and so on) only has to develop the application layer and does not have to deal with the complex SS7 interfaces. By making the network introduction complexity and integration problem much shorter, the time for marketing these new applications will be much faster. SS7 over IP also solves throughput limitations that were inherited from the SS7 standards, thus allowing high-end machines like SMSC, HLR, and so on to be able to support SS7 traffic needs. By using Signalling Gateways, both legacy and new equipment can seamlessly continue to operate over high bandwidth, scalable and available IP-based core network, instead of burdening the TDM-based legacy SS7 network.

Stream Control Transmission Protocol SCTP: To reliably transport SS7 messages over IP networks, the Internet Engineering Task force SIGTRAN working group devised the Stream Control Transmission Protocol (SCTP). SCTP allows the reliable transfer of signalling messages between signalling endpoints in an IP network.

To establish an **association** between SCTP endpoints, one endpoint provides the other endpoint with a list of its transport addresses (multiple IP addresses in combination with an SCTP port). These transport addresses identify the addresses that will send and receive SCTP packets. IP signalling traffic is usually composed of many independent message sequences between many different signalling endpoints. SCTP allows signalling messages to be independently ordered within multiple streams (unidirectional logical channels established from one SCTP endpoint to another) to ensure in-sequence delivery between associated endpoints. By transferring independent message sequences in separate SCTP streams, it is less likely that the retransmission of a lost message will affect the timely delivery of other messages in unrelated sequences (called **head-of-line blocking**). Because TCP/IP does enforce head-of-line blocking, the SIGTRAN Working Group recommends SCTP rather than TCP/IP for the transmission of signalling messages over IP networks.

User adaptation layers: SCTP was introduced about two years ago and it is not widely known yet. However in any case, there exist already some applications that use SCTP as their transport protocol. Most of them are, however, new protocols related with telephony signalling transport, which was the initial field for which SCTP was designed [17].

3.7.1 SIGTRAN protocol stack

The SIGTRAN suite [18, 19] (including SCTP and all the *User Adaptation (UA)* layers) is shown in Figure 3.40.

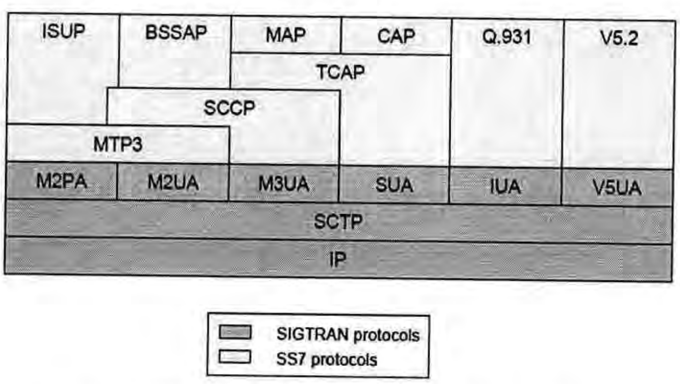


Figure3.40: SIGTRAN protocol suite

The *User Adaptation (UA)* layers are named according to the service they replace, rather than the user of that service. For example, M3UA adapts SCTP to provide the services of MTP3, rather then providing a service to MTP3. The SIGTRAN adaptation layers all serve a number of common purposes:

• To carry upper layer signalling protocols over a reliable IP-based transport,

• To provide the same class of service offered at the interface of the SS7 equivalent. For example, M3UA must provide the same look and feel to its users as MTP3 in terms of services, at least (M3UA does not actually replace the features and operations of MTP3).

• To be transparent. The user of the service should be unaware that the adaptation layer has replaced the original protocol (although this is largely dependent on the implementation).

• To remove as much need for the lower SS7 layers as possible. SIGTRAN currently defines six adaptation layers, as follows:

• ***V5.2 User Adaptation (V5UA)*** provides the services of the *V.5.2 protocol.*

• ***ISDN User Adaptation (IUA)*** provides the services of the *ISDN Data Link layer (LAPD)*. Its user would be an ISDN layer 3 (*Q.931*) entities.

• ***MTP2 User Adaptation (M2UA)*** provides the services of MTP2 in a client-server situation, such as SG to MGC. Its user would be MTP3.

• ***MTP2 Peer-to-Peer Adaptation (M2PA)*** provides the services of MTP2 in a peer-to-peer situation, such as SG-to-SG connections. Its user would be MTP3.

• ***MTP3 User Adaptation (M3UA)*** provides the services of MTP3 in both a client-server (SG to MGC) and peer-to-peer architecture. Its users would be SCCP and/or ISUP.

• ***SCCP User Adaptation (SUA)*** provides the services of SCCP in a peer-to-peer architecture. Its user would be TCAP, or another transaction-based application part. Each UA has a particular applicability, which is discussed in the following sections.

ISDN – User Adaptation (IUA): *ISDN User Adaptation (IUA),* officially known as is ***ISDN Q.921-User Adaptation Layer,*** is described in RFC 3057. Q.921 defines the data link level protocol used in ISDN subscriber loop signalling, also known as the ***Link Access Procedures on the D-channel (LAPD)***, which is used on *U interface* between Network Termination 1 (NT1) and Local Exchange (LE). The U interface between the two is shown in Figure 3.41.

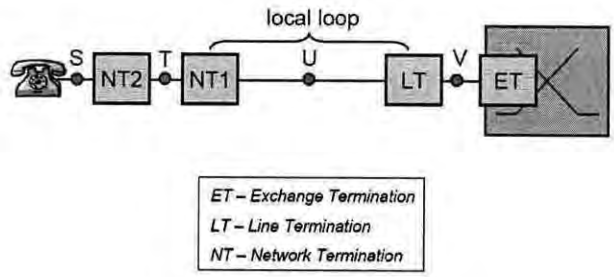


Figure 3.41: U interface

SIGTRAN *ISDN User Adaptation (IUA) Layer* provides functionality to transport ISDN signals from circuit-switched network to IP network by backhauling the *Q.921 user messages* over SCTP. IUA supports both ISDN *Primary Rate access (PRA)* as well as *Basic Rate Access (BRA)* including the support for both point-to-point and point-to-multi-point modes of communication. *IUA* enables carriers to exchange the signalling information ISDN networks systems to VoIP networks, providing smooth transition of new converged IP telephony services. ISDN signals are terminated at the *Signalling Gateway (SG)* from where the *IUA* transports signalling information from *Q.921* to the *Q.921 user* (typically *Q.931*) at the *Media Gateway Controller (MGC). IUA* provides same set of services as *Q.921* to the user at the *MGC*. The backhauling of signals is completely transparent to the *Q.921* user and it runs as it would be running directly over *Q.921*. The ISDN user adaptation is shown in Figure 3.42.

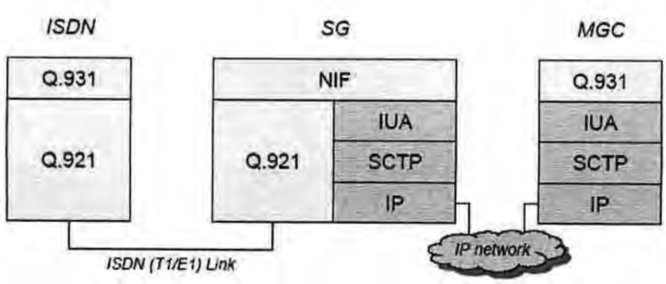


Figure 3.42: ISDN User Adaptation (IUA)

The possible application scenario is shown in Figure 3.43. Thanks to *IUA* protocol, that it is now possible to attach standard ISDN user equipment as PBX to VoIP network.

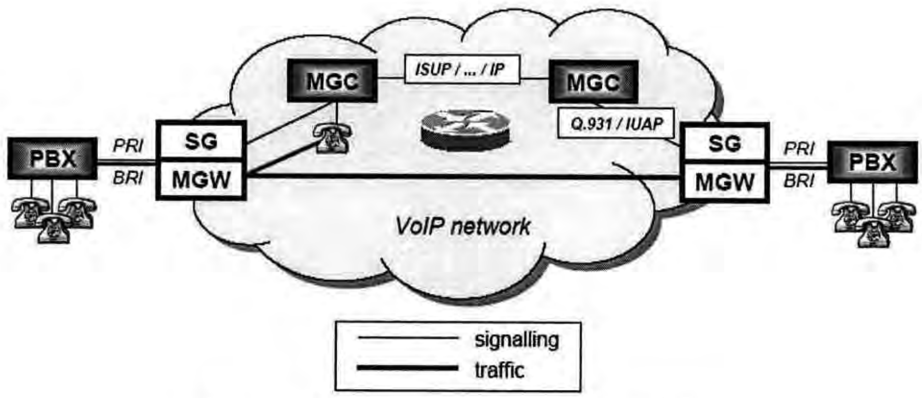


Figure 3.43: Integrated network (IUA)

MTP2 – User Adaptation Layer (M2UA): *M2UA* is used to transfer *MTP2 user data* between the *MTP2* instance on a SG and the *MTP3* instance on an MGC. As such, it operates a **client-server model**, where the MGC is the client and the SG is the server. *M2UA* provides a means by which an MTP2 service may be provided on an MGC. In essence, extending SS7 into the IP network. In a Signalling Gateway, the SS7 signalling is received over a standard SS7 network termination, using the *SS7 Message Transfer Part (MTP)* to provide transport of SS7 signalling messages to and from an SS7 Signalling End Point (SEP) or *SS7 Signalling Transfer Point (STP)*. In other words, the SG acts as a *Signalling Link Terminal (SLT)*. The SG then provides an interworking of transport functions with IP Signalling Transport, in order to transport the *MTP3* signalling messages to the MGC where the peer *MTP3* protocol layer exists, as shown in Figure 3.44.

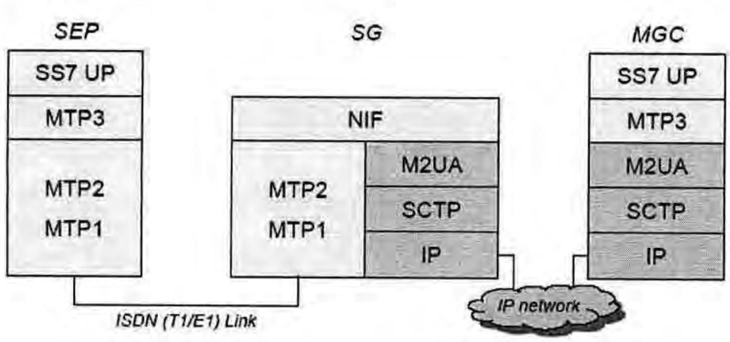


Figure 3.44: MTP2 User Adaptation (M2UA)

Effectively, the *MTP3* instance on the MGC is the user of the *MTP2* instance on the SG. Neither *MTP2* nor *MTP3* are aware that they are remote from one another. This process, by which signalling messages are passed over IP from the top of one SS7 layer to the bottom of another, is described as backhauling. The MTP3 user at the MGC would usually be ISUP. This architecture is most applicable in the following circumstances where,

• there is a low density of SS7 links at a particular physical point in the network.
• there are a large number of physically separate SG functions (due to the SS7 links being physically located remotely from each other).
• the SG function is co-located with an MGW (usually due to one or more of the previous conditions).

The example of an integrated network is shown in Figure 3.45. In this case, it makes sense to host *MTP3* in the MGC. The SS7 address (the Point Code) of the system resides with *MTP3*. If each SG had its own *MTP3 layer*, a large number of Point Codes would be required to implement a (logically) single gateway. This particular SIGTRAN configuration is likely to be common in European networks, where the SS7 signalling links share the physical medium with voice circuits.

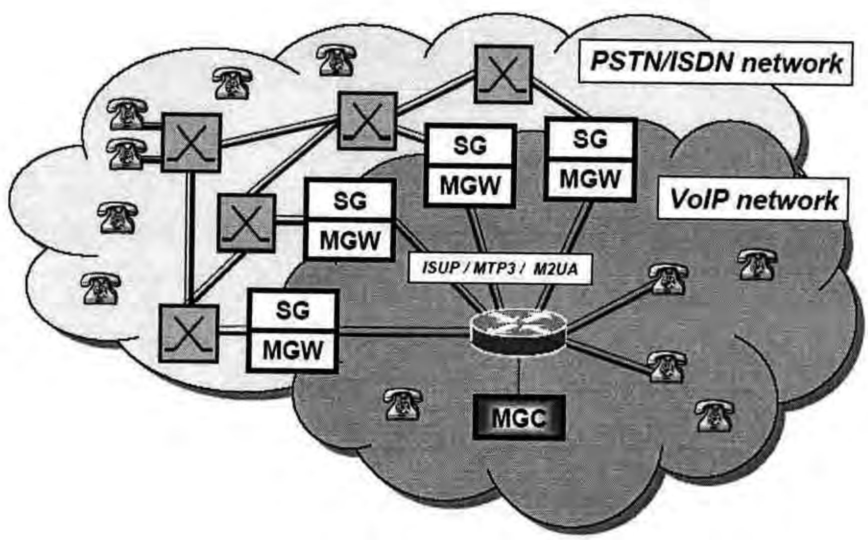


Figure 3.45: Integrated network (M2UA)

At the SG side, the depiction of *M2UA* at the peer level to *MTP2* is slightly misleading. *M2UA* is, in many ways, a user of *MTP2*. The specification defines that

M2UA is responsible for initiating protocol actions, which would normally be issued by MTP3, such as:

• link activation and deactivation,
• sequence number requests,
• MTP2 transmit/retransmit buffer updating procedures,
• buffer flushing.

These are implementation issues, however. Such functionality could well reside within the *Nodal Interworking Function (NIF)*. M2UA Protocol is described in *RFC 3331*.

MTP2 – User Peer-to-Peer Adaptation Layer (M2PA): *M2PA* is the **peer-to-peer** equivalent of *M2UA*. Rather than just providing a link between remotely located *MTP2* and *MTP3* instances; it replaces an *MTP2* link beneath *MTP3*. The user of *M2PA* is *MTP3* at both ends of the connection (with *M2UA*, one user is *MTP3* and the other is an SG *NIF*). *M2PA* provides a means for peer *MTP3* layers in SGs to communicate directly. In essence, it extends the reach of SS7 over the IP network. The architecture of M2PA is shown in Figure 3.46.

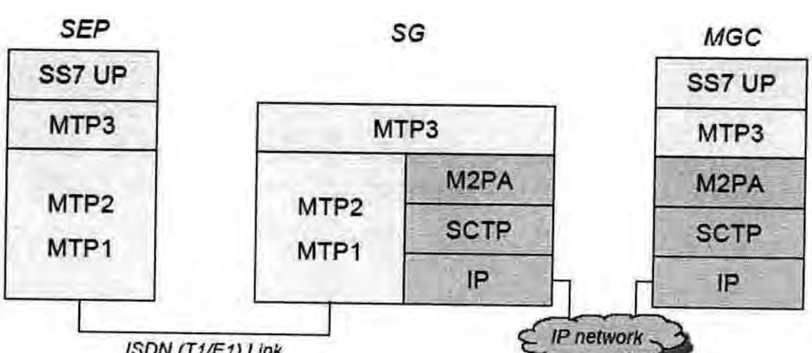


Figure 3.46: MTP2 User Peer-to-Peer Adaptation Layer

The *M2PA* can also be used to transfer SS7 messages between two IP Server Processes (IPSP). The SCTP association acts as one SS7 link between the IPSPs, (refer to Figure 3.47). An IPSP may have the *Signalling Connection Control Part (SCCP)* and other SS7 layers above *MTP3*.

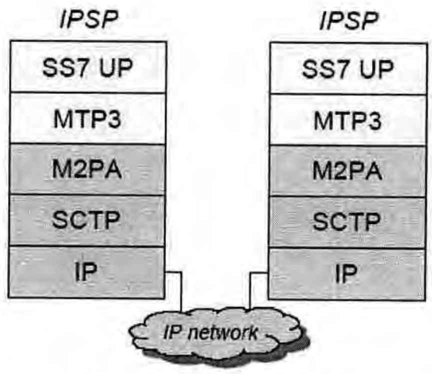


Figure 3.47: M2PA Symmetrical Peer-to-Peer Architecture.

This architecture is most applicable for an SG to SG connection, used to bridge two SS7 network "islands". In this case, each SG may connect to multiple other SGs, none of which need to know about the upper layer that they are supporting. The integrated network using SS7 Ups and M2PA is shown in Figure 3.48 [16].

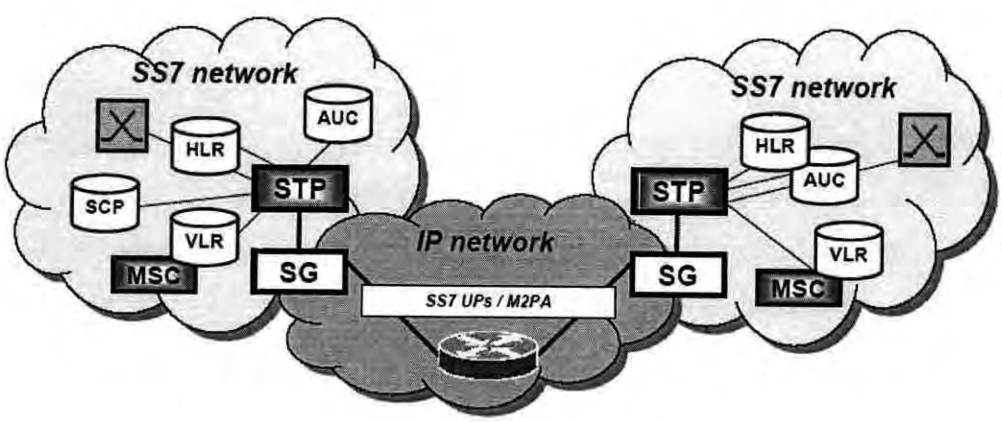


Figure 3.48: Integrated Network (M2PA).

MTP3 is present on each SG, to provide routing and management of the *MTP2/M2PA links*. Because of the presence of *MTP3*, each SG would require its own *SS7 Point Code*. The significant difference in function from *M2UA* is that *M2PA* actually provides an *MTP2 - like service* itself. *M2UA* merely provides an interface to a *remote MTP2 service*. This means that *M2PA* is responsible for:

- link activation/deactivation (in response to requests from *MTP3*),
- maintaining link status information,

• maintaining sequence numbers and re-transmit buffers, for retrieval by *MTP3*,
• maintaining local and remote processor outage status.

M2PA protocol is described in Internet draft *m2pa*. The brief comparison of MTP2 Adaptation Layers is presented in Figure 3.49.

	M2PA	M2UA
MTP3 messages	transports MTP3 messages	transports MTP3 messages
SAP to MTP3	presents an MTP2 SAP to MTP3	presents an MTP2 SAP to MTP3
Primitives	IPSP processes MTP3-to-MTP2 primitives	IPSP sends MTP3-to-MTP2 primitives to SG for processing
Types of links	SG to IPSP connection is an SS7 link	SG to IPSP connection is not an SS7 link; it is an extension of MTP2 to a remote node
Point Codes	SG is an SS7 node with an SPC	SG is not an SS7 node and has no SPC
SS7 upper layers	SG can have upper SS7 layers, e.g. SCCP	SG has no upper SS7 layers because it has no MTP3
Management	relies on MTP3 for management procedures	uses M2UA management procedures

Figure 3.49: M2PA, M2UA – comparison [16].

MTP3 – User Adaptation Layer (M3UA): The *M3UA Layer* at an *Application Server Process (ASP)* or *IPSP* provides the equivalent set of primitives at its upper layer to the *MTP3-users* as provided by the *MTP Level 3* to its local *MTP3-users* at an SS7 SEP. In this way, the *ISUP* and/or *SCCP* layer at an ASP or IPSP is unaware that the expected *MTP3* services are offered remotely from an *MTP3 layer* at an SG, and not by a local *MTP3 layer*. The *MTP3 layer* at an SG may also be unaware that its local users are actually **remote user parts** over *M3UA*. In effect, the *M3UA* extends access to the *MTP3 layer* services to a remote IP-based application. The *M3UA layer* does not itself provide the *MTP3 services*. However, in the case where an ASP is connected to more than one SG, the *M3UA layer* at an ASP should maintain the status of configured SS7 destinations and route messages according to the availability and congestion status of the routes to these destinations via each SG. The interconnection of MTP3 user adaptation layers is shown in Figure 3.50.

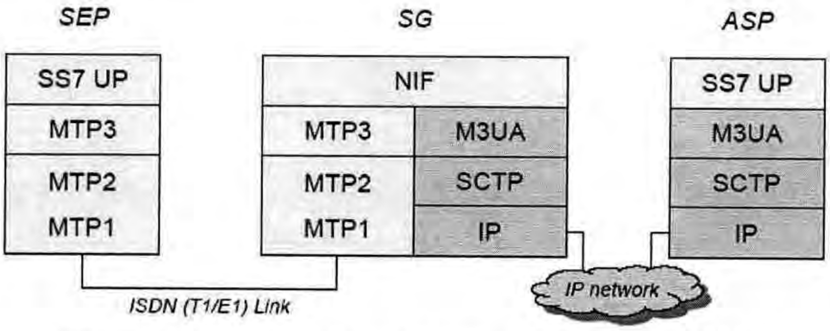


Figure 3.50: MTP3 User Adaptation Layer (M3UA).

The SG has a local *MTP3* instance and therefore must have its own SS7 Point Code. Application Servers can be represented under the same Point Code of the SG, their own individual Point Codes or grouped with other Application Servers for Point Code preservation purposes. A single Point Code may be used to represent the SG and all the Application Servers together, if desired. This architecture is most appropriate in the following circumstances where,

- there is a high enough density of SS7 links to make a standalone SG viable.
- the SS7 links are physically accessible at a single point.

These conditions are common in North American networks, where the SS7 links are physically separate from the voice circuits. In this case, a number of links are gathered together into a single physical medium (such as a T1 line). The integrated network with PSTN/ISDN and VOIP is shown in Figure 3.51.

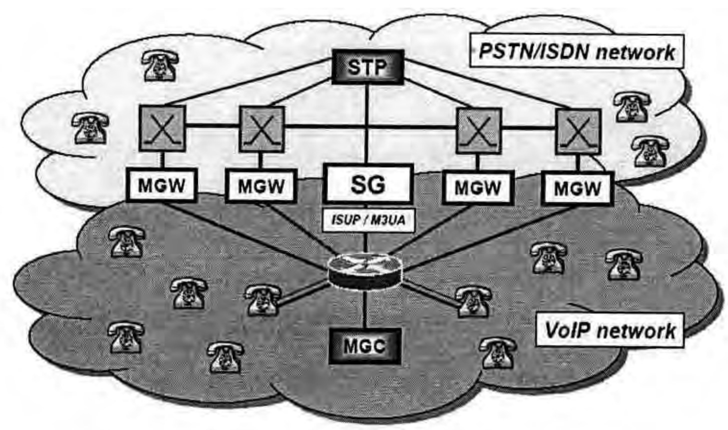


Figure 3.51: Integrated Network (M3UA).

The *M3UA layer* may also be used for point-to-point signalling between two *IP Server Processes (IPSPs)*. In this case, the *M3UA layer* provides the same set of primitives and services at its upper layer as the *MTP3*. However, in this case the expected *MTP3 services* are **not offered remotely** from an SG. The *MTP3 services* are provided but the procedures to support these services are a subset of the *MTP3 procedures* due to the simplified point-to-point nature of the IPSP-to-IPSP relationship (refer to Figure 3.52)

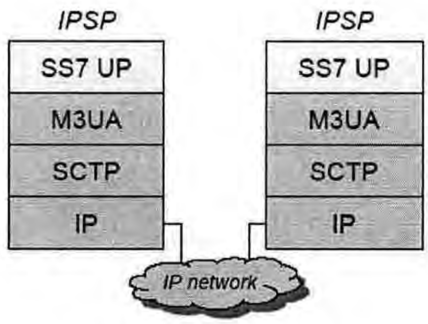


Figure 3.52: M3UA between two IPSP.

