"Design of Sigtran Protocol Suit for the SS7 over IP Signaling Gateway"

A MAJOR THESIS

SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENT FOR THE DEGREE OF

MASTER OF ENGINEERING

IN

ELECTRONICS & COMMUNICATION

ENGINEERING

BY

BAL KRISHNA KESHARWANI

Roll No. 9111

UNDER THE GUIDANCE OF

Mr. Rajesh Rohilla

ELECTRONICS & COMMUNICATION ENGINEERING
DELHI COLLEGE OF ENGINEERING
(UNIVERSITY OF DELHI), DELHI

CERTIFICATE

This is to certify that ***Mr. BAL KRISHNA KESHARWANI*** has carried out this thesis work under my supervision. The project entitiled "***Design of SIGTRAN Protocol suit for the SS7 over IP signaling gateway",*** which is being submitted in fulfillments of the requirements for award of the degree of Master of Engineering in Electronics and Communication in the Department of Electronics and Communication, Delhi College of Engineering, University of Delhi is a record of bonafide work done by him under my supervision and guidance.

It is also certified that the dissertation has not been submitted elsewhere for any other degree to the best of my knowledge and belief.

(Prof. ASOK BHATTACHARYYA)
H.O.D.,
ECE Dept.,
Delhi College of Engineering
Delhi – 110042

(RAJESH ROHILLA)
Project Guide,
Asst. Prof., ECE Dept.,
Delhi College of Engineering,
Delhi - 110042

ACKNOWLEDGEMENT

The satisfaction and euphoria that accompanies the successful completion of any task would be incomplete without a mention of the people who made it possible, whose constant guidance and encouragement crown all the efforts with success.

I am grateful to **Mr. RAJESH ROHILLA** (Asst. Prof., ECE Dept. DCE) for providing me an opportunity to undertake this project and for being my project guide for taking keen interest in my work and for his constant monitoring and invaluable guidance and support through out the course of my project. I profusely thank him for having patience to clear my doubts and channelise my efforts. His cheerful disposition made my work all the more enjoyable.

I am also grateful to **Prof. ASOK BHATTACHARYYA (**H.O.D., ECE Dept. DCE) and other faculty members who helped me directly or indirectly for the completion of this dissertation.

Last, but not the least I wish to express out sincere gratitude to one and all who have contributed their suggestions and encouragement in successful completion of this project work.

BAL KRISHNA KESHARWANI
College Roll No. 13/EC/03
University Roll No. 9111
Delhi College of Engineering
University of Delhi, Delhi.

Table of Content

Table of Figures

CHAPTER 1

1. INTRODUCTION

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 a 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 networks and IP networks. Fixed and mobile telephone network operators are designing all IP architecture, which includes support for signaling system 7 (SS7) signaling protocols. IP provides an effective way to transport user data and for operators to expand their networks and build new serves. Mass popularization of communication services, including short message services (SMS), contribute to the rapid growth of signaling networks. As such, more scalable and flexible networks, such as the Internet and its technologies, are needed. The benefits of using and IP network in comparison to a legacy time division multiplex (TDM) based network include:

- Ease of deployment – When using signaling gateways (such as access service group [ASG], 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 signaling elements.
- Better efficiency – SIGTRAN over IP network doesn't require the physical E1/T1 over synchronous digital hierarchy (SDH) rings. Using new technologies like IP over SDH and IP over fiber, for instance, can achieve much higher throughput.

- Higher bandwidth – SIGTRAN information over IP does not constrain to link capacity as it does in the SS7 network. The IP network is much more flexible than the TDM-based legacy network.
- Enhanced services – Implementing a core IP network facilitates a variety of new solutions and value-added services (VAS).

Using SIGTRAN porticoes such as an MTP3 user application (M3UA) and a signaling connection control part user application (SUA), the application vendor (i.e. Short Message service center [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 the throughput limitation that was inherited from the SS7 standards, thus allowing high-end machines like SMSC, HLR, and so on to be able to support heavy SS7 traffic needs. By suing signaling 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.

Organization of Thesis

This chapter has talked about the introduction of SS7 over IP, why it is required and the different aspects related to SS7 over IP.

Chapter 2 covers the description of SS7 protocol which includes MTPs and other user parts like SCCP, TCAP and ISUP. Also it covers the SS7 topologist network nodes, network links etc. It has also covered the addressing and routing issues related to SS7.

Chapter 3 covers the description of Internet Protocol (IP). How the addressing routing takes place in IP networks and also describes the header of the IP packet.

Chapter 4 describes the requirements of SS7 over IP transport. It indicates the different function requirements, different types of layers and also describes the approaches for implementing SS7 over IP transport.

Chapter 5 covers the design of SIGTRAN protocol in the C-DOT's environment. It elaborates how it can be implemented with the existing C-DOT hardware.

Chapter 6 describes the conclusion from this dissertation work.

Chapter 7 contains the list of references.

CHAPTER 2

2. SIGNALING SYSTEM NO. 7

2.1 What is Signaling?

Signaling refers to the exchange of information between call components require to provide and maintain service.

As users of the PSTN, we exchange signaling with network elements all the time. Examples of signaling between a telephone user and the telephone network include: dialing digits, providing dial tone, accessing a voice mailbox, sending a call-waiting tone, dialing *66(to retry a busy number), etc.

Signaling is a means by which elements of the telephone network exchange information. Information is conveyed such as:

- I am forwarding to you a call placed from 212-555-1234 to 718-555-5678. Look for it on trunk 067.
- Someone just dialed 800-555-1212. Where do I route the call?
- The called subscriber for the call on trunk 11 is busy. Release the call and play a busy tone.
- The route to XXX is congested. Please don't send any message to XXX unless they are of priority 2 or higher.
- I am taking trunk 143 out of service for maintenance.

2.2 Why is signaling needed?

To understand the answer to this question, we must first understand the mechanics of a telephone call. When a subscriber picks up a telephone receiver, an electrical signal is sent over a wire to a telephone switch. The telephone switch detects the electrical current on this wire and interprets this "signal" as a request for a dial tone.

But let's say the subscriber wants to transmit data over this same line using packet switching rather than an analog modem. The information sent to the telephone switch has to define the transmission as digital data and not voice before the switch can determine how to handle the call. This is only one portion of the call.

To transmit the data to another network, the switch must determine first, how the data is to be routed (to what destination) and which circuits to use to reach the destination. After this has been determined, some form of request must be sent to the telephone switch on the other end of the circuit to request a connection. This continues all the way through the network, with the same requirements at each leg of the call. Telephone switches need the capability to signal one another and share information regarding the type of transmission, how the transmission is to be routed (call destination), and what the contents of the transmission are (audio, video, data, and so on).

If there is to be special handling or routing for a call, the telephone switches involved in routing the call must be able to obtain these instructions. Rather than store routing instructions for every single telephone number in the world within each and every telephone switch, each network is responsible for their own network database. The telephone switches then need the capability to connect and communicated with these databases to obtain the special instructions.

This is a high-level view of what signaling networks really do. They enable telephone switches to communicate directly with one another and share information needed to process any type of call autonomously.

2.3 Problem with earlier signaling methods

Early signaling methods were analog and had a limited number of states or values that could be represented. They were also limited to sudible tones because they used the same circuit for both signaling and voice. The tones would sometimes interfere with the call in progress, and sometimes the voice transmission itself would be interpreted as part of the signaling and release the call.

Another problem with early signaling methods was the fact that the circuit used for the call would be busy from the time the caller started dialing until the call was completed. Since the signaling was send through the same circuit as the voice transmission, it was necessary to connect the facility end to end even if there was no voice transmission. For example, if the number being called was busy, the facility would still be connected end to end so a busy tone could be sent through the circuit to the caller. This is not an efficient use of facilities, and as the demand grew for telephone service, it placed a heavy burden on telephone companies with limited facilities.

2.4 Types of signaling

1. Channel Associated Signaling (CAS)
2. Common Channel Signaling (SS7)

2.5 Channel Associated Signaling (CAS)

In-band signaling is used when DC signaling is not possible, such as in tandem offices. In-band signaling uses tones in place of a DC current. These tones may be single frequency (SF) tones, multi frequency (MF) tones, or DTMF. The tones are transmitted with the voice. Because these tones must be transmitted over the same facility as the voice, they must be within the voice band (0 to 4 kHz). There is the possibility of false signaling when voice frequencies duplicate signaling tones. The tones are designed for minimal occurrence of this, but this is not 100 percent fault tolerant. Signal delays and other mechanisms are used to prevent the possibility of voice frequencies from imitating SF signals.

SF signaling is used for interoffice trunks. Two possible states exist: on-hook (idle line) or off-hook (busy line). To maintain a connection, no tone is sent while the circuit is up. When either party hangs up, a disconnect is signaled to all interconnecting offices by sending a tone (2.6 kHz) over the circuit. Detectors at each end of the circuits detect the tone and drop the circuit.

SF signaling has become the most popular of all the in-band method, and the most widely used of all signaling methods. SF is still in use today in some parts of the telephone network. However, as deployment of the SS7 network spreads, SF is no longer needed.

The CAS is also known as in-band signaling:

- Call setup information (off-hook, dial tone, address digits, ring back, busy) is transmitted in the same band of frequencies as used by the voice signal.
- Voice (talk) path is cut over only when the call setup is complete, using the same path that the call setup signals used.
- SF (single-frequency) signaling uses tones to represent on-hook or payphone deposits.
- MF (multi-frequency) signaling is used for switch-to-switch call setup

The principal advantage of CAS is that it is inexpensive to implement and can be used on any transmission medium.

However, CAS has the following **disadvantages**:

- Fraud— "phone freaks" can build boxes to play call setup and teardown tones.
- Interference is possible between signaling tones used by the network and frequencies of human speech patterns.
- Speed—call setup and teardown is slower, less efficient use of resources.

2.6 Common Channel Signaling (SS7)

Signaling System 7 (or Common Channel Signaling) is architecture for performing out-of-band signaling in support of call-establishment, billing, routing, and information-exchange functions of the public switched telephone network (PSTN). It identifies functions to be performed by a signaling-system network and a protocol to enable their performance.

The SS7 is also known as Out-of-band signaling.

The Out-of-band signaling is signaling that does not take place over the same path as the conversation.

We are used to thinking of signaling as being in-band. We hear dial tone, dial digits, and hear ringing over the same channel on the same pair of wires. When the call completes, we talk over the same path that was used for the signaling. Traditional telephony used to work in this way as well. The signals to set up a call between one switch and another always took place over the same trunk that would eventually carry the call. Signaling took the form of a series of multi frequency (MF) tones, much like touch tone dialing between switches.

CCS establishes a separate digital channel for the exchange of signaling information. This channel is called a signaling link. Signaling links are used to carry all the necessary signaling messages between nodes. Thus, when a call is placed, the dialed digits, trunk selected, and other pertinent information are sent between switches using their signaling links, rather that the trunks which will ultimately carry the conversation.

Advantages of Out-of-Band signaling:-

Out-of-Band signaling has several advantages that make it more desirable than traditional in-band signaling.

- It allows for the transport of more data at higher speed.
- It allows for signaling at any time in the entire duration of the call, not only at the beginning.
- It enables signaling to network elements to which there is no direct trunk connection.

Common Channel Signaling System No. 7 (SS7 or C7) is a global standard for telecommunications defined by the International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T). The standard defines the procedures and protocol by which network elements in the public switched telephone network (PSTN) exchange information over a digital signaling network to effect wireless (cellular) and wire line call setup, routing and control. The ITU definition of SS7 allows

for national variants such as North America's American National Standards Institute (ANSI) and Bell Communications Research (Telcordia Technologies) standards and Europe's European Telecommunications Standards Institute (ETSI) standard.

The SS7 network and protocol are used for:

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

2.6.1 Modes of Signaling

There are three modes of signaling described as below

2.6.1.1 Associated Signaling

With this type of signaling, the signaling link directly parallels associated voice trunks. Thus, dedicated links must be provisioned between every interconnected switch.

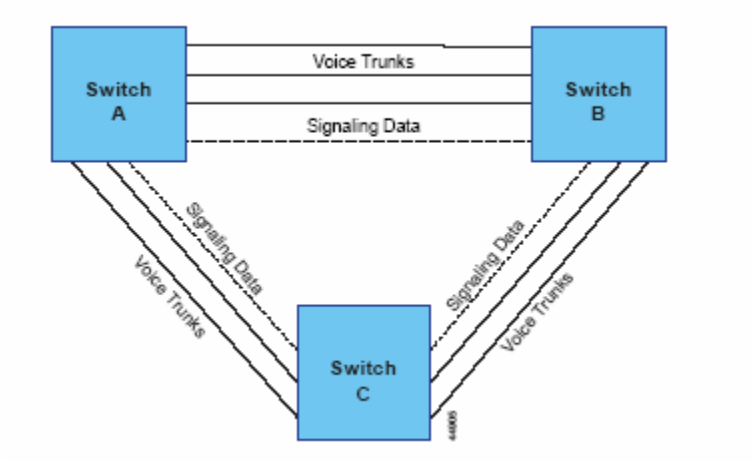


Figure 1: Associated Signaling

2.6.1.2 Non-Associated Signaling

With this type of signaling, voice/data and signaling are carried on separate, logical paths. Multiple nodes in the signaling path to the final destination can causes delays. Although used in the SS7 network, it is not preferred

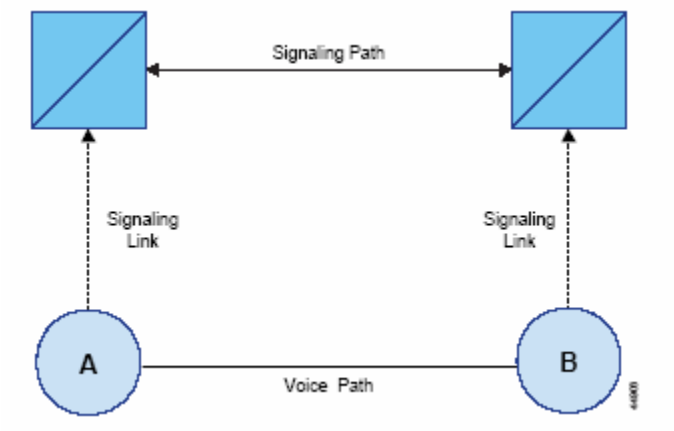


Figure 2 : Non Associated Signaling

2.6.1.3 Quasi-Associated Signaling

This type of signaling employs a minimal number of nodes, thus minimizing delays. Quasi-associated signaling is the preferred signaling mode for SS7.

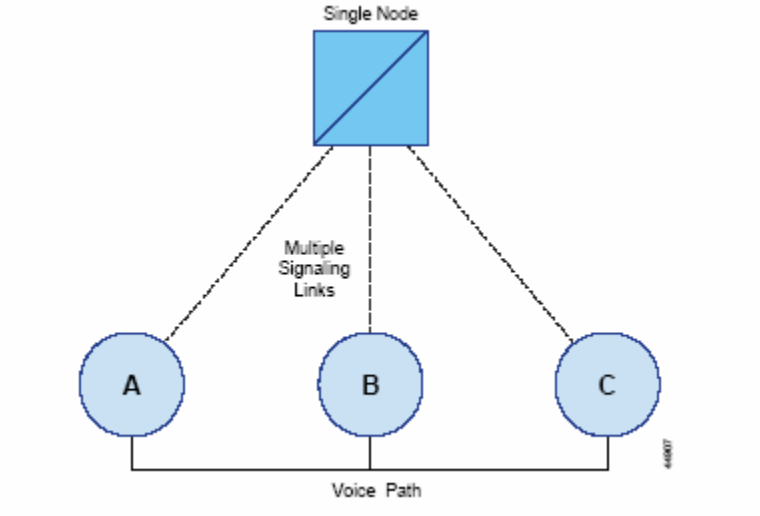


Figure 3 : Quasi Associated Signaling

2.6.2 Signaling System No. 7-Based Services

In addition to setting up and releasing calls, SS7/C7 is the workhorse behind a number of telecommunication services, including:

- Telephone-marketing numbers such as toll-free and freephone
- Televoting (mass calling)
- Single Directory Number
- Enhanced 911 (E911)—used in the United States
- Supplementary services
- Custom local area signaling services (CLASS)
  - Call block
  - Distinctive ringing
  - Priority ringing
  - Call completion to busy subscriber (CCBS)
- Calling name (CNAM)
- Line information database (LIDB)
- Local number portability (LNP)

- Cellular network mobility management and roaming
- Short Message Service (SMS)
- Enhanced Messaging Service (EMS)—Ring tone, logo, and cellular game delivery
- Local exchange carrier (LEC) provisioned private virtual networks (PVNs)
- Do-not-call enforcement

2.6.3 SS7 Network Nodes

Each signaling point in the SS7 network is uniquely identified by a numeric point code. Point codes are carried in signaling messages exchanged between signaling points to identify the source and destination of each message. Each signaling point uses a routing table to select the appropriate signaling path for each message.

There are three kinds of signaling points in the SS7 network

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

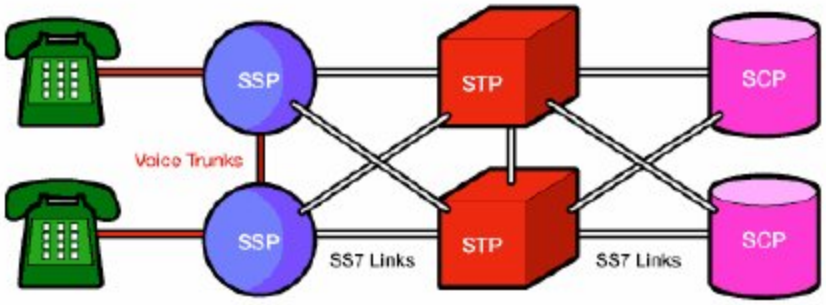


Figure 4 : Types of SS7 signaling points

SSPs are switches that originate, terminate or tandem calls. An SSP sends signaling messages to other SSPs to setup, manage and release voice circuits required to complete a call. An SSP may also send a query message to a centralized database (an SCP) to determine how to route a call (e.g., a toll-free 1- 800/888 call in North America). An SCP sends a response to the originating SSP containing the routing number(s) associated with the dialed number. An alternate routing number may be used by the SSP if the primary number is busy or the call is unanswered within a specified time. Actual call features vary from network to network and from service to service.

