

Public Network Signalling

This tutorial gives provides an introduction to the terms and structure of the Signalling System Number 7 (SS7) protocol.

- What is a signalling protocol?
- The SS7 Protocol
- Message Transfer Part (MTP)
- MTP layer 2
- MTP Layer 3
- Telephony User Part (TUP)
- ISDN User Part (ISUP)
- Signalling Connection Control Part (SCCP)
- Transaction Capabilities (TCAP)
- Mobile Application Part (MAP)
- Intelligent Networking Application Part (INAP)
- Mobile/Wireless Intelligent Networking (CAMEL, WIN)
- SS7 Standards
- SS7 and IP Convergence

What is a signalling protocol?

Signalling provides the ability to transfer information inside networks, between different networks, and more importantly between the customers that use the network services for which we charge. A signalling protocol defines a standard set of information elements and a method of transport in order to enable components of a network to interoperate.

There are two types of signalling, *Channel Associated Signalling (CAS)*, where the signalling information is carried down the same physical channel as the voice or data. Examples of such systems are loop disconnect, "robbed bit", CCITT No. 5, R2 and multi-frequency (MF) access dialling. These systems tend to be slow and provide a very limited capability to transfer information between the service users.

Common Channel Signalling (CCS) concentrates the signalling information in a single dedicated channel, such that all of the signalling information for many voice channels in a telephony system can conveyed over a single channel dedicated to signalling.

Signalling System Number 7 (SS7, C7, No 7) is an example of a common channel signalling system, defined for use in public switched networks where large numbers of circuits are switched between subscribers. SS7 is a global standard used throughout the world within networks and on international interconnects, it is the signalling technology inside the network that delivers (Integrated Services Digital Network) ISDN, mobile/wireless and Intelligent Networking.

The subscribers or service users access the network using an Access protocol, such as multi-frequency dialling or ISDN. These types of protocol are targeted at providing services to the subscribers, allowing interaction of the subscriber with the network. Inside the network however, a reliable and robust method of signalling is required, this is provided by SS7.

The SS7 protocol

SS7 is defined as a number of independent blocks of functionality, each implementing a specific function and having a defined interface. Figure 1 shows the basic SS7 protocol.

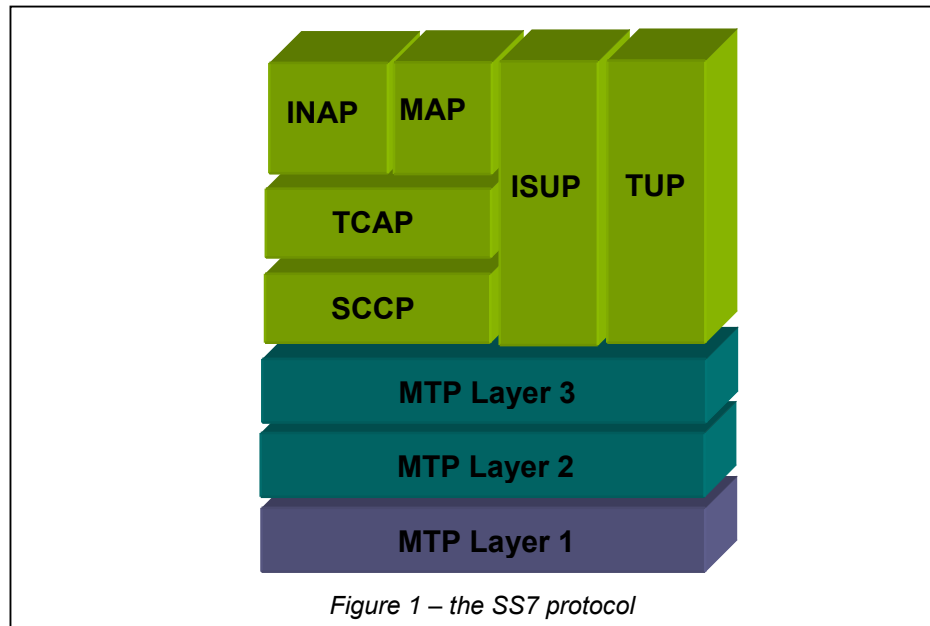


Figure 1 – the SS7 protocol

Message Transfer Part (MTP)

The Message Transfer Part (MTP) consists of three levels (levels 1 to 3 of SS7). Its purpose is to reliably transfer messages on behalf of the User Parts across the SS7 network. The MTP maintains this service despite failures in the network. Layer 1 defines the physical interface. In Europe, SS7 is generally carried on a timeslot in a 2.048Mbps E1 trunk, generally timeslot 16 (but not necessarily). In North America, SS7 may be carried on either a V.35 synchronous serial interface running at 56 or 64kbps, or multiplexed on to a 1.544Mbps T1 timeslot. The SS7 messages are constructed similar to HDLC frames (each message being delimited by 'flag' bytes or octets, and containing a Cyclic Redundancy Check, CRC).

MTP layer 2

The layer 2 part of the protocol provides reliable transfer of messages between two adjacent nodes, ensuring that messages are delivered in sequence and error free. The SS7 protocol specifies that empty frames known as *Fill in Signal Units* (FISU) should be sent when no signalling information from the upper layers is waiting for transmission, hence the SS7 receiver always expects to receive frames (information or empty) continuously, enabling rapid detection of any failure or break in communication.