M3UA is the solution chosen by major GSM/UMTS equipment vendors for Core Network signalling . This is because *M3UA* can transport *ISUP, BICC* protocols and application layer protocols that run over *SCCP* and *TCAP* (as *MAP*, *CAP* and *INAP*), between two IPSPs as well as between IPSP and SG. *M3UA* requires standard SCCP layer to enable *MAP* communication, thus the implementation of GSM/UMTS database or IN nodes (e.g. HLR, EIR, SCP) by IP/datacom equipment vendors is more difficult. The M3UA in GSM/UMTS core network is shown in Figure 3.35.

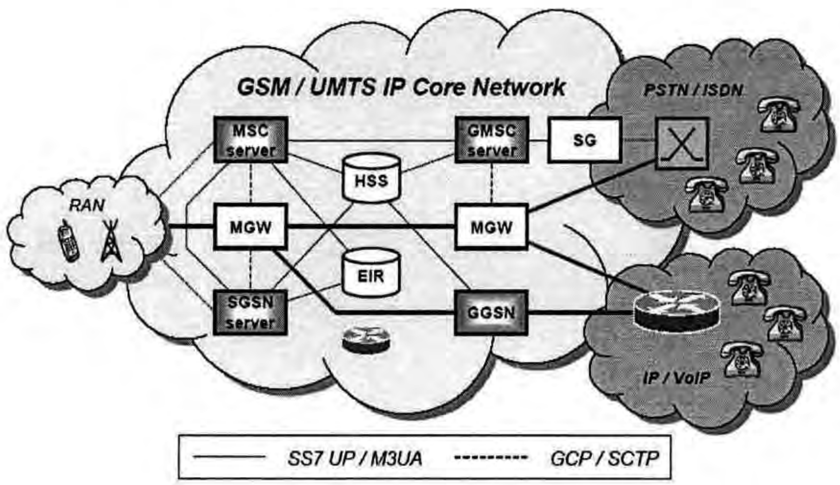


Figure 3.53: M3UA in GSM/UMTS Core Network.

SCCP – User Adaptation Layer (SUA): *SUA* provides a means by which an application part (such as *TCAP*) on an IPSP may be reached via an SG. The network architecture associated with *SUA* allows for multiple IPSPs to be reached via a single SG. The IPSPs do not have local *MTP3* instances, and so do not require their own SS7 Point Codes (*MTP3* and the Point Code, reside on the SG). The architecture of *SUA* use between an SG and IPSP is shown in Figure 3.54.

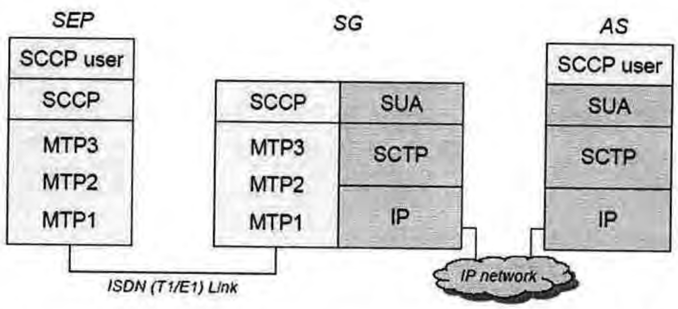


Figure 3.54: SCCP User Adaptation Layer (SUA).

The functionality of *SUA* could be provided by the *MTP2* or *MTP2 UAs*. However, *SUA* provides the mapping between *SCCP addresses* and IP addresses (at the SG). Without such a function, *SCCP* would have to be present at each IPSP and the external SS7 network would require knowledge of each such *SCCP* instance. *SUA* can abstract the presence of each IPSP, providing one *SCCP address* to cover all nodes. The integrated network with PSTN/ISDN/PLMN and IP is shown Figure 3.55.

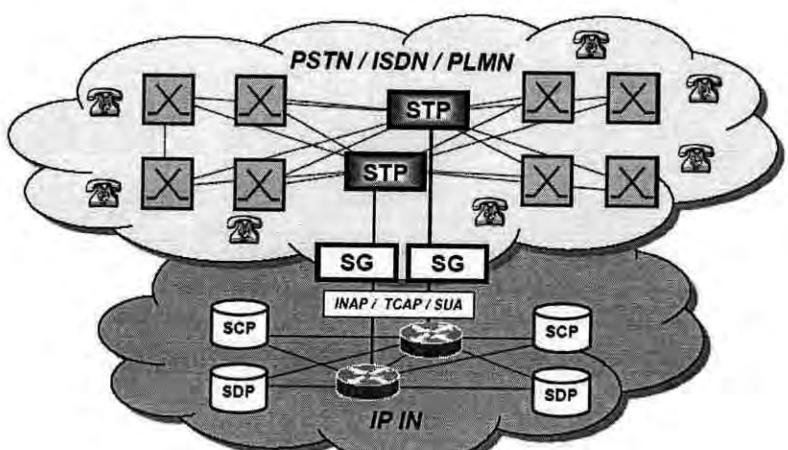


Figure 3.55: Integrated Network (SUA).

SUA is also flexible enough to support Application Parts running between two network nodes within the total IP network. This is particularly relevant to emerging networks, where there may be no need for an underlying "traditional" SS7 network. In this case, the IPSP stack would be the same on both (IP based) nodes. The SUA between two IPSPs is shown in Figure 3.56.

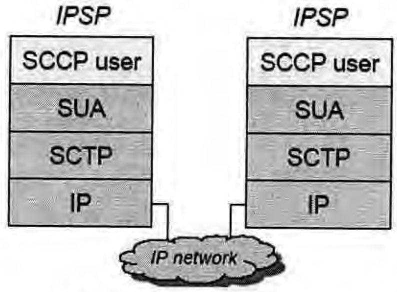


Figure 3.56: SUA between two IPSP

As a continuation of the telecommunication signalling system, some non-SS7 protocol will be described in the next chapter.

CHAPTER 4

NON-SS7 CALL CONTROL PROTOCOLS

In continuation of the telecommunications signalling system, this chapter describes the non-SS7 call control and media control signalling system and protocol in detail. Some protocols will also be described that are not used for call or media control, but used as a transmission layer for some telecommunications signalling or data.

Following is a list of different types of protocol used in an NGN-Soft-switch network for signalling and media control and also for transmission. Among these, H.323 and SIP are mainly used for Call control and for voice transmission it uses RTP. In this chapter such commonly used protocols will be described in detail [20].

Signalling:	H.323	H.323
	Megaco H.248	Gateway Control Protocol
	MGCP	Media Gateway Control Protocol
	RVP over IP	Remote Voice Protocol Over IP Specification
	SAPv2	Session Announcement Protocol
	SGCP	Simple Gateway Control Protocol
	SIP	Session Initiation Protocol
	Skinny	Skinny Client Control Protocol (Cisco)

Media:	DVB	Digital Video Broadcasting
	H.261	Video stream for transport using the real-time transport
	H.263	Bitstream in the Real-time Transport Protocol
	RTCP	RTP Control protocol
	RTP	Real-Time Transport

4.1 H.323

H.323 is an ITUT specification for transmitting audio, video, and data across an IP network. The H.323 standard addresses call signalling and control, multimedia transport and control, and bandwidth control for point-to-point and point-to-multipoint connections [20, 21].

The H.323 standard components and protocols are shown in Table 4.1.

Table 4.1 H.323 Components and protocols.

Feature	Protocol
Call Signalling	H.225
Media Control	H.245
Audio Codec's	G.711, G.722, G.723, G.728, G.729
Video Codec's	H.261, H.263
Data Sharing	T.120
Media Transport	RTP/RTCP

4.1.1 H.323 Elements

Figure 4.1 illustrates the elements of an H.323 system. These elements include terminals, gateways, gatekeepers, and multipoint control units (MCU). Endpoints/terminals provide point-to-point and multipoint connection for audio and optionally, video and data. Gateways interconnect to PSTN or ISDN networks for H.323 endpoints inter-working. Gatekeepers provide admission control and address translation services for terminals or gateways. MCUs are devices that allow two or more terminals or gateways to communicate with either audio and/or video sessions.

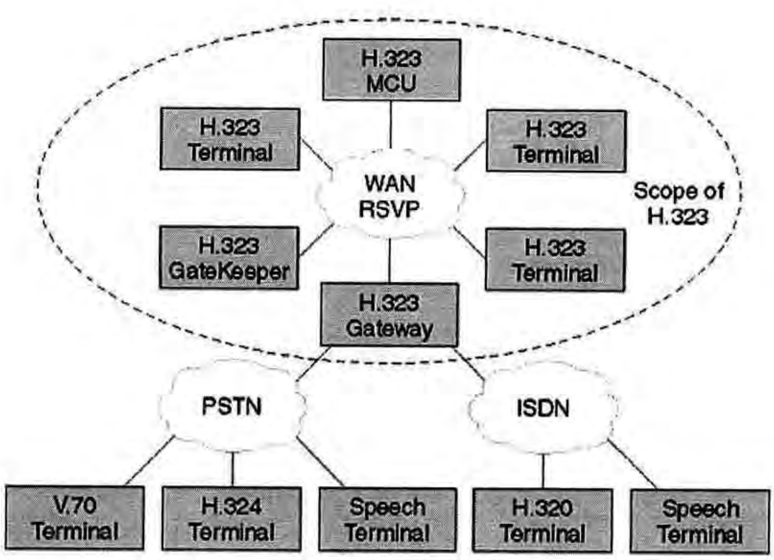


Figure 4.1: Elements of H.323 Networking

4.1.2 H.323 Protocol Suite

The H.323 protocol suite is based on several protocols, as illustrated in Figure 4.3. The protocol family supports call admissions, setup, status, teardown, media streams, and messages in H.323 systems. These protocols are supported by both reliable and unreliable packet delivery mechanisms over data networks.

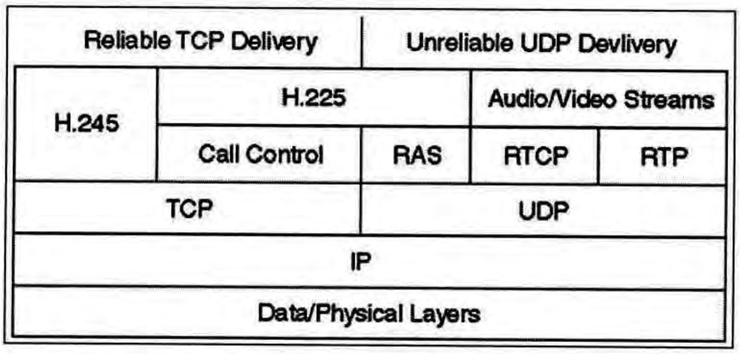


Figure 4.3: Layers of the H.323 Protocol Suite

The H.232 protocol stack is shown in Figure 4.1. The H.323 system will be discussed focusing mainly on voice communication in the following subsections.

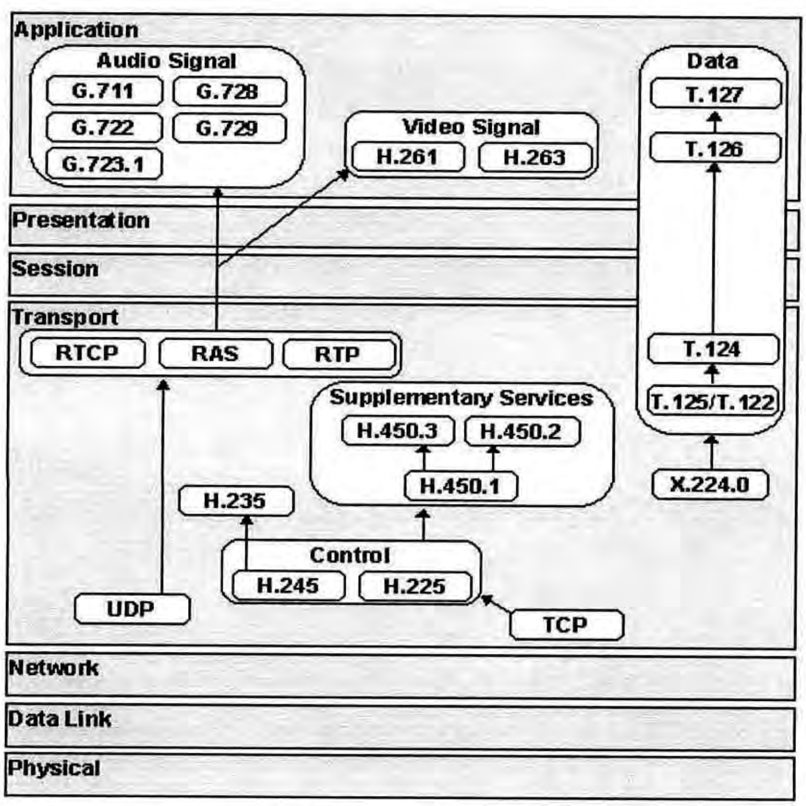


Figure 4.1: H.323 Protocol Stack

Although most H.323 implementations today utilize TCP as the transport mechanism for signalling, H.323 version 2 does enable basic UDP transport. Also, other standards bodies are investigating the use of other reliable UDP mechanisms to create more scalable signalling methods. The H.323 protocol suite is split into three main areas of control:

- Registration, Admissions, and Status (RAS) Signalling
- Call Control Signalling
- Media Control and Transport

RAS Signalling: RAS signalling provides pre-call control in H.323 networks where gatekeepers and a zone exist. The RAS channel is established between endpoints and gatekeepers across an IP network. The RAS channel is opened before any other channels are established and is independent of the call control signalling and media transport channels. This unreliable UDP connection carries the RAS messages that perform registration, admissions, bandwidth changes, status and disengage procedures.

Call Control Signalling (H.225): In H.323 networks, call control procedures are based on ITU Recommendation H.225, which specifies the use and support of Q.931 signalling messages. A reliable call control channel is created across an IP network on TCP port 1720. This port initiates the Q.931 call control messages between two endpoints for the purpose of connecting, maintaining, and disconnecting calls.

The actual call control and the keep alive messages move to ephemeral ports (Short-lived port, which is a TCP, UDP or SCTP port number that is automatically allocated from a predefined range by the TCP/IP stack software at the client end for a client-server communication.) after the initial call setup. 1720 is the well-known port for H.323 calls. H.225 also specifies the use of Q.932 messages for supplementary services.

The following Q.931 and Q.932 messages are the most commonly used signalling messages in H.323 networks:

• **Setup:** A forward message sent by the calling H.323 entity in an attempt to establish connection to the called H.323 entity. This message is sent on the well-known H.225 TCP port 1720.

• **Call Proceeding:** A backward message sent from the called entity to the calling entity to advise that call establishment procedures were initiated.

• **Alerting:** A backward message sent from the called entity to advise that called party ringing was initiated.

• **Connect:** A backward message sent from the called entity to the calling entity indicating that the called party answered the call. The connect message can contain the transport UDP/IP address for H.245 control signalling.

• **Release Complete:** Sent by the endpoint initiating the disconnect, which indicates that the call is being released. You can send this message only if the call signalling channel is open or active

• **Facility:** A Q.932 message used to request or acknowledge supplementary services. It also is used to indicate whether a call should be directed or should go through a gatekeeper.

Figure 4.4 illustrates the signalling messages for call setup. Interaction with the gatekeeper is limited to RAS messages for call permission and, possibly, on status messages.

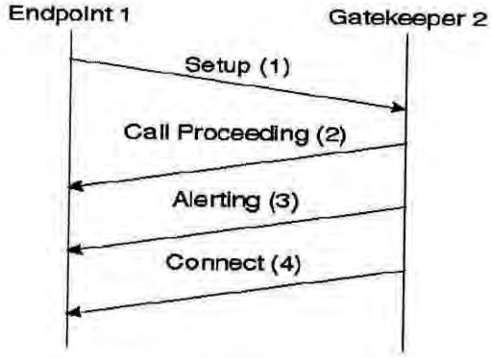


Figure 4.4: Call Setup Signalling Messages.

One can route the call signalling channel in an H.323 network in two ways: through Direct Endpoint Call Signalling and GKRCS. In the Direct Endpoint Call Signalling method, call signalling messages are sent directly between the two endpoints, as illustrated in Figure 4.5.

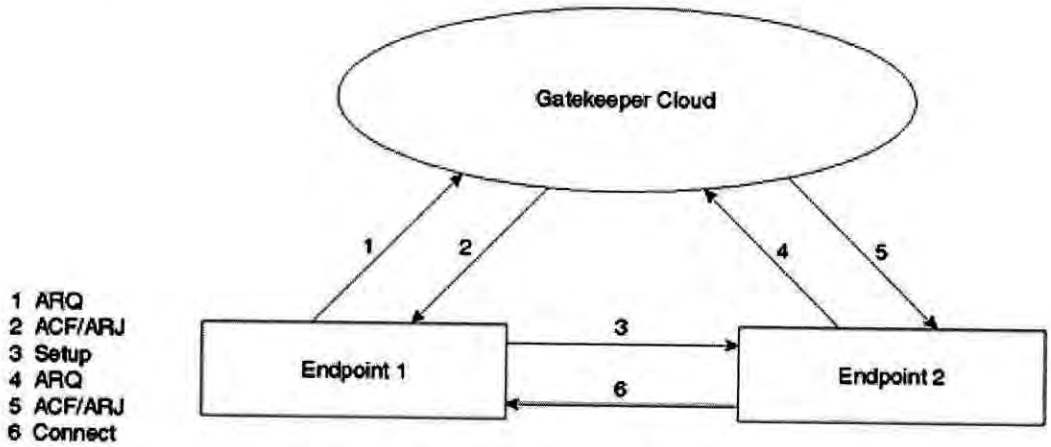


Figure 4.5: Direct Endpoint Call Signalling

In the GKRCS method, call signalling messages between the endpoints are routed through the gatekeeper, as illustrated in Figure 4.6.

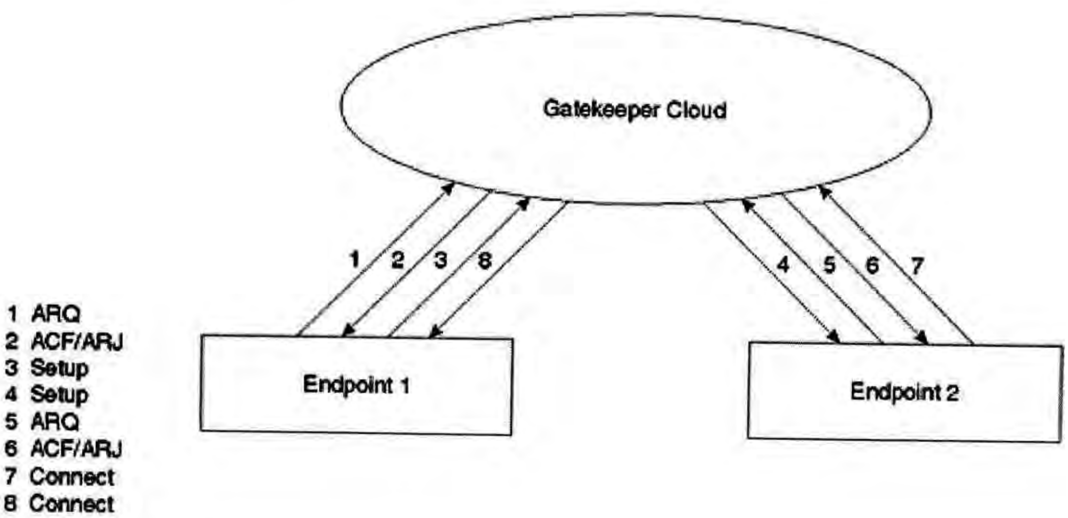


Figure 4.6: Gatekeeper Routed Call Signalling

One can offer supplementary services through the GKRCS method if the call signalling channel is left open during the call. Gatekeepers can also close the call signalling channel after call setup is complete.

Media Control and Transport (H.245 and RTP/RTCP): H.245 handles end-to-end control messages between H.323 entities. H.245 procedures establish logical channels for transmission of audio, video, data, and control channel information. An endpoint establishes one H.245 channel for each call with the participating endpoint. The reliable control channel is created over IP using the dynamically assigned TCP port in the final call signalling message.

The exchange of capabilities, the opening and closing of logical channels, preference modes, and message control take place over this control channel. H.245 control also enables separate transmit and receive capability exchange as well as functions negotiation, such as determining which codec to use.

If we use Gatekeeper Routed call signalling, we can control channel routing in the following two ways. We can use Direct H.245 Control, which occurs directly between two participating endpoints. Or, we can use Gatekeeper Routed H.245 Control, which occurs between each endpoint and its gatekeeper.

We can use the following procedures and messages to enable the H.245 control operation:

- **Capability Exchange:** It consists of messages that securely exchange the capabilities between two endpoints, also referred to as terminals. These messages indicate the terminal's transmit and receive capabilities for audio, video, and data to the participating terminal. For audio, the capability exchange includes speech transcoding codec's such as G-series G.729 at 8 kbps, G.728 at 16 kbps, G.711 at 64 kbps, G.723 at 5.3 or 6.3 kbps, or G.722 at 48, 56, and 64 kbps. It also includes International Organization for Standardization (ISO) series IS.11172-3 with 32-, 44.1-, and 48 kHz sampling rates, and IS.13818-3 with 16-, 22.05-, 24-, 32-, 44.1-, and 48 kHz sampling rates; and GSM full-rate, half-rate, and enhanced full-rate speech audio codec's.

- **Master-Slave Termination:** Procedures are used to determine which endpoint is master and which endpoint is slave for a particular call. The relationship is maintained for the duration of the call and is used to resolve conflicts between endpoints. Master-slave rules are used when both endpoints request similar actions at the same time.

• **Round-Trip Delay:** Procedures are used to determine delay between the originating and terminating endpoints. The Round Trip Delay Request message measures the delay and verifies whether the remote H.245 protocol entity is alive

• **Logical Channel Signalling:** It opens and closes the logical channel that carries audio, video and data information. The channel is set up before the actual transmission to ensure that the terminals are ready and capable of receiving and decoding information. The same signalling messages establish both unidirectional and bidirectional channels. After logical channel signalling is successfully established, the UDP port for the RTP media channel is passed from the terminating to the originating endpoint. Also, when using the Gatekeeper Call Routed model, this is the point at which the gatekeeper can divert the RTP streams by providing the actual UDP/IP address of the terminating endpoint.

• **Fast Connect Procedures:** The two procedures available to establish media channels between endpoints are H.245 and Fast Connect. Fast Connect enables media connection establishment for basic point-to-point calls with one round-trip message exchange. These procedures dictate that the calling endpoint include the fast start element in the initial setup message. The fast start portion consists of logical channel sequences, media channel capabilities, and the necessary parameters to open and begin media transmission. In response, the called endpoint returns an H.225 message (call proceeding, progress, alerting, or connect) containing a fast start element that selects the accepted terminal capabilities. At this point, both the calling and the called endpoints can begin transmitting media if the setup sequence based on H.225 reached the connected state.