Network traffic between signaling points may be routed via a packet switch called an STP. An STP routes each incoming message to an outgoing signaling link based on routing information contained in the SS7 message. Because it acts as a network hub, an STP provides improved utilization of the SS7 network by eliminating the need for direct links between signaling points. An STP may perform global title translation, a procedure by which the destination signaling point is determined from digits present in the signaling message (e.g. the dialed 800 number, calling card number or mobile subscriber identification number).

An STP can also act as a "firewall" to screen SS7 messages exchanged with other networks. Because the SS7 network is critical to call processing, SCPs and STPs are usually deployed in mated pair configurations in separate physical locations to ensure network-wide service in the event of an isolated failure. Link between signaling points are also provisioned in pairs. Traffic is shared across all links in the link-set. If one of the links fails, the signaling traffic is rerouted over another link in the link-set. The SS7 protocol provides both error correction and retransmission capabilities to allow continued service in the event of signaling point or link failures.

2.6.4 SS7 Protocol Stack

This section will define the functions of the SS7 protocol in a conventional network based on time-division multiplexing (TDM). The SS7 protocol differs somewhat from the OSI model (see Figure 5). The OSI model consists of seven different layers, whereas the SS7 standard uses only four levels. The term level is used in the same context as layers.

The functions carried out by these four levels correspond with the OSI model's seven layers. Some of the functions called for in the OSI model have no purpose in the SS7 network and are therefore undefined.

It should also be noted that the functions in the SS7 protocol have been refined over the years and tailored for the specific requirements of the SS7 network. For this reason, many discrepancies exist between the two protocols and their corresponding functions.

Regardless of the differences, the SS7 protocol has proven to be a highly reliable packet-switching protocol, providing all of the services and functions required by the telephone service providers. This protocol continues to evolve as the network grows and the services provided by the telephone companies change. The following descriptions only apply to SS7 networks deployed using TDM circuit-switching networks. Networks using true packet-switching facilities (such as Transmission Control Protocol/Internet Protocol [TCP/IP]) do not use the same techniques.

The hardware and software functions of the SS7 protocol are divided into functional abstractions called "levels." These levels map loosely to the **Open Systems Interconnect** (OSI) 7-layer model defined by the International Standards Organization (ISO).

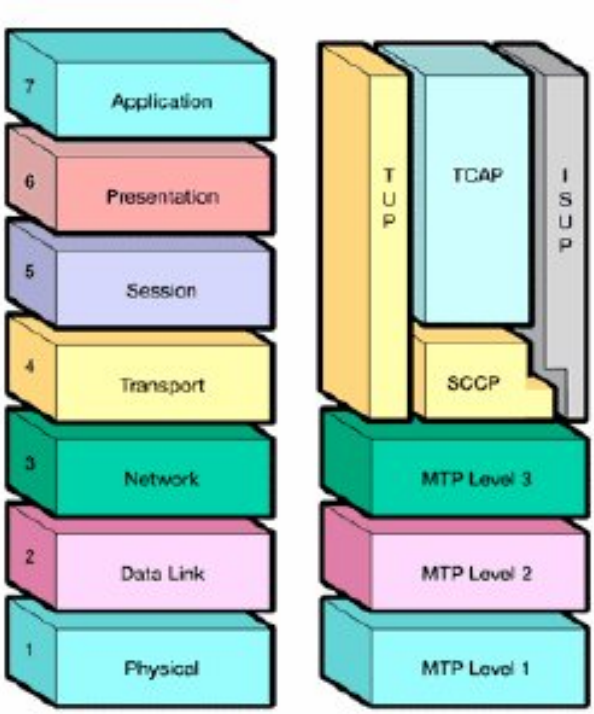


Figure 5 : SS7 Protocol Stack

2.6.4.1 MTP-1: Physical Connection

This is the physical level of connectivity, virtually the same as Layer 1 of the OSI model. SS7 specifies what interfaces will be used, both Bellcore (Telecordia) and ANSI call for either the DS0A or the V.35 interface.

Because central offices are already using DS1 and DS3 facilities to link one another, the DS0A interface is readily available in all central offices, and is preferred in the SS7 network. As the demands on the SS7 network increase (local number portability), and as the industry migrates toward ATM networks, the DS1 interface will become the link interface.

2.6.4.2 MTP-2: Data Link Layer

The data link level provides the network with sequenced delivery of all SS7 message packets. Like the OSI data link layer, it is only concerned with the transmission of data from one node to the next, not to its final destination in the network.

Sequential numbering is used to determine if any messages have been lost during transmission. Each link uses its own message numbering series independent of other links.

SS7 uses CRC-16 error checking of data and requests retransmission of lost or corrupted messages. Length indicators allow Level 2 to determine what type of signal unit it is receiving, and how to process it.

2.6.4.3 MTP-3: Network Level

The network level depends on the services of Level 2 to provide routing, message discrimination and message distribution functions. There are three main functions of the MTP-3 level:

2.6.4.3.1 Message handling

- **Message Discrimination**

This function determines whether a message is local or remote using the point code and data contained in a lookup table. Messages to remote destinations are passed to the message routing function for additional processing.

- **Message Distribution**

Message distribution provides link, route and traffic management functions.

- **Message Routing**

This function routes the packet to the correct destination according to the DPC present in the message.

2.6.4.3.2 Network Management

- **Link Management**

This function uses the Link Status Signal Unit (LSSU) to notify adjacent nodes of link problems. Level 3 will send LSSUs via Level 2 to the adjacent node, notifying it of the problems with the link and its status.

Diagnostics consists of realigning and re-synchronizing the link.

• **Realignment** - All traffic is removed from the link, counters are reset to zero, timers are reset and Fill-In Signal Units (FISUs) are sent in the meantime (called the proving period).

• **Proving Period**—Amount of time FISUs are sent during link realignment. The duration of the proving period depends on the type of link used. Bellcore specifies the proving period for a 56 Kbps DS0 link is 2.3 seconds for normal proving and 0.6 seconds for emergency proving.

Another form of link management uses changeover and change-back messages sent using Message Signal Units (MSUs). MSUs advise the adjacent node to send traffic over another link within the same link set.
The alternate link must be within the same link set. The bad link is being realigned by Level 3 while traffic is rerouted over alternate links. Change-back message is sent to advise the adjacent node that it can use the newly restored link again. Change-back messages are typically followed by a change-back acknowledgement message.

- **Route Management**

This function provides a means for rerouting traffic around failed or congested nodes. Route management is a function of Level 3 and works together with link management. Route management informs other nodes of the status of the affected node. It uses Message Signal Units (MSUs) generated by adjacent nodes and is not usually generated by the affected nodes. (Link management only informs adjacent nodes.)

- **Traffic Management**

This function provides flow control if a node has become congested. It allows the network to control the flow of certain messages based on protocol. Traffic management deals with a specific user part within
an affected node. For example, if ISUP is not available at a particular node, a traffic management message can be sent to adjacent nodes informing them that ISUP is not available, without affecting TCAP messages on the same node.

As discussed earlier the network level provides three functions for the message handling: message routing, message discrimination, and distribution. All three functions depend on the services of level 2. When a message is received, it is passed by level 2 to level 3 for message discrimination.

Message discrimination determines to whom the message is addressed. If the message contains the local address (of the receiving node), then the message is passed to message distribution. If the message is not addressed to the local node, then it is passed to the message-routing function. The message-routing function reads the called and calling party addresses in the message to determine which physical address to route to. The called and calling party addresses can be considered logical addresses and the physical address can be considered the node address.

The physical address in SS7 networks is referred to as a point code. Every node in the network must have a unique point code. The routing function determines which point code to route the message is based on information stored in its administrable routing

tables. These routing tables are maintained by the service providers themselves and are network dependent.

The point code in many cases is not the final destination for a message, but the adjacent point code for this node. This enables messages to be routed through the network and rerouted to another node in the event of a network failure. The routing scheme is determined by the network providers and can vary depending on philosophy.

Message distribution is used when message discrimination determines that the address is a local address. Message distribution is responsible for identifying which user part the message is addressed to (based on the service information octet field of the message) and routes the message to its internal user.

As discussed earlier the network layer has three network management functions at level 3**: link management**, **route management**, and **traffic**. Each type of network management uses different mechanisms to achieve results.

The link management function uses the ***link status signal unit*** (LSSU) to notify adjacent nodes of link problems. A link problem does not necessarily mean that the link cannot transmit messages. Software errors or processor problems on link interface cards can cause a link to become unusable.

When this occurs, it is quite possible for a link to remain operational at level 2 and even level 3, but non-operational at level 4. When this occurs, the adjacent node must be notified that the indicated link cannot be used for traffic because there is a problem at the affected signaling point.
Level 3 sends LSSUs via level 2 to the adjacent node, indicating the problems with the link and advising of its status. The link can be removed from service (which means that no MSUs are transmitted over the affected link) and diagnostics can begin. Diagnostics consist of realigning the link or re-synchronizing the link.

Realignment occurs when traffic is removed, all counters are reset to zero, all timers are reset to zero, and ***fill-in signal units*** (FISUs) are transmitted for a prescribed duration of time, which is called the *proving period*. The duration of the proving period is dependent on the type of link being used. Telcordia has specified that the proving period for a DS0 at 56 kbps is 2.3 seconds for normal proving and 0.6 seconds for emergency proving periods. At 64 kbps, the normal proving period duration is defined at 2.0 seconds and the emergency proving period is at 0.5 seconds. When a 1.536 Mbps link is used, the normal proving period is defined at 30 seconds and the emergency proving period is defined at 5 seconds. During the proving period, any errors that may occur with the FISUs' transmission are counted.

When link management has determined that too many errors have occurred on the link, the entire process begins over again and timers and counters are reset to zero and FISUs are transmitted for a prescribed duration of time.

Another form of link management entails the use of **changeover** and **change-back messages**. These are sent using ***message signal units*** (MSUs) and advice the adjacent node to begin sending traffic over another link. The alternate link must be within the same link set. During the time that all MSUs are being rerouted over different links, the affected link is being realigned by level 3.

A change-back message is sent to tell the adjacent node that traffic may be sent over the affected link once again because it has been restored to service. The change-back message is typically followed by a change-back acknowledgment message.

Route management provides the mechanisms for rerouting traffic around nodes that have failed or have become congested. This is a function of level 3 and works with the link management function.

Usually, when a link management message has been received, if the route of the node is affected, it may trigger the generation of a routing message depending on the

impact on other nodes. Route management is used to inform other nodes in the network of the status of a particular node that has become unavailable or congested. This differs from link management, which only notifies an adjacent node about link status.

Route management messages use the MSU and are generated by nodes that are adjacent to affected nodes and not usually by the affected nodes themselves. The messages are called the **transfer-prohibited** and **transfer-restricted messages**.

Traffic management is used as a flow control mechanism. Flow control is used in the event that a node has become congested, but only at a single level. For example, if a particular user part is not available (such as the *ISDN User Part* [ISUP]), a traffic management message can be directed at adjacent nodes informing them that ISUP at a particular node is not available without having any impact on *Transaction Capabilities Application Part* (TCAP) messages to the same node. Traffic management, then, is different from the previous two functions in that it deals with a specific user part within an affected node rather than with the entire entity. This mechanism enables the network to control the flow of certain messages based on protocols without impeding other traffic that should not be affected. **In packet-switched networks using TCP/IP, *MTP3 User Adaptation Layer* (M3UA)** provides many of the previous services.

2.6.4.4 User Parts

2.6.4.4.1 TCAP

Transaction Capability Application Part (TCAP) facilitates connection to an external database. Information data received is sent back in the form of a TCAP message. TCAP also supports remote control – ability to invoke features in another remote network switch.

OMAP (Operations, Maintenance and Administrative Part) is an applications entity that uses TCAP services for communications and control functions through the network via a remote terminal.

Map (Mobile Application Part) is used to share cellular subscriber information among different networks. It includes information such as the mobile identification number and the serial number of the cellular handset. This information is used by the IS-41 protocol during cellular roaming.

2.6.4.4.2 SCCP

Signaling Connection Control Part (SCCP) is a higher level protocol than MTP that provides end-to-end routing. SCCP is required for routing TCAP messages to their proper database. The SCCP provides two major functions that are lacking in the MTP. The first of these is the capability to address applications within a signaling point. The MTP can only receive and deliver messages from a node as a whole; it does not deal with software applications within a node.

While MTP network-management messages and basic call-setup messages are addressed to a node as a whole, other messages are used by separate applications (referred to as subsystem) within a node. Examples of subsystems are 800 call processing, calling card processing, advanced intelligent network (AIN), and custom local-area signaling services (CLASS) services (e.g., repeat dialing and call return). The SCCP allows these subsystems to be addressed explicitly.

The second function of the SCCP is the Global Title Translation. i.e. the ability to perform international routing using a capability called global title translation (GTT). GTT frees originating signaling points from the burden of having to know every potential destination to which they might have to route a message. A switch can originate a query, for example, and address it to an STP along with a request for GTT. The receiving STP can then examine a portion of the message, make a determination as to where the message should be routed, and then route it.

2.6.4.4.3 TUP

Telephone User Part (TUP) is an analog protocol that performs basic telephone call connects and disconnect. It has been replaced by ISUP, but is still used in some parts of the world (China).

2.6.4.4.4 ISUP

ISDN User Part (ISUP) supports basic telephone call connect disconnect between end offices. Used primarily in North America, ISUP was derived from TUP, but supports ISDN and intelligent network functions. ISUP also links the cellular and PCS network to the PSTN.

ISUP is the protocol used to set up and tear down telephone connections between end offices. This protocol was derived from the TUP, which is the ITU-TS equivalent to ISUP, but offers the added benefit of supporting *Intelligent Networking* (IN) functions and *integrated services digital network* (ISDN) services. ISUP is used throughout the United States today and provides not only call connection services within the PSTN, but also links the wireless network and the *Personal Communications Service* (PCS) network to the public telephone network

2.6.5 SS7 Signaling Messages

Signaling information is passed over the signaling link in messages called signal units (SUs).

Three types of SUs are defined in the SS7 protocol

- Message signal units (MSU)
- Link status signal units (LSSU)
- Fill-in signal units (FISU)

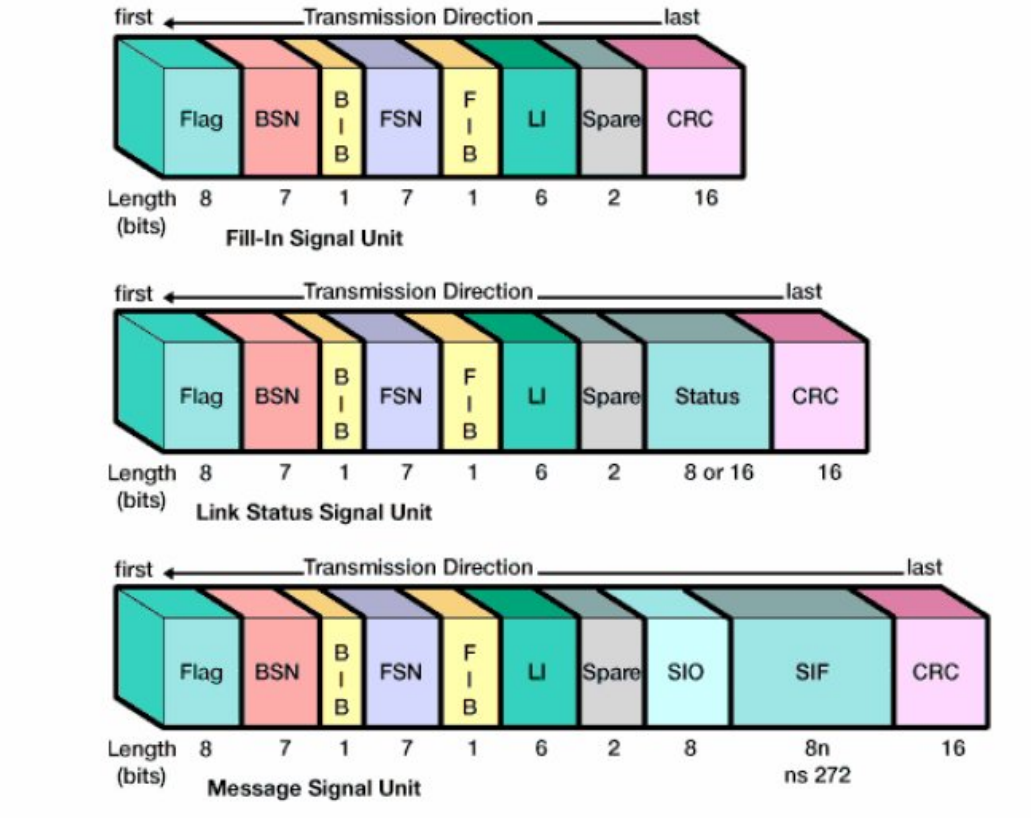


Figure 6 : Types of Signaling Units

Flag

The flag indicates the beginning of a new signal unit and implies the end of the previous signal unit (if any). The binary value of the flag is 0111 1110. Before transmitting a signal unit, MTP Level 2 removes "false flags" by adding a zero-bit after any sequence of five one-bits. Upon receiving a signal unit and stripping the flag, MTP Level 2 removes any zero-bit following a sequence of five one-bits to restore the original contents of the message. Duplicate flags are removed between signal units.