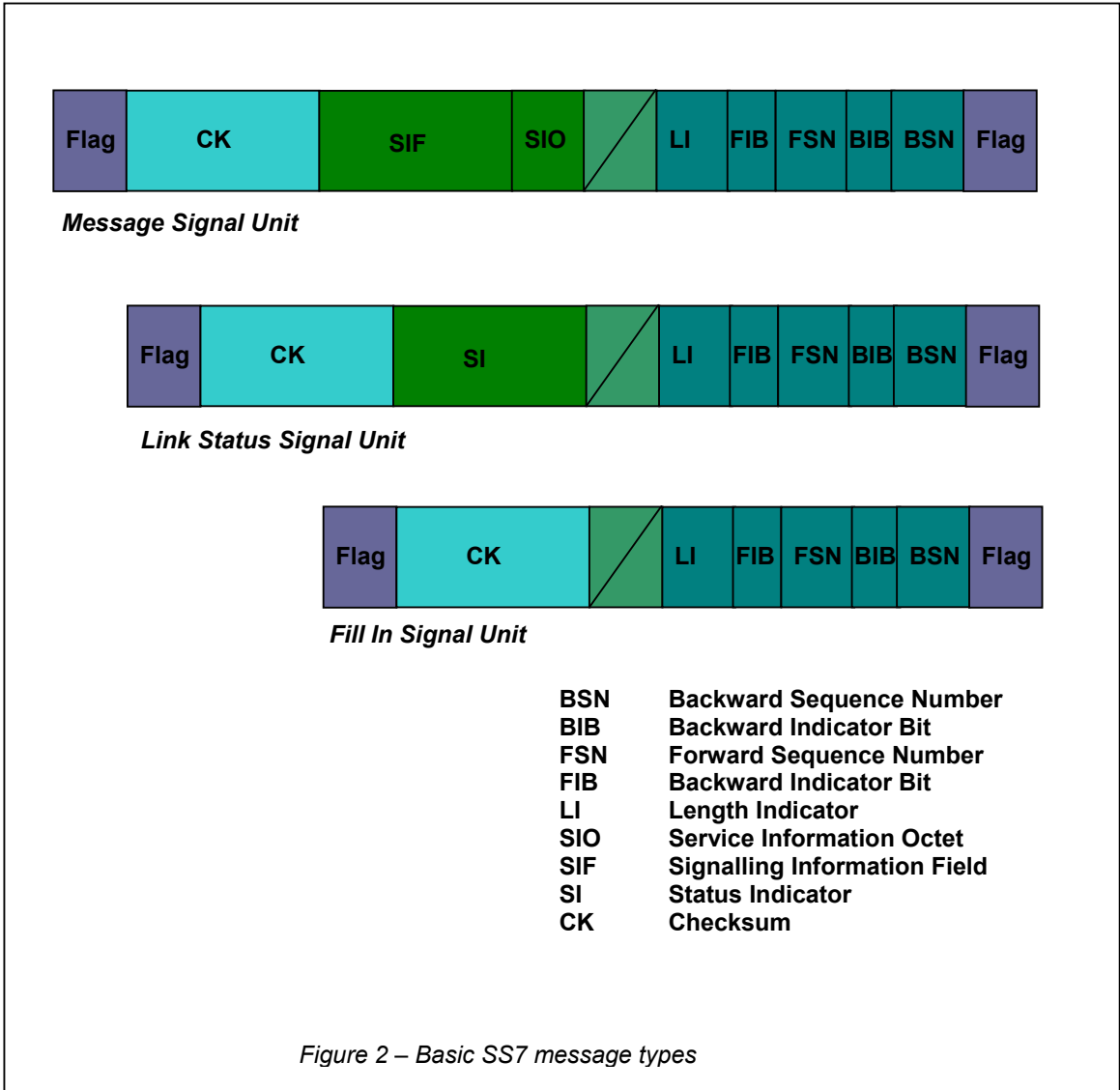
Layer 2 provides a method of message acknowledgement using sequence numbers and indicator bits in both the forwards and backward direction. Each information message carries a Forward Sequence Number (FSN) uniquely identifying that message. The message also carries a Backwards Sequence Number (BSN) acknowledging the FSN of the last message successfully received. Forward and Backward Indicator bits are toggled to indicate positive or negative acknowledgement.

The two common methods for handling errors on SS7 links are either the *basic method*, whereby a message is only retransmitted on receipt of a negative acknowledgement, and *Preventative Cyclic Retransmission (PCR)*, whereby a frame is repeatedly sent when the upper layers have no information to be sent to the network. PCR is generally only used over transmission paths where the transmission delay is large, such as satellite links.

Before an SS7 link is able to convey information from the higher layers, the layer 2 entities at each end of the link follow a handshaking procedure known as the *proving period*, lasting for 0.5 to 8.2 seconds (depending on the availability of routes served by the link in question). During this time, *Link Status Signal Units (LSSU)* are exchanged between the layer 2 parts of the protocol, enabling both ends to monitor the number of received errors during this time. If less than a pre-set threshold, the link enters the IN SERVICE state, and may now carry *Message Signal Units (MSU)* containing information from the upper layers.

The layer 2 entities also monitor the state of the link and communicate link state information to their peers in layer 2 messages or Link Status Signal Units (LSSU). These are transmitted, for example, when links become congested or are taken out of service.

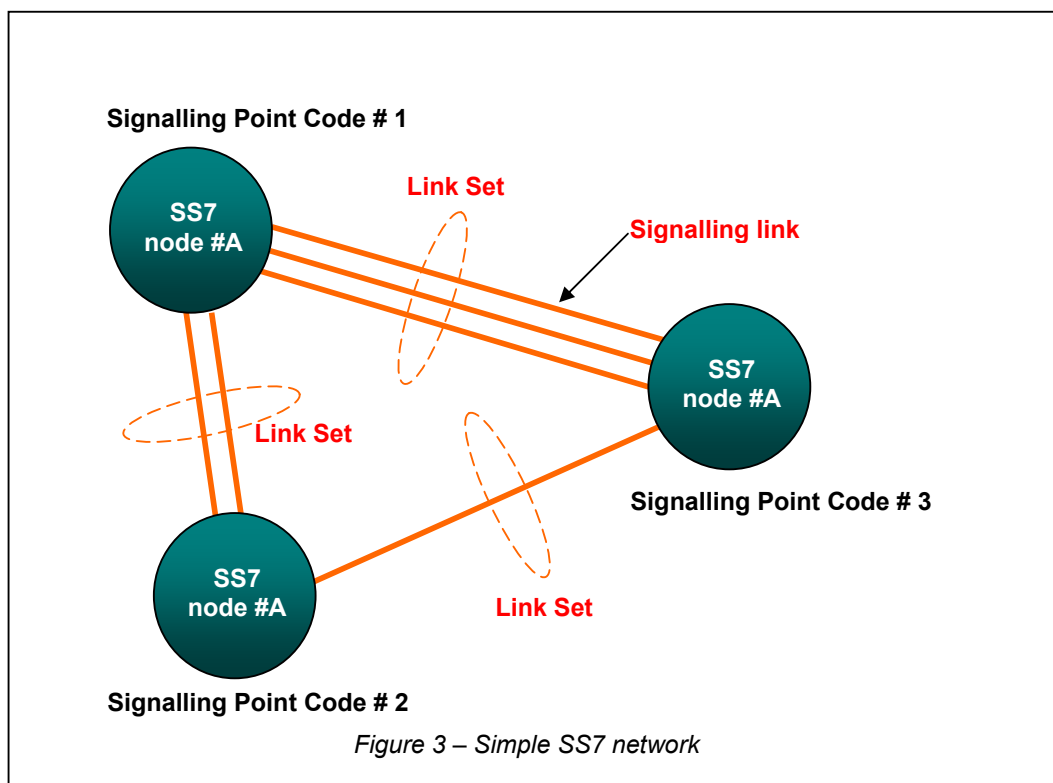
Figure 2 illustrates the three basic types of messages passed by layer 2 are therefore Fill In Signal Units FISU, Link Status Signal Units LSSU and message Signal Units MSU.