• **Tunneling H.245:** We can encapsulate or tunnel H.245 messages within the H.225 call signalling channel instead of creating a separate H.245 control channel. This method improves the call setup time and resource allocation, and it provides synchronization between call signalling and control. We can encapsulate multiple H.245 messages in any H.225 message. Also, at any time either endpoint can switch to a separate H.245 connection.

• **Call Termination:** Either endpoint participating in a call can initiate call termination procedures. First, the endpoint must cease media transmissions (such as audio, video, or data) and close all logical channels. Next, it must end the H.245 session and send a release complete message on the call signalling channel, if it's still open or active. At this point, if no gatekeeper is presents, the call is terminated. When a gatekeeper is present, the following messages are used on the RAS channel to complete call termination.

• **Disengage Request (DRQ)**—sent by an endpoint or gatekeeper to terminate a call

• **Disengage Confirm (DCF)**—sent by an endpoint or gatekeeper confirming disconnection of the call

• **Disengage Reject (DRJ)**—sent by the endpoint or gatekeeper rejecting call disconnection

• **Media Transport (RTP/RTCP):** RTP provides media transport in H.323. More specifically, RTP enables real-time, end-to-end delivery of interactive audio, video, and data over unicast or multicast networks. Packetization and transmission services include payload identification, sequencing, time stamping, and monitoring. RTP relies on other mechanisms and lower layers to ensure on-time delivery, resource reservation, reliability, and QoS. RTCP monitors data delivery as well as controls and identifies services. The media channel is created using UDP, where RTP streams operate on an even port number and the corresponding RTCP stream operates on the next-higher (odd) port number.

The direct endpoint signalling scheme for the same gatekeeper is shown in Figure 4.7.

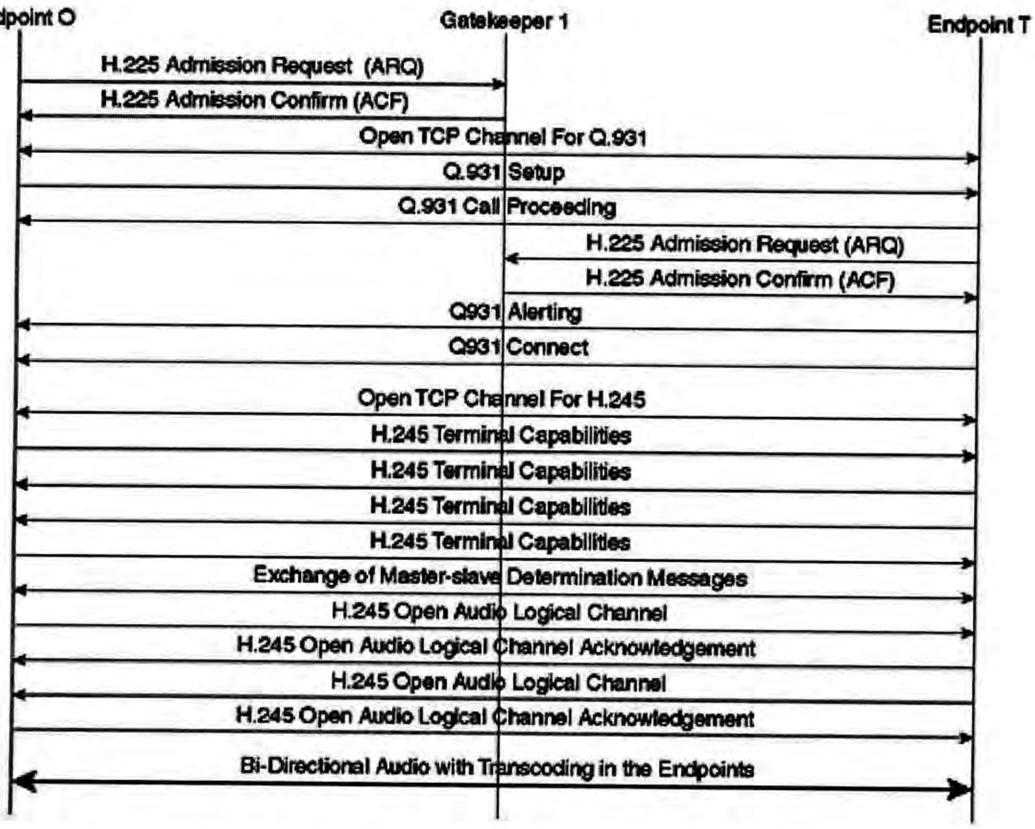


Figure 4.7: Direct Endpoint Signalling—Same Gatekeeper

4.1.3 H.323 Call-Flows

The call-flows outlined in this section demonstrate ways the H.323 family of protocols provides call setup between two endpoints. Let us assume these are speech calls and that all endpoints already completed registration with the appropriate gatekeeper. The call setup examples include two different gatekeeper implementations as well as two different call signalling methods. The gate-keeper-routed call signalling for the same gatekeeper is shown in Figure 4.8.

The details of the call setup procedures for single gatekeeper implementations are shown in the example of Figures 4.7 and 4.8.

Figure 4.8, on the other hand, illustrates call-flows using gatekeeper call routed signalling between two endpoints sharing the gatekeeper. Note that the H.245 procedure is handled directly between the endpoints and is not gatekeeper-routed.

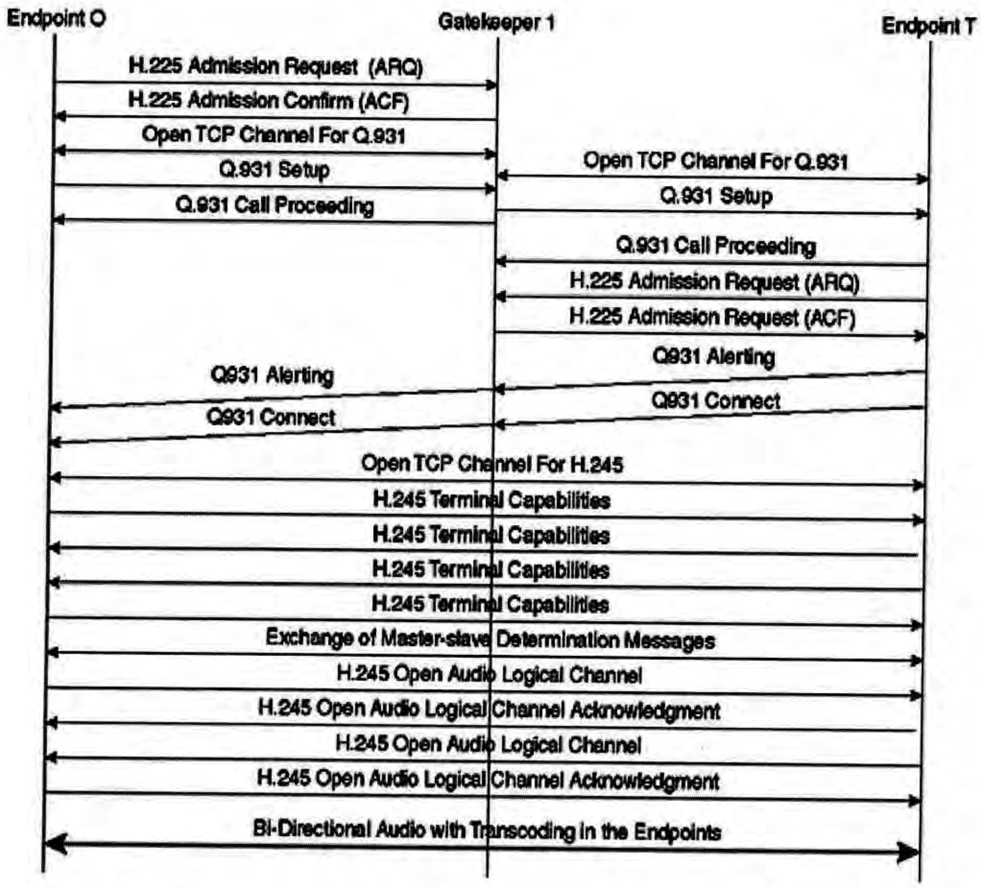


Figure 4.8: Gatekeeper-Routed Call Signalling—Same Gatekeeper

The examples in Figures 4.9 and 4.10 detail call setup procedures for dual-gatekeeper implementations. Specifically, Figure 4.9 illustrates call-flows using direct endpoint signalling between two endpoints that have different gatekeepers. The main difference between GKRCS and Directed Call Signalling is that in GKRCS the setup message is directed to the gatekeeper, and in Directed Call Signalling it is directed to the terminating endpoint. Figure 4.9 illustrates call-flows using direct endpoint signalling between two endpoints sharing the gatekeeper.

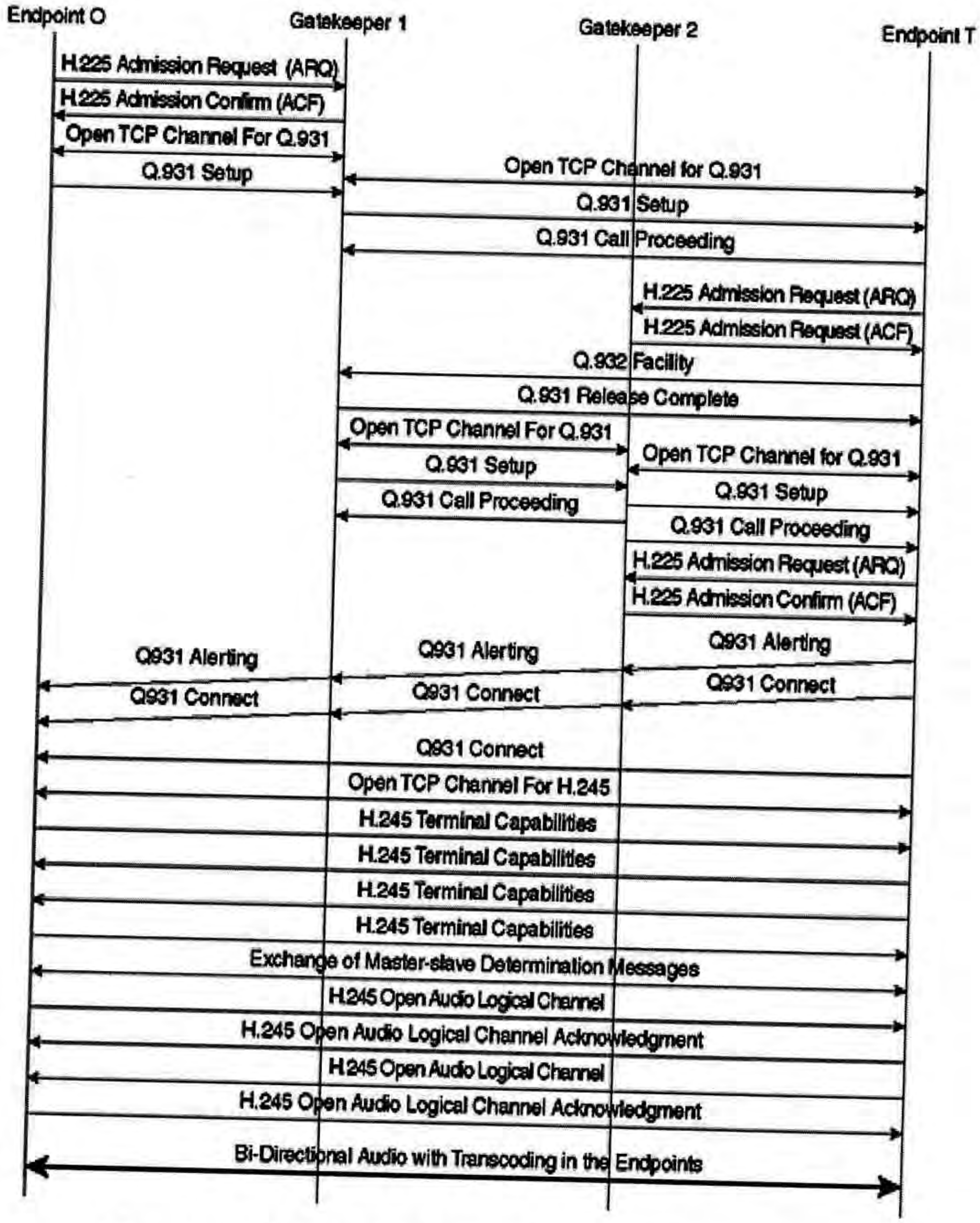


Figure 4.9: Direct Endpoint Signalling—Two Gatekeepers

The final H.323 call-flow example demonstrates call setup procedures for the GKRCS method, whereby each endpoint has a different gatekeeper. This enables LRQs and LCFs to be sent between the two gatekeepers, which enables control of billing records at the gatekeeper, as all the setup and control messages pass through the gatekeeper.

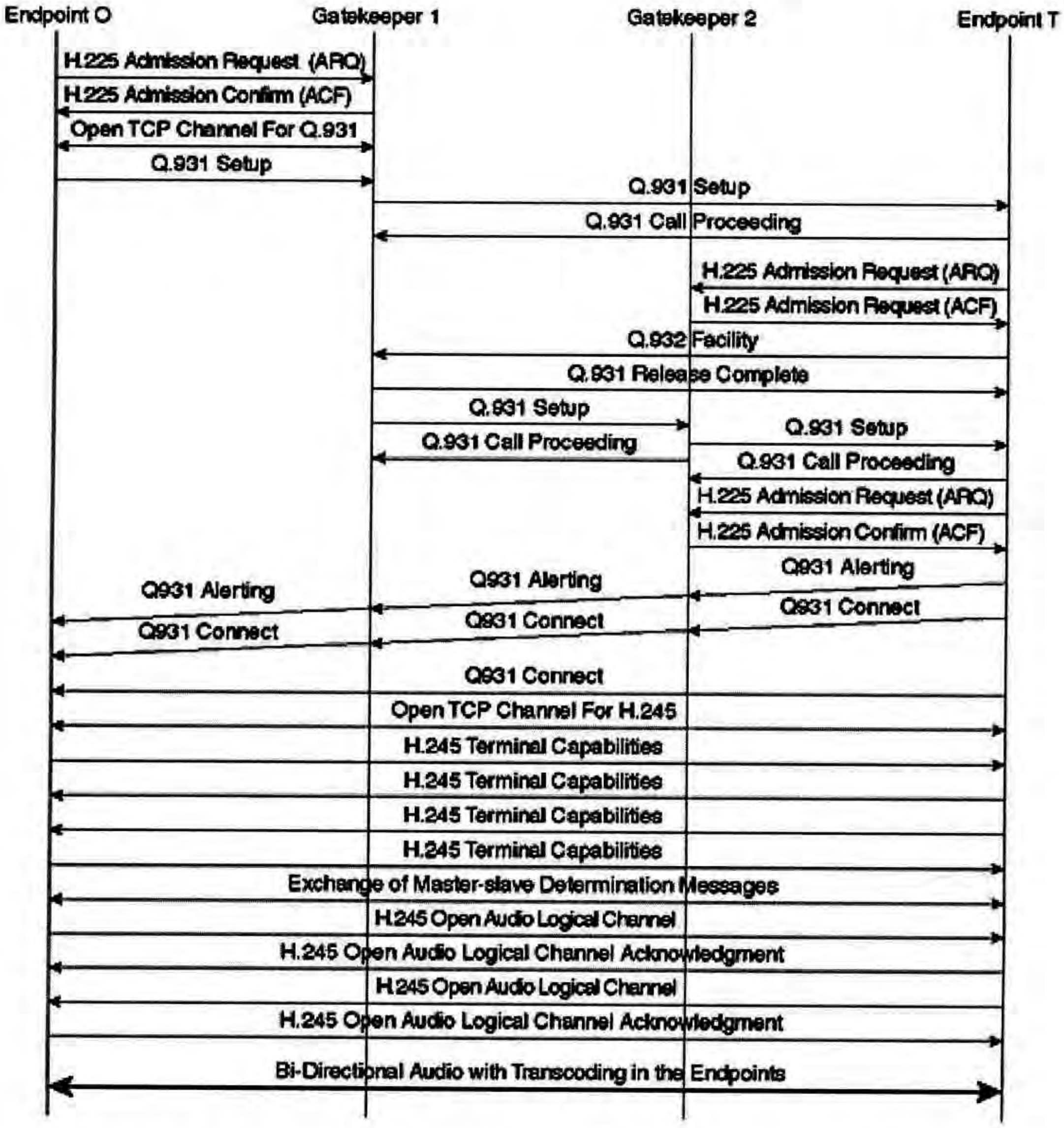


Figure 4.10: Gatekeeper Routed Call Signalling—Two Gatekeepers

4.2 Session Initiation Protocol (SIP)

The Session Initiation Protocol (SIP) is an application-layer signalling-control protocol used to establish, maintain, and terminate multimedia sessions. Multimedia sessions include Internet telephony, conferences, and other similar applications involving such media as audio, video, and data.

We can use SIP invitations to establish sessions and carry session descriptions. SIP supports unicast and multicast sessions as well as point-to-point and multipoint calls.

We can establish and terminate communications using the following five SIP facets: user locations, user capability, user availability, call setup, and call handling.

SIP, on which Request for Comments (RFC) 2543 is based, is a text-based protocol that is part of the overall Internet Engineering Task Force (IETF) multimedia architecture. The IETF also includes the Resource Reservation Protocol (RSVP; RFC 2205), Real-Time Transport Protocol (RTP; RFC 1889), Real-Time Streaming Protocol (RTSP; RFC 2326), Session Announcement Protocol (SAP; internet draft), and SDP (Session Description Protocol; RFC 2327). SIP's functions are independent, however, so it does not depend on any of these protocols. It is important to note that SIP can operate in conjunction with other signalling protocols, such as H.323.

Internet Protocol (IP) telephony is still being developed and will require additional signalling capabilities in the future. The extensibility of SIP enables such development of incremental functionality. SIP message headers are versatile, and we can register additional features with the Internet Assigned Numbers Authority (IANA). SIP message flexibility also enables elements to construct advanced telephony services, including mobility type services. As of the writing of this chapter, the IETF has not yet ratified SIP, so this chapter focuses on the basics of SIP and does not discuss extensibility or services. The following issues are covered in this topic:

- SIP overview: Components, addressing, and invitations
- Messages: Headers, requests, and responses
- Basic operation: Proxy and redirect server operation.

4.2.1 SIP overview

This section describes the basic functionality and key elements of SIP. The two components in a SIP system are user agents and network servers. Calling and called parties are identified by SIP addresses; parties need to locate servers and users. SIP transactions are also covered as part of this overview [22, 23].

User Agents: User agents are client end-system applications that contain both a user-agent client (UAC) and a user-agent server (UAS), otherwise known as client and server, respectively.

- **Client**: Initiates SIP requests and acts as the user's calling agent.
- **Server**: Receives requests and returns responses on behalf of the user; acts as the user-called agent.

Network Servers: Two types of SIP network servers exist: proxy servers and redirect servers. Functional examples of these servers are provided in section 4.2.3 under the heading "Basic Operation of SIP."

- **Proxy server:** Acts on behalf of other clients and contains both client and server functions. A proxy server interprets and can rewrite request headers before passing them on to other servers. Rewriting the headers identifies the proxy as the initiator of the request and ensures that replies follow the same path back to the proxy instead of the client.

- **Redirect server:** Accepts SIP requests and sends a redirect response back to the client containing the address of the next server. Redirect servers do not accept calls, nor do they process or forward SIP requests.

4.2.2 SIP Messages

Two kinds of SIP messages exist: requests initiated by clients, and responses returned from servers. Every message contains a header that describes the details of communication. SIP is a text-based protocol with message syntax and header fields identical to Hypertext Transfer Protocol (HTTP). SIP messages are sent over TCP or UDP with multiple messages carried in a single TCP connection or UDP datagram.
Message Headers: Message headers are to specify the calling party, called party, route, and message type of a call. The four groups of message headers are as follows:

- **General headers:** Apply to requests and responses.
- **Entity headers:** Define information about the message body type and length.
- **Request headers:** Enable the client to include additional request information.
- **Response headers:** Enable the server to include additional response information.

These main header groups, along with 37 corresponding headers, are listed in Table 4.2.

Table 4.2: SIP Headers

General Headers	Entity Headers	Request Headers	Response Headers
Accept	Content-Encoding	Authorization	Allow
Accept-Encoding	Content-Length	Contact	Proxy-Authenticate
Accept-Language	Content-Type	Hide	Retry-After
Call-ID		Max-Forwards	Server
Contact		Organization	Unsupported
CSeq		Priority	Warning
Date		Proxy-Authorization	WWW-Authenticate
Encryption		Proxy-Require	
Expires		Route	
From		Require	
Record-Route		Response-Key	
Timestamp		Subject	
To		User-Agent	
Via			

Short explanations of some key headers are provided in Table 4-3.

Table 4.3: Explanations for Some Key SIP Headers

Header	Explanation
To	Identifies the recipient of the request.
From	Indicates the initiator of the request.
Subject	Describes the nature of the call.
Via	Indicates the path taken by the request.
Call-ID	Uniquely identifies a specific invitation or all registrations of a specific client.
Content-Length	Identifies the size of the message body in octets.
Content-Type	Indicates the media type of the message body.
Expires	Identifies the date and time when the message content expires.
Route	Indicates the route taken by a request.

Message Requests: SIP communication features six kinds of message requests. These requests, also referred to as methods, enable user agents and network servers to locate, invite, and manage calls. The six SIP requests are as follows:

- **Invite**: This method indicates that the user or service is invited to participate in a session. It includes a session description and, for two-way calls, the calling party indicates the media type. A successful response to a two-party INVITE (200 OK response) includes the called party's receive media type. With this simple method, users can recognize the capabilities of the other end and open a conversation session with a limited number of messages and round trips.

- **ACK**: These requests correspond to an INVITE request. They represent the final confirmation from the end system and conclude the transaction initiated by the INVITE command. If the calling party includes a session description in the ACK request, no additional parameters are used in the session. If a session description is absent, the session parameters in the INVITE request are used as the default.

- **Options**: This method enables you to query and collect user agents and network server capabilities. This request is not used to establish sessions, however.

- **Bye**: This method is used by calling and called parties to release a call. Before actually releasing the call, the user agent sends this request to the server indicating the desire to release the session.

- **Cancel**: This request enables user agents and network servers to cancel any in-progress request. This does not affect completed requests in which final responses were already received.

- **Register**: This method is used by clients to register location information with SIP servers.

Message Responses: SIP message responses are based upon the receipt and interpretation of a corresponding request. They are sent in response to requests and indicate call success or failure, including the status of the server. The six classes of responses, their status codes, and explanations of what they do are provided in Table 4.4. The two categories of responses are provisional, which indicates progress, and final, which terminates a request. In Table 4.4 informational responses are provisional, and the remaining five are final responses.

Table 4.4: SIP Responses.

Class of Response	Status Code	Explanation
Informational	100	Trying
	180	Ringing
	181	Call is being forwarded
	182	Queued
Success	200	OK
	300	Multiple choices
	301	Moved permanently
	302	Moved temporarily
Success	303	See other
	305	Use proxy
	380	Alternative service
Client-Error	400	Bad request
	401	Unauthorized
	402	Payment required
	403	Forbidden
	404	Not found
	405	Method not allowed
	406	Not acceptable
	407	Proxy authentication required
	408	Request timeout
	409	Conflict
	410	Gone
	411	Length required
	413	Request entity too large

Class of Response	Status Code	Explanation
Client-Error	414	Requested URL too large
	415	Unsupported media type
	420	Bad extension
	480	Temporarily not available
	481	Call leg or transaction doesn't exist
	482	Loop detected
	483	Too many hops
	484	Address incomplete
	485	Ambiguous
	486	Busy here
Server Error	500	Internal server error
	501	Not implemented
	502	Bad gateway
	503	Service unavailable
	504	Gateway timeout
	505	SIP version not supported
Global Feature	600	Busy everywhere
	603	Decline
	604	Does not exist anywhere
	606	Not acceptable

4.2.3 Basic Operation of SIP

SIP servers handle incoming requests in two ways. This basic operative is based on inviting a participant to a call. The two basic modes of SIP server operation described in this section are the following:

- Proxy servers
- Redirect servers

Example of a Proxy Server: The communication exchange for the INVITE method using the proxy server is illustrated in Figure 4.11.