BSN (Backward Sequence Number)

The BSN is used to acknowledge the receipt of signal units by the remote signaling point. The BSN contains the sequence number of the signal unit being acknowledged. (See description under FIB below.)

BIB (Backward Indicator Bit)

The BIB indicates a negative acknowledgment by the remote signaling point when toggled. (See description under FIB below.)

FSN (Forward Sequence Number)

The FSN contains the sequence number of the signal unit. (See description under FIB below.)

FIB (Forward Indicator Bit)

The FIB is used in error recovery like the BIB. When a signal unit is ready for transmission, the signaling point increments the FSN (forward sequence number) by one (FSN = 0..127). The CRC (cyclic redundancy check) checksum value is calculated and appended to the forward message. Upon receiving the message, the remote signaling point checks the CRC and copies the value of the FSN into the BSN of the next available message scheduled for transmission back to the initiating signaling point. If the CRC is correct, the backward message is transmitted. If the CRC is incorrect, the remote signaling point indicates negative acknowledgment by toggling the BIB prior to sending the backward message. Where the originating signaling point receives a negative acknowledgment, it retransmits all forward messages, beginning with the corrupted message, with the FIB toggled. Because the 7-bit FSN can store values between zero and 127, a signaling point can send up to 128 signal units before requiring acknowledgment from the remote signaling point. The BSN indicates the last in-sequence signal unit received correctly by the remote signaling point. The BSN acknowledges all previously received signal units as well. For example, if a signaling point receives a signal unit with

BSN = five followed by another with BSN = ten (and the BIB is not toggled), the latter BSN implies successful receipt of signal units six through nine as well.

SIO (Service Information Octet)

The SIO field in an MSU contains the 4-bit sub-service field followed by the 4-bit service indicator. FISUs and LSSUs do not contain an SIO.

SIF (Signaling Information Field)

The SIF in an MSU contains the routing label and signaling information (e.g., SCCP, TCAP and ISUP message data). LSSUs and FISUs contain neither a routing label nor an SIO as they are sent between two directly connected signaling points.

CRC (Cyclic Redundancy Check)

The CRC value is used to detect and correct data transmission errors.

2.6.6 SS7 Signaling Link Types

SS7 Signaling links are characterized according to their use in the signaling network. Virtually all links are identical in that they are 54 Kbps or 64 Kbps bi-directional data links that support the same lower layers of the protocol. What is different however is their use in the signaling network.

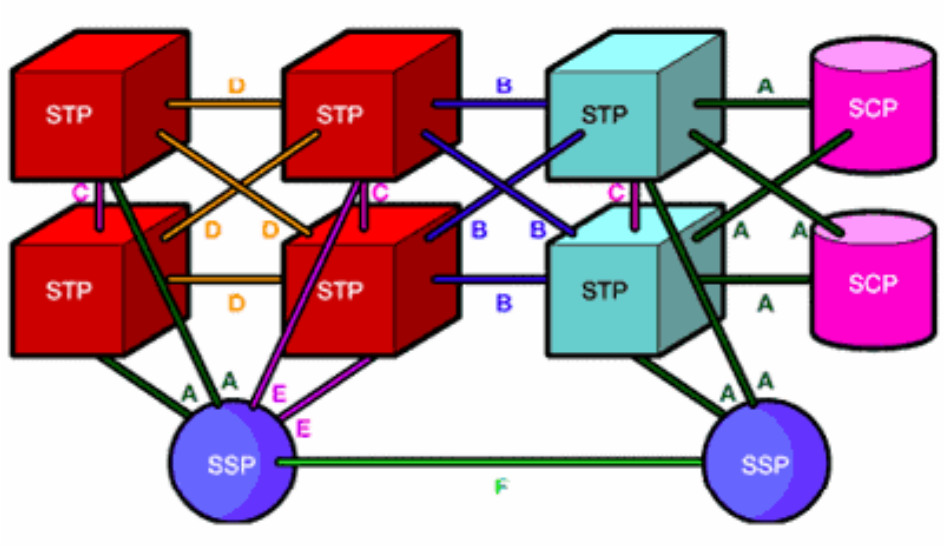


Figure 7 : SS7 link types

Links are labeled according to their relationship on the network. Although there is no technical difference between these different links, there are differences in how the links are engineered. There are six different types of links used in SS7:

A-links

B-links

Cross links (C-links)

Diagonal links (D-links)

E-links

F-links

Access Links (A-Links)

A-links (as shown in Figure 3) are used between the SSP and the STP, or the SCP and STP. These links provide access into the network and to databases through the STP. There are always at least two A-links, one to each of the home STP pairs. In the event that STPs are not deployed in pairs, there can be one A-link; however, this is highly unusual. The maximum number of A-links to any one STP is 16. A-links can be configured in a combined linkset that has 16 links to each STP, providing 32 links to the mated pair. When connecting switches in a network to hub providers, A-links are used.

When trying to determine how many A-links are required, the easiest formula is to calculate the number of access lines supported by the switch. One simple formula is to calculate one signaling link for every 9,600-access lines. Many other formulas are used, but this simple formula will provide close enough results for general usage.

Bridge Links (B-Links)

B-links are used to connect mated STPs to other mated STPs at the same hierarchical level. B-links are deployed in a quad fashion, as shown in Figure 3, which is why these are often referred to as quad links. A maximum of eight B-links can be deployed between mated STPs. Although this practice is closely followed in North America, European networks do not use B-links as depicted. Mated STPs are connected to an-other mated pair via one set of links, but each STP does not have a connection to each of the other mated STPs.

Cross Links (C-Links)

C-links connect an STP to its mate STP. They are always deployed in pairs to maintain redundancy on the network. Normal SS7 traffic is not routed over these links, except in congestion conditions. The only messages to travel between mated STPs during normal conditions are network management messages. If a node becomes isolated and the only available path is over the C-links, then normal SS7 messages can be routed over these links. A maximum of eight C-links can be deployed between STP pairs.

Diagonal Links (D-Links)

D-links (see Figure 3) are used to connect mated STP pairs at a primary hierarchical level to another STP mated pair at a secondary hierarchical level. For example, a carrier may have STPs deployed in every Local Access Transport Area (LATA). They could then deploy STPs in regions, acting as concentrators. This would prevent the need to interconnect every STP to every other STP. The LATAs within a

defined region would all connect to one STP, which would provide connections to the other regional STPs. This hierarchical approach would only be found in very large SS7 networks. Not all networks deploy D-links because not all networks use hierarchical network architecture. D-links are deployed in a quad arrangement like B-links. A maximum of eight D-links can be used between two mated STP pairs

Extended Links (E-Links)

E-links are used to connect to remote STP pairs from an SSP. The SSP connects to its home STP pair, but, for diversity, may also be connected to a remote STP pair using E-links. E-links then become the alternate route for SS7 messages in the event that congestion occurs within the home STP pairs. A maximum of 16 E-links can be used between any remote STP pairs.

Fully Associated Links (F-Links)

F-links are used when a large amount of traffic exists between two SSPs or when an SSP cannot be connected directly to an STP. F-links enable SSPs to use the SS7 protocol and access SS7 databases even when it is not economical to provide a direct connection to an STP pair. When traffic is particularly heavy between two end offices, the STP may be bypassed altogether, provided that both SSPs are local to each other. Only call setup and teardown procedures would be sent over this link-set.

4.2.7 SS7 Vs OSI Model

Following is the list of the major differences between the OSI and SS7 protocol stack

While all the functions called for in the OSI model are addressed in the SS7 protocols, the SS7 protocol stack is condensed and does not address connection-oriented services used to establish a session with an-other user.

In addition to providing connection requests in the voice network, SS7 also provides for database access from any entity on the network. This is the most important feature of the SS7 network and the main reason why SS7 has been deployed in the PSTN all over the world: so that all telephone companies can share subscriber information and call-handling procedures on a call-by-call basis.

CHAPTER 3

3. INTERNET PROTOCOL (IP)

3.1 Introduction

Just like every other protocol, the Internet Protocol has a place in the OSI Model. Because it's such an important protocol and other protocols depend upon it, it needs to be placed before them, that is why we will find it in Layer 3 of the OSI model:

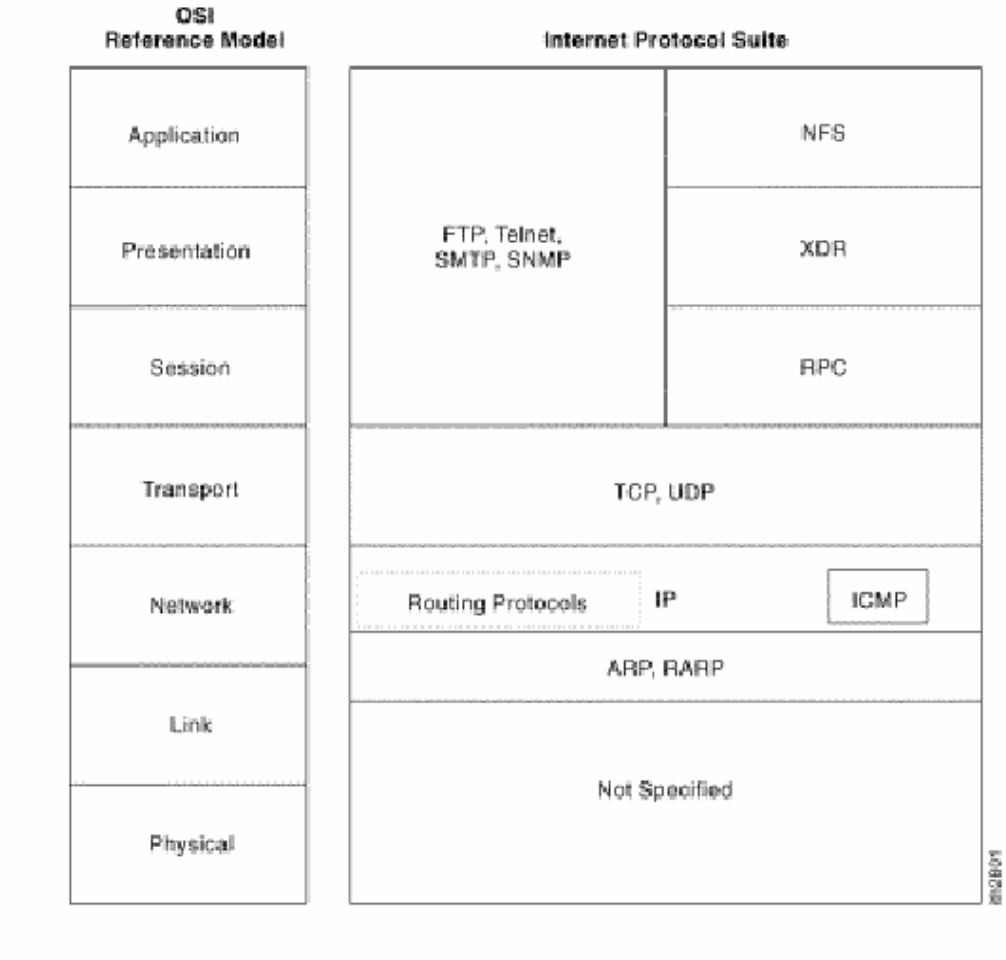


Figure 8: TCP/IP Protocol Stack

When a computer receives a packet from the network, the computer will firstly check the destination MAC address of the packet at the Datalink layer (2) and if it passes, it's then passes on to the Network layer At the Network layer it will check the packet to see if the destination IP Address matches with the computer's IP Address (if the packet is

a broadcast, it will pass the network layer anyway).From there, the packet is processed as required by the upper layers.

On the other hand, if the computer is generating a packet to send to the network then, as the packet travels down the OSI model and reaches the Network layer, the destination and source IP Address of this packet are added in the IP Header.

3.2 IP Header

Now we are going to analyze the Internet Protocol header, so you can see the fields it has and where they are placed. In here you will find the destination and source IP Address field which is essential to every packet using the protocol.

The unit of data that IP sends to the network interface is called an IP datagram. Figure 7 shows the format of an IP datagram. This is the IPv4 (IP version 4) header. The normal size of IP header is 20 bytes, unless options are present.

The 4-bit *version* indicates the version number of the IP protocol. Currently IPv4, IPv5 and IPv6 versions are there. IPv5 has lots of problems so that is not used.

The *header length* is the number of 32-bit words in the header, including any options which limits the header to 60 bytes at the most.

The 8-bits *type-of-service* (TOS) is composed of a 3-bits precedence field, 4 TOS bits and an unused bit that must be 0. The 4 TOS bits are:

Minimize delay, maximize throughput, maximize reliability & minimize monetary cost.

Only one out of these 4 bits can be turned on. If all the 4 bits are 0 it implies normal service.

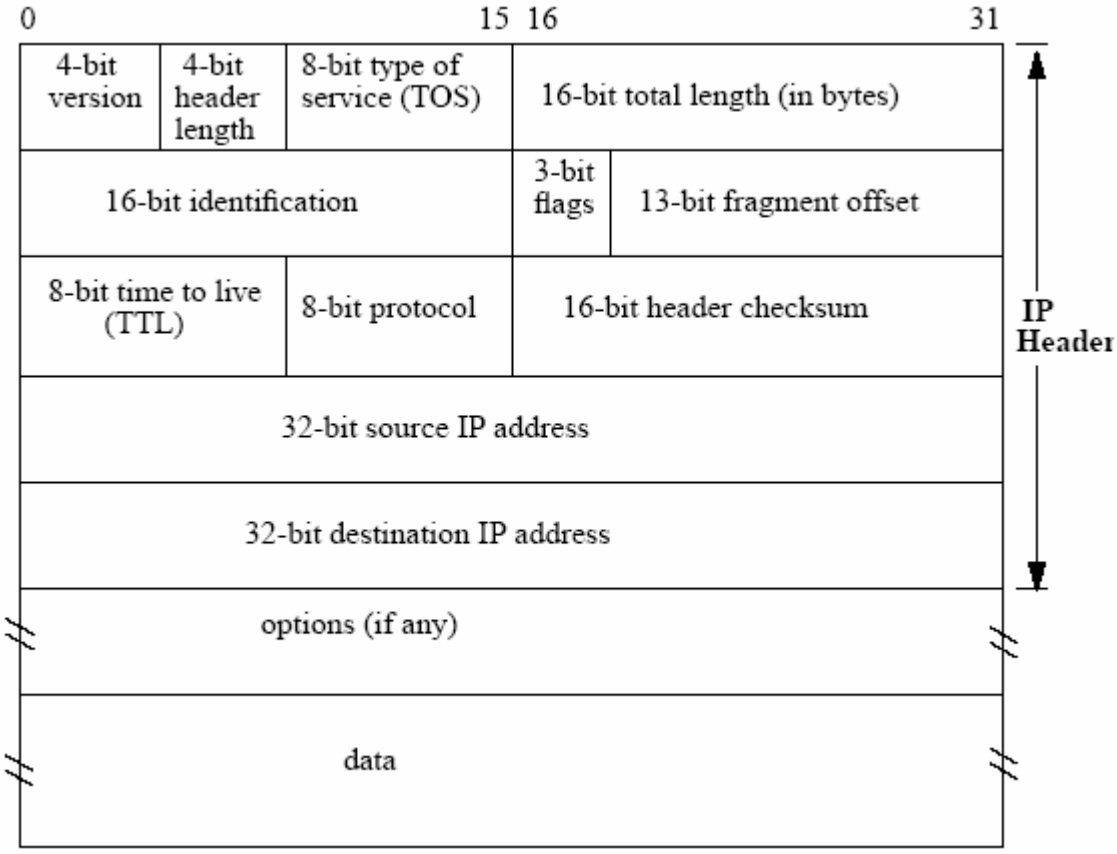


Figure 9: IP Header

The *total length* field is the total length of the IP datagram in bytes. Using this field and the header length field the position of data portion of the IP datagram and its length can be found. Maximum size of an IP datagram can be 65535 bytes.

The *identification* field uniquely identifies each datagram sent. It increments by one each time a datagram is sent. When an IP datagram is to sent on a physical layer whose maximum size is smaller than the IP datagram size then it needs to be fragmented and again reassembled at the destination end.

The *flag* field in the IP header uses one bit as the 'more fragments' bit. This bit is set in all the fragments except the final fragment. One of the bits in the flag field is called the 'don't fragment' bit. If this is set, IP will not fragment the datagram.

The *fragment offset* field contains the offset (in 8-bytes) of this fragment from the beginning of the original datagram.

The *time-to-live*, or TTL, sets an upper limit on the number of routers through which a datagram can pass. It limits the lifetime of the datagram. It is initialized by the sender to some value (often 32 or 64) and decremented by one by every router that handles the datagram. When this field reaches 0, the datagram is thrown away and the sender is notified by an ICMP error message. This prevents packets from getting caught in routing loops forever.

The *protoco*l field is used to identify to which protocol (ICMP, IGMP, TCP or UDP) the IP data is to be delivered by IP.

The *header checksum* is calculated over the IP header only. To compute the IP checksum for an outgoing datagram, the value of the checksum field is set to 0. Then the 16-bit one's complement sum of the header is calculated. The 16-bit one's complement of this sum is stored in the checksum field. When an IP datagram is received, the 16-bit one's complement sum of the header is calculated. Since the receiver's calculated checksum contains the checksum stored by the sender, the receiver's checksum is all one bits if nothing in the header is modified. If the result is not all one bits (a checksum error), IP discards the received datagram. No error message is generated. Is up to the higher layers to somehow detect the missing datagram and retransmit.

