IP Telephony Gateways

Gonzalo Camarillo
Royal Institute of Technology

Master's Thesis in
Teleinformatics

Supervisors:

Elin Wedlund
SwitchLab
Ericsson Telecom AB

Zsolt Haraszti
SwitchLab
Ericsson Telecom AB

Ulf Bilting
Department of Teleinformatics
Royal Institute of Technology

Examiner:

Fredrik Orava
Department of Teleinformatics
Royal Institute of Technology

Stockholm 1998-11-02

I would like to thank Henning Schulzrinne, professor at Columbia University and father of SIP, for his direction and all his advice on the implementation of the gateway prototype.

Abstract

There are two different approaches to provide telephone services at present: to use the traditional switched network and to use the Internet. Both approaches employ different ways to establish connections, transmit the voice and terminate calls.

This study focuses on the establishment of connections and the release of them. Different protocols are analysed and finally SIP and SS7 are described. The possible compatibility between them and the mapping between both message formats are also analysed. Features of both networks are described, and the functions of a gateway between them are outlined.

Table of Contents

Appendices

1 Introduction

The release of new products related with IP telephony, the increasing number of users, and the growing amount of telephony traffic over the Internet make a way to provide compatibility between the traditional telephone network PSTN (Public Switched Telephone Network) and the telephone over IP necessary.

Several protocols are used in both systems. This project focuses on two of them: SIP (Session Initiation Protocol) and SS7 (System Signalling No. 7).

SS7 is a common channel signalling system. It is an ITU-T (International Telecommunication Union) standard. It provides the signalling needed to control telecom traffic. SS7 consists of four levels with different protocols. ISUP (ISDN User Part) belongs to the 4th level of SS7 and provides services required by ISDN (Integrated Services Digital Network).

SIP is a signalling protocol for Internet conferencing and telephony. It is being developed by the MMUSIC (Multiparty Multimedia Session Control) working group inside the IETF (Internet Engineering Task Force) . SIP handles the associations between Internet end systems. It provides the signalling for establishing and releasing connections.

The compatibility between ISUP and SIP will be studied. This study involves the investigation of the mapping between the different formats of the messages and the translation of the information contained in those messages.

2 Traditional Circuit-Switched Telephony

Two types of networks are used to provide the traditional telephone services: ISDN and PSTN. In both of them, there is a need for controlling the calls with all their parameters and for charging for the use of the service. The exchange of this control information is referred to as signalling.

There are two types of signalling:

- Subscriber Loop Signalling: between a subscriber terminal and the local exchange.
- Inter-exchange Signalling: between exchanges.

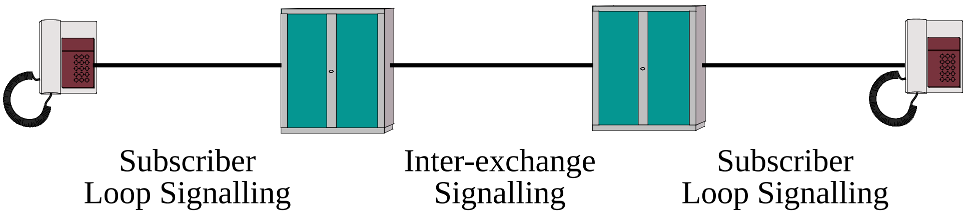


Figure 1: Types of signalling

The subscriber loop signalling and the inter-exchange signalling are usually performed using different protocols. The subscriber loop signalling keeps the user of the phone informed of the status of the call and the different events that occur. The inter-exchange signalling is concerned with the set-up of the connection, the supervision of the status of the call during the transmission of the speech and the release of the connection when the call is finished.

There are two approaches for transmitting the signalling associated to a certain call:

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

In Channel Associated Signalling, the signals are transmitted through the speech path in form of tones or pulses (in-band signalling) or through a signalling channel associated with the speech path. This kind of signalling was common in the sixties. Examples of it are 1VF, 2VF, MFP and MFC.

In common channel signalling, the signals are carried on dedicated signalling data links. One data link can support the transmission of the signals associated with many (several thousands) speech paths. All the control signals of the different calls are transmitted in a common signalling channel.

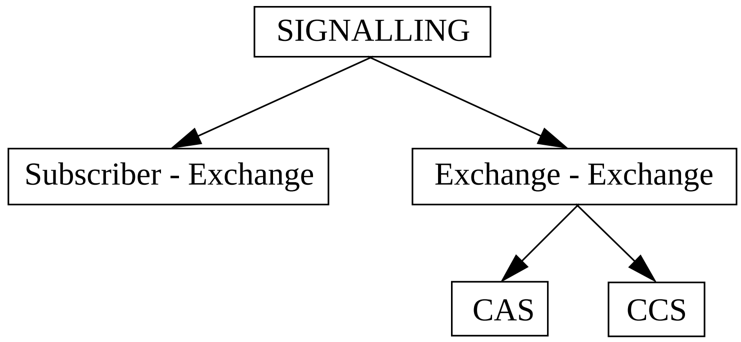


Figure 2: Types of signalling

There are two standards for Common Channel Signalling: SS6 (System Signalling No. 6) and SS7 (System Signalling No. 7). SS6 is used on analog lines. SS7 is used on digital networks, although it can be used on analog lines as well.

2.1 ISDN and PSTN

The main goal of ISDN (Integrated Services Digital Network) was to become a worldwide telecommunications network and to provide many different services. ISDN was standardized by ITU-T (International Telecommunication Union -Telecommunication Standardization Sector) and it supports voice and non-voice applications. Circuit switched connections and packet switched connections are provided by ISDN.

For transmission of data or voice, 64 kbps links are used. A rate of 64 kpbs is suitable for digitized voice, but it is too slow for some data transmissions. This rate could be increased in future developments. Each ISDN user is connected to a local ISDN exchange by a digital pipe. This digital pipe contains different communication channels. The number and the structure of these channels depends on the services required by the user.

There are three types of channels: B channels (64 kbps), D channels (16 or 64 kbps) and H channels (H0 384 kbps, H11 1536 kbps, H12 1920 kbps).

- B channels can carry digital data and PCM-encoded digital voice. B channels support circuit and packet switched modes.
- D channels can be used for transmitting packet switched data and to control circuit switched calls on B channels. This signalling information is essential for this study.
- H channels provides high-speed links for services which require high data rates.

These channels are grouped in different ways. The so called basic access consists of 2 B channels and 1 D channel. This is the most common service. It is mainly used by single users without large requirements. There are other possible configurations using different channels if greater capacity is needed.

In circuit-switched calls, the B channel is used for the exchange of data or voice, and the D channel is used to exchange control information. The signalling between a user and his local ISDN exchange and between two ISDN exchanges follow different protocols. Hence, the control of the calls is performed in a different way depending on which part of the network is involved.

Between the user and the local exchange, DSS 1 (Digital Subscriber Signalling 1) is used.

Between ISDN exchanges, the signalling is performed using SS7. SS7 establishes the connection with all the necessary parameters and releases the link when the call is completed. It sets up the circuit to be used for the connection.

Figure 3: Signalling protocols

PSTN (Public Switched Telephone Network) uses SS7 to control calls. Digital or analog signalling links can be used. Digital channels have a rate of 64 kbps and analog ones employ modems (4 kHz). The signalling protocol used in the forth level of SS7 is TUP (Telephone User Part), and in ISDN ISUP is used. TUP and ISUP cannot be directly linked. Therefore, nodes in the boundary of both networks (PSTN and ISDN) must be capable to deal with both ISUP and TUP.

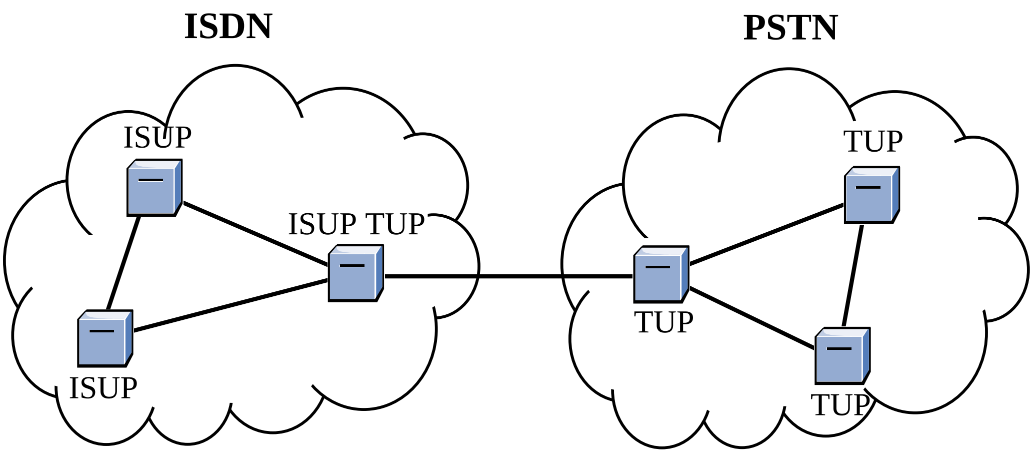


Figure 4: ISUP-TUP Interworking

Since the interworking between PSTN and ISDN is already solved, it does not represent a problem. Therefore, ISDN has been chosen for this study since it provides the means to handle much more services than PSTN.

For the rest of this paper, the term GSTN (General Switched Telephone Network) will be used to refer to any circuit-switched telephony network.

2.2 SS7

SS7 is a common channel signalling system. It has four different levels. Each level provides a set of services to the higher levels.

SS7 consists of various protocols which provide the different user-groups with their own set of messages. The general architecture of SS7 is shown below.

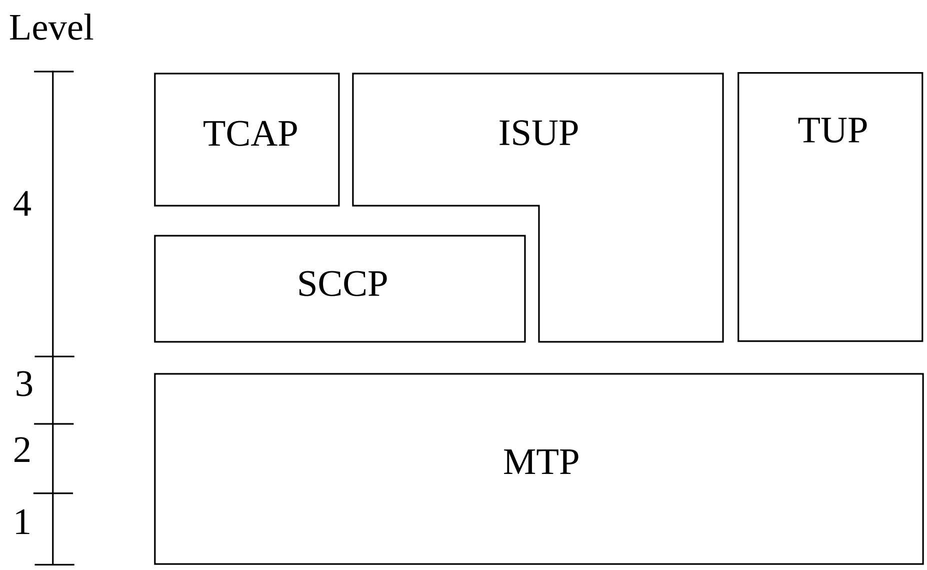


Figure 5: SS7 architecture

2.2.1 MTP

MTP (message Transfer Part) is the common underlying infrastructure for all the higher level protocols. MTP consists of three levels (levels 1 to 3 of SS7):

- Level 3: Signalling Network Functions
- Level 2: Signalling Link Functions
- Level 1: Signalling Data Link.

Signalling data link (level 1)

The Signalling Data Link interconnects two exchanges.It can be digital or analog. The digital links typically have a rate of 64 kbps, and the analog transmission channels have a bandwidth of 4 kHz.

This first level of the SS7 architecture is concerned with the physical characteristics of the medium.