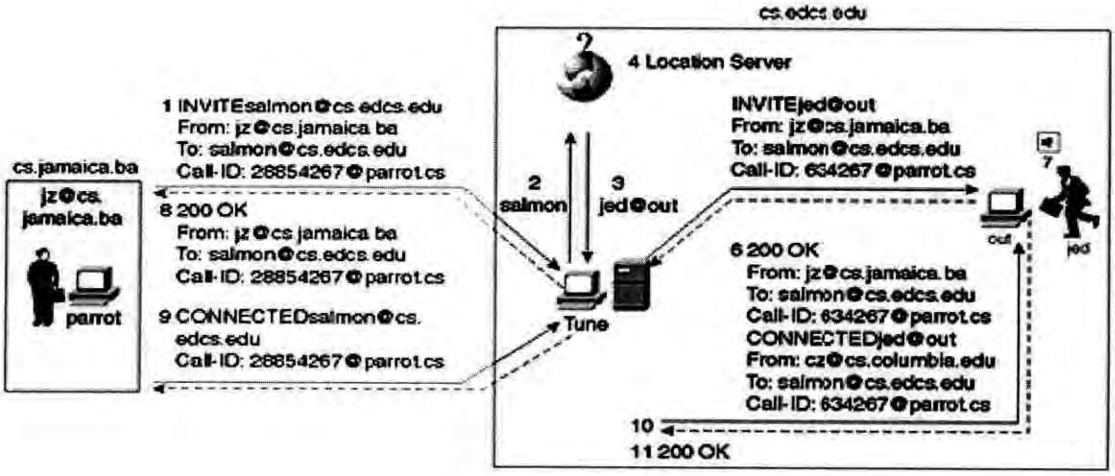


Figure 4.11: Proxy Mode of Operation

The operational steps in the proxy mode needed to bring a two-way call to succession are as follows:

1. The proxy server accepts the INVITE request from the client.
2. The proxy server identifies the location by using the supplied addresses and location services.
3. An INVITE request is issued to the address of the location returned.
4. The called party user agent alerts the user and returns a success indication to the requesting proxy server.
5. An OK (200) response is sent from the proxy server to the calling party.
6. The calling party confirms receipt by issuing an ACK request, which is forwarded by the proxy or sent directly to the called party.

Example of Redirect Server: The protocol exchange for the INVITE request using the redirect server is shown in Figure 4.12.

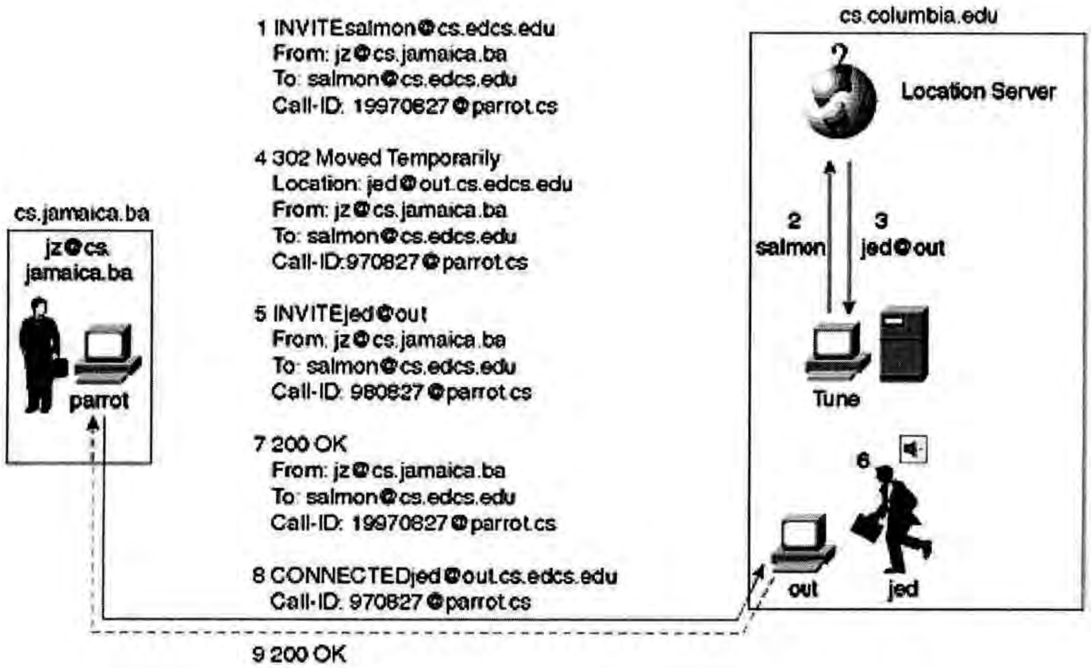


Figure 4.12: Redirect Mode of Operation

The operational steps in the redirect mode to bring a two-way call to succession are as follows:

1. The redirect server accepts the INVITE request from the calling party and contacts location services with the supplied information.

2. After the user is located, the redirect server returns the address directly to the calling party. Unlike the proxy server, the redirect server does not issue an INVITE.

3. The user agent sends an ACK to the redirect server acknowledging the completed transaction.

4. The user agent sends an INVITE request directly to the address returned by the redirect server.

5. The called party provides a success indication (200 OK), and the calling party returns an ACK.

4.3 RS-232

In telecommunications, RS-232 (Recommended Standard 232) is a standard for serial binary data signals connecting between a DTE (Data terminal equipment) and a DCE (Data Communications Equipment). It is commonly used in computer serial ports [24].

In RS-232, data is sent as a time-series of bits. Both synchronous and asynchronous transmissions are supported by the standard. In addition to the data circuits, the standard defines a number of control circuits used to manage the connection between the DTE and DCE. Each data or control circuit only operates in one direction that is, signalling from a DTE to the attached DCE or the reverse. Since transmit data and receive data are separate circuits, the interface can operate in a full duplex manner, supporting concurrent data flow in both directions. The standard does not define character framing within the data stream, or character encoding.

Diagrammatic oscilloscope trace of voltage levels for ASCII "K" character (0x4b) with 1 start bit, 8 data bits, 1 stop bit. The RS-232 standard defines the voltage levels that correspond to logical one and logical zero levels. Valid signals are plus or minus 3 to 15 volts. The range near zero volts is not a valid RS-232 level; logic one is defined as a negative voltage, the signal condition is called marking, and has the functional significance of OFF. Logic zero is positive; the signal condition is spacing, and has the function ON. The standard specifies a maximum open-circuit voltage of 25 volts; signal levels of ±5 V,±10 V,±12 V, and ±15 V are all commonly seen depending on the power supplies available within a device. RS-232 drivers and receivers must be able to withstand indefinite short circuit to ground or to any voltage level up to +/-25 volts. The slew rate, or how fast the signal changes between levels, is also controlled [25].

Because the voltage levels are higher than logic levels used by integrated circuits, special intervening circuits are required to translate logic levels, and to protect circuitry internal to the device from short circuits or transients that may appear on the RS-232 interface.

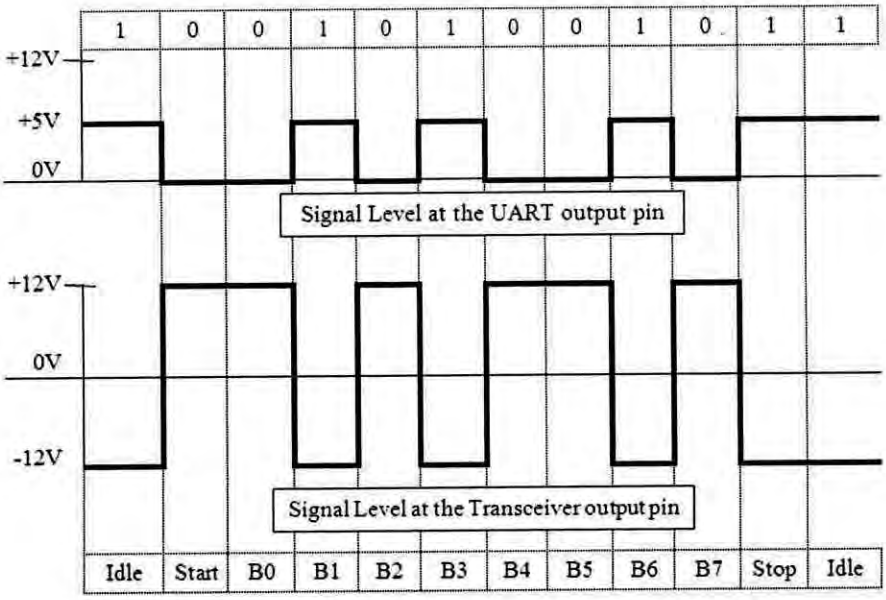


Figure 3-15: RS-232 Voltage Level for the letter 'J'.

Because both ends of the RS-232 circuit depend on the ground pin being zero volts, problems will occur when connecting machinery and computers where the voltage between the ground pin on one end and the ground pin on the other is not zero. This may also cause a hazardous ground loop.

4.3.1 RS-232 Signals

Commonly-used signals in the RS-212 standard are shown in the Table 4.5.

Table 4.5: RS-232 Signals.

Name	Description	Dir
CD	Carrier Detect	In
RXD	Receive Data	In
TXD	Transmit Data	Out
DTR	Data Terminal Ready	Out
GND	System Ground	Power
DSR	Data Set Ready	In
RTS	Request to Send	Out
CTS	Clear to Send	In
RI	Ring Indicator	In

Transmitted Data (TxD): Data sent from DTE to DCE.

Received Data (RxD): Data sent from DCE to DTE.

Request To Send (RTS): Asserted (set to 0) by DTE to prepare DCE to receive data. This may require action on the part of the DCE, e.g. transmitting a carrier or reversing the direction

Clear To Send (CTS): Asserted by DCE to acknowledge RTS and allow DTE to transmit.

Data Terminal Ready (DTR): Asserted by DTE to indicate that it is ready to be connected. If the DCE is a modem, this may "wake up" the modem, bringing it out of a power saving mode. This behaviour is seen quite often in modern PSTN and GSM modems. When this signal is de-asserted, the modem may return to its standby mode, immediately hanging up any calls in progress.

Data Set Ready (DSR): Asserted by DCE to indicate an active connection. If DCE is not a modem (e.g. a null modem cable or other equipment), this signal should be permanently asserted (set to 0), possibly by a jumper to another signal.

Data Carrier Detect (DCD): Asserted by DCE when a connection has been established with remote equipment.

Ring Indicator (RI): Asserted by DCE when it detects a ring signal from the telephone line.

The standard defines RTS/CTS as the signalling protocol for flow control for data transmitted from DTE to DCE. The standard has no provision for flow control in the other direction. In practice, most hardware seems to have repurposed the RTS signal for this function.

4.4 RS-485

EIA-485 (formerly RS-485 or RS485) is an OSI model physical layer electrical specification of a two-wire, half-duplex, multipoint serial connection. The standard specifies a differential form of signalling. The difference between the wires' voltages is what conveys the data. One polarity of voltage indicates a logic 1 level, the reverse polarity indicates logic 0. The difference of potential must be at least 0.2 volts for valid operation, but any applied voltages between +12 V and -7 volts will allow correct operation of the receiver [26].

RS-485 can be used to communicate with remote devices at distances up to 4000 ft (1200 m) at speeds of up to 100 kbit/s at this distance. Converters between RS232 and RS485, USB and RS485, Ethernet and RS485 are available to allow your PC to communicate with remote devices. By using "Repeaters" and "Multi-Repeaters" very large RS485 networks can be formed. The Application Guidelines for TIA/EIA-485-A has one diagram called "Star Configuration. Not recommended." Using an RS485 "Multi-Repeater" can allow for "Star Configurations" with "Home Runs" (or multi-drop) connections similar to Ethernet Hub/Star implementations (with greater distances). Hub/Star systems (with "Multi-Repeaters") allow for very maintainable systems, without violating any of the RS485 specifications. Repeaters can also be used to extend the distance and/or number of nodes on a network.

4.4.1 Uses of EIA-485

SCSI-2 and SCSI-3 (for instance) use this specification to implement the physical layer. EIA-485 is often used with common UARTs to implement low-speed data communications in commercial aircraft cabins. For example, some passenger control units use it. It requires minimal wiring, and can share the wiring among several seats. It therefore reduces the system weight.

EIA-485 also sees some use in programmable logic controllers and on factory floors in order to implement proprietary data communications. Since it is differential, it resists electromagnetic interference from motors and welding equipment.

EIA-485 is used in large sound systems, as found at music events and theatre productions, for remotely controlling high-end sound-processing equipment from a standard computer running special software. The EIA-485 link is typically implemented over standard XLR cables more usually used for microphones, and so can be run between stage and control desk without laying special cables.

EIA-485 also is used in Building automation as the simple bus wiring and long cable length is ideal for joining remote devices.

EIA-485 also is used to control theatrical and disco lighting where it is used as the communications protocol for DMX signals.

4.4.2 RS-485 Pin labeling

The RS485 differential line consists of two pins:
A: TxD-/RxD- inverting pin which is negative when the line is idle (i.e. data is 1).
B: TxD+/RxD+ non-inverting pin which is positive when the line is idle (i.e. data is 1).
These names are all in use on various equipment, but the actual standard released by EIA only uses the names A and B. However, despite the unambiguous standard there is much confusion about which is which.

The RS485 signalling specification states that signal A is the inverting or '-' pin and signal B is the non-inverting or '+' pin. [1] The same naming is specified in the NMEA standards.

This is in conflict with the A/B naming used by a number of differential transceivers manufacturers, including the Texas Instruments application handbook on RS422/485 communications (A=non-inverting, B=inverting). These manufacturers are incorrect, but their practice is in a widespread use.

Therefore, care must be taken when using A/B naming. In addition to the A and B connections, the EIA standard also specifies a third interconnection point called C, which is the common ground.

A new signalling system named "Bus Independent Signalling" system (BIS) will be proposed in the next chapter. BIS network and protocol architecture, its implementation and applications, performance and advantages will also be discussed in the subsequent chapters.

CHAPTER 5

THE PROPOSED BUS INDEPENDENT SIGNALLING SYSTEM AND ITS ARCHITECTURE

The last few chapters have described the existing SS7 protocol and its variants. In fact, SS7 is designed for large scale telecommunication networks, which is not suitable for small scale point to multi-point communication networks. There are, however, some protocols such as F-Bus, M-Bus etc., for small scale communication networks, but they are designed only for point to point applications. Therefore, for small scale point to multi-point applications a simpler signalling system is needed, which would be independent from the transmission bus and transmission layer. For this purpose a new signalling system has been proposed as part of the current research, which has been named as "Bus Independent Signalling" system (BIS). The additional requirements of this system over the existing SS7, SIGTRAN and other similar signalling systems and protocols have also been highlighted.

5.1 Basic Definition of BIS

The very name "Bus Independent Signalling" is self-explanatory, that it is completely independent from the transmission bus. Thus BIS can transfer signalling data using a network completely different from the bearer network. BIS has also the capability of carrying the payload or the bearer data by itself within the same physical and logical network.

5.2 Need for a New Signalling System

The BIS has been proposed keeping in mind the usability of a signalling system for both small and medium point to multi-point networks, the implementation of which is not possible using the existing standard signalling system. The reasons for the implementation complexity are briefly explained in sections 5.2.1 and 5.2.2.

5.2.1 The signalling systems for large networks

The mostly used signalling system for large networks is SS7 and SIGTRAN, which are for point to point real time communication networks. A standard SS7/SIGTRAN Network is shown in Figure 5.1.

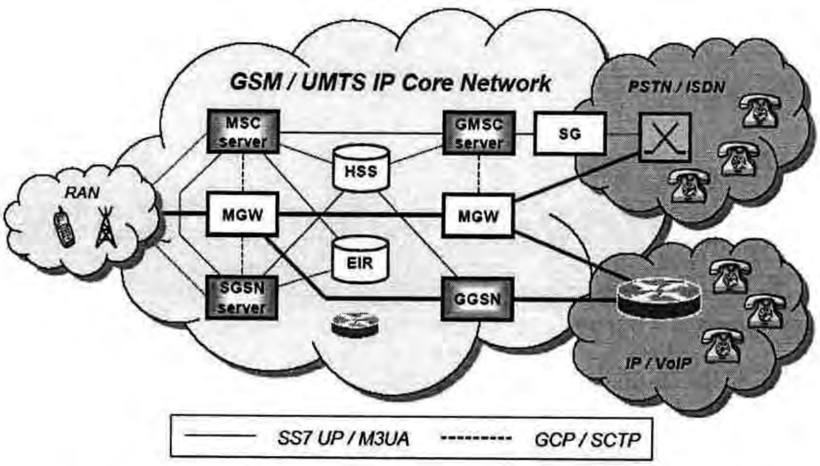


Figure 5.1: SS7 – SIGTRAN network connection.

Therefore, it is not possible to use SS7 or SIGTRAN even in a small network where point to multi-point signalling is required. However, this limitation has been solved in the fully IP signalling system (like SIP, H.323, etc), where point to multi-point communication is possible only over a point to multi-point physical network. However, to implement these IP signalling systems in some small or medium scale networks are difficult, as these systems have limitations in the processing capacity (8/16 bit MCU, low speed MCU, low memory) and would require complex physical interfaces.

5.2.2 The Signalling Systems for Small Networks

The existing small scale signalling systems intended for the small system networks are well-suited for point to point communication. An F-Bus communication between a mobile phone and a PC as an example of such a small network is shown in Figure 5.2.

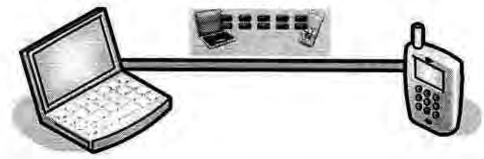


Figure 5.2: Data Transfer from a Mobile Phone to a PC using F-Bus Protocol.

However, these protocols are not suitable for point to multi-point small system networks, which we have termed as "Small System Distributed Networks" (SSDNs). There are some signalling systems designed for SSDNs, which are developed by manufacturers of special devices and are usually proprietary items. Therefore, they are not available for the general purpose use and also are not standardized.

5.3 The Proposed Signalling System

To get rid of the above limitations, BIS has been proposed. It possesses the combined characteristic of the TCP/IP and SS7 with an added simplicity. It has been designed for point to multi-point small scale communication networks, and is a protocol which is IP portable. It would also have the real-time communication capability of the SS7 and is very simple.

The architecture and protocol stack of the BIS will be described in section 5.4 in a grater detail. The implementation of the BIS protocol in both hardware and software modules will be presented in Chapter 6

5.4 Architecture of the Bus Independent Signalling System

The proposed signalling system, namely, the "Bus Independent Signalling" system has been introduced in the previous section. This section describes the architecture and protocol stack of the proposed BIS system, which is designed for a small scale network named as "Small System Distributed Network" (SSDN). The Bus Independent Signalling is named as it is totally independent from the type of bus used for data transfer. All types of data (both voice and digital lossless data, packed and non-packed data) transfer is possible using the proposed BIS system. Based on the use and possible architecture, BIS networks can be of the following 2 types:

A. BIS in an Isolated Bearer Path Network and
B. BIS in an Integrated Payload Network.

A. BIS in an Isolated Bearer Path Network: In this type of network the signalling data and the traffic data (shown in Figure 5.3) use separate paths through the network for communication.

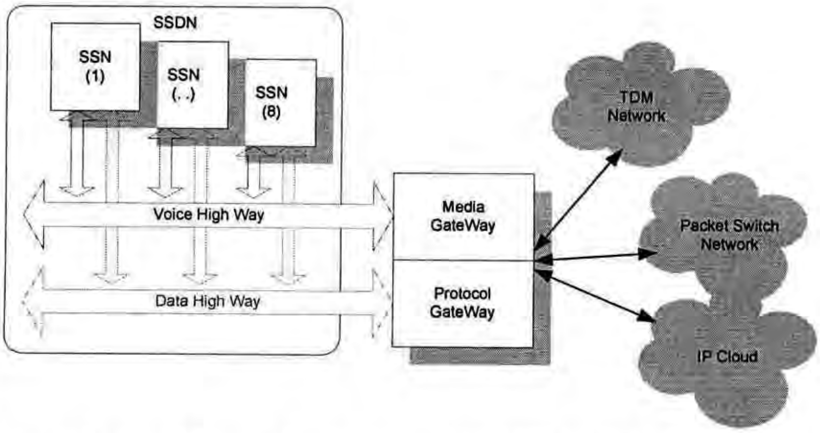


Figure 5.3: BIS- Isolated Bearer Path Network: (SSDN PBX: for PCM-Voice data).

Here the signalling network and voice network use different physical and logical networks. The signalling network can use a very simple RS-232, RS-485 or the TCP/IP as the adaptation layer. Distributed PBX (SSDN), as shown in Figure 5.3 is an example of this type of network.

B. BIS in an Integrated Payload Network: In this type of network, traffic data and signalling data will be transferred through the same physical and logical network. The traffic data will be carried as the payload of the signalling data. This type of signalling network can use RS-232, RS-485 or the TCP/IP as the bearer network. This network is actually same as the network described in serial 1 above, but without a separate voice/bearer network. This option is possible here as BIS would be able to carry both packed and unpacked data as its payload. This scheme is very useful for small system networks. The BIS Integrated Payload Network is shown in Figure 5.4.

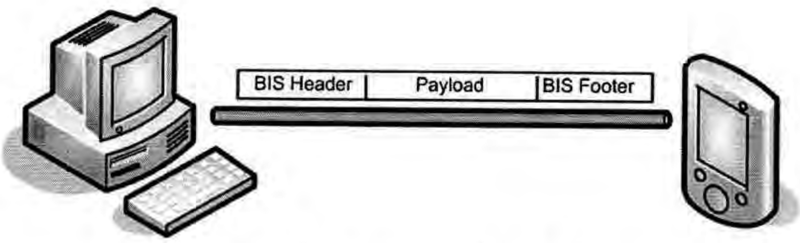


Figure 5.4: BIS-Integrated Path Network.

The network architecture and protocol stack for the BIS have been designed right from the scratch as part of the research. All the parameters are also defined, which will be described in sections 5.5 to 5.7.

5.5 BIS Architecture

The dynamic payload size has actually made it possible to use BIS both in the isolated bearer path and integrated path signalling networks as described in the beginning of this chapter. In the proposed architecture the BIS layer is independent from the transmission layer. This independency of the BIS layer from the transmission layer is utilized in the proposed architecture to gain advantage. The main BIS stack has been designed to include 3 functional layers, which can be associated with any transmission layer such as the RS-232, RS-485 and TCP. The association of the BIS stack over the transport layer of different protocol layers such as RS-232, RS-485 and TCP/IP is shown in Figure 5.5.