Every IP datagram contains the *source IP address* and the *destination IP address*. These are 32-bit values as described in sec. 3.3.

The final field, the *options*, is a variable-length list of optional information for the datagram. The options can be:

- Security and handling restrictions.
- record route, i.e., each router record its IP address (e.g. in 'ping' program)
- timestamp, i.e., each router record its IP address and time
- Loose source routing, i.e., specifying a list of IP addresses that must be traversed by the datagram.
- strict source routing, i.e., specifying a list of IP addresses that can only be traversed by the datagram

The options field always ends on a 32-bit boundary. Pad bytes with a value of 0 are added if necessary. This assures that the IP header is always a multiple of 32 bits.

3.3 IP Addressing

Two versions of IP exist in production use today. Nearly all networks use IP version 4 (IPv4), but an increasing number of educational and research networks have adopted the next generation IP version 6 (IPv6).

IPv4 Addressing Notation

An IPv4 address consists of four bytes (32 bits). These bytes are also known as octets. For readability purposes, humans typically work with IP addresses in a decimal notation that uses periods to separate each octet. For example, the IP address

00001010 00000000 00000000 00000001

Usually appears in the equivalent dotted decimal representation

10.0.0.1

Because each byte is 8 bits in length, each octet in an IP address ranges in value from a minimum of 0 to a maximum of 255. Therefore, the full range of IP addresses is from 0.0.0.0 through 255.255.255.255. That represents a total of 4,294,967,296 possible IP address.

IPv6 Addressing Notation

IP addressing changes significantly with IPv6. IPv6 addresses are 1 bytes (128 bits) long rather than four bytes (32 bits). That represents more than

300,000,000,000,000,000,000,000,000,000,000,000,000

Possible addresses! In the coming years, as an increasing number of cell phones, PDAs, and other network appliances expand their networking capability, this much larger IPv6 address space will probably be necessary. IPv6 addresses are generally written in the following form:

hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh

In this notation, pairs of IPv6 bytes are separated by a colon and each byte in turns is represented as an equivalent pair of hexadecimal numbers, like in the following example:

E3D7:0000:0000:0000:51F4:9BC8:C0A8:6420

IPv4 Address Classes:

There are five different classes of Internet addresses as shown in figure

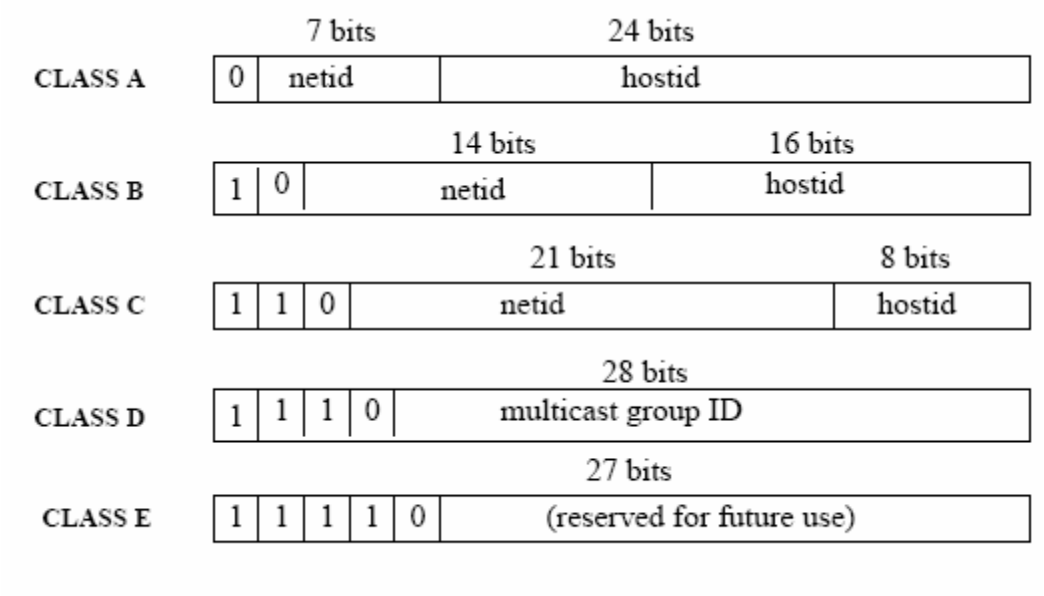


Figure 10: Types of IPv4 address classes

The network id of the IP address is assigned by a central authority called InterNIC (Internet Network Information Centre) and the host id can be assigned by the system administrator. Class A and Class B IP addresses can also support the subnet addressing. The host ID portion is divided into a subnetID and a host ID. It depends on the system administrator on how to divide the hostID into subnets. Subnetting hides the details of the internal network organization to external routers and hence reduces the size of the Internet's routing tables described in sec. 3.4. Table 2 below shows the seven special case IP addresses. The first two entries are special case source addresses, the next one is the special loopback address, and the final four are the broadcast addresses. The first two addresses with the network ID of 0, can only appear as the source address as part of initialization procedure when a host is determining its own IP address.

IP address			Can appear as		Description
net ID	subnet ID	host ID	source?	destination ?	
0		0	OK	never	this host on this net
0		hostid	OK	never	specified host on this net
127		anything	OK	OK	loopback address
-1		-1	never	OK	limited broadcast(never forwarded)
netid		-1	never	OK	net-directed broadcast to netid
netid	subnetid	-1	never	OK	subnet-directed broadcast to netid, subnetid
netid	-1	-1	never	OK	all-subnets-directed broadcast to netid

Figure 11: IP address, net IP, Subnet ID description

There are three types of IP addresses:

Unicast:

A unicast address designates a single node within a IP network. The address may be globally unique or be a private pointcode. Unicast transmission, in which a packet is sent from a single source to a specified destination, is still the predominant form of transmission on LANs and within the Internet.

Broadcast:

Destined for all hosts on a given network.

Multicast:

The message is send to all nodes belonging/attached to that multicast address/group, destined for a set of hosts that belong to a multicast group

All LANs (e.g. Ethernet) and IP networks support both unicast and broadcast transfer mode. Since TCP supports only the unicast mode, multicast applications must use the UDP transport protocol. The majority of installed LANs (e.g. Ethernet) are able to support the multicast transmission mode.

3.4 IP Routing

Routing is one of the most important functions of IP. Figure 9 shows a simplified view of the processing done at the IP layer. Datagram to be routed can be generated either on the local host or on some other host. In the latter case this host must be configured to act as a router, or the datagram received through the network interfaces that are not ours are dropped. IP can receive a datagram from TCP, UDP, ICMP or IGMP to send or one that has been received from a network interface. The IP layer has a routing table in memory that it searches each time it receives a datagram to send. When a datagram is received from a network interface, IP first checks if the destination IP address is one of its own IP addresses or an IP broadcast address. If so, the datagram is delivered to the protocol module as specified in the protocol field of the IP header. If the datagram is not destined for this IP layer then if the IP later was configured to act as a router the packet is forwarded else the datagram is silently discarded. Each entry in the routing table contains the following information:

- Destination IP addresses. This can be either a complete host address or a network address as specified by the flag field for this entry. A host address has a nonzero hosted and identifies a particular host while a network address has a hostis of 0 and identifies all hosts on that network.

- IP address of a next-hop router. This is the one that is directly connected, may not be the final destination but it takes the datagram and forwards them to the final destination.

- Flags. One flag specifies whether the destination IP address is the address of the network or the address of a host. Another flag says whether the next-hop router field is really a next-hop router or a directly connected interface.

IP routing is done on a hop-by-hop basis and IP does not know the complete route to the final destination. IP routing performs the following actions:

1) Search the routing table for an entry that matches the complete destination IP address (matching the network ID and the host ID). If found, send the packet to the indicated next-hop router or to the directly connected interface(depending upon the flags field).

2) Search the routing table for an entry that matches just the destination network ID. If found, send the packet to the indicated next-hop router or to the directly connected interface (depending on the flags field). All the hosts on the destination network can be handled with this single routing table entry.

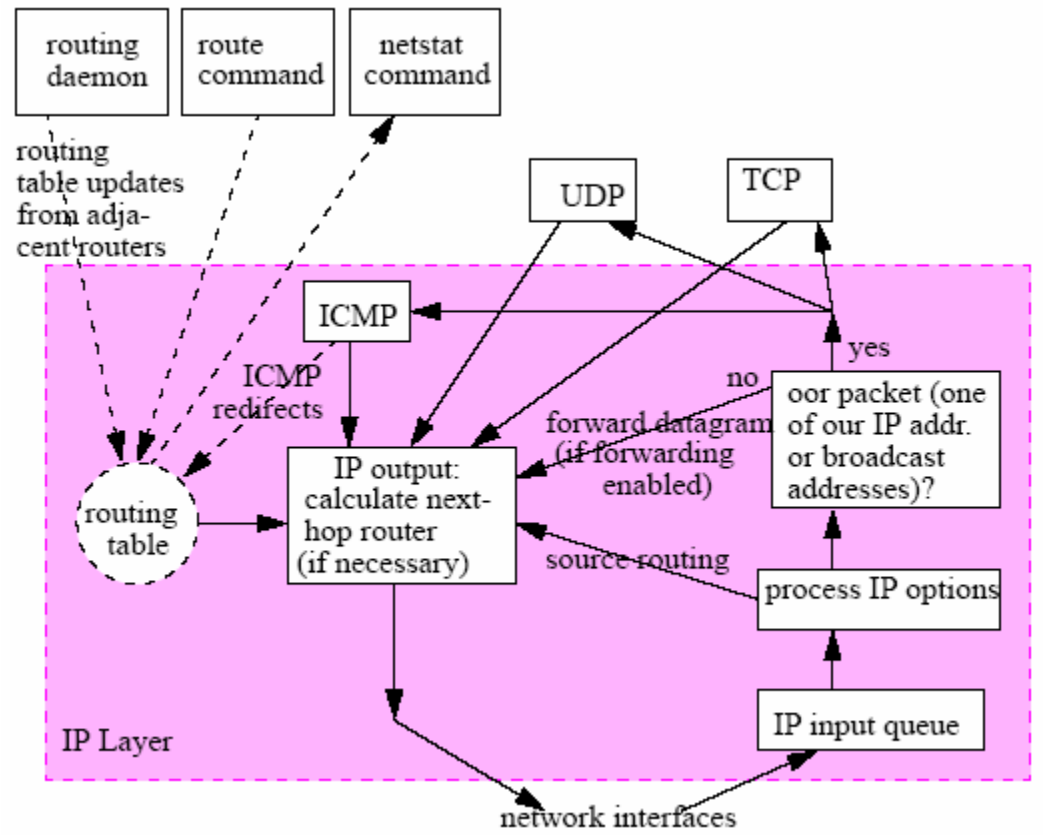


Figure 12: IP routing

3) Search the routing table for an entry labelled ‘default’. If found, send the packet to the indicated next-hop router.

If none of the steps work, the datagram is undeliverable. A ‘host unreachable’ or the ‘network unreachable’ error is normally returned to the application that generated the datagram. All this is static routing, that is , the routing table entries are created by default

when an interface was configured (for directly connected interfaces), added by the route command or created by an ICMP redirect. This is fine if the network is small, there is a single connection point to other networks, and there are no redundant routes. If any of these three conditions is false, dynamic routing is normally used. The dynamic routing protocols used by the routers to communicate with each other are RIP (Routing Information Protocol) , OSPF(Open Shortest Path First) and BGP(Border Gateway Protocol) .

There are certain problems in IP. IP addresses are 32-bits, which are inadequate for the long-term growth of the internet. IPv4 routing structure is not hierarchial, requiring one routing table entry per network. IPv6 is short for "Internet Protocol Version 6". IPv6 is the "next generation" protocol designed by the IETF to replace the current version Internet Protocol, IP Version 4 ("IPv4"). IPv6 fixes a number of problems in IPv4, such as the limited number of available IPv4 addresses. It also adds many improvements to IPv4 in areas such as routing and network auto configuration. IPv6 is expected to gradually replace IPv4, with the two coexisting for a number of years during a transition period.

CHAPTER 4

4. SS7 over IP Signaling Transport (SIGTRAN)

4.1 Introduction

IP networks will play an important role as carriers of signaling traffic on the future telecom networks. Traditionally, signaling has been transmitted over dedicated networks using specialized software and hardware. By using IP as carriers for signaling traffic, operators can achieve substantial cost savings. It also provides opportunities for developing new IP-based services that combine the strengths of Internet and telecommunications. Integration and interconnection of equipment from different vendors will also be much easier with standardized IP connectivity.

SS7 strengths of reliability and capacity must be combined with those of IP that include cost, flexibility and portability to create a whole that is greater than the sum of its parts.

4.2 SIGTRAN Overview

SIGTRAN (Signaling Transport) is a working group within the IETF standard organization. Its primary purpose is to address the transport of packet-based public switched telephone network (PSTN) signaling over IPP networks, taking into account the function and performance requirements of the PSTN signaling. In order to inter-work with the PSTN, IP networks need to transport signaling such as integrated service digital line (ISDN) (e.g. Q.931) or SS7 (e.g. ISDN user part (ISUP), SCCP, and so on) messages between IP nodes such as a signaling gateway (SG), a media gateway controller (MGC), a media gateway (MG), or an IP-based database.

The SIGTRAN working group specific goals are:

4.2.1 Functional Requirements

Different functional requirements for ss7 transport over IP are

- Transport of a variety of SCN protocol types, such as the application and user parts of SS7 (including MTP Level 3, ISUP, SCCP, TCAP, MAP, INAP, IS-41, etc.).

- Provide a means to identify the particular SCN protocol being transported.

- Provide a common base protocol defining header formats, security extensions and procedures for signaling transport, and support extensions as necessary to add individual SCN protocols if and when required.

- In conjunction with the underlying network protocol (IP), provide the relevant functionality as defined by the appropriate SCN lower layer. Relevant functionality may include (according to the protocol being transported):

  - flow control

  - In sequence delivery of signaling messages within a control stream

  - Logical identification of the entities on which the signaling messages originate or terminate

  - Logical identification of the physical interface controlled by the signaling message

  - Error detection

  - Recovery from failure of components in the transit path

  - Retransmission and other error correcting methods

  - Detection of unavailability of peer entities.

- Support the ability to multiplex several higher layer SCN sessions on one underlying signaling transport session. In general, in-sequence delivery is required for signaling messages within a single control stream, but is not necessarily required for messages that belong to different control streams. The

protocol should if possible take advantage of this property to avoid blocking delivery of messages in one control stream due to sequence error within another control stream.

The protocol should also allow the SG to send different control streams to different destination ports if desired.

- Be able to transport complete messages of greater length than the underlying SCN segmentation/reassembly limitations. For example,] signaling transport should not be constrained by the length limitations defined for SS7 lower layer protocol (e.g. 272 bytes in the case of narrowband SS7) but should be capable of carrying longer messages without requiring segmentation.

- Allow for a range of suitably robust security schemes to protect signaling information being carried across networks. For example, signaling transport shall be able to operate over proxyable sessions, and be able to be transported through firewalls.

- Provide for congestion avoidance on the Internet, by supporting appropriate controls on signaling traffic generation (including signaling generated in SCN) and reaction to network congestion.

4.2.2 Performance Requirements of SCN Signaling Protocols

This section provides basic values regarding performance requirements of key SCN protocols to be transported. Currently only message-based SCN protocols are considered. Failure to meet these requirements is likely to result in adverse and undesirable signaling and call behavior.

4.2.2.1 SS7 MTP requirements

The performance requirements below have been specified for transport of MTP Level 3 network management messages. The requirements given here are only applicable if all MTP Level 3 messages are to be transported over the IP network.

- Message Delay

- MTP Level 3 peer-to-peer procedures require response within 500 to 1200 ms. this value includes round trip time and processing at the remote end. Failure to meet this limitation will result in the initiation of error procedures for specific timers, e.g., timer T4 of ITU-T Recommendation Q.704.

4.2.2.2 SS7 MTP Level 3 requirements

The performance requirements below have been specified for transport of MTP Level 3 user part messages as part of ITU-T SS7 Recommendations [SS7].

- Message Loss
  No more than 1 in 10E+7 messages will be lost due to transport failure
- Sequence Error
  No more than 1 in 10E+10 messages will be delivered out-of- sequence (including duplicated messages) due to transport failure
- Message Errors
  No more than 1 in 10E+10 messages will contain an error that is undetected by the transport protocol (requirement is 10E+9 for ANSI specifications)
- Availability
  Availability of any signaling route set is 99.9998% or better, i.e., downtime 10 min/year or less. A signaling route set is the complete set of allowed signaling paths from a given signaling point towards a specific destination.
- Message length (payload accepted from SS7 user parts)
  272 bytes for narrowband SS7, 4091 bytes for broadband SS7

To achieve the functional and performance requirements for MTP, the IETF sigtran Working Group has recommended three new protocols: M2UA, M2PA, and M3UA.

4.2.2.3 SS7 User Part Requirements

- ISUP Message Delay - Protocol Timer Requirements

One example of ISUP timer requirements is the Continuity Test procedure, which requires that a tone generated at the sending end be returned from the receiving end within 2 seconds of sending an IAM indicating continuity test. This implies that one way signaling message transport, plus accompanying nodal functions need to be accomplished within 2 seconds.

- ISUP Message Delay - End-to-End Requirements

  - the requirement for end-to-end call setup delay in ISUP is that an end-to-end response message be received within 20-30 seconds of the sending of the IAM. Note: while this is the protocol guard timer value, users will generally expect faster response time.