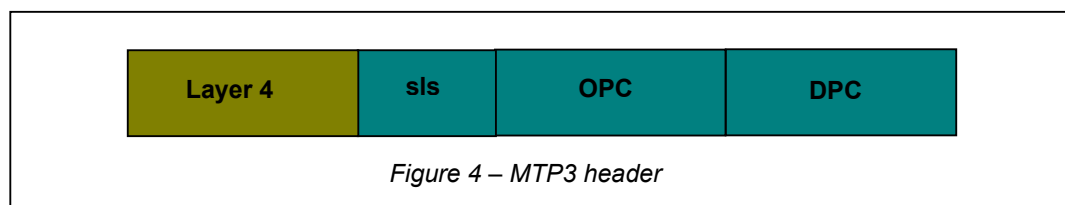
MTP Layer 3

Layer 3 provides the message routing and failure handling capabilities for the message transport. Each SS7 node (this could be a classic switch or a node containing 800 number translation records) is uniquely identified within a network using an SS7 address called a *Point Code*. European networks use 14 bit point codes, North American 24 bit point codes.

A single SS7 link is able to carry traffic for thousands of circuits (depending on traffic a single SS7 link is normally engineered to control 1000 to 2000 circuits), however, failure of this single link would disable all of the circuits that are controlled, hence for resilience and also to increase traffic capacity, more than one signalling channel is normally provisioned between any two nodes communicating using SS7. The collection of *signalling links* between two adjacent nodes is known as a *link set*, each link set can contain up to 16 signalling links. Figure 3 shows a simple SS7 network containing 3 nodes.



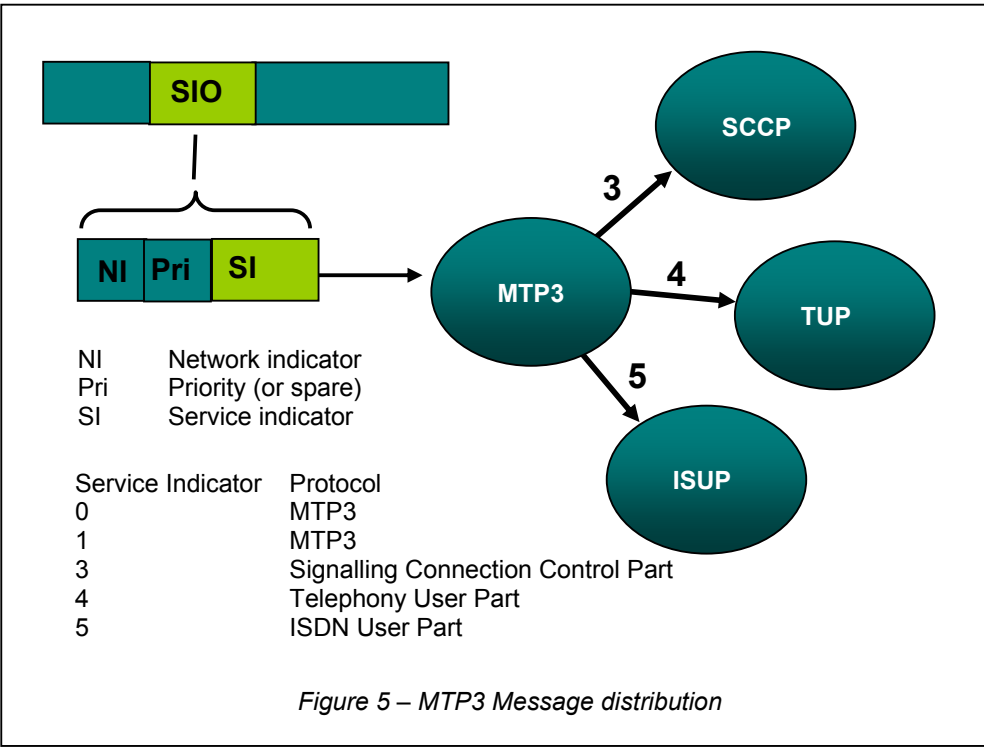
MTP3 adds information into the Signalling Information Field (SIF) of the MSU described in Figure 2. This includes a Destination Point Code (DPC) identifying the destination for a message, an Originating Point Code (OPC) identifying the originator of a message and a *Signalling Link Selection* (sls) value used by MTP3 to load share messages between links in a link set. Figure 4 shows the basic format of the MTP3 header part of an SS7 message.



The MTP automatically load shares between the links within a link set, and re-routes traffic from failed links to a working link within the same link set on detection of failure. MTP layer 3 also attempts to automatically restore failed links and returns traffic to a recovered link, these two procedures being termed *Changeover* and *Changeback*. MTP3 is also able to load share between two link sets that serve the same destination (through the use of intermediate nodes), the link sets here being contained within a *route set*.

MTP3 provides a reliable message transport service to the higher layer protocols, which use MTP as a message transport service, hence their generic name, *User Parts*. In order to deliver a received message to the correct user part, MTP3 examines the *Service Indicator* (SI) which forms part of the *Service Information Octet* (SIO) in the received message, as shown in Figure 5.

The SIO also contains the *Network Indicator* (enabling identification of a message travelling on a national or international network)



Routing of messages to a destination by MTP3 can either be *Quasi Associated*, where a message passes through an intermediate node before reaching its final destination or *Fully Associated*, in which case there is a direct signalling connection between the sender and recipient of a message. The intermediate nodes are known as *Signalling Transfer Points* (STP) which act as SS7 routers to provide multiple paths to a destination in order to handle failures within the network. The Classic SS7 architecture also defines two other types of nodes, a *Service Switching Point* (SSP) which is the point where the service user access the network (using an access protocol), and a *Service Control Point* (SCP) that contains network and data control functions (such as billing or free-phone number translation).