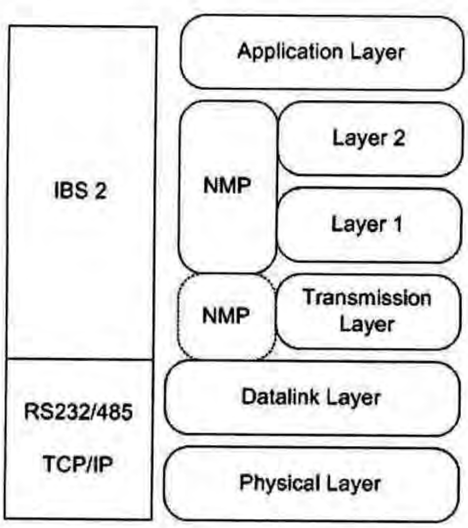


Figure 5.5: Association of BIS Stack over the transport layer.

5.6 BIS Stack

The basic BIS stack has 3 functional layers; layer-1 is the Transmission Adaptation Part (TAP), layer-2 is mainly a network management part (MNP) and layer-3 is the Application Part (AP), where the payload or the massage will reside. The BIS stack is shown in Figure 5.6.

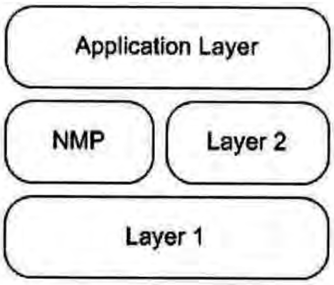


Figure 5.6: The BIS Stack.

5.6.1 BIS-TAP

This is the main part that will make the BIS to adapt with any transport layer below the BIS stack. It consists of the following mandatory parts:

1. System Type
2. Originating System ID
3. Terminating System ID
4. Network Management Message
5. Layer-3 Data or Message Length
6. Layer-3 Data / Message / Payload

The detail of each part is listed in Table 5.1.

Table 5.1: BIS Byte Position and length.

No.	Byte Position	Field Name	Byte Length
1	0	System Type	1
2	1	Originating-System ID	1
3	2	Terminating-System ID	1
4	3	Network Management Message	1
5	4	Layer-3 length	1
6	5- 300	Layer-3 Data	1 - 256

The relative byte position of each part is shown in Figure 5.7.

<table>
<tr><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td></tr>
<tr><td colspan="8">Layer 3</td></tr>
<tr><td colspan="8">Layer 3 Length</td></tr>
<tr><td colspan="8">Layer 2 Message</td></tr>
<tr><td colspan="8">RX. System ID</td></tr>
<tr><td colspan="8">TX. System ID</td></tr>
<tr><td colspan="8">System Type</td></tr>
</table>

Figure 5.7: BIS-Byte Positions.

System Type defines the type of system that will communicate with each other. It has 3 parts. The first part (bit 5-7) defines the System Group, which divides all types of system into some functional groups. We can classify all the systems or devices into 8 System Groups. Table 5.2 summarizes the System Group name and its value.

Table 5.2: System Group.

ID	Group Name
0	Telecommunication
1	Reserved
2	Supervisory Control & Data acquisition
3	User defined
4	Reserved
5-7	Not used

The bit position of the System Type parameters is shown in Figure 5.8.

<table>
<tr><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td></tr>
<tr><td colspan="3">System Group</td><td colspan="2">CID</td><td colspan="2">SID</td><td>TID</td></tr>
<tr><td colspan="3"></td><td colspan="4">Sub Group</td><td></td></tr>
<tr><td colspan="8">System Type</td></tr>
</table>

CID: Control ID, SID: Sub group ID, TID: Transaction ID

Figure 5.8: BIS-System Type Bit position.

Sub Group is the second part of the System Type parameter and is defined by the bit 1 to 4, where bit 3, 4 indicate the Control Type of the system and bit 1 and 2 indicate the System ID. Table 5.3 lists the control ID and their description.

Table 5.3: Control ID (CID).

ID	Description
0	Host priority system
1	Client priority system
2	Both way System
3	Reserved

In Table 5.4 and Table 5.5 system names are separated according to their System Group, and the ID has been defined according to their control mode also.

Table 5.4: System ID of System Group (Telecommunication) – 0.

ID	System Name
0	SSDN
1-3	Not used
4	TDM
5	IP
6,7	Not used

Table 5.5: System ID of System Group (Supervisory Control & Data acquisition) – 2.

ID	System Name
0	Monitoring System
1	Supervisory Control
2	On line Data acquisition
3	Off line Data acquisition
4	Not used
5	Supervisory Control
6	Not used
7	SCADA

Transaction ID is represented by the least bit, which can be Synchronous or Asynchronous. Table 5.6 lists the transaction ID with description.

Table 5.6: Transaction type ID.

ID	Transaction type
0	Asynchronous
1	Synchronous

5.6.2 Layer-2 Message

This is mainly the Network Management layer, which has only one byte of data. As it is managing the network and all the transaction of the upper layer, the adaptation for different bearer layer and usability for different types of network depends on the Layer-2 message. It is the most customizable part of the proposed BIS system. Therefore, any user can define their Message for this layer. All the messages are grouped using the 3 significant bits starting from the MSB. The major message groups are shown in Table 5.7 and the bit position of the BIS Layer-2 Message is shown in Figure 5.9.

Table 5.7: Layer 2 Message type.

ID	Type Name
0	System Management
1	Network Management
2	Reserved
3	Transaction

7	6	5	4	3	2	1	0
Message Type			Message				
Layer 2 Message							

Figure 5.9: BIS-Layer-2 Message Bit position.

The System Management Messages are designed to control the system behavior dynamically. Suppose in a network of On-Line Data Acquisition system a host is controlling all the Clients in a point to multi-point scheme, and the Clients are communicating with the host in a point to point scheme. But if any Client wants extra control or time to communicate with the host than other Clients on a temporary basis, the Client can request the host for the Client-Controlled mode or Both-Way controlled mode. In this way service time for the host will be utilized properly without making any congestion of buffer over-flow at any nodes.

The operation of the BIS System Management Messages will be made clear by the following example. This example will show how the performance improvement takes place with the appropriate change of configuration of network elements.

A network of five Clients and one Host connected by the Hub is shown in Figure 5.10. Performance of the network elements, mainly the Host and the Hub will be evaluated. The network is a Host controlled network and Clients are contributing as percentage of the total traffic given in Table 5.8.

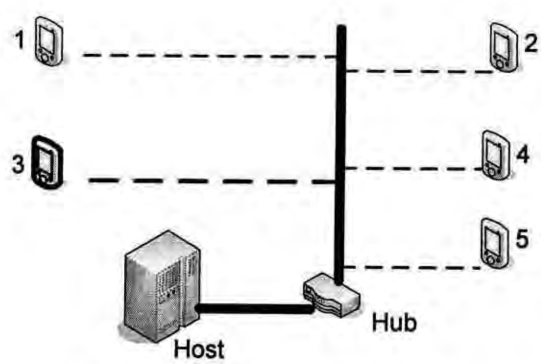


Figure 5.10: BIS Network before applying dynamic Configuration change.

Table 5.8: Network service time and utilization.

Client ID	Traffic Share	Utilization Time (ms)	Service Time (ms)	% Utilization
1	5%	5	50	10%
2	15%	15	50	30%
3	50%	50	50	100%
4	15%	15	50	30%
5	15%	15	50	30%

Total Service Time is the total time allocated by the Host to all the Clients for collecting data. That is,

$$\text{Total Service Time} = \sum_{i=1}^{i=n} \text{Service Time of } i^{th} \text{ Client} \qquad (5.1)$$

Total Utilization Time is the total actual time required by the client to transfer data to the host. That is,

$$\text{Total Utilization Time} = \sum_{i=1}^{i=n} \text{Utilization Time of } i^{th} \text{ Client} \qquad (5.2)$$

% Utilization of the host service time is the ratio of the actual time required by the client to the total service time allocated by the host, therefore from Eq. 5.1 and Eq. 5.2:

$$\% \text{ Utilization} = \frac{\text{Utilization Time}}{\text{Service Time}} \times 100 \qquad (5.3)$$

Using the above equations we can obtain:

Total Service Time = (50+50+50+50+50) = 250 ms (sum of the service times for 5 clients; Table 5.8)

Total Utilized Time = (5+15+50+15+15) = 100 ms

% Utilization = 100 ms/250 ms = 40%

Now we will observe the effect of network reconfiguration by transferring the lower traffic contributing client to an additional virtual network, as shown in Figure 5.11.

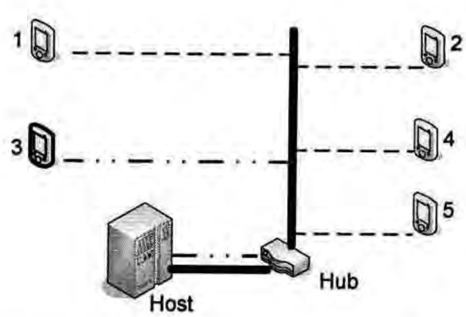


Figure 5.11: BIS Network after applying dynamic Configuration change.

As the network of Figure 5.10 is a Host controlled network, the host allocates its service time to all the Clients equally (for an integrated payload network, it would be bit complicated to allocate the service time as the payload length is variable). Under this scenario, Client-3 will utilize the whole 50ms service time allocated for it, and the other clients will utilize less than the allocated 50ms service time as they do not require 50ms. Therefore, the service time for Client-3 will be fully utilized and the service times will be underutilized for the remaining clients.

In the proposed BIS system, a node may act as a single host and all the other nodes may act as clients (refer to Figure 5.10). However, when a client's service requirement is high, it may be configured to act like another host in presence of the original host by forming a both-way dominating virtual network between them. For example, in Figure 5.11 Client-3 will form such a virtual network with the host. So, under this scenario, the total service time will be divided between the two virtual networks, where Client-3 and Host will be the member of the first network and the second network will have the remaining 4 Clients and the host. In this case the total service time of the host will be distributed as shown in Table 5.9.

Table 5.9 Network Service Time and Utilization.

Client ID	Traffic Share	Utilization Time (ms)	Service Time (ms)	% Utilization	Virtual Network
1	5%	5	15	33%	2
2	15%	15	15	100%	2
3	50%	50	50	100%	1
4	15%	15	15	100%	2
5	15%	15	15	100%	2

Total Service time = (15+15+50+15+15) = 110 ms
Total Utilization time = (5+15+50+15+15) = 100 ms
% Utilization = 100 ms/110 ms = 91%

We can now observe that in this case % Utilization of the host service time becomes (91%) more than double the % Utilization for the network shown in Figure 5.10 (40%). The dynamic allocation or network configuration will be very simple and fast for the SSDNs. Thus by introducing more virtual networks (each of which is separated by the CID) in an SSDN, a maximum of 4 (as CID has 2 bits; $2^2=4$) virtual networks is possible to accommodate at a time.

If we increase one more virtual networks (i.e., now the number of total virtual networks is 3) in the above SSDN (Shown in Figure 6.9), the % Utilization will be 100%, which is shown in Table 5.10.

Table 5.10: Network Service Time and Utilization.

Client ID	Traffic Share	Utilization Time (ms)	Service Time (ms)	% Utilization	Virtual Network
1	5%	5	5	100%	3
2	15%	15	15	100%	2
3	50%	50	50	100%	1
4	15%	15	15	100%	2
5	15%	15	15	100%	2

Using the values from Table 5.10 we can get 100 % utilization as follows:

Total Service Time = (5+15+50+15+15) = 100 ms

Total Utilized Time = (5+15+50+15+15) = 100 ms

% Utilization = 100 ms/100 ms = 100%

The change of %Utilization as a function of number of virtual networks in an SSDN is shown in Figure 5.12.

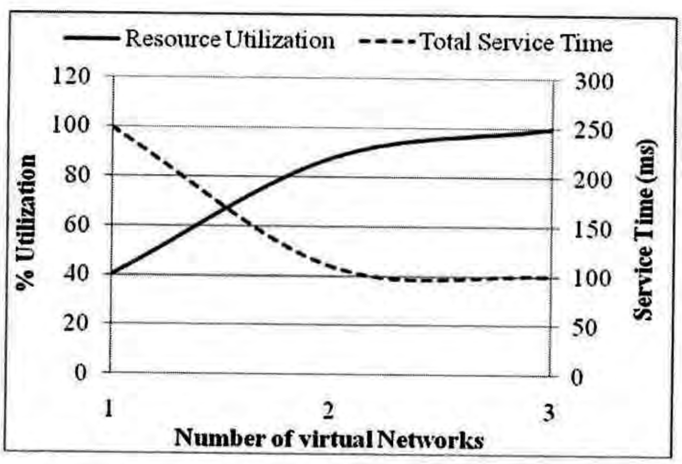


Figure 5.12: Dynamic Network Configuration Vs. Utilization.

From Figure 5.12 we can see that the network utilization is increasing with an increased number of virtual networks configured to suit the required service time and service type. However, as this type of dynamic configuration changes is not possible in the SS7 network, SS7 does not always ensure the maximum utilization of the network resources which is very important in an SSDN. An IP based protocol can manage the resource utilization dynamically by defining the Class of Service (CoS) value in the TCP/IP layer; however, the implementation of this feature would become very complex and even unrealizable in SSDNs to achieve dynamic resource utilization.

The Network Management Messages are to control the network topology or behavior dynamically. To reduce address overhead or to simplify network, remove idle part from the network, Network Management Messages can be used. A network (refer to Figure 5.13), where all the Clients are connected to the Host by star topology (network-a). Suppose, at a particular moment Client 2 needs to act as a Host for Client 4 and 5, so it can send the present host to reconfigure the system first, then to reconfigure the network (network shown in part b of Figure 5.13). After a while, client 2 will be reconnected with the host again and go back to the previous network and system configuration.

Figure 5.13: BIS Dynamic Network Management (before and after change).

By this way user can create virtual networks using a non-TCP/IP transmission layer, such as RS232. Here the hubs are RS-232 hub. More complicated network topology can be possible using very simple transmission layers and simple hardware. As the network topology or the architecture can be reconfigured dynamically, there is no need to change any physical configuration; the only requirement is that the user application needs to support the dynamic network configuration feature.

The Transaction Messages are for application level security. It can control the transaction over an unsecured transmission layer such as RS-232, RS-485. It can also control data transmission between two logical networks under the same physical network. A network (refer to Figure 5.14), where two separate networks are connected with each other by the hubs. If now the network hosted by Client-2 wants to join the network hosted by the main host; Client-2 needs to send some network management messages to the Host, which belongs to a separate network. Without proper transaction messages the Host will not receive it, considering it as a violation of security.

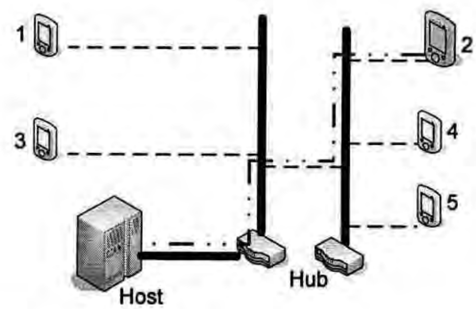


Figure 5.14: BIS Dynamic Network Transaction

5.6.3 Applications Part

In the BIS it is the layer-3 Messages or the Data to be transferred. It has a single byte message or data length. So, for a simple layer-3 message or application part message the length will be small and for the data itself the message length will be very high (a maximum up to 256 bytes). This flexibility gives the BIS the provision for use both in an isolated bearer network (shown in Figure 5.15) and in an integrated bearer network (shown in Figure 5.16).

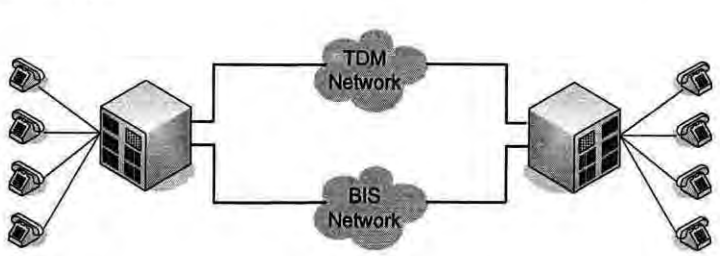


Figure 5.15: SSDN-PBX with separate physical Signalling and voice Network.

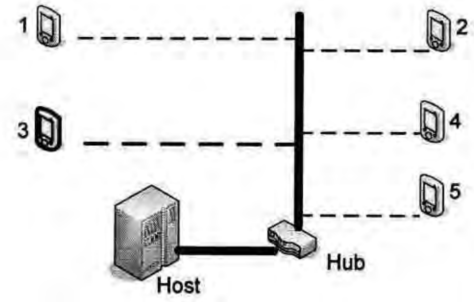


Figure 5.16: SSDN- Data Network: Integrated bearer path network.

In an SSDN – PBX, as the communication is real time and the data (here voice) volume is much higher than the Signalling Data, and as the nature of the voice and signalling data is different (voice can be compressed or continuous data stream) a separate bearer network has been kept. For a network that uses PCM voice data (TDM) and signalling data over the RS-232, these two networks are separated physically (as already shown in Figure 5.15). However, for a network that uses packed voice data (VoIP) and signalling data over a TCP/IP network, it can be made separate by a logical network within a single physical network, which is shown in Figure 5.17.

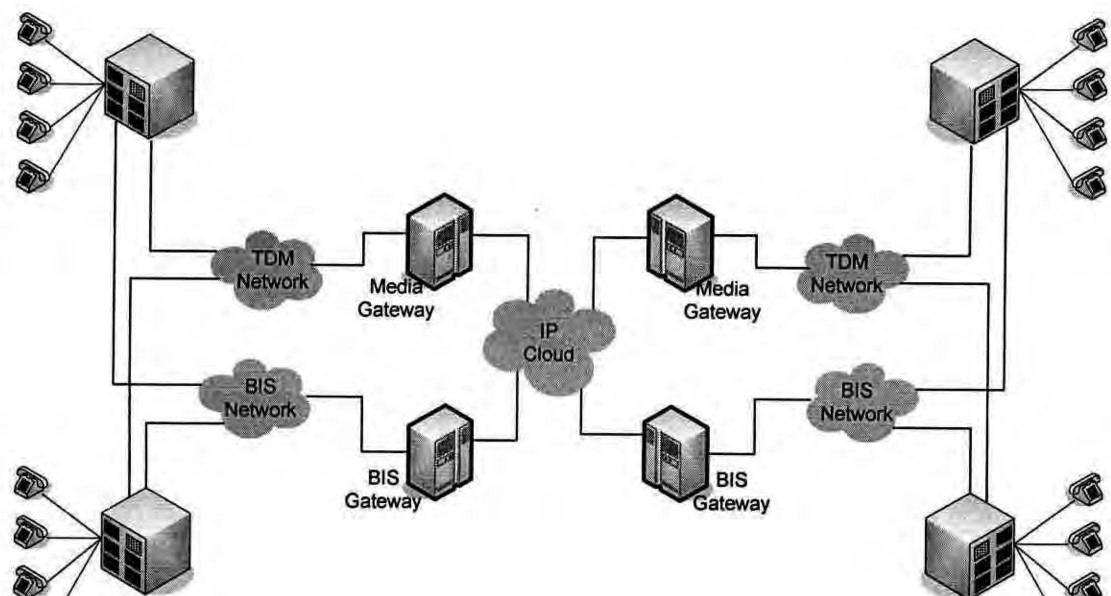


Figure 5.17: SSDN-PBX network over TCP/IP.

5.7 Protocol Conversion

For any type of signalling system protocol conversion is a must to achieve communication with other networks using different signalling systems or protocols. As already mentioned in section 5.5, that the BIS messages can be transported over various physical and transport layers and it is inherently capable of transmitting from one type of transport layer to another without any major changes in the network hardware. This is very true for any type of BIS network. However, in some cases where physical network does not support TCP/IP, RS-232 or RS-485, the protocol conversion is required even in the physical layer.

In the SSDN-PBX network shown in Figure 5.18, the SSDN-PBX is connected with the PSTN through the BIS-SS7 signalling Gateway for the signalling part. As the voice network of both the networks is TDM, so no media gateway is required for the physical and transport layer connectivity. For the BIS-SS7 gateway both physical and transport layer protocol conversions are required, as in this SSDN-PBX network BIS is transported over RS-232 for simplification of the implementation. However, in the PSTN network, the SS7 network is transported over the TDM network. This is true for an ISDN network as well.

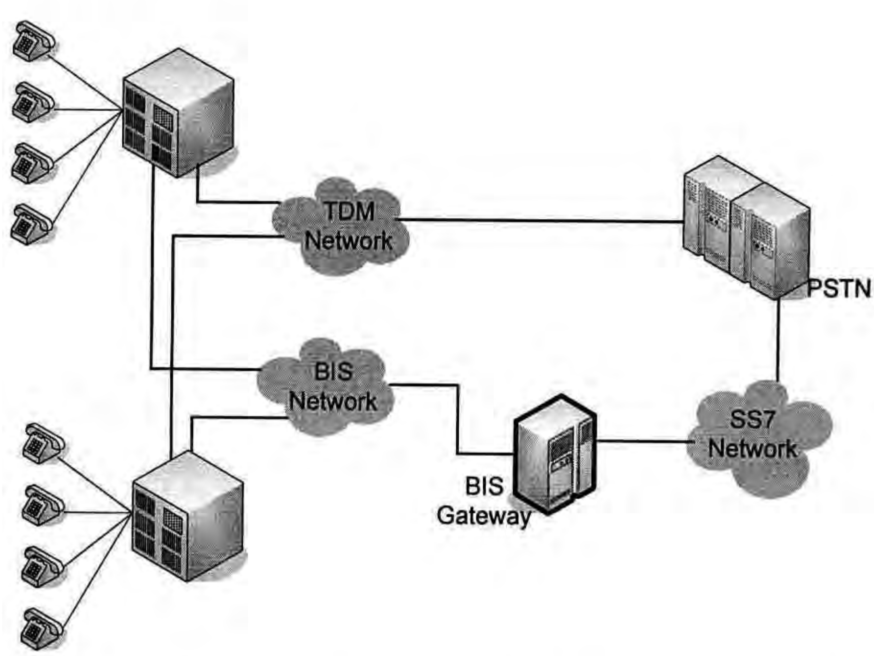


Figure 5.18: BIS Gateway (physical layer/transmission layer).

A SSDN-PBX network is shown in Figure 5.19, where the BIS-SS7/SIGTRAN Gateway works only above the transport layer. This is because the physical network for the PSTN and SSDN is the same and here the voice is the packed data over the TCP/IP network.

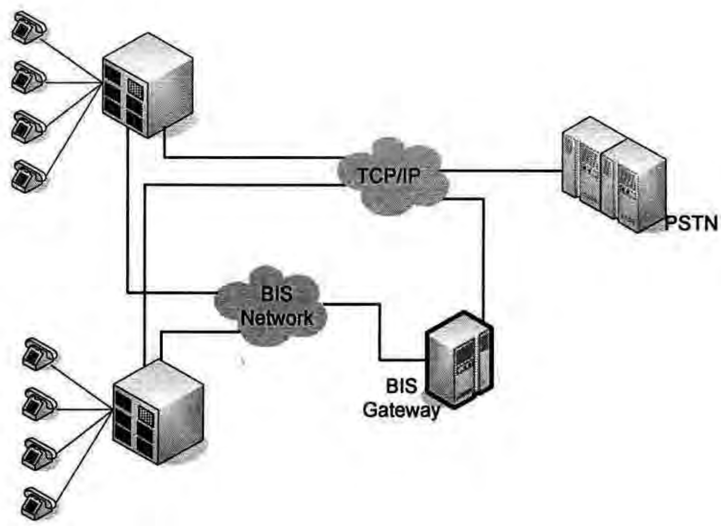


Figure 6.17: BIS Gateway (Signalling only).