- TCAP Requirements - Delay Requirements

  - TCAP does not itself define a set of delay requirements. Some work has been done to identify application-based delay requirements for TCAP applications.

4.2.2.4 Security Requirements for SS7 over IP

When SCN related signaling is transported over an IP network two possible network scenarios can be distinguished:

- Signaling transported only within an Intranet; Security measures are applied at the discretion of the network owner.

- Signaling transported, at least to some extent, in the public Internet; The public Internet should be regarded generally as an "insecure" network and usage of security measures is required.

- Generally security comprises several aspects

- Authentication:

  It is required to ensure that the information is sent to/from a known and trusted partner.

- Integrity:

  It is required to ensure that the information hasn't been modified while in transit.

- Confidentiality:

  It might be sometimes required to ensure that the transported information is encrypted to avoid illegal use.

- Availability:

  It is required that the communicating endpoints remain in service for authorized use even if under attack.

4.3 SIGTRAN Protocol Architecture

The architecture that has been defined by SIGTRAN work group consist 3 components:

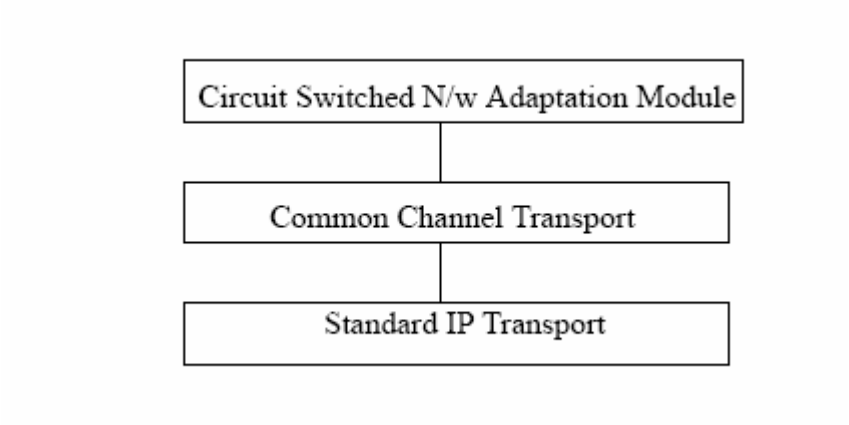


Figure 13: Sigtran protocol stack model

Adaptation sub-layer that supports specific primitives, e.g. management indications, required by a particular SCN signaling application protocol. Several new adaptation sub-layer protocols have been defined by the IETF: M2PA, M2UA, M3UA, SUA, and IUA. Only one protocol has to be implemented at a given time.

- A Common Signaling Transport Protocol that supports a common set of reliable transport functions for signaling transport. In particular, SCTP is a new transport protocol that has been defined by the IETF.

- A Standard, unmodified IP transport protocol.

Now the question arises why to develop a new transport protocol SCTP when we already have a TCP (Transmission Control Protocol) protocol which is working very fine over the IP.

4.4 Why develop a new Transmission protocol?

Transmission Control Protocol (TCP) (RFC 793) performs an enormous service as the primary transport protocol in the means of reliable data transfer in IP networks. However, because it was defined a long time ago and was designed as a packet-oriented protocol, TCP imposes several limitations for new emerging applications. An increasing number of recent applications have found TCP too limiting. Some of the limitations include the following:

- Reliability mechanisms – TCP provides both reliable data transfer, through acknowledgments mechanism, and strict order of transmission delivery of data, through sequencing mechanism. Some applications need reliable transfer without sequence maintenance, while others would be satisfied with partial ordering of the data. In both of these cases the head-of-line blocking caused by TCP adds unnecessary delay.
- Real-time issues – The above mentioned acknowledgement mechanism (which added the unnecessary delay) makes the TCP inappropriate for the real-time applications.
- TCP sockets – The limited scope of TCP sockets complicates the task of providing highly available data transfer capability using multi-homed hosts.
- Security issues – TCP is relatively vulnerable to denial-of-service attack.

All the above mentioned limitations of TCP are relevant while trying to transport SS7 signaling over IP networks, and this is the direct motivation for the development of SCTP as a new transport protocol for SIGTRAN. SCTP has not been developed solely for SIGTRAN; thus SCTP may be a good solution for the requirements of other applications.

4.5 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 signaling messages between signaling 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 which will send and receive SCTP packets. IP signaling traffic is usually composed of many independent message sequences between many different signaling endpoints. SCTP allows signaling 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 signaling messages over IP networks.

There are three types of messages in SS7:

- Message Signal Units (MSUs)
- Link Status Signal Units (LSSUs)
- Fill-In Signal Units (FISUs)

MSUs originate at a higher level than MTP Level 2 and are destined for a peer at another node. LSSUs allow peer MTP Level 2 layers to exchange link status information. FISUs are sent when no other signal units are waiting to be sent across the synchronous link. This purpose is preserved by the heartbeat messages in SCTP. FISUs also carry acknowledgment of messages, a function also assumed by SCTP.

In summary, SCTP provides:

- Acknowledged error-free non-duplicated transfer of signaling information.
- in-sequence delivery of messages within multiple streams, with an option for order of- arrival delivery of individual messages
- optional bundling of multiple messages into a single SCTP packet
- data fragmentation as required
- network-level fault tolerance through support of multi-homing at either or both ends of an association
- appropriate congestion avoidance behavior and resistance to flooding (denial-of-service) and masquerade attacks

To meet stringent SS7 signaling reliability and performance requirements for carrier-grade networks, VoIP network operators ensure that there is no single point of failure in the end-to-end network architecture between an SS7 node and a media gateway controller. To achieve carrier-grade reliability in IP networks, links in a link-set are typically distributed amongst multiple signaling gateways, media gateway controllers are distributed over multiple CPU hosts, and redundant IP network paths are provisioned to ensure survivability of SCTP associations between SCTP endpoints.

4.6 Various Issues with the SCTP

There are two major issues with need to be dealt for the SCTP here:

4.6.1 Issues related to Routing and Addressing

One of the basic problems in any network is to get from point A to point B. Another problem is how to choose between different point B. The first problem is solved via SCTP associations (put the message in SCTP at one end, and voila, it pops out at the other end). The second problem is solved via addressing. Some signaling is point-to-point, meaning that it simply needs a SCTP association to get to the other side. Other Signaling needs to route based on its addressing contained in the message (M3UA, SUA). As the meaning of the point codes is only known to IP and it has a relation to the link and its interface to the link, layers which only know about destinations (such as SCCP), must not try to interpret the IP address. The IP point code does not strictly identify the node in the network but rather the interface to the IP network layer. Thus IP nodes can have more than 1 Point code (and those PC can be used for having 2 links between 2 adjacent nodes, a feature that is called multi-homing). Examples of usage for SS7-over- IP include:

- PSTN to IP - terminating call-related and non-call related signaling to a Media gateway Controller (MGC).

- PSTN-IP-PSTN - Transparent transport of signaling information across an intranet or internet infrastructure between 2 intermediate SS7 nodes.

- IP to PSTN - Originating call-related and non-call related signaling from the SS7-over-IP net to the PSTN.

- IP-PSTN-IP or IP-IP - SS7-over-IP to SS7-over-IP networks.

SS7 messages are transported across IP using the Stream Control Transmission Protocol (SCTP). SCTP provides a high reliable, redundant transport between 2 SS7-over-IP nodes. A SS7-over IP node is a SCTP endpoint. The interface with SS7 is message based. Therefore a adaptation later is needed to prevent changes to the upper

layer SS7protocols. Within an association between 2 endpoint, 1 or more stream(s) may be available. These streams are not directly visible to the adaptation layers.

The link-set towards a certain destination is the collection of all the links which can send traffic to that destination, even with a intermediate node in between (so different path towards that destination exist). The MTP link-set is thus equivalent to the SCTP association. The streams within SCTP may be regarded as the links. A advantage of SCTP streams is, when one of the multi-homed paths fails, the stream will migrate to one of the still open paths (Soft changeover). In SS7 when a link fails, a a change over procedure has to be initiated towards a still working link of the same link set (=hard changeover)).

In a MTP based network, the capacity of the links is fixed at n times 64Kb (with n=1,32,...). SCTP association does not have a fixed capacity assigned to them. The bandwidth used/provided by SCTP is dependant on the rest of the traffic(other SCTP, TCP, RTP,UDP...) going through the same links of the path followed by the SCTP association. The M3UA layer has to handle at least one or more SCTP associations. The selection of a SCTP association can be done by via a single part or multiple parts of the DPC, OPC, SLS, CIC fields of the MTP routing label. If a association were to fail then alternate mappings may be done. RIP, OSPF and BGMP protocols of IP influence the M3UA and SCCP routing for transporting SS7 over IP.

As the signaling is in fact transported over a “SS7” overlay network on top of IP, both SS7 point codes and IP point codes are used. The basic routing in the overlay network is done using SS7 point codes. However at a certain point, that SS7 point code must be mapped to a IP point code because (1) SCTP uses the IP point code(+port number) for selecting the correct association and (2) IP routes only on IP point codes. IP addresses are required to be globally unique. If SS7 wants to transport its messages over an IP network, then they should be treated as global addresses. This means that SS7 shall look at them as global titles it shall NOT rely of the specific handling of the addresses by the underlying IP layer and below. This also means that SCCP is a prerequisite for

transporting message over an IP infrastructure when non-call related messages are to be transported over IP. ISUP and other signaling protocols will have to the same for call related messages, translating the addresses it has in the adaptation layers to IP addresses. They can all invoke the GTT function if wanted. The types of translations that need to be supported are as listed out in table 3.

TABLE 3. Global Title Translations(GTT)

Sl. No.	Input of GTT	Output of GTT
1.	E164, E212	IPv4 or Ipv6
2.	IPv4, IPv6	IPv4, IPv6
3.	IPv4, IPv6	E164, E212
4.	IPv4, IPv6	MTPaddress (Pointcode)

The GTT function could support IP point codes. The IP point code must be put in the digit block of the GT. The representation may be in BCD, the meaning of it should not. The length of a Ipv4 address (32bits) should then be 8 digits (always fixed). The length of a Ipv6 address (128bits) should be 32 digits. The GT number of digits in the SCCP header should allow for at least 32 digits (some extra digits may need to be inserted for proper routing). The result attached to a certain translation must be or a MTP PC (14,24) or a Ipv4 PC or a Ipv6 PC. The nature of address may be defined as indicating a international address with bitmap format. This could even lead to a new GTT operation (besides insert, copy, delete replace) called bitmapPCCopy. The bitmapPCcopy takes the IPvx point code out of the GT and uses it as the resulting point code of the GTT for further routing. The same effect can also be achieved via proper engineering of the GT database.

Other possibilities include user adaptation layers which maps the MTP point code to IP point code or a mapping from MTP point code to a certain SCTP session.

If GTT is used then IP must need a Numbering plan indicator (NP value normally assigned by SG11). This may or may not be agreed with SG11. This is not mandatory (but it is encouraged) as already there exists private numbering plans not known to SG11.

This is a bilateral agreement between operators/Internet Service providers). Also maybe the port number may become part of the input/output to the GTT function.

Problems may occur with dynamically assigned IP addresses. The node could obtain a IP address that is later reclaimed and/or replaced by another IP address out of a pool of IP addresses. The destination address in the routing tables would have to be invalidated or changed. Therefore it is strongly recommended to use a fixed assigned IP address. It should not be regarded as a dial-up user (for which Dynamic assigned addresses are meant). Also, dynamically assigned address may invalidate security features of SCTP.

If transport addresses may change during the lifetime of a SCTP association, it is impossible to reliably ensure that the current transport address is the transport address which was used in the setup of the association. If this practice should turn out to be unavoidable, then a Q3/SNMP Management message would be required to be exchanged between DHCP and SCCP network element configuration part so that the point code attached to a certain GT must be updated, deleted or added. The same solution is also feasible for working in NAT's with dynamical assigned addresses.

4.6.2 Issues related to Security

Security Mechanisms Currently Available in IP Networks: Several security mechanisms are currently available for use in IP networks.

- IPSEC ([RFC2401]) : IPSEC provides security services at the IP layer that address the above mentioned requirements. It defines the two protocols AH and ESP respectively that essentially provide data integrity and data confidentiality services. The ESP mechanism can be used in two different modes:

- Transport mode;

- Tunnel mode.

In Transport mode IPSEC protects the higher layer protocol data portion of an IP packet, while in Tunnel mode a complete IP packet is encapsulated in a secure IP tunnel. If the SIG embeds any IP addresses outside of the SA/DA in the IP header, passage through a NAT function will cause problems. The same is true for using IPsec in general, unless an IPsec ready RSIP function is used as described in RFC 2663 .

The use of IPSEC does not hamper the use of TCP or UDP as the underlying basis of SIG. If automated distribution of keys is required the IKE protocol ([RFC2409]) can be applied.

a. SSL, TLS ([RFC2246]):

SSL and TLS also provide appropriate security services but operate on top of TCP/IP only.

It is not required to define new security mechanisms in SIG, as the use of currently available mechanisms is sufficient to provide the necessary security. It is recommended that IPSEC or some equivalent method be used, especially when transporting SCN signaling over public Internet.

Various aspects of security in transporting SS7 over IP are:

Authentication:

Information is sent/received from a known and/or trusted partner. Until recently the number of interconnects of a SS7 node with another SS7 node belonging to another operator was relatively limited and those other operators were implicitly known (and sometimes trusted). Due to the increasing interconnect demands between different operators on a voluntary or mandatory basis the trusted relation does not longer exist.

That means that a operator will not accept all SS7 message send to him by another operator. This is done using MTP and SCCP screening: depending on the information in

the different MTP fields(example OPC...) and/or SCCP fields(example Calling party address, SSN...) a message may be rejected or accepted for transport across or termination into the network. In the worst case it may try to screen up to the application level. A SS7 gateway using screening does behave like a firewall.

Integrity:

Information may not be modified while in transit. The integrity of a msg in a over a IP network the integrity may be guaranteed at 2 levels.

- The IP level using IPsec: Which is equivalent to providing integrity on SS7 link level basis. Keydistribution is at most limited to the network of that operator.

- End-To-End integrity using TCAP.

Confidentiality:

Confidentiality of the user data must be ensured. User data can not be examined by unauthorized users.

Availability:

The communicating endpoint must remain in service in all circumstances. All SS7 nodes have to remain active for the 99.999% of the time.

4.7 M2UA: MTP2 User Adaptation Layer

M2UA is a protocol defined by the IETF sigtran Working Group for transporting SS7 MTP Level 2 user (i.e. MTP Level 3) signaling messages over IP using the SCTP (see section on 'SCTP: Stream Control Transmission Protocol'). The M2UA protocol layer provides the equivalent set of services to its users as MTP Level 2 provides to MTP Level 3.

M2UA is used between the Signaling Gateway and Media Gateway Controller in VoIP networks. The signaling gateway receives SS7 messages over an MTP Level 1 and Level 2 interface from a signaling end point (SCP or SSP) or signal transfer point (STP) in the public switched telephone networks. The signaling gateway terminates the SS7 link at MTP Level 2 and transports MTP Level 3 and above to a Media Gateway Controller or other IP endpoint using M2UA over SCTP/IP.

The signaling gateway maintains the availability state of all media gateway controllers to manage signaling traffic flows across active SCTP associations.

4.8 M2PA: MTP2 User Peer-to-Peer Adaptation Layer

Like M2UA, **M2PA** is a sigtran protocol for transporting SS7 MTP Level 2 user part signaling messages (i.e. MTP Level 3) over IP using the Stream Control Transmission Protocol (SCTP). Unlike M2UA, M2PA is used to support full MTP Level 3 message handling and network management between any two SS7 nodes communicating over an IP network. IP signaling points function as traditional SS7 nodes using the IP network instead of the SS7 network. Each switched circuit or IP signaling point has an SS7 point code. The M2PA protocol layer provides the same
set of services as MTP Level 2 provides to MTP Level 3.

M2PA can be used between a signaling gateway and a media gateway controller, between a signaling gateway and an IP signaling point, and between two IP signaling points. Signaling points may use M2PA over IP or MTP Level 2 over standard SS7 links to send and receive MTP Level 3 messages.

M2PA facilitates the integration of SS7 and IP networks by enabling nodes in switched circuit networks to access IP telephony databases and other nodes in IP networks using SS7 signaling. Conversely, M2PA allows IP telephony applications to access SS7 databases, such as local number portability, calling card, free-phone, and mobile subscriber databases. In addition, using M2UA over IP may result in cost advantages if traditional SS7 links are replaced by IP connections.

In summary, M2PA and M2UA differ in the following ways:

- M2PA: the signaling gateway is an SS7 node with a point code;
  M2UA: the signaling gateway is not an SS7 node and has no point code.
- M2PA: the connection between the signaling gateway and IP signaling points is an SS7 link;
  M2UA: the connection between the signaling gateway and the media gateway controller is not an SS7 link. Rather, it is an extension of MTP from the signaling gateway to the media gateway controller.
- M2PA: the signaling gateway can have upper SS7 layers, such as SCCP;
  M2UA: the signaling gateway has no upper SS7 layers as it has no MTP Level 3.
- M2PA: relies on MTP Level 3 for management procedures;
  M2UA: uses M2UA management procedures.
- M2PA: IP signaling points processes MTP Level 3 and MTP Level 2 primitives;
  M2UA: the media gateway controller transports MTP Level 3 and MTP Level 2 primitives to the signaling gateway's MTP Level 2 for processing.

4.9 M3UA: MTP Level 3 User Adaptation Layer

M3UA is a protocol defined by the IETF sigtran Working Group for transporting MTP Level 3 user part signaling messages (e.g., ISUP, TUP, and SCCP) over IP using the Stream Control Transmission Protocol (SCTP). TCAP or RANAP messages, as SCCP user protocols, may be carried by SCCP using M3UA or by a different sigtran protocol called SUA, as described below.