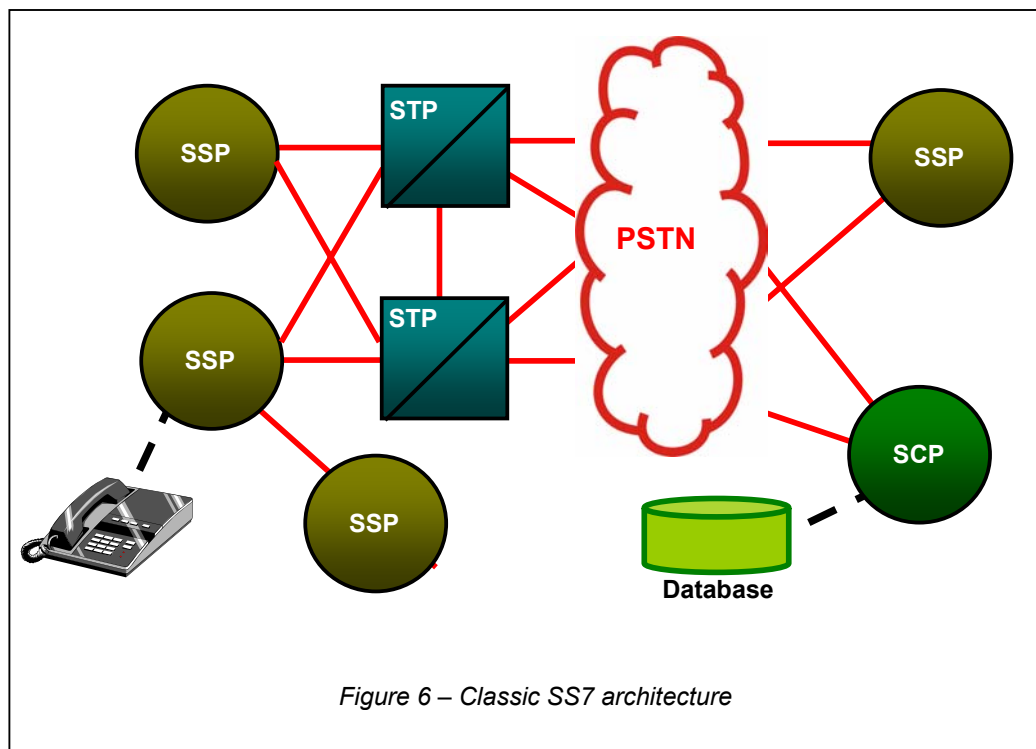
Types of SS7 Nodes

Service Switching Points (SSP), connecting subscribers' telephones and terminal equipment to the network. These nodes contain large switching matrices in order to switch the high volumes of traffic from the interconnected subscribers.

Signalling Transfer Points (STP) act as SS7 routers and give alternate paths to destinations when one possible route to a destination fails. A true STP does not have any layer 4 (User Part) protocol.

Signalling Control Points (SCP) provide database and data processing functions within the network, such as billing, maintenance, and subscriber control and number translation.

Figure 6 illustrates the three classic types of SS7 nodes



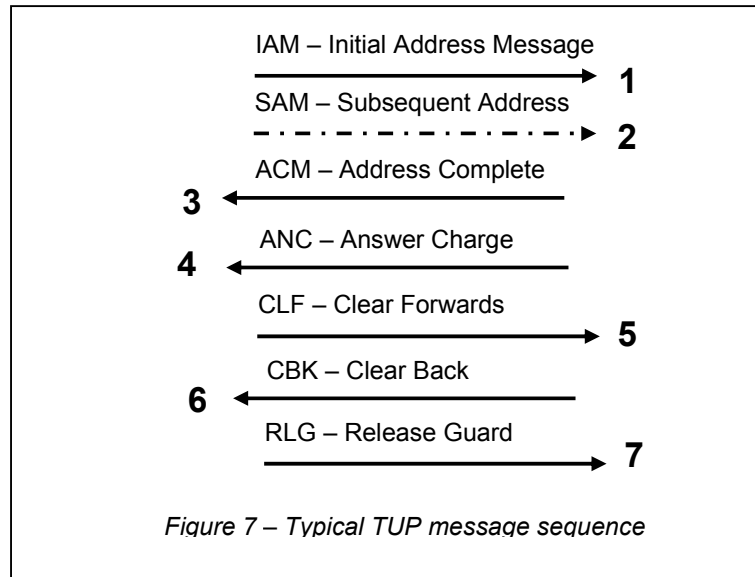
Layer 4 protocols

The layer 4 protocols define the contents of the messages sent to MTP3 and sequences of messages in order to control network resources, such as circuits and databases.

Telephony User Part (TUP)

Telephony User Part (TUP) provides conventional PSTN telephony services across the SS7 network. TUP was the first layer 4 protocol defined by the standards bodies and as such did not provision for ISDN services. Prior to the introduction of ISUP, national variants of TUP have evolved which provide varying degrees of support for ISDN.

For example the United Kingdom uses a variant of TUP variously known as NUP, BTUP, IUP, PNO-ISC CP001, France a national variant specified as SSUTR-2 and China a Chinese national variant. The majority of networks are slowly migrating to use the ISUP protocol described below. Figure 7 shows a typical TUP message sequence in setting up a circuit for a call.



- 1 Circuit selected for outbound call attempt, dialled digits collected from calling user analysed and a route for the call selected. The IAM contains information relating to the called subscribed and optionally the calling subscriber.
- 2 Optionally additional address digits can be sent following the IAM if the calling subscriber continues to enter destination digits.
- 3 The destination switch recognises the called party number and starts to alert the called party (by ringing the telephone). At this point, the speech path is made in the backward direction enabling the calling subscriber to listen to ring tone. The speech path may be completed in the forward direction at this point.
- 4 The called subscriber answers. The speech path is completed in the forward direction.
- 5 The calling subscriber hangs up.
- 6 The destination switch signals that all resources associated with the circuit used for this call have been released and may be re-used.
- 7 The originating switch signals that all outbound resources associated with the circuit used for this call have been released and may be re-used.

ISDN User Part (ISUP)

The ISDN User Part (ISUP) provides the services required by the Integrated Services Digital Network (ISDN). ISDN supports basic telephony in a manner similar to TUP, but with a greater variety of messages and parameters in order to implement ISDN type services within the network. Many telephony networks worldwide are migrating to ISUP.

The basic ISUP call message flow is similar to TUP, but is able to convey a larger amount of information between the subscribers during the establishment of the call.