Signalling link (level 2)

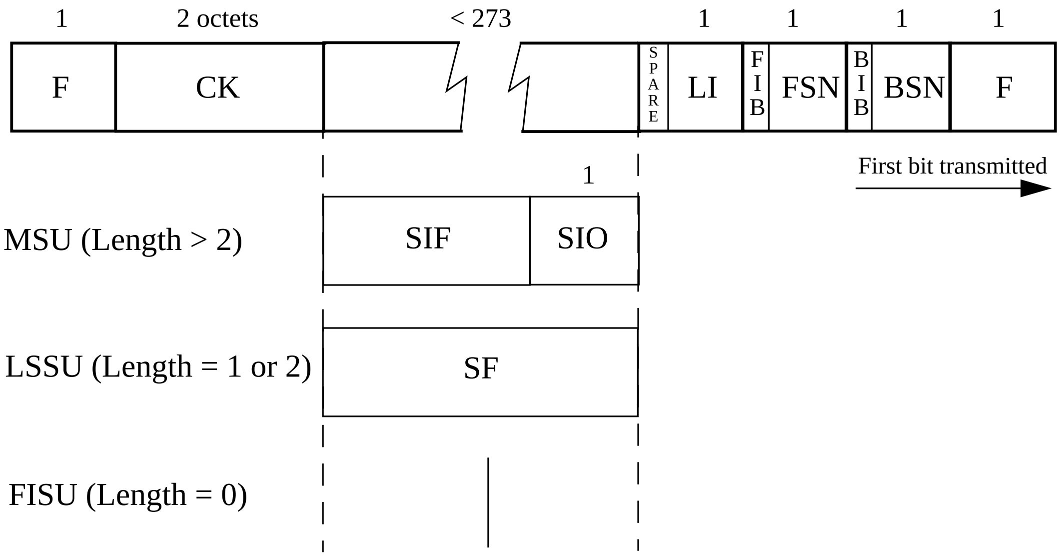
The signalling link functions are concerned with the control of the data links for sending and receiving messages.The functions contained in this level provide a reliable transmission of messages between two points that are directly connected to each other. This level provides the higher levels with messages in the correct order and without loss or duplication of them.

The messages transferred between two entities are called Signal Units (SUs). There are three kinds of signal units:

- MSU Message Signal Unit

- LSSU Link Status Unit
- FISU Fill In-band Signal Unit

They can be distinguished through the use of the length indicator field (see figure below). The format of the different signal units is shown below.



F	Flag	BIB	Backward Indicator Bit
CK	Checksum	BSN	Backward Indicator Bit
LI	Length Indicator	SIF	Signalling Information Field
FIB	Forward Indicator Bit	SIO	Service Information Octet
FSN	Forward Sequence Number	SF	Status Filed

Figure 6: Format of Signal Units

The LSSUs are used for initialization and alignment of the network. The MSUs transport the information related to the signalling. Through the transfer of MSUs, the network is controlled.

The functions contained in this level are:

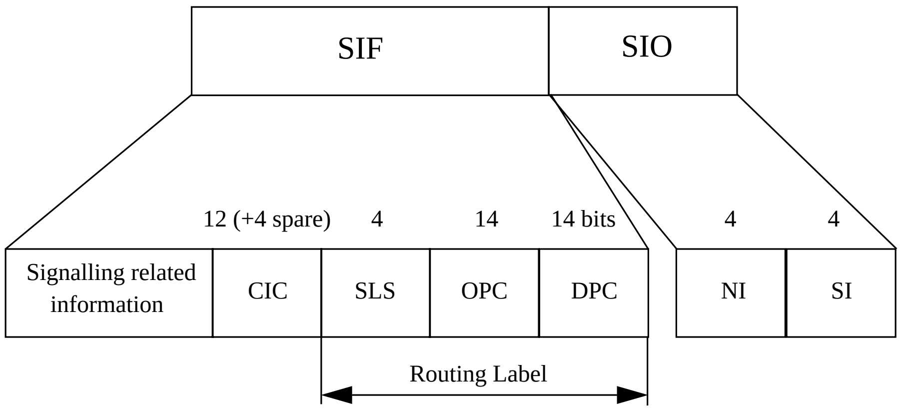
- Error detection: using a 16-bit checksum
- Error correction: through retransmissions of MSUs
- Flow control: using LSSUs carrying information about the status of the link.

Signalling Network Functions (Level 3)

The signalling network functions are divided into two categories:

- Signalling Message Handling
- Signalling Network Management

The signalling message handling functions use the routing label to deliver messages to the proper higher level protocol in the destination point. Therefore, these functions take care of routing the messages between different points and distributing them to the correct protocol when the messages reach their destination.



SIF	Signalling Information Field	OPC	Originating Point Code
SIO	Service Information Octet	DPC	Destination Point Code
CIC	Circuit Identification Code	NI	Network Indicator
SLS	Signalling Link Selection	SI	Service Indicator 0101 = ISUP

Figure 7: Message format

The signalling network management functions control the routing of the signalling traffic through the network and the reconfigurations of the network.. The management of the traffic is specially necessary in case of link failure or in case of congestion due to link overload.

The MTP has evolved over time. There has been two previous versions (yellow version and red version) before the current one (blue version).

2.2.2 SCCP

MTP was originally designed for controlling calls. Thus, MTP is suitable for circuit-related signalling. Therefore, MTP deals with communication channel control signals. Sometimes it is necessary to transfer signals that are non-circuit related. In this kind of application there is no speech channel to set-up or to control. Examples of this are data base services or credit card validation.To fulfil the requirements of non-circuit related applications, SCCP (Signalling Connection Control Part) is placed above MTP. When SCCP is used, the stack formed by MTP and SCCP is called Network Service Part (NSP).

SCCP provides two modes of operation: connectionless and connection oriented.

In the connectionless service, all routing information required to route the data to its destination is contained in each packet.

In the connection oriented service, a logical connection is established between the two systems. After the transfer of the data, the connection is released in order to free resources.

SCCP is placed in the 4th level of the SS7 architecture and in the 3rd layer of the OSI model.

2.2.3 TCAP

This 4th level protocol provides non-circuit related signalling. An example of this kind of service is the transfer of data between databases. TCAP (Transaction Capabilities Application Part) runs over SCCP and MTP. TCAP provides an end-to-end connectionless service.

TCAP is placed in the 7th layer of the OSI model.

2.2.4 TUP

TUP (Telephone User Part) is a 4th level protocol. TUP provides telephone signalling functions. It runs over MTP. TUP has an international version, but many countries have national variants with special characteristics. International TUP supports interworking with ISUP. All the functions supported by TUP are also covered by ISUP.

2.3 ISUP

ISUP (ISDN User Part) runs over MTP and can run also over SCCP for signalling without any circuit connection. The services provided by ISUP are divided into two types: basic services and supplementary services. An example of basic service is a two-party call and examples of supplementary services are multi-party calls and call forwarding when the user is busy or he does not answer.

There are different national versions of ISUP which are not compatible. Due to these differences between the protocols employed to provide signalling in national telephone networks, there exists a special version of ISUP for international interconnections. The gateways which connect national networks with international ones must support both versions of ISUP.

ISUP for international interconnections will be used for this project, since it is the common interface between all the networks in different countries. Therefore, from now on, everything said about ISUP applies to ISUP for international interconnections. In this kind of communications, ISUP runs always directly over MTP. SCCP is not used.

The information exchanged between ISUP and MTP is transferred in form of parameters carried by primitives. There are four primitives: MTP-Transfer, MTP-Pause, MTP-Resume and MTP-Status.

They provide the functional interface between MTP and ISUP. ISUP messages are encapsulated by MTP. This way, ISUP makes use of all the services available in MTP.

An ISUP message consists of a set of parameters. Each parameter contains indicators, and these indicators contains the information of the message. The parameters contained in each message are grouped in three parts: mandatory fixed part, mandatory variable part and optional part.

The mandatory fixed part contains the parameters that have fixed length and that must always appear in a certain message

The mandatory variable part contains the mandatory parameters with variable length.

The optional part includes the parameters that may appear in the message, but that are purely optional.

Every message also contains a Message Type Code (MTC) which uniquely identifies the type of the message.

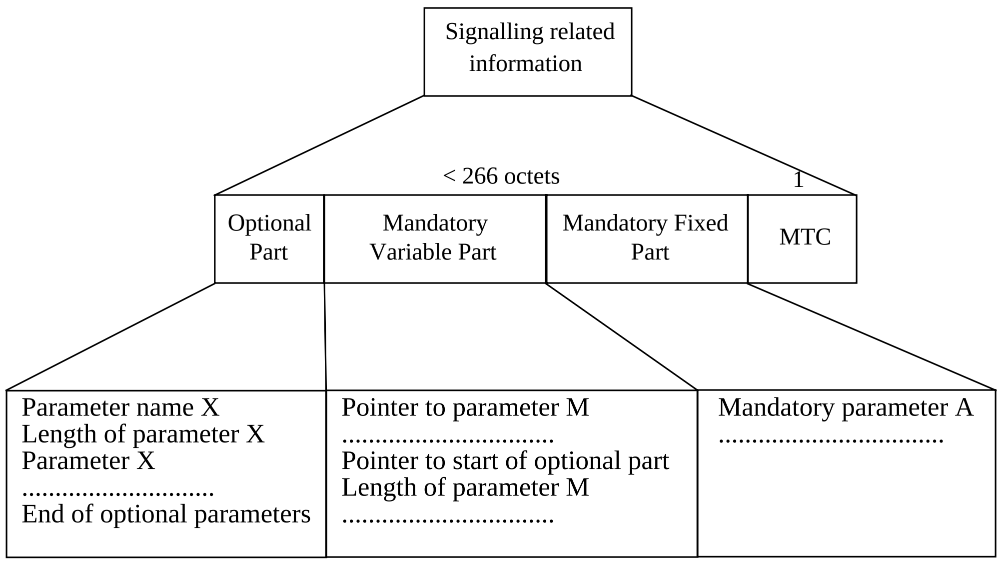


Figure 8: Structure of ISUP messages

All ISUP message types are listed below:

Table 2.1: ISUP messages

ACM	Address Complete message
ANM	Answer message
BLO	Blocking message
BLA	Blocking ACK message
CPG	Call progress message
CBG	Circuit group blocking message
CGBA	Circuit group blocking ACK message
GRS	Circuit group reset message
GRA	Circuit group reset ACK message
CON	Connect message
COT	Continuity message

Table 2.1: ISUP messages

FOT	Forward transfer message
IAM	Initial address message
CGU	Circuit group unblocking ACK message
CGUA	Circuit group unblocking ACK message
CCR	Continuity check request message
REL	Release complete message
RLC	Release complete message
RSC	Reset circuit message
RES	Resume message
SAM	Subsequent address message
SUS	Suspend message
UBL	Unblocking message
UBA	Unblocking ACK message

For a more detailed description of ISUP messages see Appendix A.

All ISUP parameters are listed below:

Table 2.2: ISUP parameters

Access transport	Continuity indicators
Automatic congestion level	End of optional parameters
Backward call indicators	Event information
Called party number	Forward call indicators
Calling party number	Optional forward call indicators
Calling party’s category	Transmission medium requirement
Cause indicators	User service information
Circuit group supervision message type indicator	User-to-user indicators
Closed used interlock code	User-to -user information
Connected number	

For a more detailed description of ISUP parameters see Appendix B.

2.3.1 Example of signalling operation

There are two kinds of signalling sequences: en bloc and overlap. In en bloc signalling the whole destination number is contained in the IAM message. In overlap signalling, several SAM messages are sent to transmit the whole destination number.

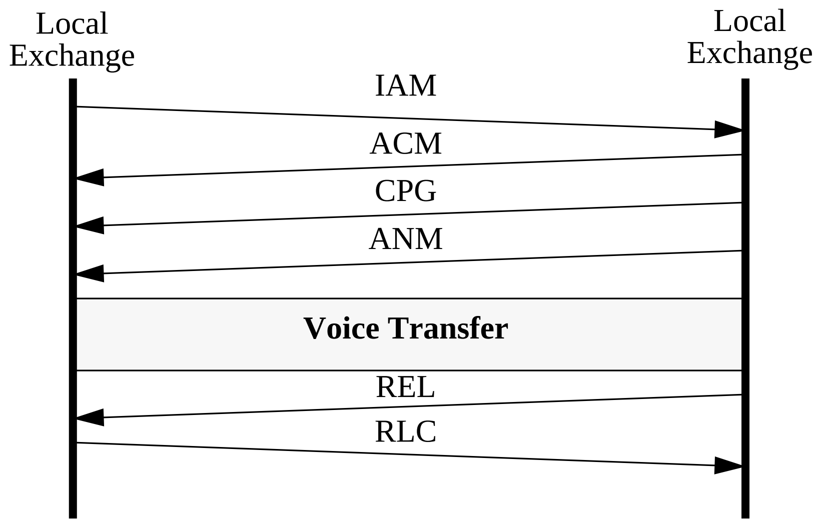


Figure 9: En bloc signalling sequence

When the local exchange receives the IAM message with the destination number, it sends back an ACM message. When the user picks up the phone, an ANM is sent back and the connection is established.

To release the connection, a REL message is sent. The other exchange returns a RLC message.