M3UA is used between a signaling gateway and a media gateway controller or IP telephony database. The signaling gateway receives SS7 signaling using MTP as transport over a standard SS7 link. The signaling gateway terminates MTP-2 and MTP-3 and delivers ISUP, TUP, SCCP
and/or any other MTP-3 user messages, as well as certain MTP network management events, over SCTP associations to media gateway controllers or IP telephony databases.

The ISUP and/or SCCP layer at an IP signaling point is unaware that the expected MTP-3 services are not provided locally, but rather by the remote signaling gateway. Similarly, the MTP-3 layer at a signaling gateway may be unaware that its local users are actually remote parts over M3UA. Conceptually, M3UA extends access to MTP-3 services at the signaling gateway to remote IP endpoints. If an IP endpoint is connected to more than one signaling gateway, the M3UA layer at the IP endpoint maintains the status of configured SS7 destinations and route messages according to the availability and congestion status of the routes to these destinations via each signaling gateway.

M3UA does not impose a 272-octet signaling information field (SIF) length limit as specified by SS7 MTP Level 2. Larger information blocks can be accommodated directly by M3UA/SCTP without the need for an upper layer segmentation/re-assembly procedure as specified by the SCCP and ISUP standards. However, a signaling gateway will enforce the maximum 272-octet limit when connected to a SS7 network that does not support the transfer of larger information blocks to the destination. For broadband MTP networks, the signaling gateway will fragment ISUP or SCCP messages larger than 272 octets as required.

At the signaling gateway, the M3UA layer provides inter working with MTP-3 management functions to support seamless operation of signaling between the SS7 and IP networks. For example, the signaling gateway indicates to remote MTP-3 users at IP endpoints when an SS7 signaling point is reachable or unreachable or when SS7 network congestion or restrictions occur. The M3UA layer at an IP endpoint keeps the state of the routes to remote SS7 destinations and may request the state of remote SS7 destinations from the M3UA layer at the signaling gateway.

The M3UA layer at an IP endpoint may also indicate to the signaling gateway that M3UA at an IP
End-point is congested.

4.10 SUA: SCCP User Adaptation Layer

SUA (SCCP User Adaptation Layer) is a protocol defined by the IETF sigtran Working Group for transporting SS7 SCCP (Signaling Connection Control Part) user part signaling messages (e.g., TCAP and RANAP) over IP using the Stream Control Transmission Protocol (SCTP). SUA is used between a signaling gateway and an IP signaling endpoint and between IP signaling endpoints. SUA supports both SCCP unordered and in-sequence connectionless services and bidirectional connection-oriented services with or without flow control and detection of message loss and out-of-sequence errors (i.e., SCCP protocol classes 0 through 3).

For connectionless transport, SCCP and SUA interface at the signaling gateway. From the perspective of an SS7 signaling point, the SCCP user is located at the signaling gateway. SS7 messages are routed to the signaling gateway based on point code and SCCP subsystem number. The signaling gateway then routes SCCP messages to the remote IP endpoint. If redundant IP endpoints exist, the signaling gateway(s) can load share amongst active IP endpoints using a round-robin approach. Note that load sharing of TCAP messages occurs only for the first message in a TCAP dialogue; subsequent TCAP messages in the same dialogue are always sent to the IP endpoint selected for the first message, unless endpoints share state information and the signaling gateway is aware of the message allocation policy of the IP endpoints. The signaling gateway may also perform Global Title Translation (GTT) to determine the destination of an SCCP message. The signaling gateway routes on global title, i.e. digits present in the incoming message, such as called party number or mobile subscriber identification number.

For connection-oriented transport, SCCP and SUA interface at the signaling gateway to associate the two connection sections needed for connection-oriented data transfer between an SS7 signaling end point and an IP endpoint. Messages are routed by the signaling gateway to SS7 signaling points based on the destination point code (in the MTP-3 address field) and to IP endpoints based on IP address (in the SCTP header).

SUA can also be used to transport SCCP user information between IP endpoints directly rather than via the signaling gateway. The signaling gateway is needed only to enable interoperability with SS7 signaling in the switched circuit network.

If an IP resident application is connected to multiple signaling gateways, multiple routes may exist to a destination in the SS7 network. In this case, the IP endpoint must monitor the status of remote signaling gateways before initiating a message transfer.

4.11 SS7 over IP Performance

Signaling quality requirements could be expressed by simply stating that call set-up time, and generally signaling delays, should be similar to those observed in classic telephony networks. However, one could certainly envisage different trade off between network performance, net-work cost, and user services. When analyzing the requirements, we will distinguish between absolute requirements, which are mandated for proper interaction with the classic telephone network, and quality objectives, which are mostly desirable goals. General performance target for SS7 networks the performance objectives of a SS7 network are dealt with in two ITU-T recommendations, Q.706 and Q.709. The design of the SS7 provides for error detection, correction and sequential transfer of signal units. The main objectives to be met are:

1) To limit delay in signaling connections in the network.

2) To achieve a high degree of availability of signaling connections.

The availability and dependability objectives for the transport of signaling messages by the MTP in these networks are:

- No more than one in 10E+7 (1 in 10,000,000) messages should be lost.
- No more than one in 10E+10 messages should be delivered out of sequence or duplicated.

- No more than one in 10E+9 message errors should remain undetected.
- The signaling route between an origination and destination SP should be available 99.9998% of the times or better. This implies a maximum permissible downtime or unavailability of 10 minutes per year per route.
- Though there are no specific end-to-end delay objectives for SS7, they are specified for specific services or uses of the SS7 protocol. Further there are delay objectives for some network components, and others can be calculated. Thus an estimate can be made for any given network configuration.

Performance parameters for specifying signaling delays are given in terms of a hypothetical signaling reference connection (HSRC), for international working.. The maximum signaling delays in International and National Components of an HSRC, estimated for link-by-link processing over the entire connection, for 95% of signaling connections are:

- National Component (large): 520 (800) ms
- National Component (average): 390 (600) ms
- International Component (large to large): 410 (620) ms
- International Component (large to average): 540 (820) ms
- International Component (average to average): 690 (1040) ms

The values are for simple message type and for complex message types in parentheses. The definition for an average-sized country is one where maximum distance of a subscriber from an ISC is within 1,000 km or where the number of subscribers is fewer than n x 10 million (n is not yet specified). Moreover the maximum number of nodes (includes all SPs, STPs, SEPs etc), in an HSRC, for 95% of signaling connections are also fixed.

- National Component (large): 8* National Component (average): 6
- International Component (large to large): 7

- International Component (large to average): 9
- International Component (average to average): 12

The delays within each of the network elements such as the STP are made up of the Processor Handling time and the Message Transfer time. The values vary with the length of the message being transmitted. For a range of message lengths of (23 - 279) bytes, mean and 95% values for these times are:

STP Processor Handling Time:

Normal Processor Load	19 - 55 ms	35 - 75 ms
+ 30% Load	60 - 160 ms	120 - 320 ms

STP Outgoing Link Delay with Basic Error Correction and no Disturbances:

Link Load 0.2 erlang	4.0 - 39.6 ms	14 - 61.5 ms
Link Load 0.4 erlang	5.2 - 46.9 ms	14 - 61.5 ms

Thus the allowed signaling link delays can be computed for any given network. For an average-sized country with 6 nodes, a simple message of 50 bytes, with normal processor load and 0.2 erlang link load will require about 290 ms of signaling delays within its various nodes. This implies we have approximately 100ms at most for signaling link delay.

Expected performances of the underlying IP network

The quality of service delivered by IP transport mechanisms depends on the quality of the underlying IP network service. We have studied this quality under three assumptions:

- Basic Internet quality, as derived from the observation of today's network.
- Internet telephony quality, supposing that the IP network has been engineered to provide a quality of service compatible with the transmission of voice over PSTN.

- Best possible quality, assuming that the signaling runs at a high level of priority, that there are no congestion losses, and that we are only limited by the underlying loss rate of the transmission network, which we will assume here to be a SONET based network.

- Basic Internet quality

Several measurement efforts going on today have reported figures of transmission quality that vary heavily with the network path:

- Statistical measurements and analysis by Guy Almes and also Sanghi et. al., show that the losses in the Internet today are in the range of 2-10%. Losses have a direct correlation with delay and we will discuss some of these issues in the section that covers TCP and UDP.

- Experiments conducted at Bellcore show that the busy hour average packet loss rate on random cross-Internet connections can be as high as 16%.

- The busy hour transmission delays round trip delay between well connected sites varies between 100 and 300 ms.

A general conclusion from these observations is that the basic Internet quality, today, would not really allow the transmission of toll quality voice, except on some "lucky" subsets.

Internet Telephony IP quality

We may expect that Internet Telephony will often be transported over dedicated IP networks, and that prioritization and access control will be used to guarantee a level of service that is compatible with quality expectation of telephony users.

Telephony applications can be described as relatively tolerant to a small amount of packet losses (e.g. 1% or 2%), but very dependent on a small network delay. In fact, the key characteristic of the quality of service is the end to end voice delay:

- An end to end delay lower than 100 or maybe 150 ms is generally deemed compatible with “toll quality.”

- An end to end delay between 150 and 350 ms is generally considered mediocre but can be accepted in some circumstances. System using geo-stationary satellites incur this kind of delay.

- And end to end delay larger than 350ms is generally not considered acceptable, except under exceptional circumstances such as, for example, space exploration. The end to end speech delay is the sum of several components:

- Coding and packetization delays,
- Network transmission delays,
- Jitter compensation delays at the receiver,
- Decoding and play out delays.

In consequence, we may expect cross network transmission delays to not exceed 50 to 100 ms, while the packet loss rate could reach value of 1% or 2%.

Adequacy of TCP

The requirement of losing less than 10E-7 packets could, on the surface, be met by simply sending packets over a TCP-IP connection. TCP meets the reliability strategy by retransmitting lost packets either after a transmission delay (duplicate ack detection) or after the expiration of a timer. However, the delay introduced by these retransmissions affect the remaining in-sequence packets and may lead to expiration of the signaling (e.g. ISUP) timers. Thus, guaranteed delivery by TCP may in fact be its pitfall. It is observed that the delay of the number of consecutive packets following a fast retransmit depends on the round trip time (RTT) and the Inter Packet Interval (IPI). Packets following a loss event must wait to be delivered to the application until the missing packet is resent and received correctly at the destination host. This effect of the in-order delivery requirement of TCP results in each loss event depicted resembling a comb: several spikes with the

same amplitude are equally spaced by the packet inter arrival interval. The first three spikes represent the number of duplicate acknowledgments needed at the source to trigger a fast retransmit. The remaining spikes represent the number of additional packets in flight that are delayed at the receiver from being delivered to the application by the absence of the lost data packet. In the 1980's, TCP was often used for remote terminal applications that would send "one character per packet". It was observed that TCP's flow control, which limits the number of bytes in transit, was very inefficient under these circumstances, because it would allow stations to transmit a very large number of small packets before reaching the flow control window. For this reason, TCP implementations incorporate a rate limiting algorithm. A station that transmits a "small" packet should wait for its acknowledgement before transmitting the next packet.

The SS7 packets are short enough that if sent one at a time, they may well trigger the rate limitation algorithm, which will have two effects:

- The next packet (or packets) will be queued for a full round trip time before transmission, which will affect performance.

- Because the short packet will be the last of a batch, losses of that packet will have to be corrected by timer-based retransmission.

We can summarize the hard requirements of ISUP by saying that transmission delays should not be larger than 1 second in more than in one case in 10,000,000. The main problem with TCP in these conditions is the timer based retransmission: a typical timer value of 1 second, combined with three transmission delays, exceeds the 1 second limit. The worse performances will be obtained in the case of isolated packets, due to either a low level of traffic or the triggering of a rate limitation algorithm. In this case, the only way to guarantee that the performance will be met is to make sure that the packet loss rate is lower than 10E-7, which is a very low number. It is much lower than the average packet loss rate values observed. Hence the calculations for theoretical performance levels of ISUP messages over a SONET network using TCP/IP may get

affected by another order of magnitude. If the delay introduced by these losses exceeds the delay bounds set by the ISUP timeouts, then those messages are considered to be lost. Delay due to loss of packets, increases net message loss rate by factor of 10 => 2 x 10E-5 to 2 x 10E-4.

Adequacy of UDP

The complex connection-oriented protocol state machines in TCP add overhead for a simple request/response exchange between two hosts. Moreover, the retransmission mechanisms in TCP get triggered by any unacknowledged byte, adding an unnecessary delay to a number of subsequent signaling messages. UDP on the other hand does not provide any loss protection to the messages transported. ARQ enhancement allow for retransmission of lost or corrupted packets, but these require at least an additional 1.5 round trip times. Recently, versions of UDP are being discussed which are sup- pose to provide a guarantee against loss of data. One such proposal is Reliable UDP or RUDP which supports different levels of services based on the reliability negotiated between the two endpoints. RUDP extends the datagram service of UDP to include reliable and ordered delivery, based on timer values which trigger retransmission.

4.12 Conclusion

Using ISUP directly over UDP we cannot get adequate loss performance to meet the ISUP loss requirements. Use of a simple TCP's retransmission mechanisms to protect against loss of ISUP messages is feasible, but at the cost of introducing latency. The interaction between IP routing protocols and SS7 routing may require some study especially in the case that routes start changing due to routing re-computation. The load-sharing and primary/backup systems of GTT seems not to be impacted as it relies on destinations and not on links but it requires to understand the IP addresses as well. Adaptation layers (M3UA, M2UA and SUA) are required over the common transport layer of SCTP in order to transport SS7 over IP. These protocols fulfill the functional requirements QoS on the internet can be improved by the use of protocols like RSVP. Security considerations can be met with the IPsec, SSL and TLS protocols.

CHAPTER 5

5. IMPLEMENTATION

5.1 Lab Demo Setup

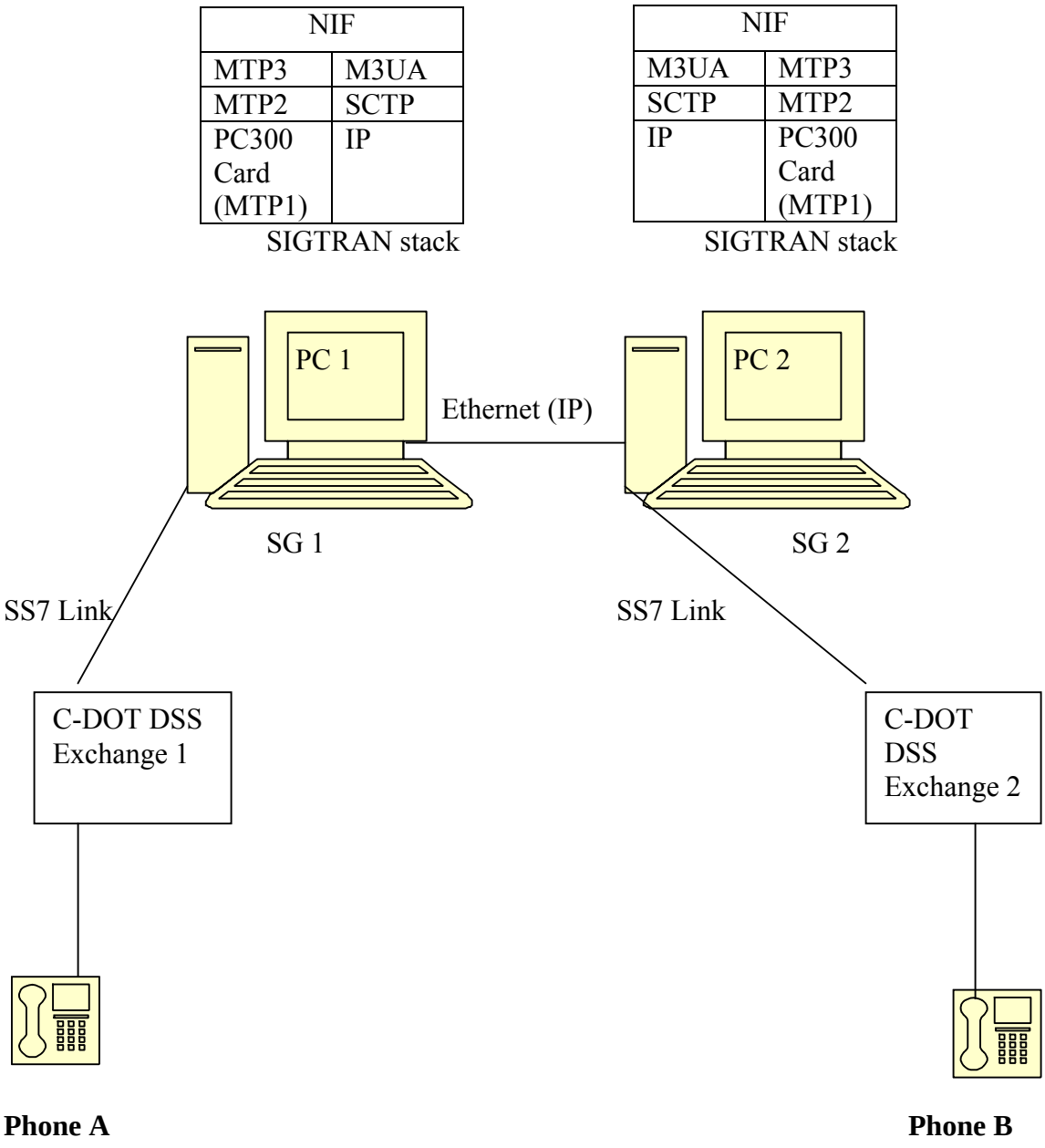


Figure 14: Lab Demo Setup

For the above shown Demo set up we require following Hardware and software.