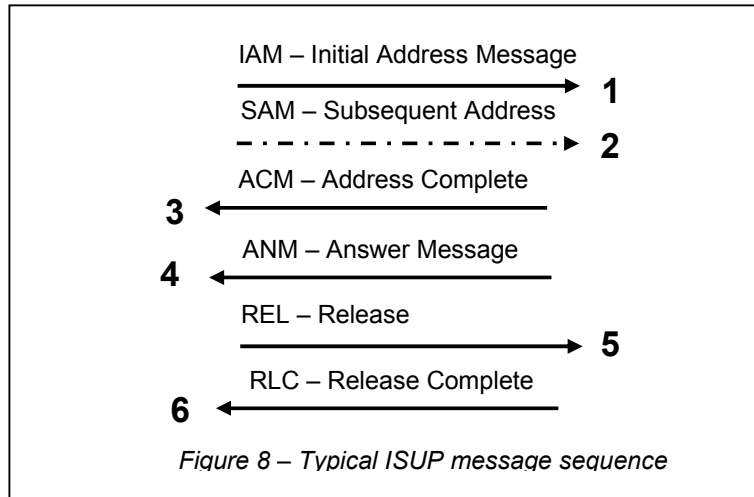
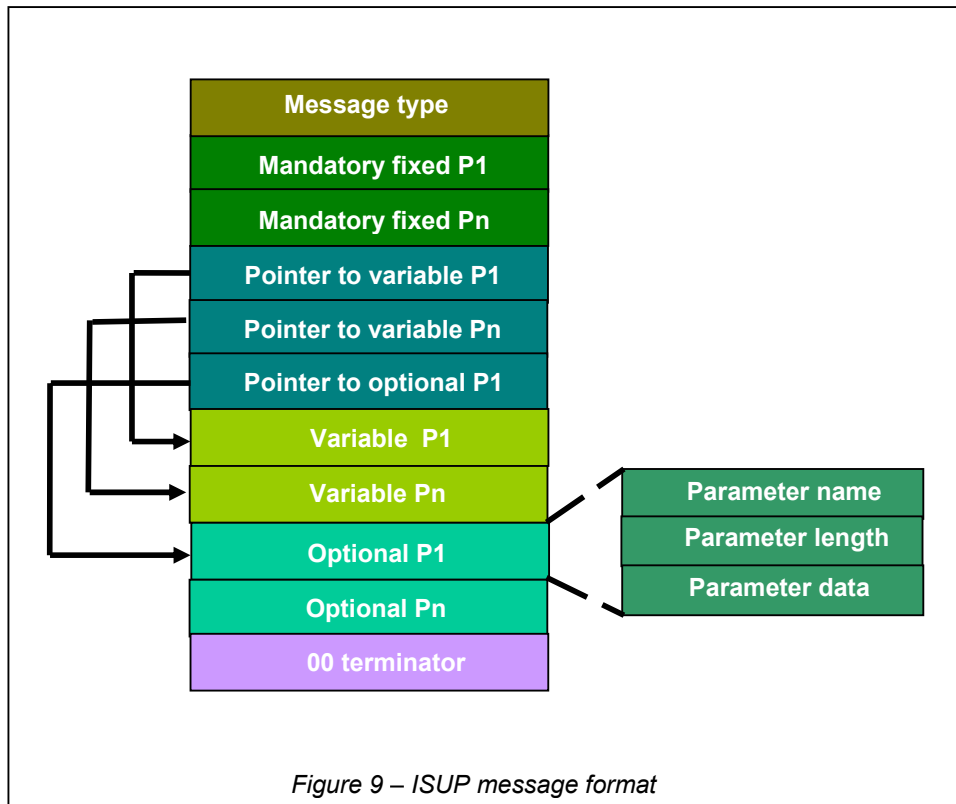


Figure 8 shows a typical ISUP message sequence, many other messages may be exchanged during a call in order to support a variety of subscriber services. Each ISUP message conveys parameter data associated with the call, such as the called address, calling party category. Every message is specified to contain mandatory fixed length parameters that will always be present, mandatory variable length parameters (such as the called party address digits) and optional parameters which can be used to convey additional information relating to a call, such as the identification of the calling party. Figure 9 presents the structure of an ISUP message, carried in the Signalling Information field of a MSU.



Both TUP and ISUP identify circuits using a *Circuit identification Code* (CIC), carried in every message. Each timeslot in a network is uniquely identified by its CIC code and the two point codes that terminate the circuit. CICs are generally assigned by starting at the first timeslot on the first trunk and incrementing by 1 for each additional channel. Hence, in a two E1 trunk system, the first trunk is generally CIC 1 to 15 and 17 to 31; the second is CIC 33 to 47 and 49 to 63. The CIC corresponding to timeslot 0 is missed since that channel is used to carry the E1 frame alignment signal. Timeslot 16 is missed out since that may carry SS7 signalling or is empty. In T1 networks, the situation is simpler since generally the SS7 signal is carried separately, no timeslots are missed. The first T1 trunk is numbered CIC 1 to 24, the second 25 to 48.

ISUP and TUP both provide additional messaging and management for circuit state control. It is possible to reset circuits (or rather reset the circuit state machine at both ends of a signalling relationship) by issuing a *single circuit reset* or *group reset* (for a range of circuits). Circuits are normally reset on system initialisation or following a failure. Similar procedures exist for *blocking* circuits, making a circuit temporarily unavailable for calls. Any call received for a blocked circuit is automatically rejected. Blocking may either wait for any active calls to terminate before taking effect, this is known as either *maintenance blocking* or *blocking without release* and is used prior to maintenance action (such as temporarily disconnecting a PCM trunk). *Hardware blocking* or *blocking with release* is used on detection of failure of physical equipment or trunks that disrupt a voice circuit, and causes instant release of associated circuits and calls.

Signalling Connection Control Part (SCCP)

The Signalling Connection Control Part (SCCP) enhances the routing and addressing capabilities of MTP to enable the addressing of individual processing components or *sub-systems* at each signalling point.

Basic SCCP addressing routes messages through the network using a sub-system number and point code to identify a destination. Each sub-system could be a number translation database; an SS7 point code can potentially have many sub-systems attached.

SCCP provides four classes of service, numbered 0 to 3, as shown below

Class	Properties
0	Connectionless, data is sent to a destination without negotiation of a session
1	Connectionless with sequence control. Messages are guaranteed to be delivered to a destination in sequence.
2	Connection oriented. A session (SCCP connection) is negotiated prior to the exchange of data.
3	Connection orientated with flow control.

SCCP maintains a state of every sub-system that it is aware of, sub-systems may be on-line (*Allowed*) or off-line (*Prohibited*). A message or connection session can only be delivered to an allowed destination sub-system.

The most commonly used class of SCCP is 0 and 1, used by TCAP and higher layers in the control of mobile/wireless and intelligent networks. Class 2 and 3 can be used by mobile networks in the communication between radio base-stations and the base-station controller.