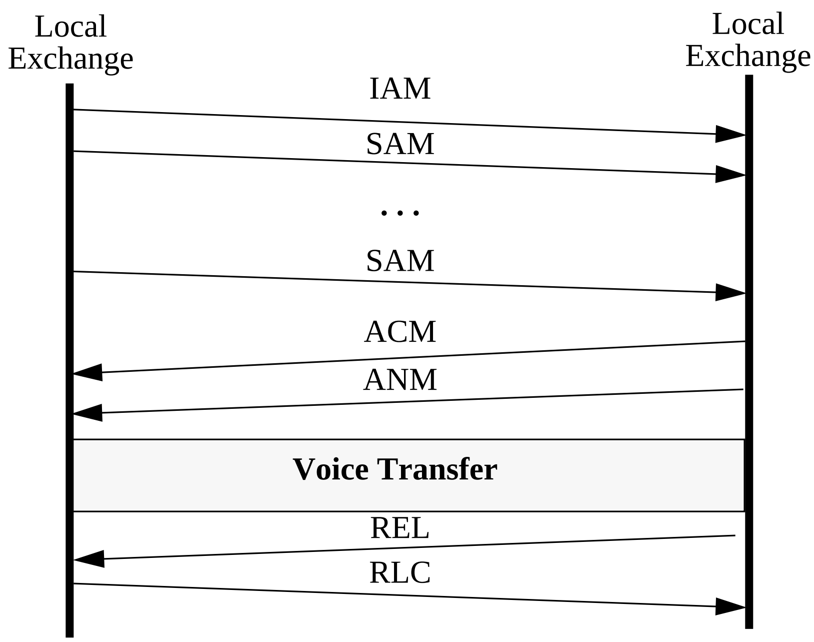


Figure 10: Overlap signalling sequence

In overlap operation, the local exchange does not send an ACM message until it has received all the SAM messages containing the destination number.

3 IP Telephony

IP telephony consists basically of sending digitized voice over the Internet. These packets containing the digitized voice can use different formats. For two-parties calls, on one side the user uses the microphone of his computer to speak. This voice is digitized and encapsulated in RTP (Real-Time Transport Protocol) packets. RTP packets are sent over the Internet using the services provided by the lower layers protocols (UDP, IP...). They are received by the other party involved in the call. The packets are decapsulated, and the original message is played through the speakers of the computer.

There are two factors which contribute to the quality of the audio received: the voice coding technology employed and the latency of the network.

The voice coding algorithm must be able to work in real time providing enough quality. The speech must be understandable by the other party involved in the communication. The algorithm must include a way for lost packet reconstruction.

In real time communications, when a packet is lost, it is not retransmitted. A retransmitted packet may arrive too late to be played.Therefore, the end system receiving the packets must generate audio during the time that the lost packet was supposed to be played. This avoids disruptions in the speech.

If the latency in the network is too high, it is difficult for the communicating parties to maintain a normal conversation. The pace of the conversation gets slower the higher the latency is. The maximum latency that humans can tolerate is about 300 ms (round trip delay). Employing QoS techniques, the latency of IP telephony can be kept below this threshold.

Before the transmission of all the real time packets containing the audio samples, the connection between the two end systems has to be established. There are two protocols that perform this operation: H.323 and SIP.

After the establishment of the connection, these protocols control the call and, when it is finished, they indicate that the resources used can be released. The messages sent by these protocols are also transmitted in IP packets through the Internet. However, the requirements of these packets are much lower than the ones containing real time data, and they can admit higher latencies.

IP telephony achieves a better utilization of the available bandwidth than the circuit-switched telephony. In the circuit-switched telephony, a circuit is reserved during the call, and it cannot be used by anybody else even if no traffic is being generated at that moment. IP telephony consumes bandwidth only if it has some data to send.

3.1 Underlying architecture

A communication protocol is a set of conventions between the entities involved in the communication describing the rules to follow during the connection.

The TCP/IP protocol suite is the most widely used protocol architecture. It started in the sixties as a government-financed research project conducted on the experimental packet-switched network ARPANET (Advanced Research Projects Agency Net), funded by the Defense Advanced Research Agency (DARPA).

The functions needed in the communication process are distributed in layers. Thus, each layer is responsible of some aspects of the communication. The TCP/IP protocol suite consists of 4 layers: data-link layer, network layer, transport layer and application layer.

- Application layer: includes all the functions of each concrete application.
- Transport layer: provides a flow of data between the two end systems involved in the communication.
- Network layer: provides communication between two systems attached to different (but interconnected) networks. It deals with the routing of packets through the path to the destination system.
- Data-link layer: handles the access to the physical medium. It provides an interface between the "cable" and the rest of the system which is generating or receiving the data.

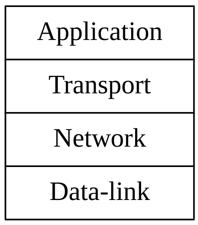


Figure 11: TCP/IP protocol suite

Some authors add an additional 5th layer below the data-link layer called physical layer. This layer is concerned with the mechanical and electrical characteristics to access the physical medium.

In a layered architecture like this, every layer uses the services of all the lower layers and provides services to the higher layers. The user data is encapsulated by every layer, from the application layer to the data-link layer, adding its control information for handling the packet.

The OSI (Open System Interconnection) model by ISO (International Organization for Standardization) constituted another approach. It consists of seven layers: physical layer, data-link layer, network layer, transport layer, session layer, presentation layer and application layer.

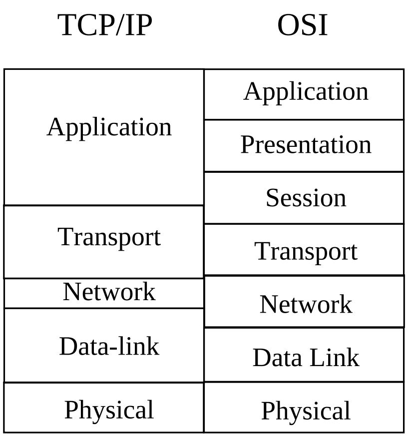


Figure 12: Mapping between OSI and TCP/IP

Since the TCP/IP protocol suite has become the dominating architecture, this project focuses on it.

3.1.1 IP

The Internet Protocol (IP) belongs to the network layer. It provides a connectionless service between end systems. All the intermediate systems between the two ends just have to implement IP and the layers below it. It is not necessary to implement higher layers.

IP receives data from higher layers. It adds a header containing information related to the data received and passes it to the lower layer. These packets are called IP datagrams.

The most important service of IP is to send the packets to the proper next hop. All the routing information necessary for this purpose is contained in the IP header.

When the size of the data coming from the transport layer is bigger than the maximum size than the link can handle, the IP protocol takes care of fragmentation and reassembly of packets.

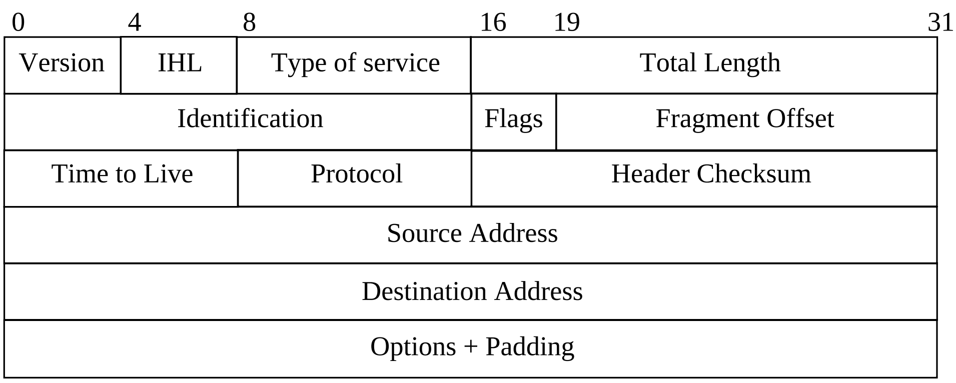


Figure 13: IP header

The current version of IP is four, but it may be replaced by the version six of the protocol. It uses 128-bit addresses instead of the 32-bit IPv4 addresses. It overcomes the problem of running out of available IP addresses. This problem is present in IPv4.

The special options present in some IPv4 packets are placed in IPv6 in separate optional headers, optimizing the processing of them.

IPv6 supports resource allocation through labelling flows of packets. This way, special flows like audio packets with low delayment requirements can be treated in a different way than packets without real time data.

IPv6 also includes security features such as authentication or privacy.

<table>
<tr><td>0</td><td>4</td><td>8</td><td>16</td><td>24   31</td></tr>
<tr><td>Version</td><td>Priority</td><td colspan="3">Flow Label</td></tr>
<tr><td colspan="3">Payload Length</td><td>Next Header</td><td>Hop Limit</td></tr>
<tr><td colspan="5">Source Address</td></tr>
<tr><td colspan="5">Destination Address</td></tr>
</table>

Figure 14: IPv6 header

3.1.2 UDP

UDP (User Data Protocol) is a transport layer protocol. It provides a connectionless service to higher layers. UDP does not assure that the packets will reach their destination. However, this lack of reliability makes UDP suitable for some applications, like real time audio, since the reliability mechanisms are built on top of UDP. Thus, the application can decide whether retransmission of packets is suitable and a better control of the data flow is achieved from the application point of view.

UDP header just contains the source and destination ports, the length of the packet and an optional checksum for error detection.

0	16 31
Source Port	Destination Port
Length	Checksum

Figure 15: UDP header

The port numbers are used to deliver the data to the correct application, since UDP can be used simultaneously by several processes.

3.1.3 TCP

TCP (Transmission Control Protocol) provides a reliable connection oriented transport layer service. Before transferring any data, a connection is established between the two end systems. After this establishment, TCP takes care of all the packets to assure that all of them arrive at the destination. Timeouts and retransmissions are implemented in order to provide this connection oriented service.

TCP includes flow control and error detection. The packet rate can be increased or decreased depending on the level of load of the network. Corrupted packets are discharged and retransmitted.

Therefore, the applications running above TCP does not have to implement any of those services since TCP offers them.

0	4	10						16	31
Source Port								Destination Port	
Sequence Number									
Acknowledgement Number									
Data offset	Reserved	URG	ACK	PSH	RST	SYN	FIN	Window	
Checksum								Urgent Pointer	
Options + Pading									

URG	Urgent pointer field significant	RST	Reset connection
ACK	Acknowledgement field significant	SYS	Synchronize the sequence numbers
PSH	Push function	FIN	No more data from sender

Figure 16: TCP header

TCP uses acknowledgements to check if the packets are arriving at the destination without errors.

TCP is suitable for reliable data exchanges, but real time applications usually have to implement their own timeouts and their own flow control mechanisms, since the requirements are completely different. In data exchanges the focus is set on the correctness of the information, and real-time applications are concerned about receiving the information in time.

3.2 RTP

So far, Internet has been used mainly for file transfer and electronic mail. Nowadays, its requirements are changing. The use of multiparticipant applications is growing and the amount of real-time traffic in the Internet increases continuously.

The requirements of real-time applications are different to the traditional data services. The focus is set on the time delay more than on the data integrity. TCP is suitable for reliable communication, but its flow control and error detection make it not appropriate for low time delay transmission.

Due to this, a new protocol has been developed. RTP (Real-Time Transport Protocol) can run over connection oriented or connectionless lower layer protocols which are in charge of framing and segmentation. Unlike TCP, it does not support reliability mechanisms.

RTP uses a control protocol called RTCP which monitors the QoS (Quality of Service) of the connection and synchronizes different media through wallclock time and timestamps. RTCP contains SDES (source description) also. It uses a fraction of the bandwidth to transmit control messages.

3.3 SIP

SIP (Session Initiation Protocol) is used to establish, modify and terminate multimedia sessions. An IP telephone call is considered a kind of multimedia session in which voice is exchanged between the parties.

SIP supports personal mobility and negotiation of the capabilities of the end users. It also supports the fundamental security services: authentication, access control, confidentiality and integrity.

SIP is a text-based protocol. It is based on HTTP, which is also text-based. The messages follow the ISO 106646 character set in UTF-8 encoding. SIP can run over TCP or UDP, but the message format is independent of the transport protocol. If UDP is used, mechanisms to provide reliability such as retransmissions and loss detection have to be implemented in the application layer.

SIP is a client-server protocol. Clients issue requests and servers answer with responses. Therefore, there are two types of messages: requests and responses.

The current version of SIP (SIP 2.0) contains six types of requests. They are referred to as methods. They are: INVITE, ACK, OPTIONS, REGISTER, CANCEL and BYE.

INVITE is used to ask for the presence of a certain party in a multimedia session. The negotiation of the parameters of the session such as port which will receive the media stream or which codec will be used is carried out using this method.

In the middle of a call, it is also possible to change the current parameters of the media stream sending a new INVITE request.

The ACK method is sent to acknowledge a new connection. It can contain a session description describing the parameters of the media stream.

OPTIONS is used to get information about the capabilities of a server. The server returns the methods that it supports.

The REGISTER method informs a server about the current location of a user. This way, the user can be reached where he is logged in at that moment.

A client send a BYE method to leave a session. For two party calls, it terminates the call.

The CANCEL method terminates parallel searches. When a server is trying to reach a user, it can try several locations. When the user is reached, the rest of the searches can be cancelled.