5.2 Hardware Requirements

In order to implement this project we need following hardware setups:

1) C-DOT DSS (Digital switching system)

Currently in C-DOT SS7 signaling is implemented according to DSS (Digital switching system) architecture. There is one module called SUM (signaling unit module) which is responsible for providing number 7 signaling. In this module MTP2 and MTP3 are implemented with following cards:

HPC card on which all MTP-3 functionality is implemented and using 68040 processor of Motorola and

PHC (protocol handler card) on which all MTP-2 functionality is implemented which utilize 68302 Motorola processor.

The two PHC and HPC communicate with the help of shared memory. There are 8 PHC cards and one HPC card in SUM. Each PHC card support 16 channels, so overall 16*8 ie.128 channels can be supported. These channels can be configured to work as a SS7 signaling link between to exchanges. This hardware caters to the two types of terminations, C85 termination for the internal module communication and E1 termination for the SS7 network. C85 link supports X.25 protocol. E1's are the 32 slots PCM links. Some of its slots are used for SS7 signaling. These slots connect this hardware to the external SS7 network.

The E1's are terminated on trunk card which extract the signaling slots with the help of DSP chips and send the signaling information towards the PHC.

Each PHC card consisting of two complexes in which each complex contains a pair of 68302 processors working in master slave mode. Each pair of 68302 provides four SCCs (Serial Communication Channels). Each of these SCCs can be configured to cater to different types of protocol (some for catering to SS7 protocol and some for catering to X.25 related protocol). The ethernet terminations of IP network will terminate on an IPC, Internet processor Card. IPC will receive the IP datagram and send them to PHCs for

each transport association. For this purpose the SCCs of PHC which are configured for IP will be used. The SCCs configured as No. 7 will be connected to Trunk card. The main processor is HPC, Signaling Processor, which is 68040 based and resides in SPC, Signaling Processor Card.

There is a memory which is shared between the PHC and the HPC. The communication between the two processors is via this shared memory.

2) A Personal Computer(PC),

With Linux Operating System.

3) A PC300 Cyclade card

This card is purchased from CYCLADE Company & is used for the interfacing between PCM E1/T1 links to PC.

4) A K1297 Tektronics Protocol Analyzer

This is a Protocol analyzer tool. This is very sophisticated PC based equipment which contains all types of Protocol stacks for the testing purpose. E.g. If you want to check the performance of your exchange's SS7 protocol then you can connect your exchange with this analyzer, load this analyzer with the SS7 protocol stack, configure it to work as an another exchange (simulation mode). Now if you send any protocol message to this analyzer then it will behave as like the other exchange. Hence in telecom testing point of view this is a very important protocol analyzer tool.

5.3 Software Requirements

1) For the C-DOT DSS switches we have the C-DOT's own software which is very specific to its hardware. So we are not going to change any thing in this software. The brief description of this software is given below:

The DSS software will be residing over the above mentioned DSS hardware. For the internal communication between Trunk cards and PHCs the X.25 protocol is used. The

communication between the PHCs and the HPC will be through the common data structures in the shared memory. Terminal handler process (TRMH) at the HPC will configure the SCC's of the PHC's. It will configure some of type No.7 and others of type C85. The No. 7 types of links are used for SS7 signaling messages flow i.e. the message meant for going outside the exchange, travel on this type of link and the C85 type of links are used for the flow of information inside the DSS switch, i.e. from one module to another module of the DSS internally.

Depending on the type configured on the SCC's some processes will be created which will cater to the processing on those SCC's. The SCC of type No.7 will have MTP3 and GTT handler processes created on it.

The software for catering to SS7 transport over IP is divided into various modules.
These are shown in figure 17 along with their placement on the hardware.

SCCP Handler

It caters to the SCCP protocol and resides on the SPC. It takes care of the SCCP connection oriented, connectionless and the management functionality of the SCCP. There is no change required to be done in this for catering to SS7 transport over IP.

MTP3 Handler

It caters to the MTP layer 3 protocol and resides at the SPC. All the messages after MTP layer 2 processing is send to the MTP3 process

MTP2 Handler

It caters to the MTP layer 2 protocol and resides on the PHC. All the SCCs configured as SS7 type have this process created on it. All the messages arriving on or to be send onto No.7 link are processed by this process for layer 2 handling.

2) For the SIGTRAN protocol stack, we have purchased the whole SIGTRAN software from the US based company CCPU (Continues Computing). The CCPU provides very generic kind of software which can be run on any platform, on any operating system, with any type of hardware, etc.
For our requirement, we had taken the raw generic SIGTRAN software from the CCPU, and then change the APIs, flags etc according to our system hardware & operating system. We compiled this software for linux based operating system & prepare a final executable binary name "SigTran".

From the various user adaptation layers described above, the whole team has decided to go for the M3UA only as the user adaptation layer in the first phase.

All the layers of the CCPU software have a generic implementation which is shown in the figure below:

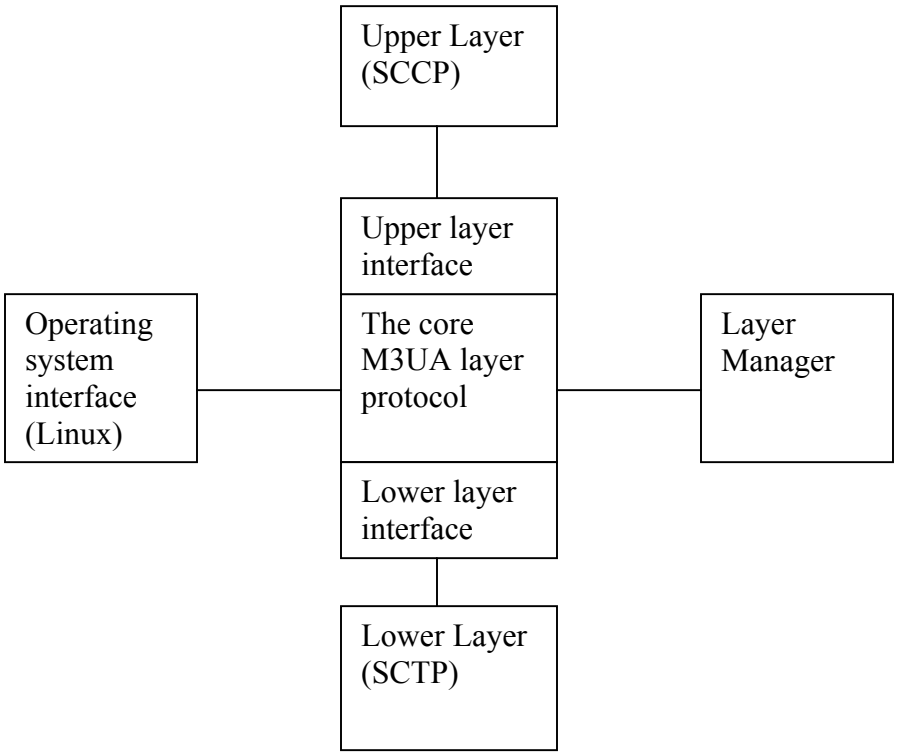


Figure 15: CCPU protocol software architecture

The core layer is completely provided by the CCPU. It contains the whole layer (e.g. M3UA) functionality.

The Layer manager manages the layer resources and provides functions such as run-time configuration, control, statistics, status, alarm, and other management functions required and provided by the M3UA protocol layer.

The Operating system interface is used obtain operating system services using a generic, portable interface that isolates the protocol layer from the underlying platform. Functions provided at this interface include initialization, task management, inter-task communication, timer management, memory management, message and queue management, date and time management, and resource checking.

The upper layer interface is used to interface the core layer with the upper layer; similarly the lower layer interface is used to interface the core layer with the lower layer protocol.

By making its software like this, the CCPU has made it generic. The core stack is same for all types of system, hardware, operating system. Only we need to port the Layer manager, Operating system interface, Upper & Lower layer interfaces according to our hardware, software architecture, and operating system.

If we see our Demo Setup then it is very clear that in order to establish this setup, we need all the above 4 mentioned hardware. As DSS is already working system, we do not need the touch it. The only thing we need to install and configure is the PC300 card into the Personal Computer (PC).

This card can be easily installed within the PC by inserting this card into the one of the PCI slot provided in the CPU.

The steps to be performed in order to configure this PC300 card so that it can work as the HDLC protocol are given below:

5.4 PC300 Card Installation

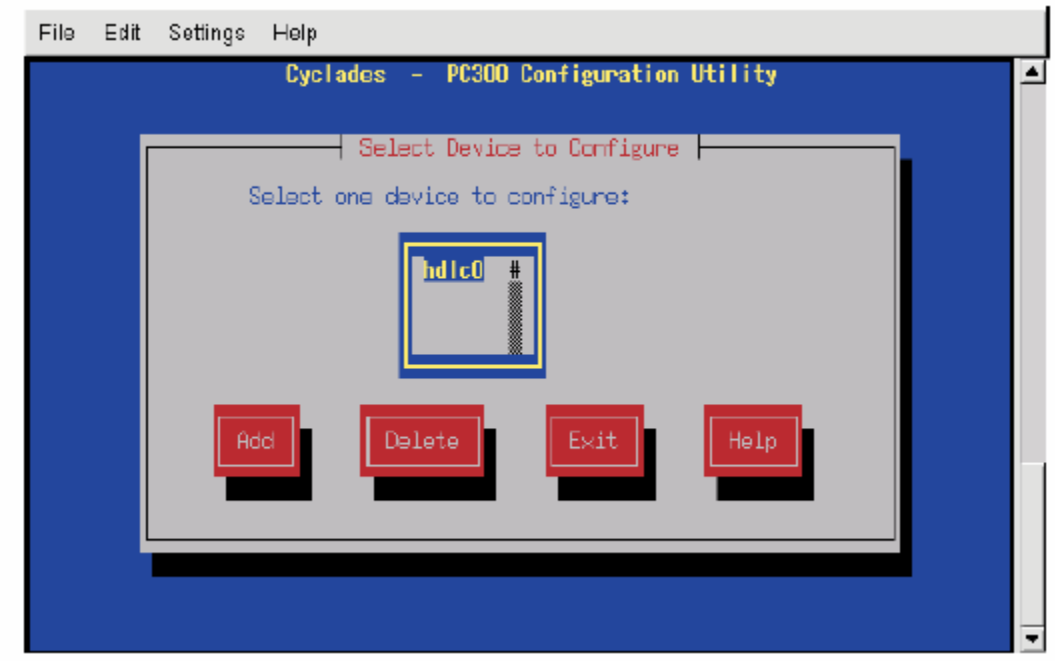
In order to connect the PC with the DSS by using E1 PCM we need to install the PC300 card inside the PC. The steps to configure this card are as follows:

Configuring the PC300 using the pc300config utility:

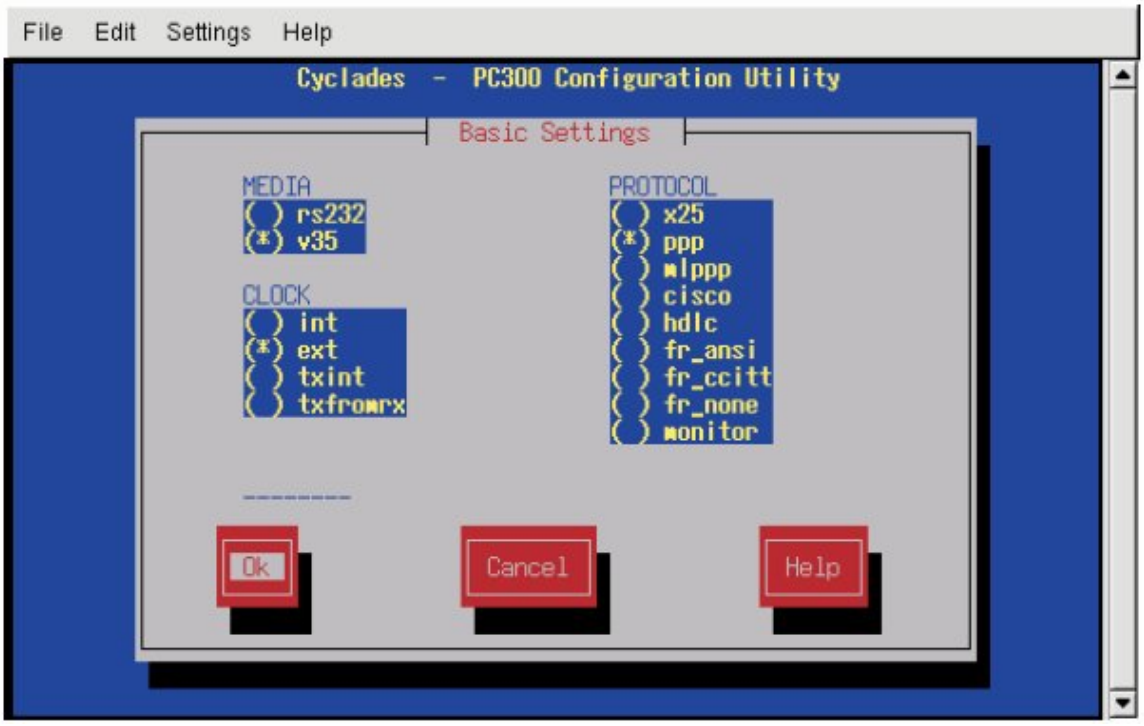
Run pc300config on the linux operating system by executing:

/usr/local/sbin/pc300config

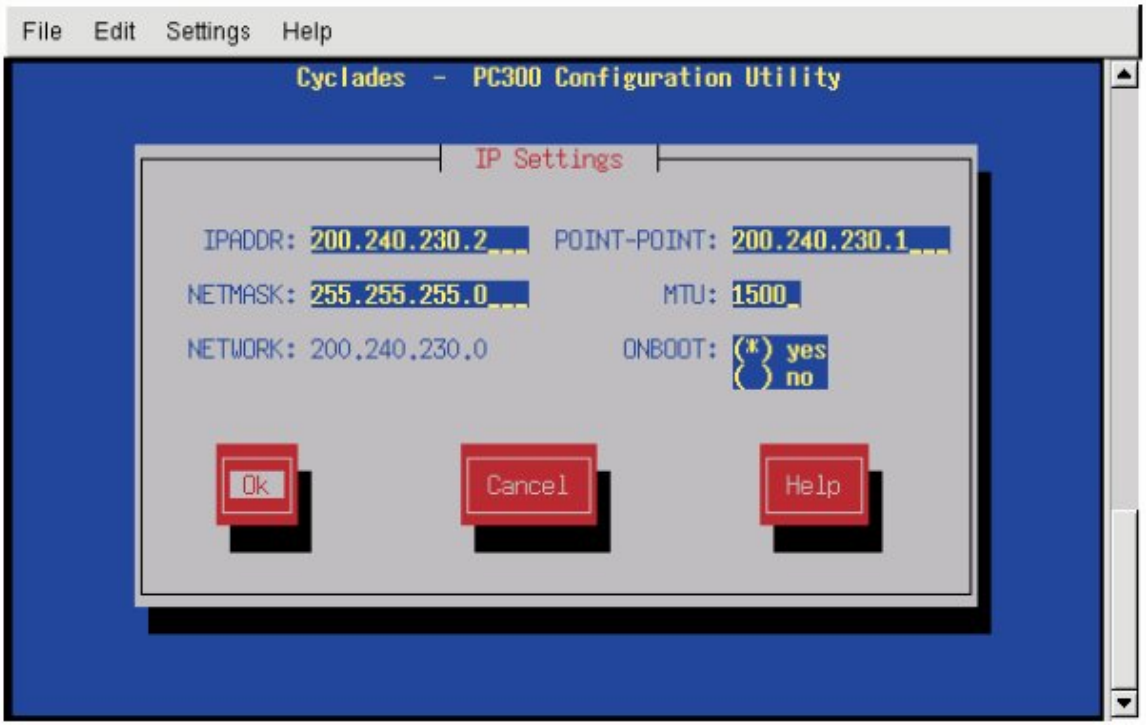
The first pc300config screen should appear:



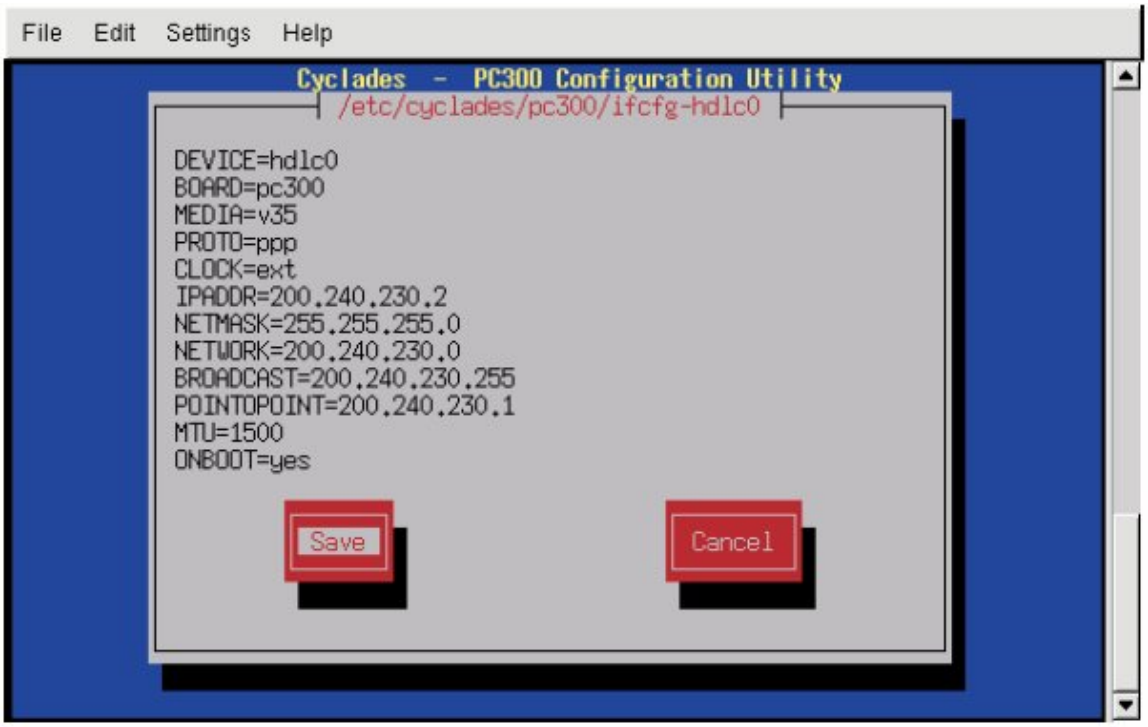
The second screen allows configuration of clock type, hardware media and encapsulation protocol.