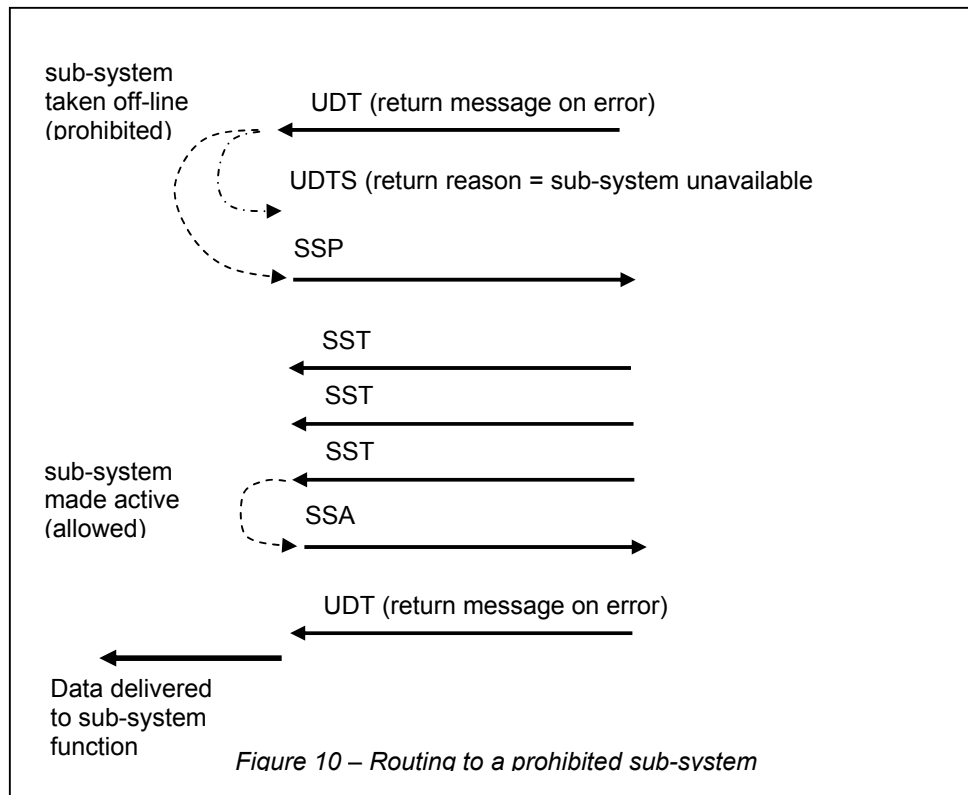
The basic message of connectionless SCCP is the SCCP UNITDATA (also called UDT). When SCCP detects that a destination for a message is prohibited, the UDT can either be discarded or returned to the originator as a UNITDATA SERVICE (UDTS) if a return option parameter is set in the quality of service field of the message.

In order to track and report the status of sub-systems, SCCP transmits management messages, encapsulated in UDT message, sent between the management entities of each SCCP. The table below lists the SCCP management messages.

Management message	Function
SSA	Sub-system allowed. Report that the affected sub-system has become available for message routing.
SSP	Sub-system prohibited. Report that the affected sub-system has been taken off-line and is no longer available for message routing.
SST	Check if the affected sub-system is available.
UOR	Check that a duplicate sub-system is prepared to take the traffic of an active sub-system wanting to go off-line.
UOG	Grant an off-line request to a duplicate sub-system.

SST messages are generated and sent periodically (approximately every 30 seconds) to all prohibited sub-systems in order to determine when routing to those destinations becomes available. SCCP also provides an option to make sub-systems *concerned* about the state of other sub-systems so that any change in routing status is reported immediately.

Figure 10 presents a typical SCCP connectionless message flow.



SCCP also provides an advanced addressing capability where a sub-system is represented as an array of digits known as a *Global Title*. A Global Title is a method of hiding the SS7 point code and sub-system number from the originator of a message, for example in inter-working between different networks where there is no common allocation of SS7 point codes. Such a method is used in GSM mobile roaming between countries.

Depending on network topology, Global Titles are translated either at a STP or at a gateway exchange where a network has an inter-working function with an adjacent network.

The addressing information delivered to SCCP for message routing may therefore contain a destination point code, a sub-system number and optionally a global title. For successful message transmission, the minimum requirement is for a destination point code in order for the message to leave the SCCP node. If none is present, the called address information is submitted for Global Title Translation that will hopefully produce as a minimum a destination point code and optionally sub-system number or new global title. The called address information in a received message contains a routing indicator to instruct SCCP to route on either point code and sub-system number or Global Title (if present). If set to route on Global Title, the called address is submitted for translation to produce a new destination address, which may be the local node or a different SCCP node in the network (which may itself translate the address information again).

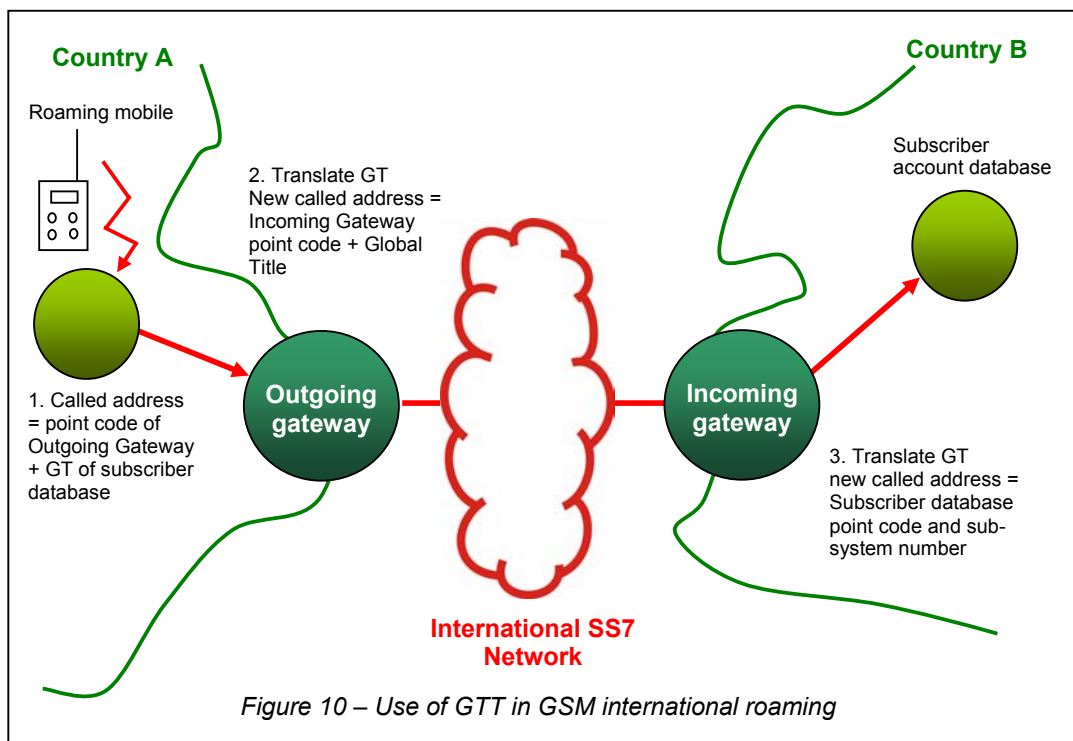
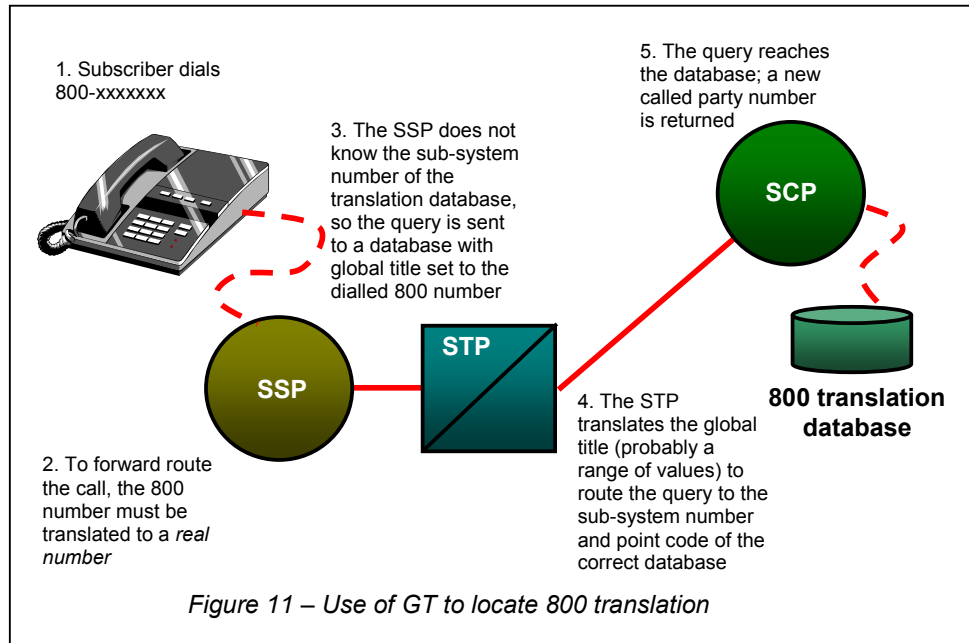