So far, the purpose of protocol conversion is explained. A gateway is a protocol converter. A protocol can be converted into two ways: one is at the physical layer and the other is at the logical layer, which is discussed in sections 5.7.1. Section 5.7.2 describes the hardware module of a BIS Gateway and Section 5.7.2 presents the software module for the BIS Gateway.

5.7.1 BIS Gateway

From the example discussed in Section 6.3, it can be seen that whatever be the bearer data and the required media, the type of a BIS-Gateway would depend entirely on the SSDN used and the type of network it gets connected to. We can also notice that BIS-Gateway can be of two types, the first type requires adaptability from the physical layer and the second type needs adaptation only above the transport layer. The first one needs both hardware and software adaptation and the second one needs only adaptation at the software level. The BIS Gateway from the transmission layer is shown in Figure 5.20.

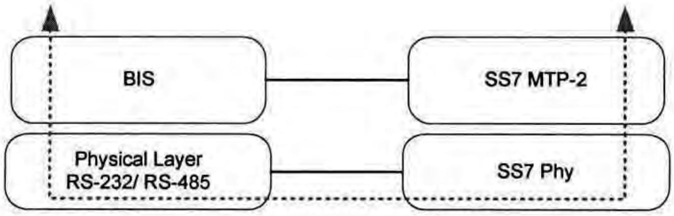


Figure 5.20: BIS Gateway (Transmission Layer Data Flow).

The BIS Gateway only at the application layer is shown in Figure 5.21.

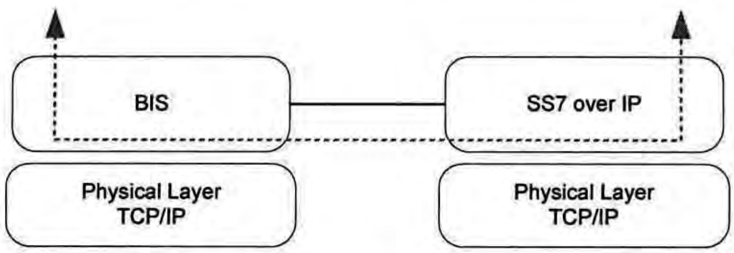


Figure 5.21: BIS Gateway (Signalling Data Flow).

5.7.2 Gateway Hardware Architecture

The hardware functional parts of a generic BIS Gateway is shown in Figure 5.22.

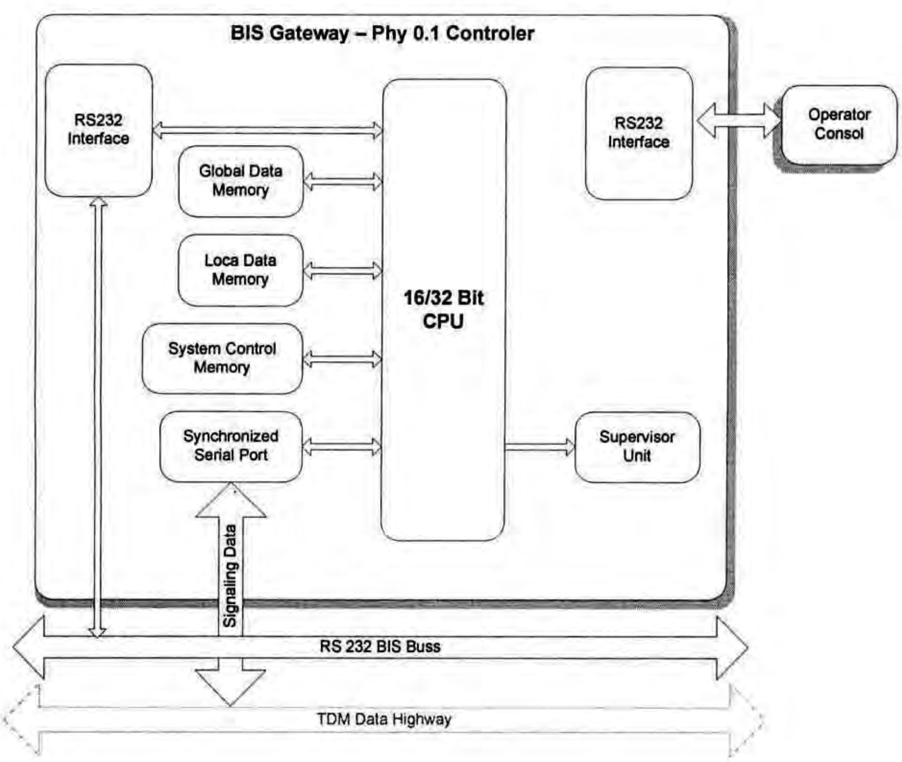


Figure 5.22: The hardware functional parts of a generic BIS Gateway.

Here the CPU interfaces both the RS-232 and the TDM layers through proper interface hardware, for example, the RS-232 level converters and Synchronous Serial Interface module(s). Multiple CPU can be connected in parallel in a load-sharing mode and the control between the CPUs will be done through the RS-232 BIS.

A general mapping diagram for the software module of a BIS Gateway is shown in Figure 5.23.

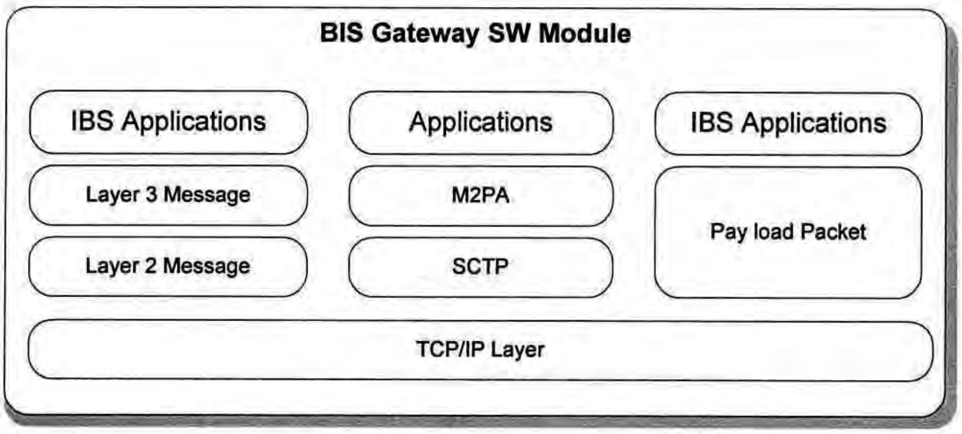


Figure 5.23: BIS Gateway Software Module.

5.8 Capacity Analysis of BIS using RS-232 compared to the SS7 Narrow Band Signalling Link

At present RS-232 interfaces can support up-to 128kbps, which is equivalent of 2 Narrow Band Signalling Links (NBSL) of 64kbps each. Hence it can control more than 1000 ISDN-Pri voice channels [14]. By the grace of present high speed USB interface, the speed of the proposed BIS and SSDNs can be raised up-to 1Mbps using very simple hardwires. Thus the signalling capacity of the BIS SSDNs can handle 7500 PCM Voice Channels at a time. This would be the great advantage of the proposed BIS system.

In the next chapter a detailed implementation of the BIS protocol for an SSDN – Data network will be described with all the necessary hardware and software functionality.

CHAPTER 6

IMPLEMENTATION OF THE PROPOSED BIS SYSTEM

Under the scope of the current research, all possible types of applications for the BIS are not possible to examine and implement. Of the major two types of BIS networks, the "The BIS in an Integrated Payload Network" has been designed and implemented as part of the current research. However, the second one, namely, the "The BIS in an Isolated Bearer Path Network" has been designed only but not implemented in full. An example of an "Integrated Payload network" is an SSDN-Data Network and an example of an "Isolated Bearer Path Network" is an SSDN-PBX network. This chapter describes the detailed implementation of the BIS system for an SSDN – Data network with all the necessary hardware and software functionality. An SSDN-PBX design and possible implementation plan will also be presented.

6.1 SSDN- Data Network: an Integrated Payload Network

This is a Small System Distributed Data Network that uses an integrated bearer network. The transmission layer used here is RS-232. This network has been implemented for data acquisition from several Fuel-Dispenser systems. The physical network connection is shown in Figure 6.1. A complete hardware and software implementation has been accomplished.

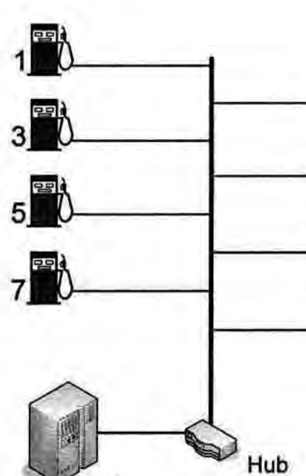


Figure 6.1: Fuel Pump connected by BIS.

6.1.1 Hardware

In this system data was collected from eight Digital Fuel Dispenser Systems. The entire Data Collector and Decoder Module (DCDM) were connected with a host by a RS-232 Hub.

The DCDM: It is the main hardware to communicate with the Fuel Dispenser and the Host, so the DCDN would be considered here as the client. It collects the data from the Fuel Dispenser display unit, decodes the data then encodes it again to fit with the BIS application layer. To keep the synchronization with the Fuel Dispenser and all other DCDMs in the network, every DCDM performs all it functions concurrently. For this parallel processing, the CPU uses one Synchronous Display Data Memory (Synchronous RAM), which is always synchronized with the Fuel Dispenser and the CPU maintains the synchronization with the network by the BIS-Layer 2 messages. The functional hardware block diagram of the DCDM module is shown in Figure 6.2.

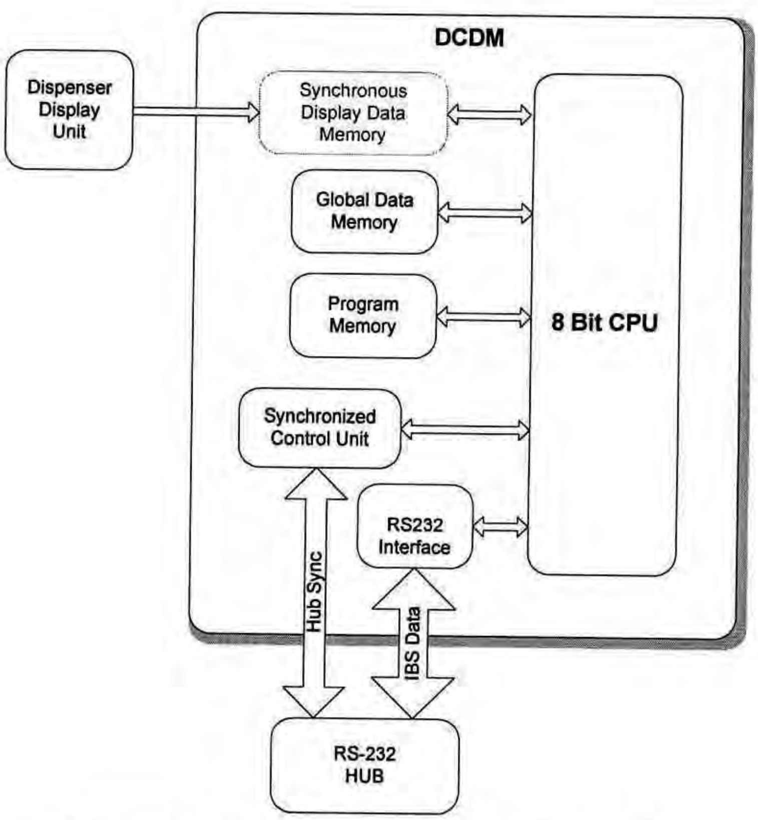


Figure 6.2: Data Collector and Decoder Module.

The RS-232 Hub: It is mainly to connect all the clients (here the DCDM) and the host in a synchronized network. As RS-232 is not capable of making point to multi-point network, this functionality has been performed in the BIS layer-2 by the Hub. It has 2 RS-232 interface modules, one is multiplexed and synchronized for the DCDM connection and the other one is for the Host connection. It is also possible to connect the Host through the synchronized RS-232 interface in a Client style. In that case multiple virtual networks between the Host and clients need to be configured. From the hardware block diagram of the DCDM and the RS-232 Hub (Refer to Figure 6.3) we can see that both hardwares are similar, except the RS-232 Module and the connection between the Synchronized RS-232 interface and Synchronized Control Unit. This coherence of the hardware module used in the BIS network is responsible for easy and simple implementation of the BIS.

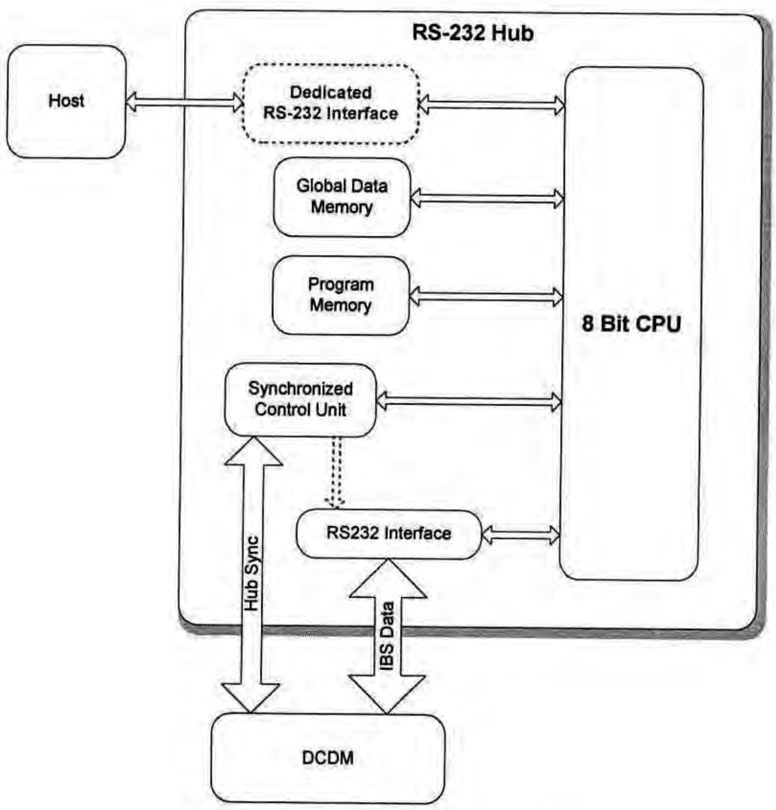


Figure 6.3: RS-232 Hub Module.

Network Architecture: The physical network topology used here is a star topology. It is also a star topology logically, or a point to multi-point host controlled network. Based on all these considerations, the configuration parameters will be as follows:

The BIS stack highlighting the Layer-1 for the SSDN- Data Network is shown in Figure 6.4 and the bit value for the layer-1 is shown in Figure 6.5.

Layer-1 data:

7	6	5	4	3	2	1	0
Layer 3							
Layer 3 Length							
Layer 2 Message							
RX. System ID							
TX. System ID							
System Type							

Figure 6.4: BIS Layer-1 for the Integrated SSDN.

7	6	5	4	3	2	1	0
0	1	0	0	0	0	0	0
2			0		0		0
System Group			CID		SID		TID
0x40							
System Type							

Figure 6.5: BIS System Type Byte for SSDN.

The above values shown in Figure 6.4 and 6.5 are derived, respectively, from the conditions included in Table 6.1 to Table 6.3 that follow.

Table 6.1: System Group value selection for the integrated SSDN.

ID	Group Name
0	Telecommunication
1	Reserved
2	Supervisory Control & Data acquisition
3	User defined
4	Reserved
5-7	Not used

Table 6.2: CID value selection for the integrated SSDN.

ID	Group Name
0	Host priority system
1	Client priority system
2	Both way System
3	Reserved

Table 6.3: TID value selection for the integrated SSDN.

ID	Transaction type
0	Asynchronous
1	Synchronous

Client ID or Dispenser ID: It can be any value from 0 to 255, but for linearity it has been chosen as 0 to 7 as shown in Figure 6.6.

7	6	5	4	3	2	1	0
0	0	0	0	0	x	x	x
0x00 to 0x07							
TX. System ID							

Figure 7.6: BIS Client ID Byte for SSDN

Host ID: As here the system is configured as a host controlled network, and most of the time data will be sent from the Fuel Dispenser to the host, the receiving node is the host. It can be any value between 0 to 255. Here it has been chosen 0x10 (hex) as shown in Figure 6.7.

7	6	5	4	3	2	1	0
0	0	0	1	0	0	0	0
0x10							
RX. System ID							

Figure 6.7: BIS Host ID Byte for SSDN

Layer-2 data: As the network was configured as permanent Host-Controlled network there will be no system management message. It is a monolithic network, i.e., single logical network over a single physical network of the same topology; no Network management message is also required. Only 3 transmission control messages are required but no security messages are required as it is a monolithic network. The Layer 2 byte positions are shown in Figure 6.8.

7	6	5	4	3	2	1	0
Layer 3							
Layer 3 Length							
Layer 2 Message							
RX. System ID							
TX. System ID							
System Type							

Figure 6.8: BIS Layer-2 for the Integrated SSDN.

The Transmission Control Messages are:

1. **No_Data_Available:** If there is no data to transfer to the host at a particular sequence then No_Data_Available Message will be transferred. The bit values for No_Data_Available are shown in Figure 6.9.

7	6	5	4	3	2	1	0
1	1	0	0	0	0	0	1
0xC1							
No_Data_Available							

Figure 6.9: BIS No_Data_Available bit value.

2. **Display_Data:** If there is any display data to be sent, this message will be sent by the DCDM. The bit values of Display_Data are shown in Figure 6.10.

7	6	5	4	3	2	1	0
1	1	0	0	0	0	1	0
0xC2							
Display_Data							

Figure 6.10: BIS Display_Data bit value.

3. **System_Status_Data:** To send the System Status, this message will be sent. In this case the layer-3 data is BIS control data; but for the Display data it will be the payload data, which is the nature of an integrated BIS network. The bit valuesof System_Status_Data are shown in Figure 6.11.

7	6	5	4	3	2	1	0
1	1	0	0	0	0	1	1
0xC3							
System_Status_Data							

Figure 6.11: BIS System_Status_Data bit value.

Layer-3 Data: In this layer, 2 types of data will be transmitted by the DCDM:

1. **Display Data:** In this type of data (refer to Figure 7.12) all the display data will be transferred along with the length of the data.

7	6	5	4	3	2	1	0
Reserved							
2 Digit of Total Price (XX--.--)							
2 Digit of Total Price (--XX.--)							
2 Digit of Total Price (----.XX)							
2 Digit of Quantity (XX--)							
2 Digit of Quantity (--XX)							
2 Digit of Unit Price (XX--)							
2 Digit of Unit Price (--XX)							
Length (8 Byte)							

Figure 6.12: BIS SSDN Layer-3 Display Data distribution

2. **System_Status_Data:** This will be a single byte data (refer to Figure 6.13) with another byte for length. The status values for different status could be as shown in Table 6.4.

7	6	5	4	3	2	1	0
Status Value							
Length (1 Byte)							

Figure 6.13: BIS SSDN Layer-3 System Status Data distribution

Table 6.4: SSDN System Status Values.

Value	Status Description
1	Under Voltage
2	Over Voltage
3	No Power
4	Low Pressure
5	Empty Tank
6	Pump Error
7	Display Error
8	System Error

6.1.2 Software Architecture

We need the following 3 software modules to implement this network:

1. DCDM Firmware
2. RS-232 Hub Firmware
3. Host Software

DCDM Firmware: It is to collect Display Data, decode the segment data to a numeric value, and pack as a 2-digit byte value. Also, it would collect all the system status as a value. Next, it will respond to the Hub signals and send the available data to the hub as required. The flow diagram of this firmware is shown in Figure 6.14.

RS-232 Hub Firmware: The function of the Hub firmware is to collect data from the DCDM in a sequence and send it to the host. The flow diagram is shown in Figure 6.15.

Host Software: Collect Display data along with the DCDM ID, unpack the display data to numeric value again and validate the values with the given conditions (Total Price=Unit Price x Quantity). Besides to display the system status according to the status data sent by the DCDM. The flow diagram of the host software is shown in Figure 6.16.