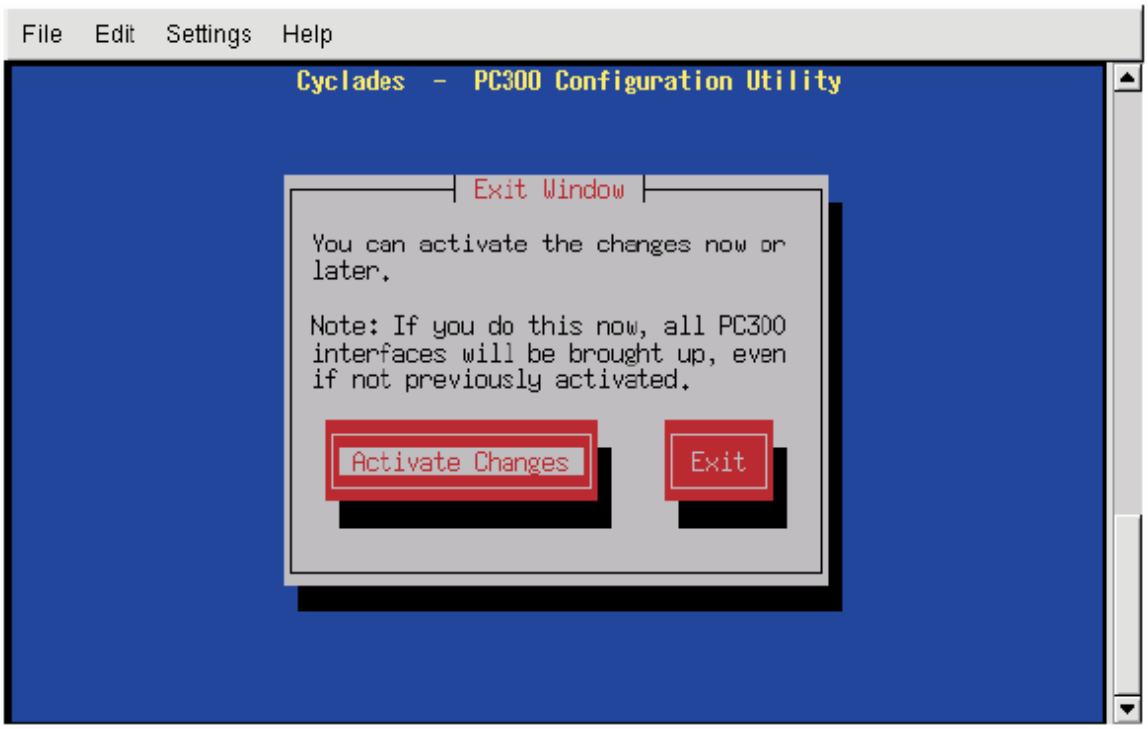
The third screen allows configuration of network parameters and whether or not the interface is activated when the computer is booted.



The fourth screen allows confirmation of the parameters entered in the previous screens before they are saved to the configuration file.



The next screen is the same as the first. The configuration utility must be exited in order for the new configuration to take effect. The last screen offeres the option to activate the changes (at that moment or later-- the configuration file has already been saved).



The PC 300 device provides APIs for accessing the card by the application running on the PC. These APIs can be accessed by using the standard socket function calls. They also provide the binaries for installation, de-installation, activate, de-activate of the link.

This card can use any 30 time-slots from the 32 E1 PCM. We have to specify in the PC300 configuration to which time slot we are going to use. This card can act for various data rates like 56 Kbps, 64 Kbps etc.

5.5 Execution

PHASE 1

In the first phase of the work it was desired to connect the PC with a K1297 using an E-1 PCM Cable. The idea was to check the functionality of the PC 300 card & to know the sending and receiving functionality of this card.

The lab set up for this phase 1 execution is shown below:

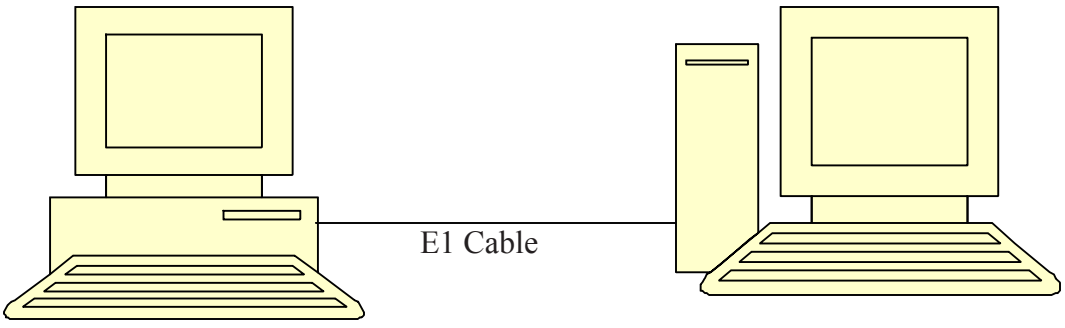


Figure 16: Lab Set Up for the Phase I execution

For this execution we need an E1 PCM cable with RJ45 connector at both ends. This is a 9 pin connector with 1,4,5,9 pins used. i.e. two for receiving the data and the two for the transmitting the data.

Now at one end of the E1 cable the RJ45 connector is inserted into the slot provided in the PC300 card & from the other end it is connected with the K1297.

In the Ist phase I started the K1297 in the monitoring mode. The K1297 is configured for the SS7 protocol and the signaling link no. 16 is given for messages transfer.

The same signaling link 16 is configured in the PC 300 also.

Now after that on PC we execute the following command to make the PC300 card in active state.

- ./pc300up

After doing this the PC 300 card will automatically make the link up with the K1297.

This can be checked by seeing the green signal in the K1297.

If this is completed, means the physical level (MTP-1 level) is UP now.

Now we want to send a SS7 message from the PC and check whether it is correctly being received at the K1297 or not.

For that the following piece of code is written:

```
/* Code for sending LSSU message from the PC to K1297 */

#include <sys/types.h>
#include <sys/socket.h>
#include <linux/if_ether.h>
#include <netinet/in.h>
#include <sys/ioctl.h>
#include <unistd.h>
```

```
#include <stdio.h>
#include <stdlib.h>
#include <time.h>
#include <linux/netdevice.h>
#include <linux/if_arp.h>
#include <signal.h>
#include <errno.h>
#include <fcntl.h>
#include <netdb.h>

#include <linux/if_packet.h>
#define   Uchar     unsigned char
#define   Ushort    unsigned short
#define   Uint unsigned int
#define   Ulong     unsigned long
#define SIO    0x3
#define BSN    8
#define BIB    0
#define FSN    8
#define FIB    0


typedef struct {
     Uchar  bsn_bib;   /*  Backward  Sequence  Number  (MSB  is
used as bib) */
     Uchar  fsn_fib;   /*  Forward   Sequence  Number  (MSB  is
used as fib) */
     Uchar li;   /* Length   Indication (1 in case of LSSU)
*/
     Uchar  sf;    /*  status  field  (5  MSBs  are  unused  and
last three are
                used to store status indication
```

```
                (SIO,SIN,SIE,SIOS,SIPO,SIB)) */
} Lssu;


main()
{
     int
sd,af,type,protocol,retval,addr_len,ifindex,count,i;
     struct ifreq req;
     struct sockaddr_ll sll;
     char name[] = "hdlc0\0";
     Lssu *msg;

     af = PF_PACKET;
     type = SOCK_RAW;
     protocol = htons(ETH_P_CUST);

     if(( sd = socket(af, type, protocol)) == -1 )
     {
          perror("socket");
          exit(1);
     }

     strcpy ( req.ifr_name, name);

     /* Bind socket to a single interface. Start by getting
the index  */

     if ( ioctl ( sd, SIOCGIFINDEX, &req ) < 0 )
     {
     printf("\nError getting interface %s index.\n",name);
     exit(1);
```

```
    }
    ifindex = req.ifr_ifindex;

    /* Now bind it */

    bzero ( &sll, sizeof ( sll ));
    sll.sll_family = AF_PACKET;
    sll.sll_protocol = htons(ETH_P_CUST);
    sll.sll_hatype = ARPHRD_RAWHDLC;
    sll.sll_ifindex = ifindex;
    addr_len = sizeof(sll);

    if (bind(sd, (struct sockaddr *)&sll, addr_len))
    {
    printf("\nProblem binding to interface %s.\n", name);
    exit(1);
    }


    msg = (Lssu *)malloc(sizeof(Lssu));
    if(msg == NULL)
    {
         printf("\n Malloc Failure \n");
         exit(1);
    }
    else
    {
    for(i=0;i<2;i++)
    {
    msg->li = 1; /* length indication is 1 in case of LSSU
*/
    msg->sf = SIO;
```

```
        msg->bsn_bib = i;
        msg->bsn_bib |= (BIB << 7);
        msg->fsn_fib = i;
        msg->fsn_fib |= (FIB << 7);
        count = sendto(sd,msg,sizeof(Lssu),0,NULL,0);
        if(count < 0 )
        {
               perror("sendto");
               exit(1);
           }
        printf("\nSend successfully \n");
        }
        }
        free(msg);
        close(sd);
}
```

/* Code for receiving the LSSU message from the K1297 */

```
#include<sys/types.h>
#include <sys/socket.h>
#include <linux/if_ether.h>
#include <netinet/in.h>
#include <sys/ioctl.h>
#include <unistd.h>
#include <stdio.h>
#include <stdlib.h>
#include <time.h>
#include <linux/netdevice.h>
```

```
#include <linux/if_arp.h>
#include <signal.h>
#include <errno.h>
#include <fcntl.h>
#include <netdb.h>

#include <linux/if_packet.h>
#define   Uchar     unsigned char
#define   Ushort    unsigned short
#define   Uint unsigned int
#define   Ulong     unsigned long
#define SIO    0x0
#define BSN    8
#define BIB    0
#define FSN    8
#define FIB    0


typedef struct {
     Uchar  bsn_bib;   /*  Backward  Sequence  Number  (MSB  is
used as bib) */
     Uchar  fsn_fib;   /*  Forward   Sequence  Number  (MSB  is
used as fib) */
     Uchar li;   /* Length   Indication (1 in case of LSSU)
*/
     Uchar  sf;    /*  status  field  (5  MSBs  are  unused  and
last three are
                used to store status indication
                (SIO,SIN,SIE,SIOS,SIPO,SIB)) */
} Lssu;
```

```
main()
{
     int
sd,af,type,protocol,retval,addr_len,ifindex,count,i,buflen;
     struct ifreq req;
     struct sockaddr_ll sll;
     char name[] = "hdlc0\0";
     Lssu *msg;
     Uchar buf[20];

     af = PF_PACKET;
     type = SOCK_RAW;
     protocol = htons(ETH_P_CUST);

     if(( sd = socket(af, type, protocol)) == -1 )
     {
          perror("socket");
          exit(1);
     }

     strcpy ( req.ifr_name, name);

     /* Bind socket to a single interface. Start by getting
the index  */

     if ( ioctl ( sd, SIOCGIFINDEX, &req ) < 0 )
     {
     printf("\nError getting interface %s index.\n",name);
     exit(1);
     }
     ifindex = req.ifr_ifindex;
```

```
        /* Now bind it */

        bzero ( &sll, sizeof ( sll ));
        sll.sll_family = AF_PACKET;
        sll.sll_protocol = htons(ETH_P_CUST);
        sll.sll_hatype = ARPHRD_RAWHDLC;
        sll.sll_ifindex = ifindex;
        addr_len = sizeof(sll);
        if (bind(sd, (struct sockaddr *)&sll, addr_len))
        {
        printf("\nProblem binding to interface %s.\n", name);
        exit(1);
        }

        for(;;)
        {
        buflen = strlen(buf);
        count= recvfrom(sd,buf,buflen,0,NULL,0);
        if(count < 0 )
        {
               perror("recvfrom");
               exit(1);
           }
        printf("Received a message of bytes %d\n",count);
        msg = (Lssu *)buf;
        printf("SF is %d\n",msg->sf);
        printf("FSN is %d\n",msg->fsn_fib);
        printf("BSN is %d\n",msg->bsn_bib);
        printf("LI is %d\n",msg->li);
        }
        close(sd);
}
```

PHASE 2

The figure 14 shows the setup in the lab for demonstrating the SS7 signaling transport over IP (SIGTRAN). In this demonstration only the signaling flow will be showed. Subscriber A and B are connected to the C-DOT DSS exchange 1 and 2 respectively. The DSS exchange 1 is connected to SG1 via an E1 PCM cable & similarly DSS exchange 2 is connected to SG2 via an E1 PCM cable. The two SG12 & SG2 are connected through the IP network.

First of all I make sure that the DSS1 and DSS2 are working properly, and then I run the SIGTRAN binary (SigTran) on the PC1 and PC2 by executing following command on the Linux operating system in order to make the SIGTRAN protocol up:

```
./SigTran &
```

This will automatically run the SIGTRAN software on the PC1 and PC2.

Now the set-up is ready for the signaling call flow.

When subscriber A picks up the telephone receiver, and dialed the called party number B, then the DSS1 analyze this called party number and found that this number does not belongs to it's own exchange, hence it creates a IAM (Initial address message) message & then routes this message towards the SG1 through the 64 Kbps SS7 signaling link. SG1 software is working in the PC1. This SS7 signaling link coming from the DSS1 is terminated on the PC1 with the PC300 Cyclade card. This card will receive this IAM message from the signaling links & pass this to its user (MTP-2) by using the APIs provided by the Cyclade.

The MTP-2 will transparently pass these signaling units to the upper layer MTP3 after doing its function of layer 2.

MTP3 will analyze the destination point code present in the message & route the message accordingly. In this case MTP3 will find that this message contains the destination address point code of the PC2 and hence forward this message to the M3UA.

M3UA has the knowledge that which destination IP is connected with which SCTP association. Hence it will analyze the destination IP address from the message & route this message on that SCTP association.

The SCTP will send this message to PC2 by using the standard Internet Protocol.

The SCTP on the PC2 will receive this message and transfer it to the upper layer M3UA. Now the M3UA will check the destination address present in the message & come to know that this message needs to be forwarded to the MTP3.

The MTP3 at PC2 will analyze the destination address present in the message & finally find that this message should be forwarded to the DSS2 via the SS7 links provided by the PC300 card.

Finally on receiving this message, the DSS2 will analyze the called party number, & find that the called party lies within its domain. Hence it will send a ringing signal to the subscriber B & alerting signal to the calling party A.

When the Calling party B picks up the phone, the DSS2 will send the connect message (CON) to the originating exchange i.e. DSS1 via the reverse traversed route (i.e. from DSS2->SG2->SG1->DSS1).

This is how the SS7 signaling information is demonstrated to be transported over an IP connection in the lab.

CHAPTER 6

6. CONCLUSION

SS7 transport over IP can be demonstrated in the C-DOT's environment as proposed in this dissertation. In this work we have also studied various issues of security, performance and the QoS involved in the transport of SS7 over IP. Then we have also discussed on the proposed strategies for them.

Overall it has been a good learning experience.

The future of the telecom networks lies on the IP based solution. The convergence of data and voice networks used for data traffic is growing beyond its limits. Some experts believe the voice network used for data traffic will be replaced by a new digital data network for data, image, and voice traffic. The new network switch will be a combination of data switches integrated with a specialized fault-tolerant computer that provides the SS7 signaling and other control and management functions.

As this technology is new in the market, very few multi-national companies (e.g. Alcatel, Motorola, Nokia, Hughes, T-mobile etc.) have implemented & deployed this technology in the market. Being the government organization, the development of such type of newer technology in India is a matter of proud for us. Developing these technologies in India itself will bring the cost of future telecommunication to the reach of general people.

CHAPTER 7

7. REFERENCES

- ITU-T Q.701-Q.705 “Message Transfer Part”
- ITU-T Q.711-Q.716 “Signaling Connection Control Part”
- ITU-T Q.761-Q.765 “ISDN User Part”
- ITU-T Q.770-Q.775 "Transaction Capabilities Application Part No. 7", 1996
- Travis Russel, Signaling system #7, Second Edition, McGraw-Hill Telecommunications, 1998.
- Link www.iec.org/online/tutorials/ss7_over
- Security Architecture for the Internet Protocol (RFC 2401)
- Architectural Framework for Signaling Transport (RFC 2719)
- Stream Control Transmission Protocol (RFC 2960)
- Internet Protocol Specification (RFC 791).
- Hedrick, “Routing Information Protocol” RFC 1058, June 1988.