Figure 10 shows how Global Titles are used in GSM-mobile operation to locate subscriber account information (stored in a *Home Location Register* sub-system, HLR) from other networks as used for international roaming. The subscribers account information is held in a database in the home network, which has to be interrogated in order for the subscriber to obtain service from the visited network. The database query is sent through SCCP, with a called address Global Title constructed from information within the subscribers handset (generally either the Equipment Identity or Mobile Subscriber Number), this giving sufficient information to route the message to the correct outgoing gateway using global title translation. Subsequent translation within the home network routes the query to the correct database.

Global title translation can also be used to determine the location of a free-phone translation database (held at a SCP), by using the 800 number as a Global Title which is translated at an STP to give the database containing the entry for a range of 800 numbers. For example, 800-1xxxxx could match to database A and 800-2xxxxx could match to database B. This is illustrated in Figure 11.

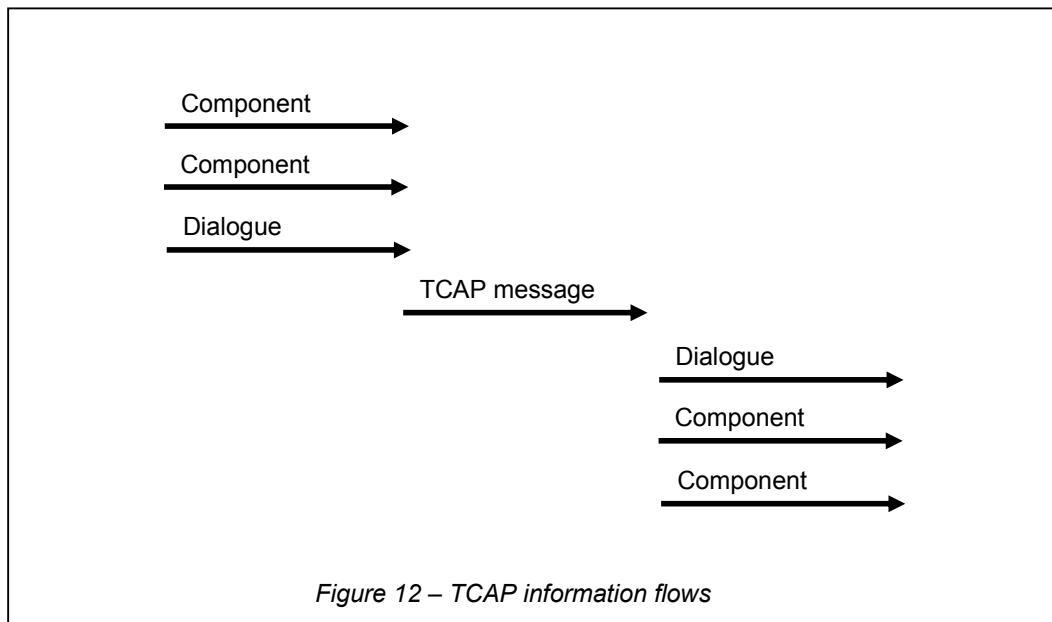


Transaction Capabilities (TCAP or TC)

The Transaction Capabilities Application Part provides a structured method to request processing of an operation at a remote node, defining the information flow to control the operation and the reporting of its result.

Operations and their results are carried out within a session known as a dialogue (at the 'top' of TCAP) or a transaction (at the 'bottom' of TCAP). Within a dialogue, many operations may be active, and at different stages of processing. The operations and their results are conveyed in information elements known as *components*. The operation of TCAP is to store component for transmission received from the higher layers until a dialogue handling information element is received, at which time all stored components are formatted into a single TCAP message and sent through SCCP to the peer TCAP.

In the receive direction, TCAP unpacks components from messages received from SCCP and delivers each as a separate information element to the upper protocol layer. Figure 12 shows a general TCAP information flow.



TCAP can control many active dialogues at any one time; each is assigned a unique transaction id to enable association of messages to each dialogue session. TCAP uses two transaction id values, one assigned at the originator of the message (the *Originating Transaction ID*) and one assigned at the destination of a message (the *Destination Transaction ID*). Within a dialogue, individual components are associated to a particular operation using an Invoke ID.