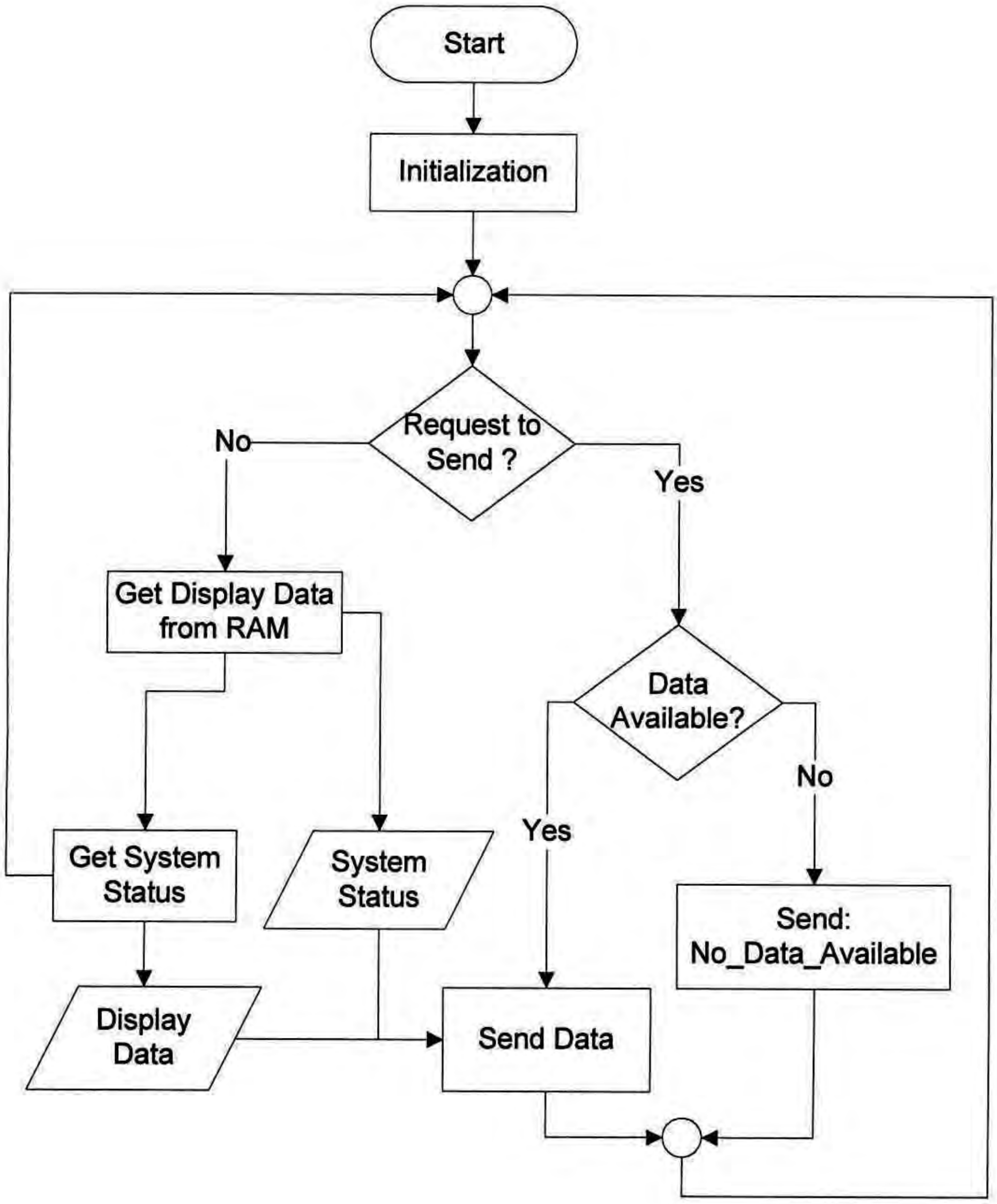


Figure 6.14: BIS SSDN DCDM Firmware Flow Chart

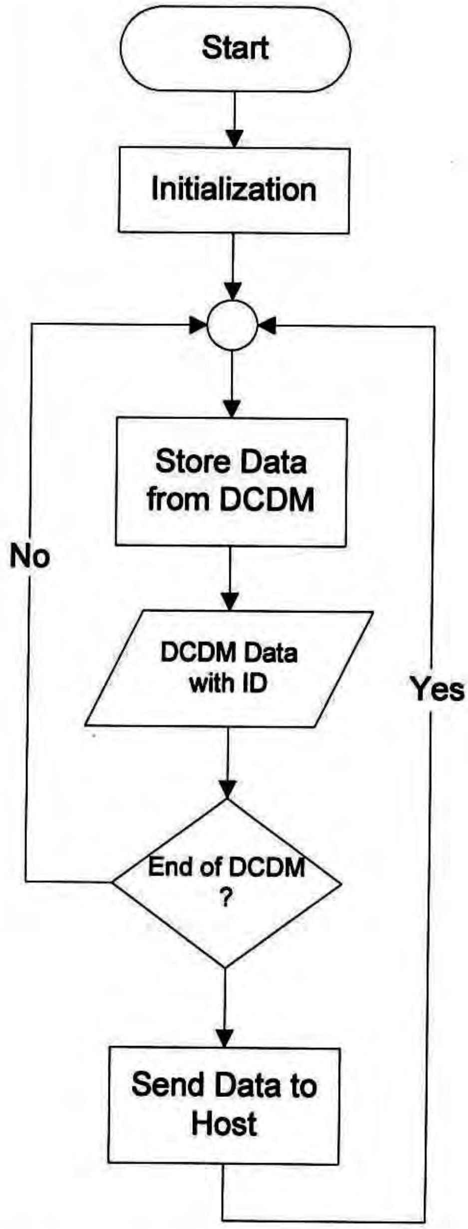


Figure 6.15: BIS SSDN RS-232 Firmware Flow Chart

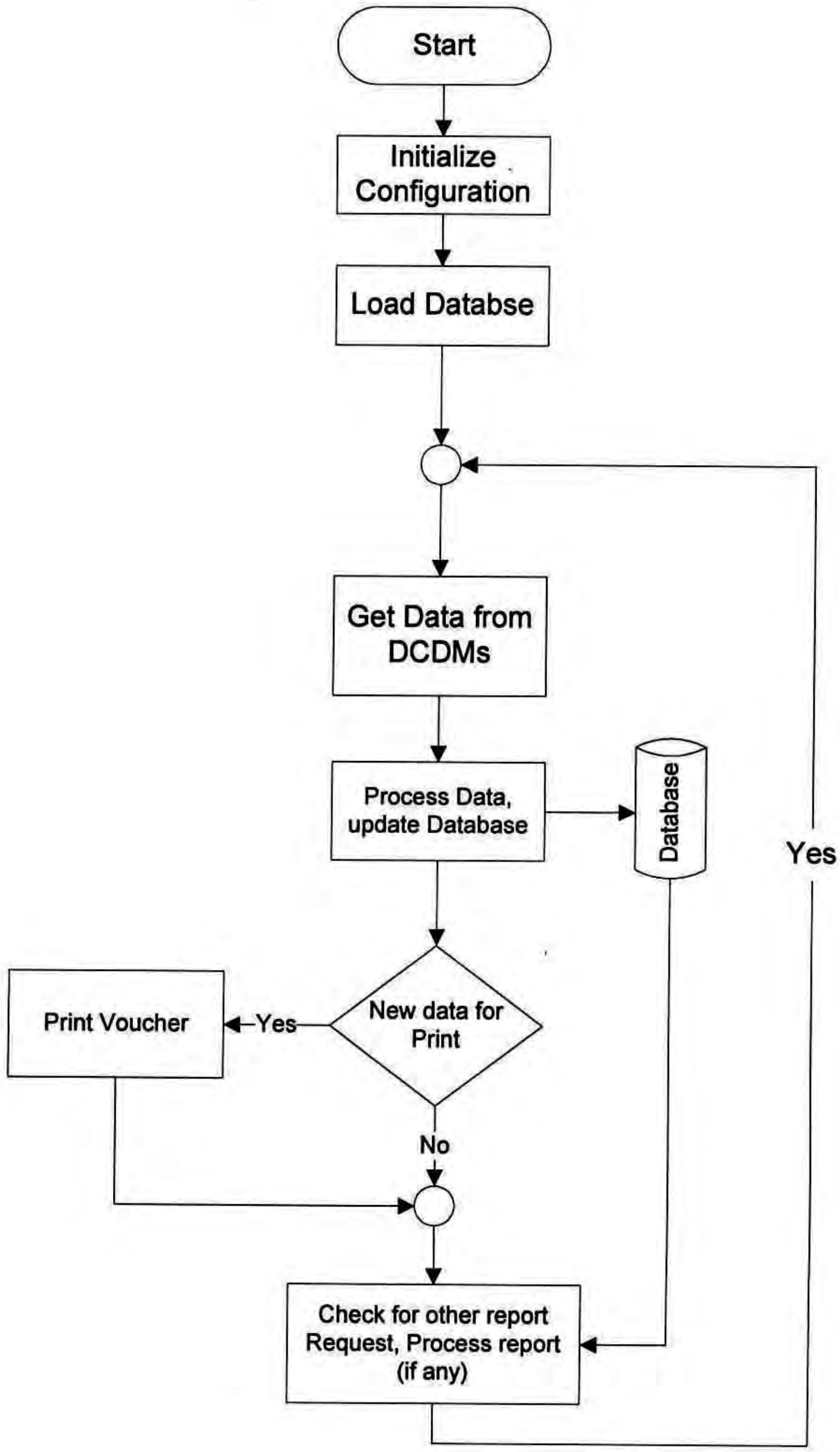


Figure 6.16: BIS SSDN Host Software Flow Chart

6.1.3 Test Scenario

Some test photographs of the hardware and data output are shown in the following pictures from Figure 6.17 to 6.23. Figure 6.17 is the test host interface to collect the data from the RS-232 Hub and the Fuel Dispenser simulation interface to test the Host data collection software is shown in Figure 6.18.

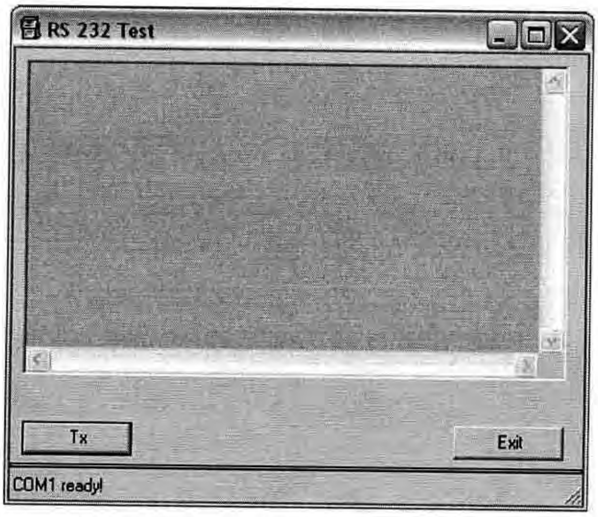


Figure 6.17: BIS Host Data Receiver

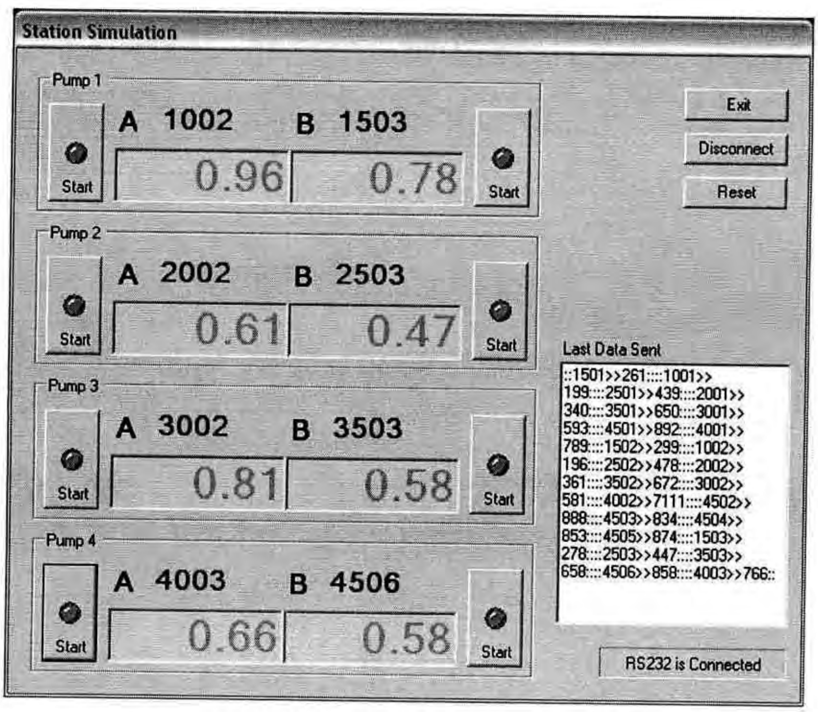


Figure 6-18: BIS Client Simulation Software

The main user interface to collect all the Fuel Dispenser data, print voucher, update cash received, generate various types of report and also to monitor and control the present status of the system is shown in Figure 6.19. The report configuration form is shown in Figure 6.20 and a sample data received by the host is shown in Figure 6.21. The template of the voucher to be printed is shown in Figure 6.22.

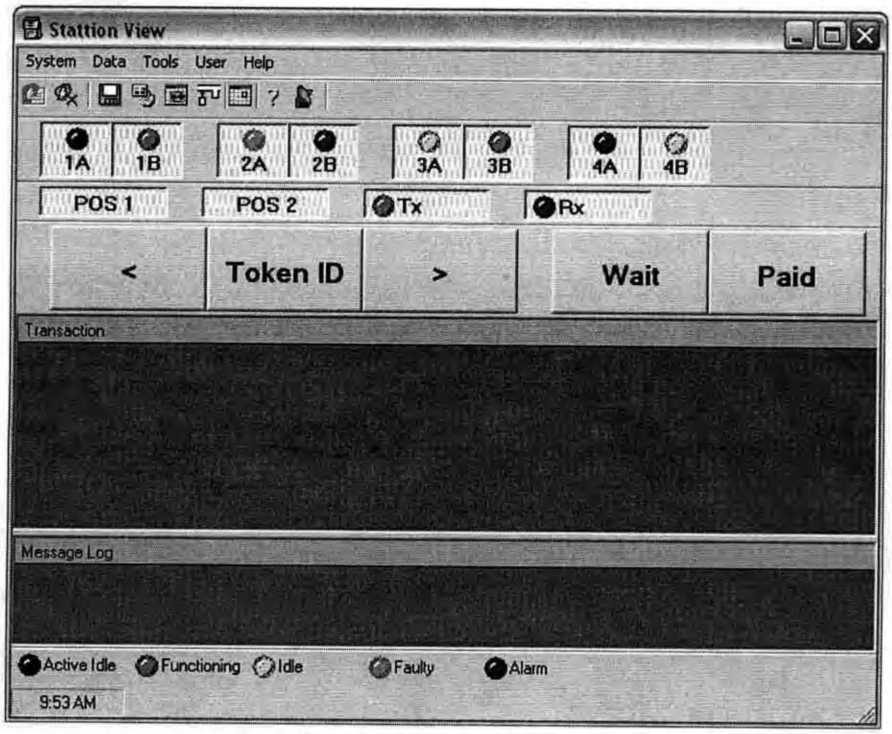


Figure6.19: BIS Host User Interface

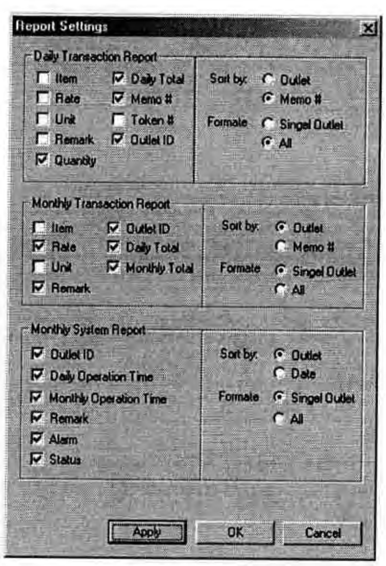


Figure 6.20: BIS Host Report Processing Tool

Outlet ID	Item	Unit	Rate Tk.	Memo #	Token #	Quentity	Amount	Total	Alarm	Remark
12-3-4	CNG	Kg	2.75	235	5	1.45	3.99	77.2		

Figure 6.21: BIS Host Data Area

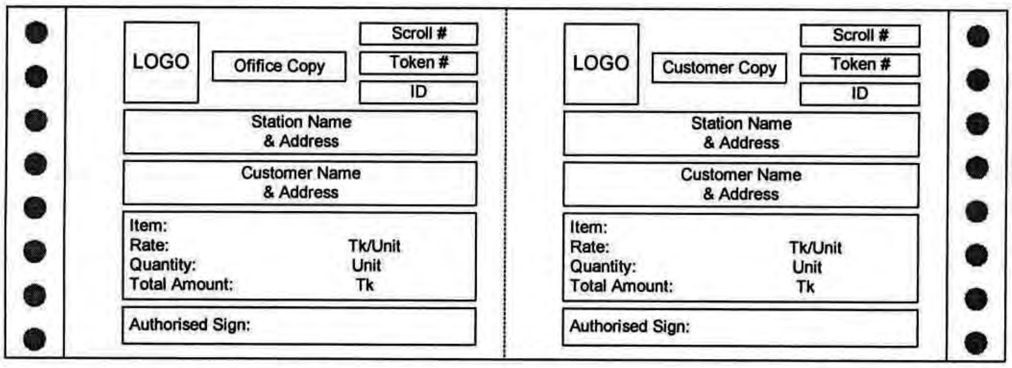


Figure 6.22: BIS Host Voucher Sample/Template

Figure 6.23 includes the pictures of the actual hardware implementation of the designed SSDN Module.

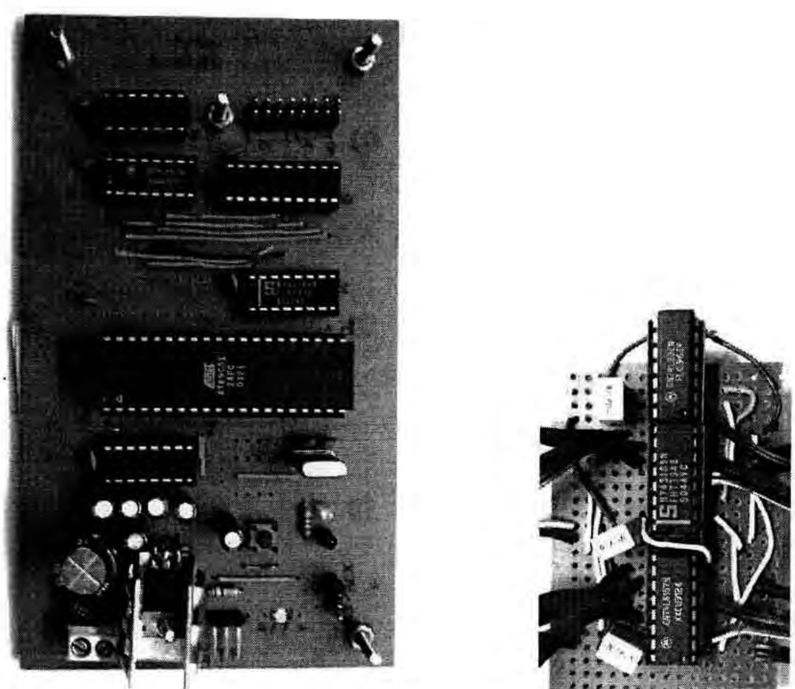


Figure 6.23: SSDN-Data Network Processor and DCDM-Interface Module

6.2 SSDN-TDM PBX: an Isolated Bearer Path Network

This application is based on TDM voice and RS-232 BIS network. Here all the call control signalling among the SSDN-PBX modules will be transmitted through the RS-232 mesh network and the signalling is the BIS. The voice network is a separate TDM (PCM) network (refer to Figure 6.24).

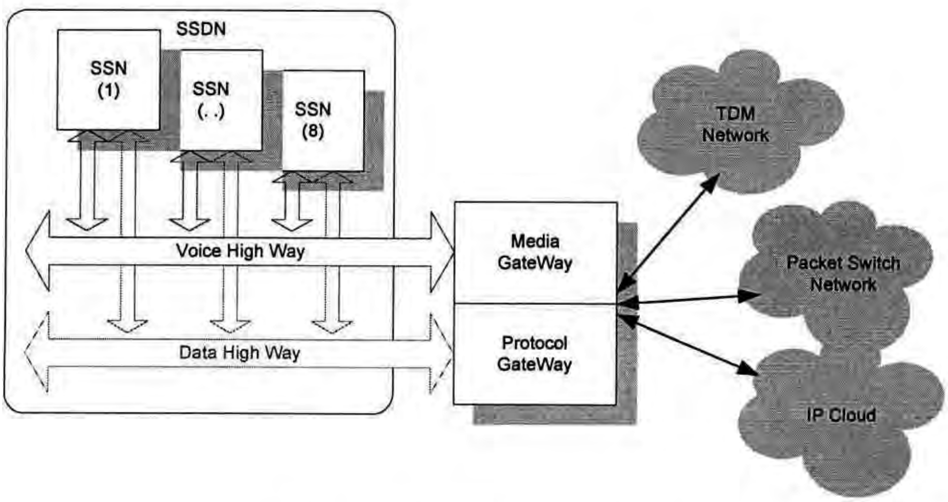


Figure 6.24: BIS SSDN-PBX

6.2.1 Hardware

In the SSDN-PBX, there are several functional modules in the following HW-Module, among which the MPR and CPR are for the Basic Functions of the SSDN-PBX.

1. SSD-MPR
2. SSD-CPR
3. SSD-TNG
4. SSD-SAU
5. SSD-HDU

SSD-MPR: It is the central control or processing unit, one unit of this module is enough to control up to 32 SSDN-CPR modules. It can also be configured as 1+1 redundant mode using 2 modules. The hardware functional blocks is shown in Figure 6.25.

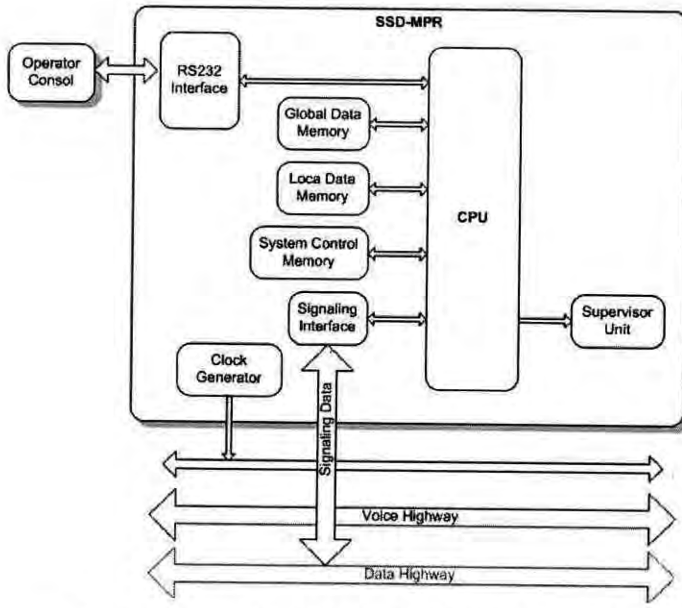


Figure 6.25: BIS SSDN-PBX MPR Module

SSD-CPR: It is the call control unit, 32CPR modules can be installed in one SSDN-PBX system, and one CPR module can handle 4E1 (128 voice channel). This card is completely different from the MPR card. The hardware functional blocks is shown in Figure 6.26.

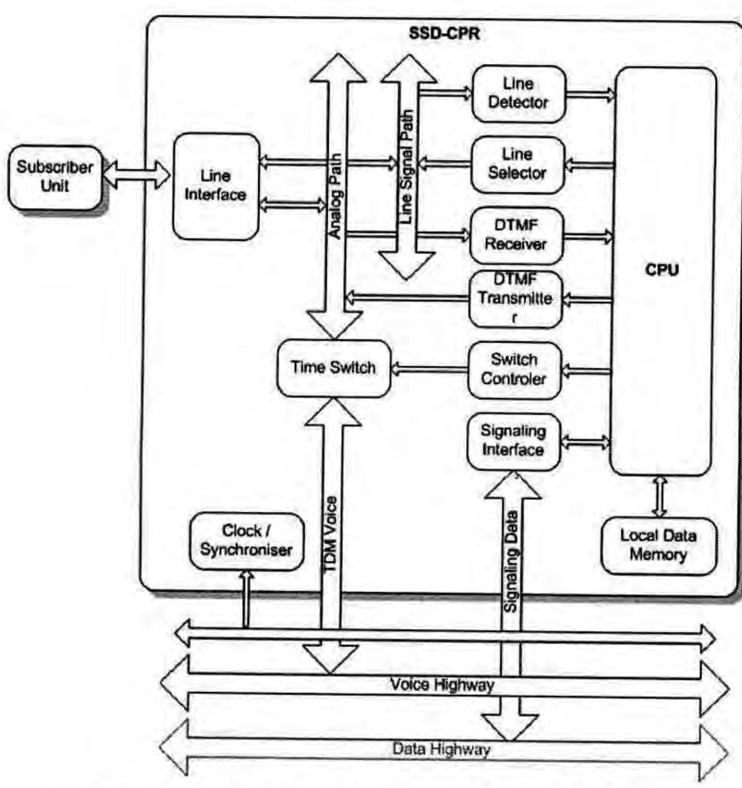


Figure 6.26: BIS SSDN-PBX CPR Module

Auxiliary Modules: Other than the MPR and CPR modules, some auxiliary modules can be used for some auxiliary functionality (refer to Figure 6.27). Such as TNG (Tone Generator) is for various types of tone or announcement generation, SAU (Supervision and Acquisition Unit) is for supervision, billing and other accounting applications and the HDU (Hard Drive Unit) module is for subscriber database storage. If the total system is not too large and does not require the auxiliary functions, these modules can be avoided to reduce the cost.