When a server receives a request, it sends back a response. Each type of response is identified by a code number. There are 6 main types of responses. They are listed in the table below.

Table 3.1: SIP responses

1xx	Informational
2xx	Successful
3xx	Redirection
4xx	Request failure
5xx	Server failure
6xx	Global failure

The server keeps the client informed of the status of the call with these responses.

There exists two modes of operation in SIP when servers are used: using a proxy server or using a redirect server. The proxy server returns responses on behalf of the user. The redirect server informs the client of the current location of the user. Then, the client can reach directly the user.

There is another mode of operation when no servers are used. The user agent can send directly requests to the other user agent. Even when a SIP server is used in the first exchange of messages between the parties, the subsequent exchanges may be addressed directly to the user agent, without traversing any server.

The normal exchange of SIP messages is described below. Both modes, proxy and redirect are outlined.

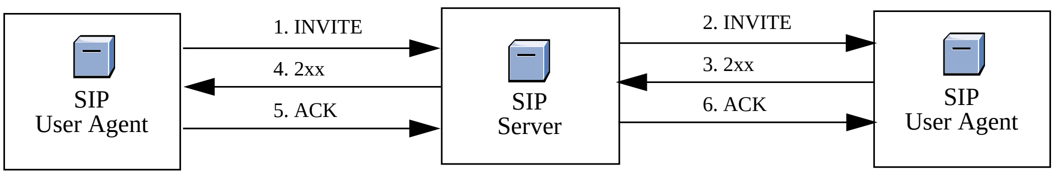


Figure 17: Proxy mode SIP operation

The proxy server takes care of the location of the user. Thus, the process is transparent to the client.

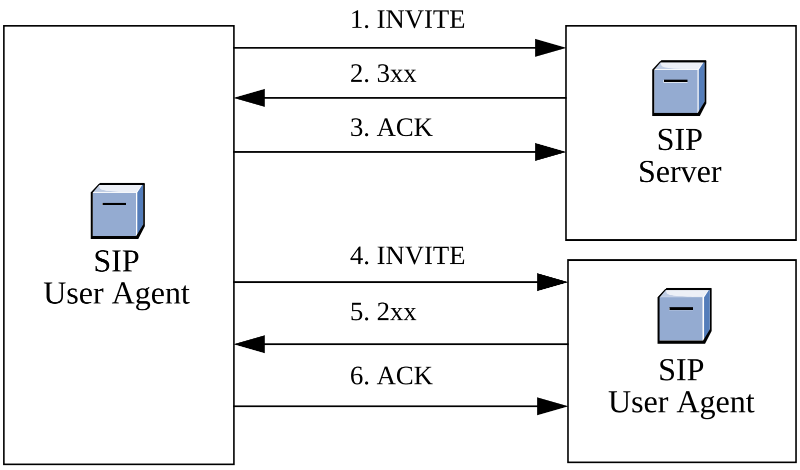


Figure 18: Redirect mode SIP operation

The redirect server locates the user and responds with the location. The client must issue a second invitation, now addressed to that new location.

Apart from the type of method in requests and the code number in responses, SIP messages contain more information. Message consist of a start-line, several header fields, an empty line and an optional message body that may contain a session description.

All possible header fields are listed in the table below.

Table 3.2: SIP headers

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

The sessions are typically described using the Session Description Protocol (SDP), although other protocols can also be used. The session description is contained in the message body.

3.4 H.323

H.323 is an ITU standard. In its architecture, each client belongs to a zone, and there is a gatekeeper in each zone. All the clients of a zone are registered to its gatekeeper. The gatekeeper provides address translation (allowing aliases to be used), admission control and bandwidth control.

For multiparty conferences, Multipoint Controllers (MCs) are employed. All the clients involved in the conference are connected to this controller. The negotiation of terminal capabilities is performed by the MC.

To send the realtime stream (it can consist of data, voice and/or video) to each client, taking into account its specific capabilities, multipoint processors (MPs) are used. They convert the realtime stream into a proper format and send it to the user.

H.323 defines three different signalling channels: H.225.0 / RAS, H.225.0 / Q.931 and H.245.

The RAS (Registration, Admission and Status) channel is established between the user and the gatekeeper. This channel is used to perform registrations and request bandwidth and resources for the call. It uses UDP.

H.225 / Q.931 is a signalling channel used to establish and terminate the connections. Messages related to the provision of supplementary services are also transmitted over this channel. It uses TCP.

H.245 is used to transmit control information during the call and control logical channels between end points. It uses TCP.

If the users involved in a conference know the other parties’ IP addresses, the connection can be established directly between end points. In this scenario, no gatekeeper is needed.

H.323 can be used with a faststart algorithm. It allows a quicker negotiation of capabilities between the end points when the connection is being set up.

3.5 SIP vs H.323

SIP and H.323 are both standards for signalling and control for Internet telephony. H.323 is an ITU recommendation, and SIP is being developed by IETF. Both protocols provide a similar set of services, but SIP is much simpler (it has less logical components).

H.323 uses binary notation for the messages, and it makes parsers more complicated to develop and upgrade. SIP, on the other hand, is a text-based protocol, very similar to HTTP in this sense. The overhead of these kind of protocols is bigger, but since it is used just for control purposes with short messages, it is not an important drawback.

H.323 operations require interactions between many different components (H.450, H.225.0, ...), while in SIP all the information is integrated in the SIP request or response.

The adaptability of SIP is one important feature, since it allows interactions between newer versions of the protocol and older ones. If a certain server does not support any new feature, it can warn the client, and they can agree a simpler operation. When a feature is not needed any longer, it is removed in the next version of the protocol, making SIP dynamic. H.323 offers standard parameters for backwards compatibility. This approach causes difficulties in the interactions between terminals from different vendors. H.323 is fully backwards compatible with its older versions. It produces a growth in the size of each new release of H.323.

SIP uses the Session Description Protocol (SDP) to choose the type of communication to be used. This way, SIP can work with any codec registered by a person or group with IANA. H.323 can just use ITU developed codecs. This is an important limitation when it comes to achieve compatibility among all the users, big and small ones.

SIP is modular, so it can be used in combination with H.323. For instance, H.323 can use locations services from SIP.

The scalability is another advantage of SIP. H.323 presents some loop detection problems with large numbers of domains. SIP uses a similar approach to BGP (Border Gateway Protocol). However, this factor is not important in telephone calls between a reduced number of users, such as two-party telephone calls.

Under heavy traffic, many connections pass through a certain server at the same time. H.323 requires the server to be stateful. It is a big barrier for handling a big number of connections, since the server must store information of each individual one. SIP allows the servers to be stateful or stateless. Just with the information contained in the message the server can handle it and forward it to the proper destination. It saves memory in the servers and achieves a greater communication capacity.

H.323 can achieve better control of the bandwidth used in a conference trough the use of gatekeepers. SIP does not address this problem and this control should be provided by other protocols like RSVP (ReSerVation Protocol).

In multiconferences with many users, all the H.323 traffic passes through a central control point. It represents a performance problem, since it can become a bottleneck.

Taking all these reasons into account, SIP has been chosen for this study. There are SS7-H.323 gateways already implemented. One approach consisted of using SS7 over IP as an intermediate step between both protocols.

Gateways between SIP and H.323 are being developed. From now on, this study focuses on SIP, the architecture below it and its features.

4 Mapping between ISUP and SIP

ISUP and SIP have been described in the previous chapters. To provide compatibility between these two signalling systems, there is a need for a module connected to both networks, GSTN and the Internet. This module has to handle calls which originate in either of the two sides. A way of performing this translation has been developed in this project.

The mapping between ISUP and SIP in this module is based on the type of the message received. Therefore, when a connection is being established, the most important information for the gateway is the type of message received (ACM, IAM, INVITE, BYE ...). The information contained inside the message does not modify the purpose of the message.

Thus, the translation between messages from one side of the gateway to the other can be described by a finite state machine. The state machine waits for an event and then triggers the appropriate response depending on the current state of the call.

A state machine is necessary for this translation. It leads to a stateful gateway. A stateless gateway is not used because an event can consist of a timeout, and so, a certain action will be taken by the gateway without receiving any new message. In certain states, the gateway has to send messages simultaneously to both sides, so, a straightforward translation of messages (just sending a message to one side if something is received on the other side) is not a good approach.

The gateway is provided with two different state machines. One will handle SIP to ISUP calls, and the other one will handle ISUP to SIP calls. Both state machines are designed to run over UDP, so, SIP retransmissions are taken into account.

However, to avoid drawing too many lines in the diagrams, some retransmissions are not shown in the figures. For example, when the gateway goes to the state called “SIP gives up”, the SIP message (a response or an ACK) sent by the gateway has to be retransmitted if it gets lost (if we receive the previous message again).

The next two diagrams describe the SIP to ISUP state machine and the ISUP to SIP state machine.

Since ISUP is used for media control as well as for signalling, just signalling related messages have been considered. ISUP messages related to the management of the circuits are processed in a different module of the gateway. This module just deals with the translation of signalling related messages.

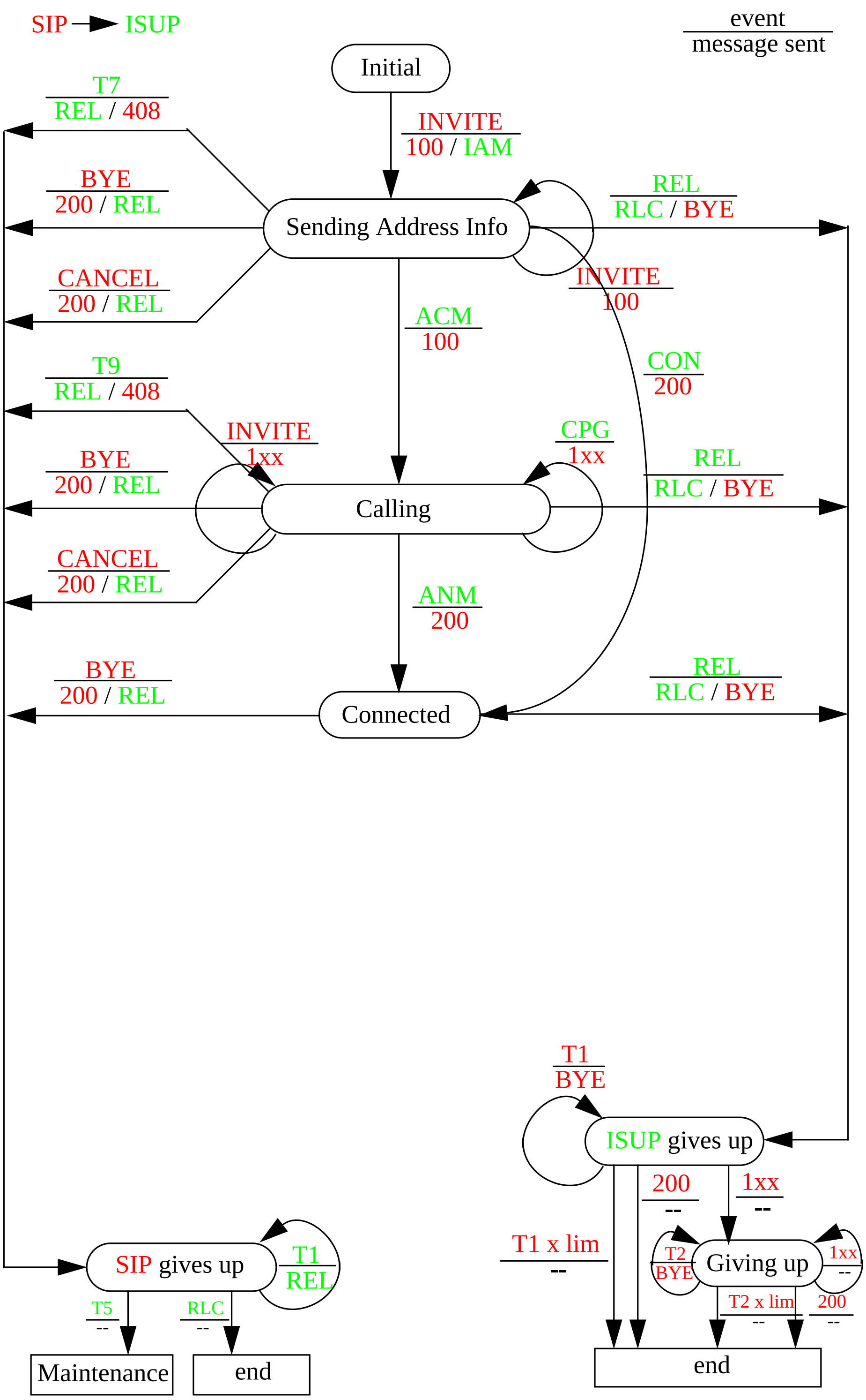


Figure 19: SIP to ISUP state machine

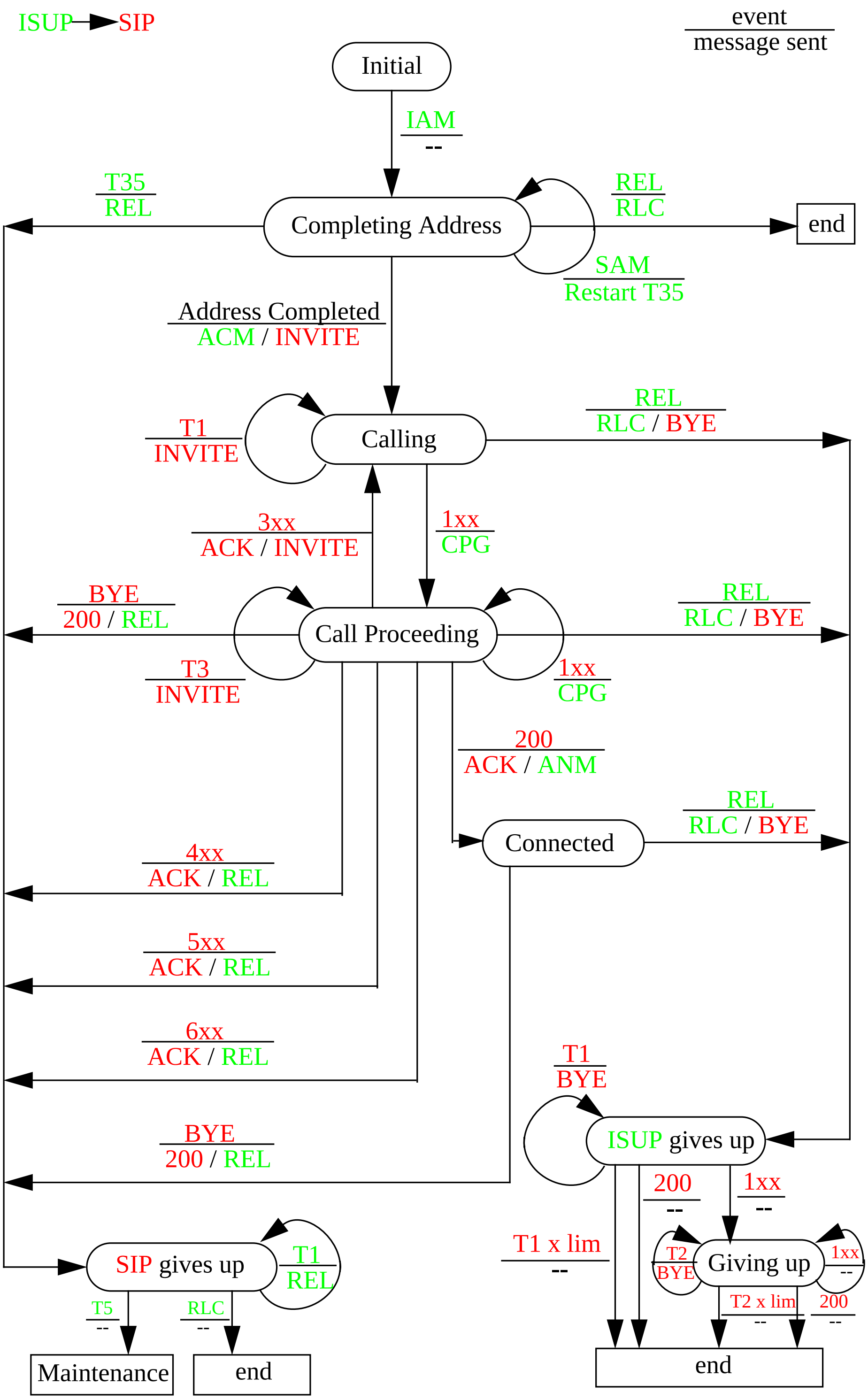


Figure 20: ISUP to SIP state machine

As previously stated, these two state machines describe the way the module works without going deeply into the details. A more detailed description of the different states follows.

4.1 SIP to ISUP State Machine

In every state, the gateway performs a certain action based on the last event that has occurred. An event consists of the reception of a message or the expiration of a timer. The actions to take after the reception of an unexpected message in any state may consist of sending back a message indicating a failure. The state of the gateway remains unchanged.

In the initial state, the gateway may receive three types of messages from the IP side: OPTIONS, REGISTER and INVITE.

If an OPTION message is received, the gateway will respond with its capabilities, describing the SIP methods that it supports.

If the gateway has proxy or redirect server capabilities, it will be able to handle a REGISTER request. Otherwise, a message indicating the methods supported by the gateway is returned to the sender.

None of these two messages initiate a call, and so, no state is stored in the gateway.

When a INVITE request arrives, it indicates the beginning of a new call. The gateway will send a 1xx informational response to the IP side indicating that it is handling the call and will try to reach the user at the ISUP side sending an IAM.

If the user cannot be reached or the timer expires, the connection will be released. If the user is reached but he is busy, a REL message or an ACM with a cause indicator will be received. In both situations the connection is released also.

If the user is reached and he answers, an ANM or a CON message will be received. Then, the gateway goes to the connected state. In this state, any of the users involved on the call can finish it.

When the gateway is in the connected state, a SUS message can arrive from the ISUP side. The gateway will go back to the connected state when a RES message is received. If the timer expires, the connection is released. A SUS message is sent when the user unplug the telephone from the socket on the wall. The RES message is sent when the telephone is reconnected again. The user on the SIP side must be informed of this event. He can decide between waiting or releasing the connection.

4.2 ISUP to SIP State Machine

In the initial state, the gateway will receive an IAM message. Once the destination address is complete, in the IAM message (en bloc operation) or in several SAM messages (overlap operation), an INVITE request is sent.

If after sending the INVITE request, a 3xx redirect response is received, another INVITE request to the new location is issued. If a 4xx, 5xx or 6xx failure response is received, the connection is released.

If a 2xx successful response is received, the gateway goes to the connected state. Any of the users can then release the call when this is finished.

4.3 Voice Path

The flow of signalling messages during a call has been described. The main purpose of all these messages is to establish a voice path between the users that makes a conversation possible. The moment the voice path is established is different between ISUP and SIP.

In the GSTN network using ISUP, we can receive information through the voice path after the ACM message and before the ANM message. The typical example is the recorded voice saying: “Welcome to Ericsson. For information about the company press one, for questions about products press two...”.

In order not to lose this information, the SIP client should listen to the voice path right after sending the INVITE request. The client should do this because the gateway is receiving ISUP for international connections, and the presence of information in the voice path may not be announced. So, the signalling gateway may not be aware of the presence of this announcement.Therefore, the gateway could not send, for instance, a 1xx response indicating that there is information in the voice path.

When the user on the ISUP side needs to provide some kind of feedback, like choosing an option, DTMF (Dual-Tone Multi-Frequency) tones are used. The user types the number on his phone, and the proper tone is sent through the voice path. Although it is possible to digitize this sound and send it as if it was voice, the algorithms used to codec the speech are not suitable for this kind of tone, and it is preferable to send them like user information.

This problem is also present when a fax is to be sent. The algorithm used has to be changed in order to transmit it. So, an INVITE request with the proper parameters for the transmission of the fax has to be issued.

4.4 Gateway architecture

A module that translates signalling messages from ISUP to SIP has been described so far. This module is known as a signalling module. To establish a connection between the GSTN network and the Internet two more modules are needed: media gateway controller and media gateway.

The media gateway transforms the voice stream from one format to another. It receives the voice stream from the GSTN circuit, codes it and sends it encapsulated in real-time packets (usually RTP). It also performs the translation in the opposite direction, from the Internet to the GSTN circuit.

The media controller controls the media gateway through a control protocol.

There are various possible dispositions of these three modules. For this project, the signalling gateway and the media controller are joined together in a box. From now on, these two modules together will be referred to as signalling gateway. So, in general terms, the signalling gateway performs the message translation and the media gateway control.This approach allows the installation of one signalling gateway that controls several distributed media gateways.

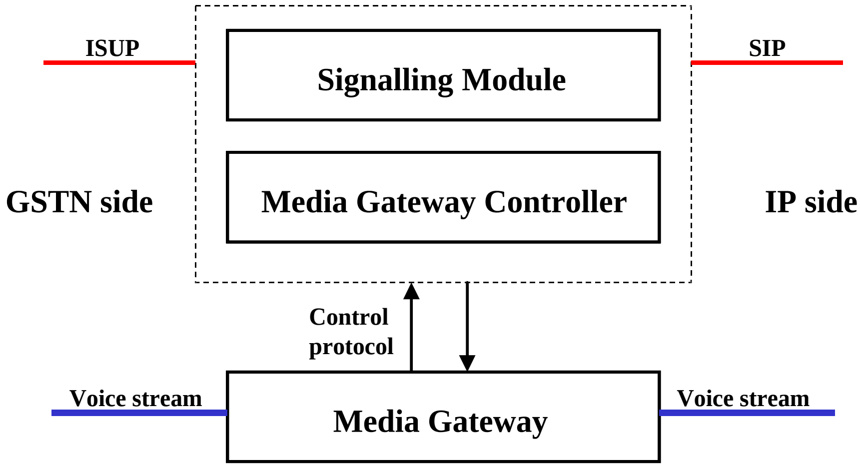


Figure 21: Gateway architecture

There are several protocols that can be employed to control the media gateway from the signalling gateway. ISUP over IP, IPDC (Internet Protocol Device Control), SGCP (Simple Gateway Control Protocol) or MGCP (Media Gateway Control Protocol) are examples of this kind of protocol. Some vendors may also use their own specific protocols for controlling media gateways.

However, it is desirable that only one protocol is used for this purpose. Using just one protocol could lead to an open architecture. Using one protocol allows the use of a signalling gateway from one vendor and media gateways from other ones. SIP could be this protocol.

In this scenario with just SIP, the signalling gateway would INVITE the media gateway to participate in the multimedia session and the media gateway would send back a response with its status.

So far, there are two approaches which make this feasible: extending SIP with two more methods (SUBSCRIBE and NOTIFY) and using SIP in conjunction with SNMP (Simple Network Management Protocol).

Hence, if SIP becomes widely used and new SIP compatible products are launched to the market, SIP could be used to control all kind of devices.

4.5 Network architecture

The signalling gateways and the media gateways have to be connected to both networks, GSTN and the Internet. There are three possible scenarios depending on the origin and the destination of a call: SIP termination, SIP bridging and SIP bridging without media gateway.

4.5.1 SIP temination

SIP termination include calls between a user in the GSTN network and a user in the Internet.

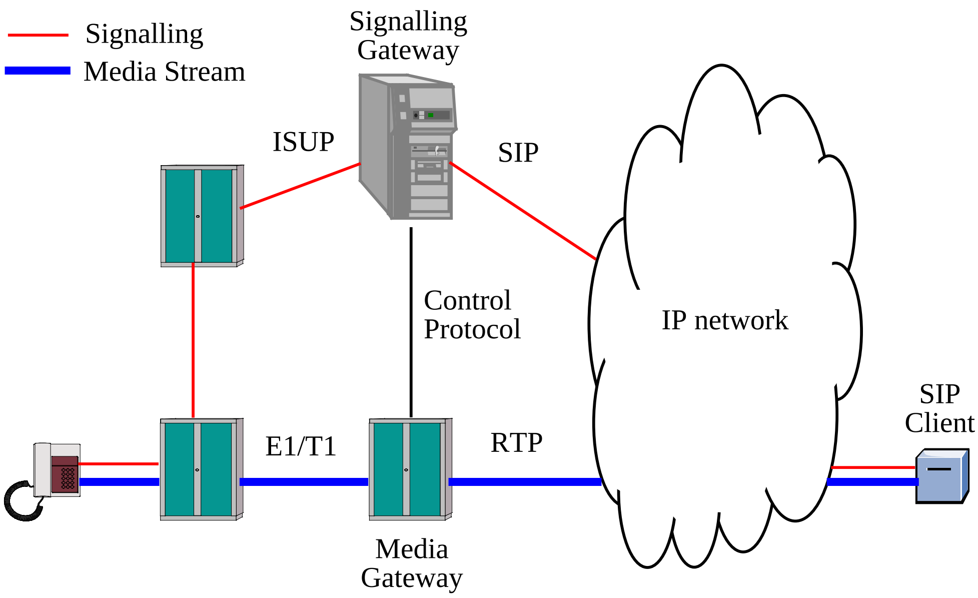


Figure 22: SIP termination

In this scenario, most of the information contained in the ISUP messages could be ignored since it is not interesting for the IP telephone. Therefore, many parameters do not need to be mapped from ISUP to SIP.

4.5.2 SIP bridging

SIP bridging includes calls between two GSTN phones that traverses the Internet. In this scenario, both the signalling and the voice stream traverse the IP cloud.