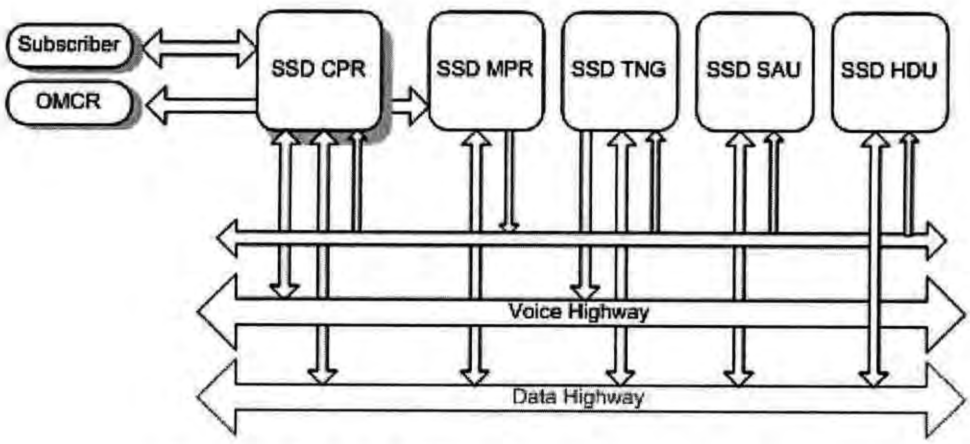


Figure 7.27: BIS SSDN-PBX Auxiliary Modules

***External Network interface modules*:** To connect an SSDN-PBX with the outside telecommunication networks, some gateway modules are needed for gateway functionality, which are:

1. SSD-E1T
2. SSD-N7G
3. IP-GW
4. SSD-GW

The connectivity of the external network interface module of an SSDN-PBX is shown in Figure 6.28.

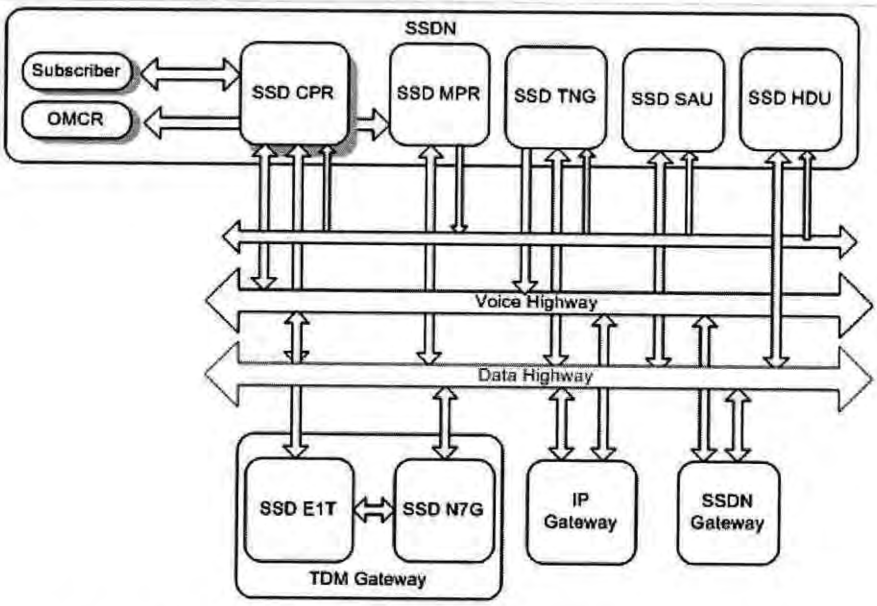


Figure 6.28: BIS SSDN-PBX External Interface Modules

SSD-E1T and SSD-N7G are mainly for the transmission layer conversion, IP-GW is for the RS-432 to IP and TDM to IP conversion, the SSDN-GW is the BIS gateway.

6.2.2 Protocol:

The protocol interface of the SSDN-PBX with external network is shown in Figure 6.29.

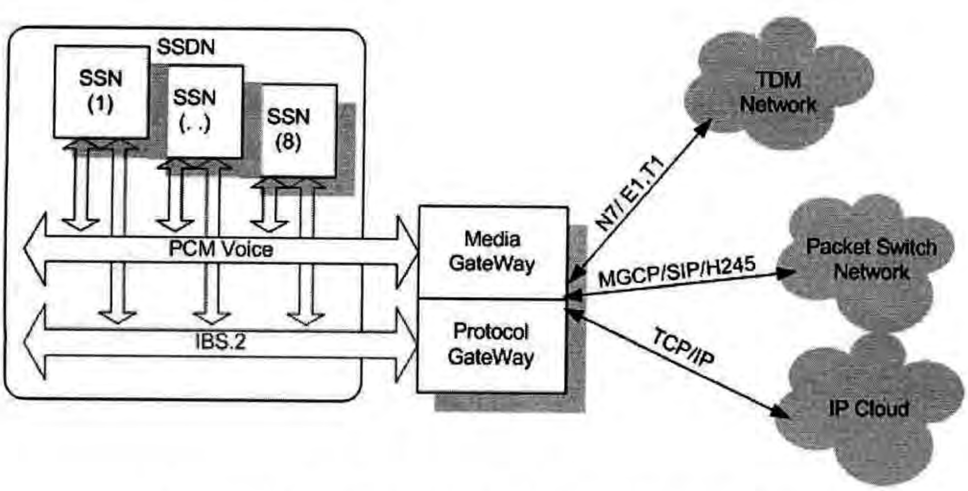


Figure 6.29: BIS SSDN-PBX Protocol Interface

In this chapter we have described the implementation (i.e., the hardware and software modules) of the proposed BIS SSDN systems. The results of the implementation, the BIS network features and advantages will be discussed in the next chapter.

CHAPTER 7

RESULTS AND DISCUSSIONS

In this chapter the results of the practical implementation of the BIS in an SSDN data network has been discussed. A detailed discussion on the advantages of the proposed BIS system over the existing signalling systems has also been presented.

7.1 Results of the BIS in an SSDN Data Network

The necessary hardware and software modules were developed as part of the current research. These modules were used to transfer data from the client to the host using the BIS system. Data transmission time has been measured; performance of the BIS system has been tested by changing various network parameters.

Data transmission – reception between the client to hub and hub to host has been tested successfully. One basic feature of the BIS- dynamic network configuration has been tested in the following 3 network configurations:

1. All clients are in a single virtual network with the hub and host as shown in Figure 7.1

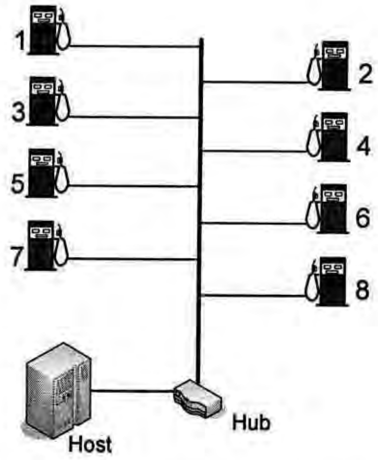


Figure 7.1: SSDN-Data network

2. Client 5 and 6 are kept in a different virtual network (red line) with the hub and host, keeping all the remaining clients under another virtual network (black line), as shown in Figure 7.2

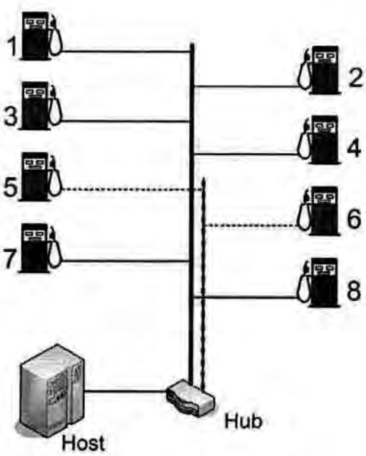


Figure 7.2: SSDN-Data network, two virtual network

3. Client 8 of the previous network (Figure 7.2) forms a separate virtual link with the host through the hub (green line) as shown in Figure 7.3.

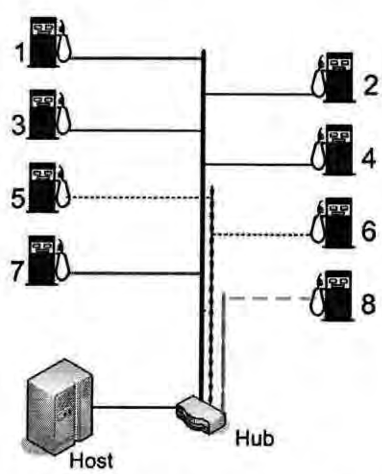


Figure 7.3: SSDN-Data network, three virtual network

The results obtained after changing the network configuration (Figure 7.2), is shown in Table 7.1. Table 7.2 on the other hand, includes the results for the network configuration shown in Figure 7.3. The test was done by collecting display data from each client at an RS-232 link speed of 9600bps. The time was calculated by the host receiver interface. As the Fuel Dispenser functional cycle (fuel delivery time) is very large compared to the data transmission time, different traffic patterns were generated by the simulation tool (the developed software module). Traffic sharing was controlled and set manually, by the software (Figure 6.18) demonstrated in section 6.18 of chapter 6.

Per client Display Data Transfer Time can be calculated using the following equation.

$$\text{Total Data Transfer Time} = \text{Total Data Length} \times \frac{1}{\text{Data Transfer Rate}} \quad \ldots\ \ldots\ \ldots (7.1)$$

In Figure 7.4, Total Data Length = 13 Bytes = 104 bits

7	6	5	4	3	2	1	0
Reserved							
2 Digit of Total Price (XX--.--)							
2 Digit of Total Price (--XX.--)							
2 Digit of Total Price (----.XX)							
2 Digit of Quantity (XX--)							
2 Digit of Quantity (--XX)							
2 Digit of Unit Price (XX--)							
2 Digit of Unit Price (--XX)							
Length (8 Byte)							
Layer 2 Message (Display Data Available)							
RX. System ID							
TX. System ID							
System Type							

Figure 7.4: BIS SSDN Byte distribution for Display_Data

Data Transmission Rate = 9600 bit/Sec

Per client Display Data Transfer Time = 104 /9600 = 10.83mS

Again, if the client does not have any display data to send, it will send No_Data_Available message. From Figure 7.5 we can see that, the total data length of No_Data_Available Message is 4 Bytes (32 bits). Therefore in this case the Total Data Transfer Time will be:

Per client Display Data Transfer Time = 32 /9600 = 3.33 mS

7	6	5	4	3	2	1	0
Layer 2 Message (No_Data_Available)							
RX System ID							
TX System ID							
System Type							

Figure 7.5: BIS SSDN Byte distribution for No_Data_Available

The System_Status_Data Message (refer to Figure 7.6) is of 6 Bytes length, therefore the transmission time for this message will be:

Per Client Display Data Transfer Time = 6x8 /9600 = 5 mS

7	6	5	4	3	2	1	0
System_Status							
Length (1 Byte)							
Layer 2 Message (System_Status_Data)							
RX System ID							
TX System ID							
System Type							

Figure 7.6: BIS System_Status_Data Byte Distribution

As Clients 5 and 6 send No_Data_Available message, rather than the Display_Data every cycle, and Client 8 sends the System_Status, the time required and allocated will be as shown in Table 7.1.

Table 7.1: Network Time distribution of Network shown in Figure 7.1

Client ID	Utilization Time (ms)	Service Time (ms)	% Utilization
1	10.83	10.83	100%
2	10.83	10.83	100%
3	10.83	10.83	100%
4	10.83	10.83	100%
5	3.33	10.83	30.75%
6	3.33	10.83	30.75%
7	10.83	10.83	100%
8	5.0	10.83	46.17%

From the Table 7.1:

Total Utilization Time = 10.83+10.83+10.83+10.83+3.33+3.33+10.83+5.0 = 65.81ms

Total Service Time = 10.83ms x 8 = 86.64ms

% Utilization for the network of Figure 7.1 = 64.14ms /86.64ms = 76%.

Now, by using the dynamic network configuration option, the network was reconfigured as shown in Figure 8.2. Also, the resource service time was redefined by the host as shown in Table 7.2.

Table 7.2: Network Time distribution of Network shown in Figure 7.2

Client ID	Utilization Time (ms)	Service Time (ms)	% Utilization
1	10.83	10.83	100%
2	10.83	10.83	100%
3	10.83	10.83	100%
4	10.83	10.83	100%
5	3.33	3.33	100%
6	3.33	3.33	100%
7	10.83	10.83	100%
8	5.0	10.83	30.75%

From the Table 7.1:

Total Utilization Time = 65.81ms

Total Service Time = 10.83ms x 6 + 3.33ms x 2 = 71.64ms

% Utilization for the network of figure 8.1 = 64.14ms /71.64ms = 91.86%.

Now, again the network was reconfigured dynamically as shown in Figure 7.3, and the resource service time was redefined by the host as shown in Table 7.3.

Table 7.3: Network Time distribution of Network shown in Figure 7.3

Client ID	Utilized Time (ms)	Service Time (ms)	% Utilization
1	10.83	10.83	100%
2	10.83	10.83	100%
3	10.83	10.83	100%
4	10.83	10.83	100%
5	3.33	3.33	100%
6	3.33	3.33	100%
7	10.83	10.83	100%
8	5.0	5.0	100%

Total Utilization Time = 65.81s

Total Service Time = 10.83ms x 5 + 3.33ms x 2 +5.0 = 65.81ms

% Utilization for the network of figure 8.1 = 64.14ms /64.14ms = 100%.

7.2 Performance Comparison and Validation

It was not possible to compare the result of the implementation of BIS as there is no similar signalling system that can be used for the same SSDN. However, the performance of the application implemented in this work has been compared with the preferred performance as discussed in sections 5.6.2 of chapter 5.

The above measured results obtained in section 7.1 and the theoretical % Utilization obtained from calculation in section 5.6.2 have been summarized in Table 7.4.

Table 7.4: Network %utilization

Number of Virtual Network	% Utilization (Theoretical)	% Utilization (Actual)
1	40%	76%
2	91%	91.86%
3	100%	100%

In both the cases, the BIS network dynamic configuration performances have been analyzed with respect to the change of number of virtual networks. The theoretical and actual %Utilization as a function of number of virtual networks is shown in Figure 7.5.

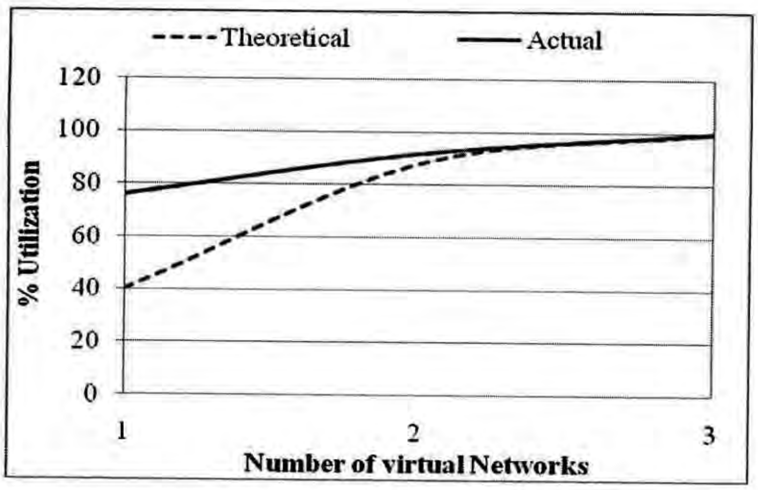


Figure 7.5: Practical Vs. Theoretical Utilization.

It can be seen from the Figure 7.5 that, with less number of virtual networks the actual %Utilization is higher than the theoretical one. It is because, the % of traffic share of each client in the network considered in section 5.6.2 of chapter six is not same of that in the actual network used for the comparison. It can also be seen, when the number of virtual network is more than two, the actual %Utilization is more or less the same as the theoretical one.

7.3 BIS Advantages

The structure of the BIS as described in chapter 5 shows the simplicity, adaptability, versatility, flexibility and easy implementation of it in any type of SSDNs. From the capacity, security and resource management point of view, the BIS can also be a proven solution for highly customized networks. The following sections highlight the advantages, capacity issues of the proposed BIS System and the comparison with other signalling systems.

7.3.1 Simplicity

BIS is very easy and simple to implement for the following reasons:

- BIS can be used independently over RS232/485 as physical-transmission-data link layer.
- BIS can work like any application part over the TCP/IP based system.
- BIS can dynamically be synchronous or asynchronous according to system requirement
- It can be self synchronized to use over an asynchronous media
- It can be fully asynchronous for faster operation.
- BIS can manage the network along with its application in the same module or in different module.
- BIS Module is highly flexible to be customized, so it can be used in SSDN-telephony, IP-telephony and other applications like supervisory or data acquisition systems.

7.3.2 Inherent Advantages

The BIS has the following advantages, which are inherent to the basic design of the BIS architecture:

- BIS is totally independent from the type of buss used for the data transfer.
- Data both voice and digital loss-less data, packed and non-packed data transfer is possible using the BIS.
- Dynamic payload size made possible to use BIS both in the integrated and separate signalling network.
- BIS can be associated with any transmission layer such as the RS-232, RS-485 and TCP.
- Simple architecture and easy implementation made it possible to use without applying any advance level of hardware, software or routing knowledge.
- A huge verity of systems can be connected using BIS based on the System Type parameter. System can of different type in nature, application, data transmission nature etc.

7.4 Maximization of Resource Utilization

The system behavior of a BIS network can be changed dynamically. In order to maximize the network and host resource utilization, clients and host can form multiple virtual separate networks, which is not possible in an SS7 or TCP/IP protocol without implementing complex routing and Class of Service (COS) policy.

7.5 Network Simplification

By Network Management Messages in a BIS network, network topology or behavior can be changed dynamically. If there is any idle part in the network, we can remove it from the network by the dynamic network configuration feature of the BIS system.

7.6 Virtual Network using not TCP/IP transmission Network

Under the proposed BIS system, users can also create virtual networks using a non-TCP/IP transmission layer, such as RS232. This is not possible in an SS7 network, only fixed nailed up connection is possible but needs configuration changes all over the network.

7.7 Simple Network Maintenance and Configuration

In the proposed BIS system, more complicated network topology can be possible using very simple transmission layers and simple hardware. As in BIS, the network topology or the architecture can be reconfigured dynamically, there is no need to change any hardware configuration, only the user application need to support dynamic network.

7.8 Security in a non-secured transmission layer

Transaction Messages can control the transaction over an unsecured transmission layer such as RS-232, RS-485. It can also control data transmission between two logical networks under the same physical network.

7.9 Simple Protocol Conversion

As already mentioned that BIS can be transported over various physical and transport layers, it is inherently capable of transmitting from one type of transport layer to another without any major changes in the network hardware. Protocol conversion is required in the physical layer only where physical network does not support TCP/IP, RS-232 or RS-485.

7.10 Huge Capacity using low profile interface hardware

As present RS-232 interfaces can support up to 128kbps, which is equivalent to 2 NBSL (narrow band signalling link of SS7) and hence can control more than 1000 ISDN-Primary voice channels. By the grace of present high speed USB interface, this speed can be raised up to 1Mbps using very simple hardware, and hence the signalling capacity can cope with a system having 7500 Channels.

CHAPTER 8

CONCLUSIONS AND SUGGESTIONS FOR FUTURE WORK

Any development of a new signalling system or protocol is a time consuming process and requires a subsequent detailed test, modifications and standardizations. This thesis covers only the initiation of the process to establish the definition, development and some examples for implementation of the proposed BIS system. The summery of the current research is included as conclusions in section 8.1 and the suggestion for future work are included in section 8.2.

8.1 Conclusions

- In this work a new signalling system named "Bus Independent Signalling" system BIS has been proposed.
- All the parameters of the BIS have been defined.
- A generic structure of the BIS protocol Stack has been defined and the protocol layers have been described in detail.
- Implementation of the BIS over RS-232/RS-485 and TCP/IP as the transmission layer, have been described with all the necessary hardware and software modules.
- Practical Implementation of BIS has been demonstrated by a SSDN-Data Network using the RS-232 as the transmission layer.
- A simple group of BIS messages have been defined and described that is used in the implementation of the BIS SSDN-Data network.
- Some hardware and software modules have been developed based on the BIS in an Integrated Payload network over the RS-232.
- The BIS Gateway Hardware and Software architecture have been proposed.
- Signalling Capacity of a BIS Network over RS-232 transmission layer has been compared with that of the SS7 system.

- Resource utilization of the BIS network has been calculated and analyzed for an Integrated Payload Network.
- Resource utilization of the implemented BIS SSDN-Network has been measured and compared with the theoretical results.
- Based on all the developments that have already been undertaken and the parts yet to be done to make the BIS a complete solution for flexible SSDNs, all the developments can be put in a road map as shown in Table 8.1.

Table 8.1: BIS Roadmap.

Phase	Development	Release/Version/ Requirement
1	BIS proposal, generic structure, Preliminary Implementation on RS-232 in a integrated physical network	BIS-RS232
2	BIS implementation of SSDN-PBX, using separate physical network of RS-232 and TDM network	BIS-TDM
3	BIS implementation over RS-485 and TCP/IP	BIS-1.0
4	BIS gateway hardware and software implementation for SS7	BIS-SGW
5	BIS gateway implementation for SIGTRAN and other VOIP protocol	BIS-IGW
6	BIS expansion for larger network, Enhanced security and scalability	BIS-e
7	BIS standardization by Standardization authority	Standardization
8	Application development for BIS	BIS-Application

8.2 Suggestions for Future Work

Following future developments and extensions of the BIS may be carried out in future:

- A complete description of the BIS layer-2 and Application layers need to be defined and described in detail.
- All type of applications needs to be implemented and tested using the BIS protocol stack.

- A complete set of the BIS messages need to be defined and described for different types of network and applications.
- The BIS gateway hardware and software need to be implemented and tested.
- A complete benchmark of the BIS with the other existing Signalling systems needs to be done.
- The BIS over other transmission layers like, ATM need to be defined, described and implemented.
- Standardization of the BIS from the Standardization Authority need to be done.

REFERENCES

[1] http://en.wikipedia.org/wiki/Proprietary_protocol, November 2008

[2] http://en.wikipedia.org/wiki/Signalling_System_7#History, November 2008

[3] http://en.wikipedia.org/wiki/FBus, November 2008

[4] http://www.embedtronics.com/nokia/fbus.html#part1, November 2008

[5] http://en.wikipedia.org/wiki/MBus_(Nokia) , November 2008

[6] http://en.wikipedia.org/wiki/Meter-Bus, November 2008

[7] http://www.m-bus.com/info/mbuse.html, November 2008

[8] Russell, Travis (2002). Signalling System #7 (4th Edition ed.). New York: McGraw-Hill. ISBN 978-0071387729.

[9] GSM Switching, Services, and Protocolr. by-Joerg Eberspaecher, Hans-Joerg Voegel, Christian Bettstetter, Publisher: Wiley. 2nd edition, 978-0471499039

[10] Q.705, Signalling network structure.

[11] Introduction to SS7; SCP, SCP, STP, and SS7 Protocol Layers Operations. by Lawrence Harte, Richard Dreher, David Bowler, Toni Beninger. # Publisher: Althos, ISBN-13: 978-1932813029, (March 2004)

[12] Q.703, Signalling link.

[13] Q.701, Functional description of the message transfer part (MTP) of Signalling System No. 7.

[14] Q.784.1, ISUP basic call test specification: Validation and compatibility for ISUP'92 and Q.767 protocols

[15] Q.716, Signalling System No. 7 - Signalling connection control part (SCCP) performance

[16] http://www.openss7.org/sigtran.html, November 2008

[17] http://www.isoc.org/briefings/017/index.shtml, November 2008

[18] http://www.openss7.org/sigtran.html, November 2008

[19] http://www.openss7.org/stack.html, November 2008

[20] http://www.protocols.com/pbook/VoIPFamily.htm, November 2008

[21] http://en.wikipedia.org/wiki/H.323, November 2008

[22] http://en.wikipedia.org/wiki/Session_Initiation_Protocol, November 2008

[23] http://www.ietf.org/rfc/rfc3261.txt, November 2008

[24] http://en.wikipedia.org/wiki/RS_485, November 2008

[25] http://en.wikipedia.org/wiki/RS-232, November 2008

[26] http://www.camiresearch.com/Data_Com_Basics/RS232_standard.html, November 2008