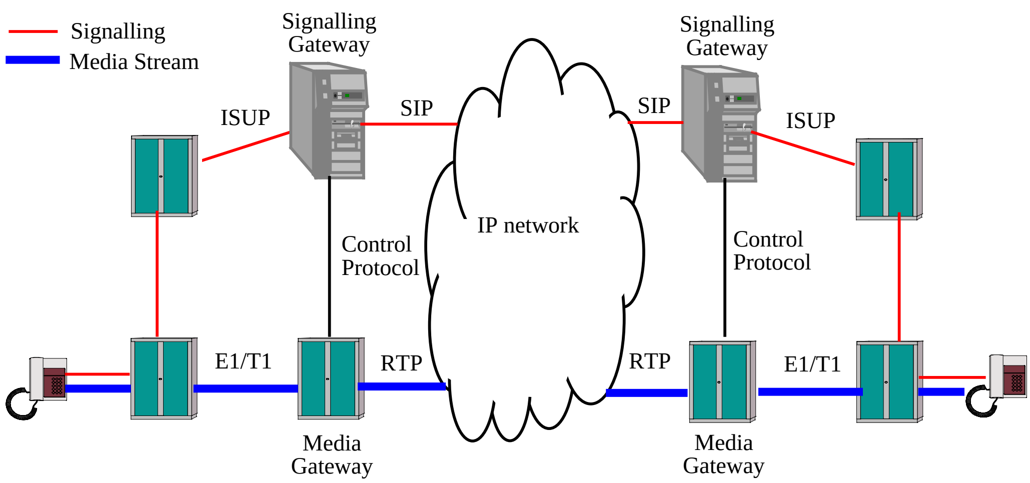


Figure 23: SIP bridging

The IP network in the middle has to be completely transparent to both GSTN phones. Therefore, in this scenario, all the information contained in the ISUP messages has to be mapped.

If some information was not mapped, it would be possible to establish a simple call, but then, the IP cloud would not be transparent and it would not be desirable.

4.5.3 SIP bridging without media gateway

In this scenario, the media stream does not traverse the Internet, so, no media gateway is needed. The signalling gateway works in the same way as in SIP bridging. The only difference is that it does not need to control any media gateway.

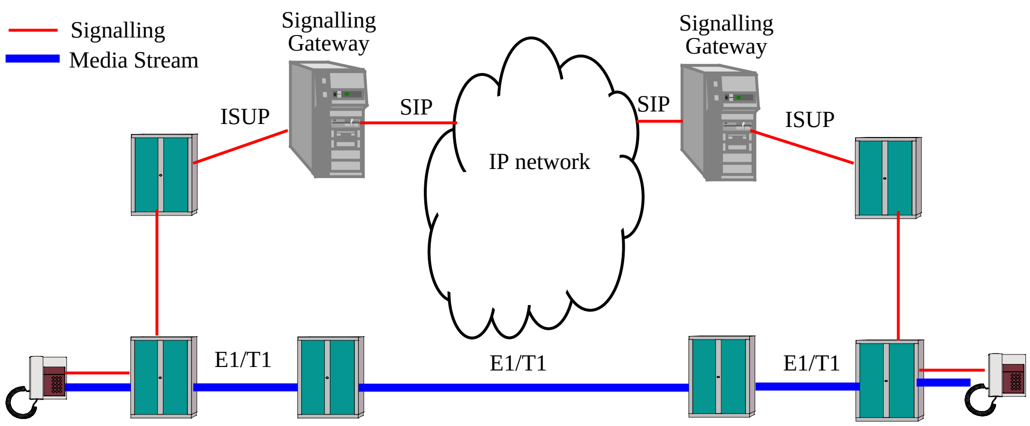


Figure 24: SIP bridging without media gateway

In the normal situation in the three scenarios, the gateway does not know if it is handling a call terminating in the Internet or if the call will end up in the GSTN network again. Due to this, the gateway always has to try to translate all the information contained in the ISUP messages.

4.5.4 Tunnelling approach

When the two ends are GSTN phones and the Internet is in the middle, another approach is to send ISUP over IP. Depending of the type of encapsulation used, some MTP layers are removed and substituted by an IP stack. This approach does not use SIP and so it is outside the scope of this project.

4.6 Mapping of parameters

As it was explained before, a gateway that only handles calls from the GSTN network to the Internet and the opposite way can discharge almost all the parameters contained in the ISUP messages. In the ISUP messages generated by the gateway, default values may be used. However, to perform SIP bridging, it is necessary to perform the translation of ISUP parameters.

There is not a clear correspondence between SIP headers and ISUP parameters. Therefore, it is not possible to distribute all the ISUP indicators among SIP headers. The best way to map these parameters would be to use the message body of SIP. The indicators would be parsed in the first gateway (GSTN-Internet) and transformed to text. Then, the second gateway (Internet-GSTN) would read the information and use it to generate its ISUP messages.

The body of the message could also be used to transport user to user information and to send DTMF tones without coding them in the voice path. These extensions to the message body should be ignored by user agents since that information is just useful for gateways that access the GSTN network again.

The structure of the ISUP signalling messages with their different parameters and indicators are described in the appendix C.

5 Conclusions

The development of gateways between GSTN networks and the Internet will make the border between the telecom world and the datacom world disappear. Merging these networks, the creation of new telephony services will be much faster and easier.

Taking advantage of the flexibility of the Internet every individual user may be provided with customized services. From the Internet point of view, IP telephony could make use of GSTN resources and could be able to reach users almost everywhere.

If SIP is finally successful and becomes a standard for controlling multimedia sessions and different devices, just one protocol would need to be employed. The use of just one protocol avoids the apparition of a bunch of different protocols doing almost the same thing. This way, the interworking between systems would be easier and a truly open architecture would be feasible.

I order to achieve this, SIP will have to join together mobility, security and QoS. Merging together these three factors would address the current problems of the emerging IP telephony technology.

Beyond all the technical details concerning the mapping between protocols or the translation of parameters there are still lots of open questions. Some examples are: who will own the gateways or how the billing will be implemented.

The business case for IP telephony is not clear enough but nobody wants to be out of this new promising business. IP telephony is bringing lower rates for callers and big phone companies are merging to try to fight against the growth of competition from non telephone companies.

Therefore, the development of IP telephony and SS7-IP gateways will lead to a rearchitecture of the communication infrastructure, and SIP may play an important role in all these changes.

6 References

6.1 Traditional Circuit-Switched Telephony

[1] Williams Stalling, “ISDN: an introduction”, Maxwell Macmillan International Editions, 1990

[2] Williams Stallings, “Data and Computer Communications”, 5th edition, Prentice Hall, 1997

[3] “ISDN User Part supplementary services”, ITU-T Q.730 recommendation, September 1997

[4] “Signalling System No. 7 - ISDN User Part functional description”, ITU-T Q.761 recommendation, September 1997

[5] “Signalling System No. 7 - ISDN User Part general functions of messages and signals”, ITU-T Q.762 recommendation, September 1997

[6] “Signalling System No. 7 - ISDN User Part formats and codes”, ITU-T Q.763 recommendation, September 1997

[7] “Signalling System No. 7 - ISDN User Part signalling procedures”, ITU-T Q.764 recommendation, September 1997

[8] “Performance objectives in the integrated services digital network application”, ITU-T Q.766 recommendation, March 1993

[9] “Application of the ISDN user part of CCITT signalling system No. 7 for international ISDN interconnections”, ITU-T Q.767 recommendation, February 1991

6.2 IP Telephony

[10] W. Richard Stevens, “TCP/IP Illustrated, Volume 1”, Addision-Wesley, 1994

[11] M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg, “SIP: Session Initiation Protocol”, Internet Draft, Internet Engineering Task Force, September 1998, work in progress

[12] M. Handley, V. Jacobson, “SDP: session description protocol”, RFC 2119, Internet Engineering Task Force, 1998

[13] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, “RTP: a transport protocol for real-time applications”, RFC 1889, Internet Engineering Task Force, 1996

[14] “A Primer on the H.323 Series Standard”, Data Beam Corporation, April 1997

[15] Henning Schulzrine, Jonathan Rosenberg, “A Comparison of SIP and H.323 for Internet Telephony”, 1998

[16] Henning Schulzrinne,”Internet Services: from electronic Mail to Real-Time Multimedia”

[17] R. Fielding, J.Gettys, J.Mogul, H.Nielsen, T. Berners-Lee, “Hypertext transfer protocol - HTTP/1.1”, RFC 2068, Internet Engineering Task Force, 1997

6.3 Implementation

[18] W. Richard Stevens, Gary R. Wright, "TCP/IP Illustrated, Volume 2", Addision-Wesley, 1995

[19] W. Richard Stevens, "UNIX Network Programming", 1st edition, Prentice Hall, 1990

[20] W. Richard Stevens, "UNIX Network Programming, Volume 1", 2nd edition, Prentice Hall, 1998

[21] Ian Sommerville, "Software Engineering", 4th edition, Addison-Wesley, 1992

A ISUP messages

This appendix describes the different ISUP messages with their parameters.There are three types of parameters:

- Mandatory parameters with fixed length (F)
- Mandatory parameters with variable length (V)
- Optional parameters (O)

A.1 Signalling messages sent just in the forward direction

A.1.1 COT: Continuity message

It indicates whether or not there is a continuity on the preceding circuit(s) as well as of the selected circuit to the following exchange, including verification of the communication path across the exchange with the specified degree of reliability.

Table A.1: Structure of COT

Type of parameter	Parameter
F	Message type
F	Continuity Indicators

A.1.2 FOT: Forward transfer message

A message sent in the forward direction on semiautomatic calls when the outgoing international exchange operator wants the help of an operator at the incoming international exchange. The message will normally serve to bring an assistance operator into the circuit if the call is automatically set up at the exchange. When the call is completed via an operator (incoming or delay operator) at the incoming international exchange, the message should preferably cause this operator to be recalled.

Table A.2: Structure of FOT

Type of parameter	Parameter
F	Message type
O	End of optional parameters

A.1.3 IAM: Initial address message

It is sent to initiate seizure of an outgoing circuit and to transmit number and other information relating to the routing and handling of a call.

Table A.3: Structure of IAM

Type of parameter	Parameter
F	Message type
F	Nature of connection indicators
F	Calling party’s category
F	Forward call indicators
F	Transmission medium requirement
V	Called party number
O	Calling party number
O	Optional forward call indicators
O	Closed user group interlock code
O	User-to-user information
O	Access transport
O	User service information
O	End of optional parameter

A.1.4 SAM: Subsequent address message

A message that may be sent in the forward direction following an initial address message, to convey additional called party number information.

Table A.4: Structure of SAM

Type of parameter	Parameter
F	Message type
V	Subsequent number
O	End of optional parameters

A.2 Signalling messages sent just in the backward direction

A.2.1 ACM: Address complete message

A message sent in the backward direction indicating that all the address signals required for routing the call to the called party have been received

Table A.5: Structure of ACM

Type of parameter	Parameter
F	Message type
F	Backward call indicators
O	Optional backwards call indicators
O	Cause indicators
O	User-to-user indicators
O	User-to-user information
O	Access transport
O	End of optional parameters

A.2.2 ANM: Answer message

A message sent in the backward direction indicating that the call has been answered. In semiautomatic working this message has a supervisory function. In automatic working this message is used in conjunction with charging information in order to:

- Start metering the charge to the calling subscriber
- Start measurement of call duration for international accounting purposes

Table A.6: Structure of ANM

Type of parameters	Parameters
F	Message type
O	Backward call indicators
O	User-to-user information
O	Connected number
O	Access transport
O	End of optional parameters

A.2.3 CPG: Call progress message

A message sent in the backward direction indicating that an event has occurred during call setup which should be relayed to the calling party.

Table A.7: Structure of CPG

Type of parameter	Parameter
F	Message type
Type of parameter	Parameter
F	Event information
O	Backward call indicators
O	Optional backward call indicators
O	Access transport
O	User-to-user information
O	End of optional parameters

A.2.4 CON: Connect message

A message sent in the backward direction indicating that all the address signals required for routing the call to the called party have been received and that the call has been answered.

Table A.8: Structure of CON

Type of parameter	Parameter
F	Message type
F	Backward call indicators
O	Connected number
O	User-to-user indicators
O	Access transport
O	End of optional parameters

A.3 Signalling messages sent in either direction

A.3.1 BLO: Blocking message

A message sent only for maintenance purposes to the exchange at the other end of a circuit, to cause an engaged condition of that circuit for subsequent calls outgoing from that exchange. When a circuit is used in the bothway mode of operation an exchange receiving the blocking message must be capable of accepting incoming calls on the concerned circuit unless it has also sent a blocking message. Under certain conditions, a blocking message is also a proper response to a reset circuit message.

Table A.9: Structure of BLO

Type of parameter	Parameter
F	Message type

A.3.2 BLA: Blocking ACK message

A message sent in response to a blocking message indicating that the circuit has been blocked.

Table A.10: Structure of BLA

Type of parameter	Parameter
F	Message type

A.3.3 CGB: Circuit group blocking message

A message sent to the exchange at the other end of an identified group of circuits to cause an engaged condition of this group of circuits for subsequent calls outgoing from that exchange. An exchange receiving a circuit group blocking message must be able to accept incoming calls on the group of blocked circuits unless it has also sent a blocking message. Under certain conditions, a circuit group blocking message is also a proper response to a reset circuit message.

Table A.11: Structure of CGB

Type of parameter	Parameter
F	Message type
F	Circuit group supervision message type indications
V	Range and status

A.3.4 CGBA: Circuit group blocking ACK message

A message sent in response to a circuit group blocking message to indicate that the requested group of circuit has been blocked.

Table A.12: Structure of CGBA

Type of parameter	Parameter
F	Message type
F	Circuit group supervision message type indications
V	Range and status

A.3.5 GRS: Circuit group reset message

A message sent to release an identified group of circuits when, due to memory mutilation or other causes, it is unknown whether for example, a release or release complete message is appropriate for each of the circuits in the group. If at the receiving end a circuit is remotely blocked, reception of this message should cause that condition to be removed.

Table A.13: Structure of GRS

Type of parameter	Parameter
F	Message type
V	Range and status

A.3.6 GRA: Circuit group reset ACK

A message sent in response to a circuit group reset and indicating that the requested group of circuits has been reset. The message also indicates the maintenance blocking state of each circuit.

Table A.14: Structure of GRA

Type of parameter	Parameter
F	Message type
V	Range and status

A.3.7 CGU: Circuit group unblocking message

A message sent to the exchange at the other end of an identified group of circuits to cause cancellation in that group of circuits of an engaged condition invoked earlier by a blocking or circuit group blocking message.

Table A.15: Structure of CGU

Type of parameter	Parameter
F	Message type
F	Circuit group supervision message type indications
V	Range and status

A.3.8 CGUA: Circuit group unblocking ACK message

A message sent in response to a circuit group unblocking message to indicate that the requested group of circuits has been unblocked.

Table A.16: Structure of CGUA

Type of parameter	Parameter
F	Message type
F	Circuit group supervision message type indications
V	Range and status

A.3.9 CCR: Continuity check request message

A message sent by an exchange for a circuit on which a continuity check is to be performed, to the exchange at the other end of the circuit, requesting continuity checking to be attached.

Table A.17: Structure of CCR

Type of parameter	Parameter
F	Message type

A.3.10 REL: Release message

A message sent in either direction to indicate that the circuit is being released due to the reason (cause) supplied and is ready to be put into the idle state on receipt of the release complete message.

Table A.18: Structure of REL

Type of parameter	Parameter
F	Message type
V	Cause indicators
O	User-to-user information
O	Automatic congestion level
O	End of optional parameters

A.3.11 RLC: Release circuit message

A message sent in either direction in response to the receipt of a released message, or if appropriate to a reset circuit message, when the circuit concerned has been brought into the idle condition.

Table A.19: Structure of RLC

Type of parameter	Parameter
F	Message type
V	Cause indicators
O	User-to-user information
O	Automatic congestion level
O	End of optional parameters

A.3.12 RSC: Reset circuit message

A message sent to release a circuit when, due to memory mutilation or other causes, it is unknown whether for example, a release complete message is appropriate. If, at the receiving end, the circuit is remotely blocked, reception of this message should cause the condition to be removed.

Table A.20: Structure of RSC

Type of parameter	Parameter
F	Message type

A.3.13 RES: Resume message

A message sent in either direction indicating that the calling or called part, after having been suspended, is reconnected.

Table A.21: Structure of RES

Type of parameter	Parameter
F	Message type
F	Suspend/Resume indicators
O	End of optional parameters

A.3.14 SUS: Suspend message

A message sent in either direction indicating that the calling or called party has been temporarily disconnected

Table A.22: Structure of SUS

Type of parameter	Parameter
F	Message type
F	Suspend/Resume indicators
O	End of optional parameters

A.3.15 UBL: Unblocking message

A message sent to the exchange at the other end of a circuit to cancel, in that exchange, the engaged condition of the circuit caused by a previously sent blocking or circuit group blocking message.

Table A.23: Structure of UBL

Type of parameter	Parameter
F	Message type

A.3.16 UBA: Unblocking ACK message

A message sent in response to an unblocking message indicating that the circuit has been unblocked.

Table A.24: Structure of UBA

Type of parameter	Parameter
F	Message type

B ISUP Parameters

This appendix describes the different ISUP parameters with their indicators and their possible values.

B.1 Access transport

- Information element

B.2 Automatic congestion level

- Spare
- Congestion level 1 exceeded
- Congestion level 2 exceeded

B.3 Backward call indicators

B.3.1 Charge indicator

Information sent in the backward direction indicating whether or not the call is chargeable.
- No indication
- No charge
- Charge
- Spare

B.3.2 Called party's status indicator

Information sent in the backward direction indicating the category of the called party.
- No indication
- Subscriber free
- Spare

B.3.3 Called party's category indicator

Information sent in the backward direction indicating the category of the called party.
- No indication
- Ordinary subscriber
- Payphone
- Spare

B.3.4 End-to-end method indicator

- Only link-by-link method available

B.3.5 Interworking indicator

- No interworking encountered
- Interworking encountered

B.3.6 End-to-end information indicator

Information sent in either direction indicating the available methods, if any, for end-to-end transfer of information

- No end-to-end information available

B.3.7 ISDN User part indicator

Information sent in either direction to indicate that the ISDN User Part is used in all preceding parts of the network connection. When sent in the backward direction, the preceding parts are those towards the called party.

- ISDN User Part not used all the way
- ISDN User Part used all the way

B.3.8 ISDN access indicator

Information sent in either direction indicating whether or not the access signalling protocol is ISDN.

- Terminating access non-ISDN
- Terminating access ISDN

B.3.9 Echo control device indicator

Information indicating whether or not a half echo control device is included in the connection.

- Incoming half echo control device not included
- Incoming half echo control device included

B.3.10 SCCP method indicator

Information sent in either direction indicating the available SCCP methods, if any, for end-to-end transfer of information.

- No indication

B.4 Called party number

B.4.1 Odd/even indicator

Information sent in association with an address, indicating whether the number of address signals contained in the address is even or odd.

- Even number of address signals
- Odd number of address signals

B.4.2 Nature of address indicator

Information sent in association with an address indicating the nature of that address.

- Spare
- National (significant) number
- International number

B.4.3 Internal network number indicator

Information sent to the destination exchange indicating whether or not the call is allowed should be called party number prove to be an internal network number (e.g. mobile access point).

- Routing to internal network number allowed
- Routing to internal network number not allowed

B.4.4 Numbering plan indicator

Information sent in association with a number indicating the numbering plan used for a number (e.g. ISDN number, telex number).

- Spare
- ISDN (Telephony) numbering plan

B.4.5 Address signal

An element of information is a network number. The address signal may indicate digit values 0 to 9, code 11 or code 12. One address signal value (ST) is reserved to indicate the end of the called party number.

- Spare
- Digit 0..9
- Code 11
- Code 12
- ST

B.5 Calling party number

B.5.1 Odd/even indicator

Information sent in association with an address, indicating whether the number of address signals contained in the address is even or odd.

- Even number of address signals
- Odd number of address signals

B.5.2 Nature of address indicator

Information sent in association with an address indicating the nature of that address.

- Spare
- International number

B.5.3 Calling party number incomplete indicator

Information sent in the forward direction indicating that the complete calling party number is not included.

- Complete

B.5.4 Numbering plan indicator

Information sent in association with a number indicating the numbering plan used for a number (e.g. ISDN number, telex number).

- Spare
- ISDN (Telephony) numbering plan

B.5.5 Address presentation restricted indicator

Information sent in either direction to indicate that the address information is not to be present to a public network user, but can be passed to another public network. It is also used to indicate the non availability of the address.

- Presentation allowed
- Presentation restricted
- Spare

B.5.6 Screening indicator

Information sent in either direction to indicate whether the address was provided by the user or network.

- User provided, verifies and passed
- Network provided

B.5.7 Address signal

An element of information is a network number. The address signal may indicate digit values 0 to 9, code 11 or code 12. One address signal value (ST) is reserved to indicate the end of the called party number.

- Spare
- Digit 0..9
- Code 11
- Code 12

B.6 Calling party’s category

- Operator, language French
- Operator, language English
- Operator, language German
- Operator, language Russian
- Operator, language Spanish
- Ordinary calling subscriber
- Calling subscriber with priority
- Data call (voice and data)
- Test call
- Spare
- Payphone

B.7 Cause indicators

B.7.1 Extension indicator

Information indicating whether or not the associated octet has been extended.

- Last octet

B.7.2 Coding standard

Information sent in association with a parameter (e.g. cause indicators) identifying the standard in which the parameter format is described.
- CCITT standard

B.7.3 Location

Information sent in either direction indicating where an event (e.g. release) was generated
- User
- Transit network
- Public network serving the remote user
- Private network serving the remote user
- International network
- Beyond an interworking point, all other values are reserved

B.7.4 Cause value

Information sent in either direction indicating the reason for sending the message (e.g. release message).
- Normal event
- Resource unavailable
- Service or option not available
- Service or option not implemented
- Invalid message
- Protocol error

B.8 Circuit group supervision message type indicator

B.8.1 Type indicator

- Maintenance oriented
- Hardware failure oriented
- Spare

B.9 Closed user group interlock code

B.9.1 Network identity

B.9.2 Binary code

A code allocated to a closed user group administered by a particular ISDN or data network.

B.10 Connected number

B.10.1 Odd/even indicator

Information sent in association with an address, indicating whether the number of address signals contained in the address is even or odd.

- Even number of address signals
- Odd number of address signals

B.10.2 Nature of address indicator

Information sent in association with an address indicating the nature of that address.
- Spare
- International number

B.10.3 Numbering plan indicator

Information sent in association with a number indicating the numbering plan used for a number (e.g. ISDN number, telex number).
- Spare
- ISDN (Telephony) numbering plan

B.10.4 Address presentation restricted indicator

Information sent in either direction to indicate that the address information is not to be presented to a public network user, but can be passed to another public network. It is also used to indicate the non availability of the address.
- Presentation allowed
- Presentation restricted
- Address not available
- Spare

B.10.5 Screening indicator

Information sent in either direction to indicate whether the address was provided by the user or network.
- User provided, verifies and passed
- Network provided

B.10.6 Address signal

An element of information is a network number. The address signal may indicate digit values 0 to 9, code 11 or code 12. One address signal value (ST) is reserved to indicate the end of the called party number.
- Spare
- Digit 0..9
- Code 11
- Code 12

B.11 Continuity indicators

B.11.1 Continuity indicator

Information sent in the forward direction indicating whether or not the continuity check on the outgoing circuit was successful. A continuity check successful indication also implies continuity of the preceding circuits and successful verification of the path across the exchange with the specified degree of reliability.

- Continuity check failed
- Continuity check successful

B.12 End of optional parameters

The last optional parameter field of a message is followed by the end of optional parameters indicator, which occupies a one octet filed containing all zeros.

B.13 Event information

B.13.1 Event indicator

Information sent in the backward direction indicating the type of event which caused a call progress message to be sent to the originating local exchange.

- Alerting
- Progress
- In-band information or an appropriate pattern is now available
- Spare

B.13.2 Event presentation restricted indicator

Information sent in the backward direction indicating that the event should not be presented to the calling party.

- No indication

B.14 Forward call indicators

B.14.1 National/international call indicator

Information sent in the forward direction indicating in the destination national network whether the call has to be treated as an international call or as a national call.

- Call to be treated as a national call
- Call to be treated as an international call

B.14.2 End-to-end method indicator

Information sent in either direction indicating the available methods, if any, for end-to-end transfer of information.

- No end-to-end method available

B.14.3 Interworking indicator

Information sent in either direction indicating whether or not SS7 is used in all parts of the network connection.

- No interworking encountered (No 7 signalling all the way)
- Interworking encountered

B.14.4 End-to-end information indicator

Information sent in either direction indicating the available methods, if any, for end-to-end

transfer of information
- No end-to-end information available

B.14.5 ISDN user part indicator

Information sent in either direction to indicate that the ISDN User Part is used in all preceding parts of the network connection. When sent in the backward direction, the preceding parts are those towards the called party.
- ISDN user part not used all the way
- ISDN user part used all the way

B.14.6 ISDN user part preference indicator

Information sent in the forward direction indicating whether or not the ISND User Part is required or preferred in all parts of the network connection.
- ISDN user part preferred all the way
- ISDN user part not required all the way
- ISDN user part required all the way
- Spare

B.14.7 ISDN access indicator

Information sent in either direction indicating whether or not the access signalling protocol is ISDN.
- Originating access non-ISDN
- Originating access ISDN

B.14.8 SCCP method indicator

Information sent in either direction indicating the available SCCP methods, if any, for end-to-end transfer of information.
- No indication

B.15 Nature of the connection indicators

B.15.1 Satellite indicator

Information sent in the forward direction indicating the number of satellite circuits in the connection.
- No satellite circuit in the connection
- One satellite circuit in the connection
- Two satellite circuits in the connection
- Spare

B.15.2 Continuity check indicator

Information sent in the forward direction indicating whether or not a continuity check will be performed on the circuit(s) concerned or being (has been) performed on a previous circuit in the connection.
- Continuity check not required

- Continuity check required on this circuit
- Continuity check performed on a previous circuit
- Spare

B.15.3 Echo control device indicator

Information indicating whether or not a half echo control device is included in the connection.

- Outgoing half echo control device not included
- Outgoing half echo control device included

B.16 Optional backward call indicators

B.16.1 In-band information indicator

Information sent in the backward direction indicating that in-band information or an appropriate pattern is now available.

- No indication
- In-band information or an appropriate pattern is now available

B.16.2 Call forwarding may occur indicator

Information sent in the backward direction indicating the call forwarding may occur, depending on the response received (or lack thereof) from the called party.

- No indication

B.17 Optional forward call indicators

B.17.1 Closed user group call indicator

Information indicating whether or not the concerned call can be set up as a closed user group call and, if a closed user group call, whether or not outgoing access is allowed.

- Non-CUG call
- Spare
- Closed user group call, outgoing access allowed
- Closed group call, outgoing access not allowed

B.17.2 Connected line identity request indicator

- Not requested
- Requested

B.18 Range and Status

B.18.1 Range

Information sent in a circuit group supervision message (e.g. circuit group blocking) to indicate the range of circuits affected by the action in the message.

- Range of the circuits affected by the message

B.18.2 Status

Information sent in a circuit group supervision message (e.g. circuit group blocking) to indicate the specific circuits, within the range of circuits stated in the message, that are affected by the action specified in the message.

In circuit group blocking message:
- No indication
- Blocking

In circuit group blocking ACK messages:
- No indication
- Blocking ACK

In circuit group unblocking messages:
- No indication
- Unblocking

In circuit group unblocking ACK messages:
- No indication
- Unblocking ACK

In circuit group reset ACK messages
- Not blocked for maintenance reasons
- Blocked for maintenance reasons

B.19 Subsequent number

B.19.1 Odd/even indicator

Information sent in association with an address, indicating whether the number of address signals contained in the address is even or odd.
- Even number of address signals
- Odd number of address signals

B.19.2 Address signal

An element of information is a network number. The address signal may indicate digit values 0 to 9, code 11 or code 12. One address signal value (ST) is reserved to indicate the end of the called party number.
- Spare
- Digit 0..9
- Code 11
- Code 12
- ST

B.20 Suspend/resume indicators

B.20.1 Suspend/resume indicator

Information sent in the suspend and resume messages to indicate whether suspend/resume was initiated by an ISDN subscriber or by the network.

- ISDN subscriber initiated
- Network initiated

B.21 Transmission medium requirement

- Speech
- Spare
- 64 kbps unrestricted
- 3.1 kHz audio

B.22 User service information

B.22.1 Extension indicator

Information indicating whether or not the associated octet has been extended.
- Octet continues through the next octet
- Last octet

B.22.2 Coding standards

Information sent in association with a parameter (e.g. cause indicators) indentifying the standard in which the parameter format is described.
- CCITT standardized coding as described below
- Reserved for other international standards
- National standard
- Standard defined for the network (either public or private) present on the network side of the interface

B.22.3 Information transfer capability

- Speech
- Unrestricted digital information
- Restricted digital information
- 3.1 kHz audio
- 7 kHz audio
- video

B.22.4 Transfer mode

- Circuit mode
- Packet mode

B.22.5 Information transfer rate

- Packetmode calls
- 64 kbps
- 384 kbps
- 1536 kbps
- 1920 kbps

B.22.6 Structure

- Default
- 8 kHz integrity
- Service data unit integrity
- Unstructured

B.22.7 Configuration

- Point-to-point

B.22.8 Establishment

- Demand

B.22.9 Symmetry

- Bidirectional symmetric

B.22.10 Layer identification

- User information layer 1 protocol
- User information layer 2 protocol
- User information layer 3 protocol

B.22.11 User information layer 1 protocol identification

- Recommendation Q.767

B.22.12 User information layer 1 protocol identification

- Recommendation Q.921 (I.441)
- Recommendation X.25, link level

B.22.13 User information layer 1 protocol identification

- Recommendation Q.931 (I.451)
- Recommendation X.25, packet level

B.23 User-to-user indicators

B.23.1 Type

- Response

B.23.2 Service 1

- No information

B.23.3 Service 2

- No information

B.23.4 Service 3

- No information

B.23.5 Network discard indicator

- UUI discarded by the network

B.24 User-to-user information

Information generated by a user and transferred transparently through the interexchange network between the originating and terminating local exchanges.

C ISUP signalling messages

This appendix describes the structure of the ISUP signalling messages with their different parameters and indicators.

Table C.1: Address Complete Message (ACM)

Parameters	Indicators
F Message type	
F Backward indicator	• Charge indicator • Called party's status indicator • Called party's category indicator • End-to-end method indicator • Interworking indicator • End-to-end information indicator • ISDN user part indicator • ISDN access indicator • Echo control device indicator • SCCP method indicator
O Optional backward call indicators	• In-band information indicator • Call forwarding may occur indicator
O Cause indicators	• Extension indicator • Coding standard • Location • Cause value
O User-to-user indicators	
O User-to-user information	
O Access transport	
O End of optional parameters	

Table C.2: Answer Message (ANM)

Parameters	Indicators
F Message type	

Table C.2: Answer Message (ANM)

O Backward call indicators	• Charge indicator • Called party's status indicator • Called party's category indicator • End-to-end method indicator • Interworking indicator • End-to-end information indicator • ISDN user part indicator • ISDN access indicator • Echo control device indicator • SCCP method indicator
O User-to-user information	
O Connected number	• Odd/even indicator • Nature of address indicator • Numbering plan indicator • Address presentation restricted indicator • Screening indicator • Address signal
O Access transport	
O End of optional parameters	

Table C.3: Connect Message (CON)

Parameters	Indicators
F Message type	
F Backward call indicator	• Charge indicator • Called party's status indicator • Called party's category indicator • Ent-to-end method indicator • Interworking indicator • End-to-end information indicator • ISDN user part indicator • ISDN access indicator • Echo control device indicator • SCCP method indicator

Table C.3: Connect Message (CON)

O Connected number	• Odd/even indicator • Nature of address indicator • Numbering plan indicator • Address presentation restricted indicator • Screening indicator • Address signal
O User-to-user indicators	
O User-to-user information	
O Access transport	
O End of optional parameters	

Table C.4: Call Progress Message (CPG)

Parameters	Indicators
F Message type	
F Event information	• Event indicator • Event presentation restricted indicator
O Backward call indicators	• Charge indicator • Called party’s status indicator • Called party’s category indicator • Ent-to-end method indicator • Interworking indicator • End-to-end information indicator • ISDN user part indicator • ISDN access indicator • Echo control device indicator • SCCP method indicator
O Optional backward call indicators	• In-band information indicator • Call forwarding may occur indicator
O User-to-user information	
O Access transport	
O End of optional parameters	

Table C.5: Initial Address Message (IAM)

Parameters	Indicators
F Message type	
F Nature of the connection indicators	• Satellite indicator • Continuity check indicator • Echo control device indicator
F Forward call indicators	• National/International call indicator • Ent-to-end method indicator • Interworking indicator • End-to-end information indicator • ISDN user part indicator • ISDN user part preference indicator • ISDN access indicator • SCCP method indicator
F Calling party's category	
F Transmission medium requirement	
V Called party number	• Odd/even indicator • Nature of address indicator • Internal network number indicator • Numbering plan indicator • Address signal
O Calling party number	• Odd/even indicator • Nature of address indicator • Calling party number incomplete indicator • Numbering plan indicator • Address presentation restricted indicator • Screening indicator • Address signal
O Optional forward call indicators	• Closed user group call indicator • Connected line indentity request indicator
O Closed user group interlock code	
O User-to-user information	
O Access transport	

Table C.5: Initial Address Message (IAM)

O User service information	• Extension indicator • Coding standard • Information transfer capability • Transfer mode • Information transfer rate • Structure • Configuration • Establishment • Symmetry • Layer identification • User information layer 1 protocol identification • User information layer 2 protocol identification • User information layer 3 protocol identification
O End of optional parameters	

Table C.6: Release Circuit Message (RLC)

Parameters	Indicators
F Message type	
V Cause indicators	• Extension indicator • Coding standard • Location • Cause value
O User-to-user information	
O Automatic congestion level	
O End of optional parameters	

Table C.7: Release Message (REL)

Parameters	Indicators
F Message type	
V Cause indicators	• Extension indicator • Coding standard • Location • Cause value
O User-to-user information	

Table C.7: Release Message (REL)

O Automatic congestion level	
O End of optional parameters	

Table C.8: Subsequent Address Message (SAM)

Parameters	Indicators
F Message type	
V Subsequent number	• Odd/even indicator • Address signal
O End of optional parameters	

Table C.9: Resume Message (RES)

Parameters	Indicators
F Message type	
F Suspend/resume indicators	• Suspend/resume indicator
O End of optional parameters	

Table C.10: Suspend Message (SUS)

Parameters	Indicators
F Message type	
F Suspend/resume indicators	• Suspend/resume indicator
O End of optional parameters	

D Glossary

Table D.1: Acronyms

1VF	One Voice Frequency
2VF	Two Voice Frequency
ACK	Acknowledgement
ACM	Address Complete Message
ARPANET	Advanced Research Projects Agency Net
BGP	Border Gateway Protocol
BIB	Backward Indicator Bit
BLA	Blocking ACK Message
BLO	Blocking Message
BSN	Backward Indicator Bit
CAS	Channel Associated Signalling
CBG	Circuit Group Blocking Message
CCITT	Comité Consultatif International Télégraphique et Téléphonique
CCR	Continuity Check Request Message
CCS	Common Channel Signalling
CGBA	Circuit Group Blocking Message
CGU	Circuit Group Unblocking Message
CGUA	Circuit Group Unblocking ACK Message
CIC	Circuit Identification Code
CON	Connect Message
COT	Continuity Message
CPG	Call Progress Message
GRA	Circuit Group Reset ACK Message
GRS	Circuit Group Reset Message
DARPA	Defence Advanced Research Project Agency
DPC	Destination Point Code
DSS 1	Digital Subscriber Signalling 1

Table D.1: Acronyms

DTMF	Dual-Tone Multi-Frequency
HTTP	Hypertext Transfer Protocol
F	Mandatory parameter with fixed length
FIB	Forward Indicator Bit
FISU	Fill In-band Signal Unit
FOT	Forward Transfer Message
FSN	Forward Sequence Number
GSTN	General Switched Telephone Network
IAM	Initial Address Message
IANA	Internet Assigned Numbers Authority
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPDC	Internet Protocol Device Control
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISUP	ISDN User Part
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
LI	Length Indicator
LSSU	Link Status Unit
MFC	Multi Frequency Code signalling
MFP	Multi Frequency Pulsing
MGCP	Media Gateway Control Protocol
MSU	Message Signal Unit
MTP	Message Transfer Part
NI	Network Indicator
NSP	Network Service Part
O	Optional Parameter

Table D.1: Acronyms

OPC	Originating Point Code
OSI	Open System Interconnection
PCM	Pulse Code Modulation
PSTN	Public Switched Telephone Network
QoS	Quality of Service
REL	Release Message
RES	Resume Message
RLC	Release Complete Message
RSC	Reset Circuit Message
RSVP	ReSerVation Protocol
RTP	Real-Time Transport Protocol
SAM	Subsequent Address Message
SCCP	Signalling Connection Control Part
SDES	Source description
SDP	Session Description Protocol
SF	Status Field
SGCP	Simple Gateway Control Protocol
SI	Service Indicator
SIF	Signalling Information Field
SIO	Service Information Octet
SIP	Session Initiation Protocol
SLS	Signalling Link Selection
SNMP	Simple Network Management Protocol
SS6	System Signalling No. 6
SS7	System Signalling No. 7
SSRC	Synchronization Source Indentifier
SU	Signal Unit
SUS	Suspend Message
TCAP	Transaction Capabilities Application Part
TCP	Transmission Control Protocol
TUP	Telephone User Part

Table D.1: Acronyms

UBA	Unblocking ACK Message
UBL	Unblocking Message
UDP	User Data Protocol
V	Mandatory parameter with variable length