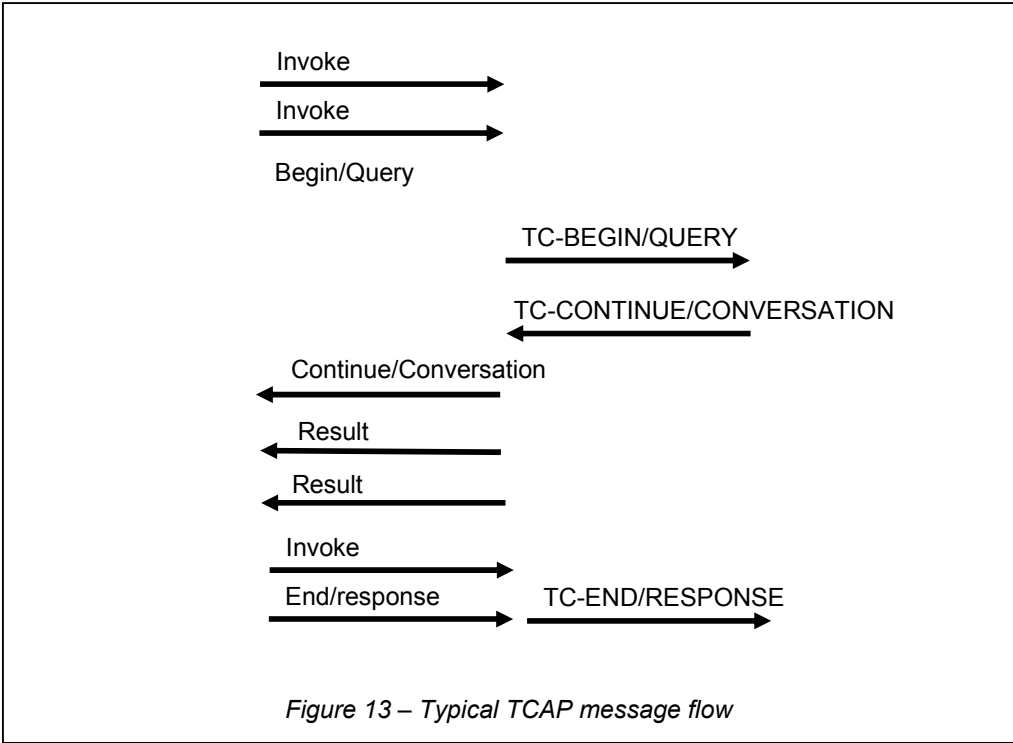
TCAP provides a set of dialogue handling information elements (or protocol primitives) to control the dialogue session as shown in the table below.

Information element	Function
Unidirectional	Request an operation with no dialogue session control
Begin/Query	Start a dialogue
Continue/Conversation	Continue a dialogue
End/Response	Terminate a dialogue
Abort	Abort a dialogue

The components that convey the operations and their results are listed below

Information element	Function
Invoke	Request an operation
Result (last/not last)	Report the outcome of an operation (may be segmented into several components)
Error	Report that an operation did not complete correctly
Reject	Reject an operation
Cancel	Cancel an operation

Figure 13 shows a typical TCAP message flow



TCAP uses Abstract Syntax Notation 1 (ASN.1) encoding rules to convey information within the components and parts of the TCAP message. ASN.1 specifies a parameter encoding method where each parameter is formatted with a context sensitive name octet, followed by a length indicator and finally the parameter data. Parameters formatted in this way can be combined to form compound parameters and sets.

Typical applications of TCAP are mobile services (e.g. registration of roamers), Intelligent Network services (e.g. free-phone and "calling card" services), and operations, administration and maintenance (OA&M) services.

Mobile Application Part (MAP)

The Mobile Application Part (MAP) is used within mobile/wireless networks to access roaming information, control terminal hand-over and provide short message services (SMS). It typically uses TCAP over SCCP and MTP as a transport mechanism. In Europe, networks use GSM-MAP, in North America ANSI 41 (formerly IS-41) MAP is used.

Mobile networks are database intensive; the point of subscription of a subscriber is a database known as a *Home Location Register (HLR)*. When a subscriber roams to a cell and registers with the network, information regarding the subscriber is temporarily stored at the visited equipment in a second database type known as Visitor Location register (VLR). MAP specifies a set of services and the information flows that implement these services to enable information to be transferred from these databases, in order to register, locate and deliver calls to a roaming subscriber.

Figure 14 shows a typical mobile network architecture.

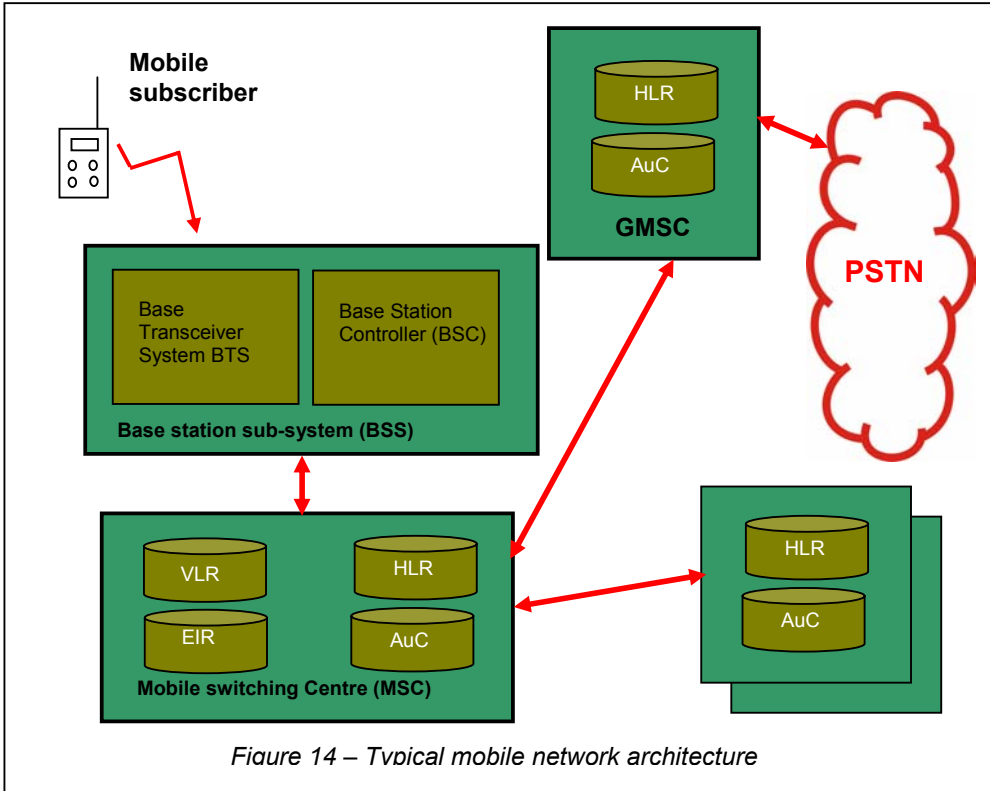
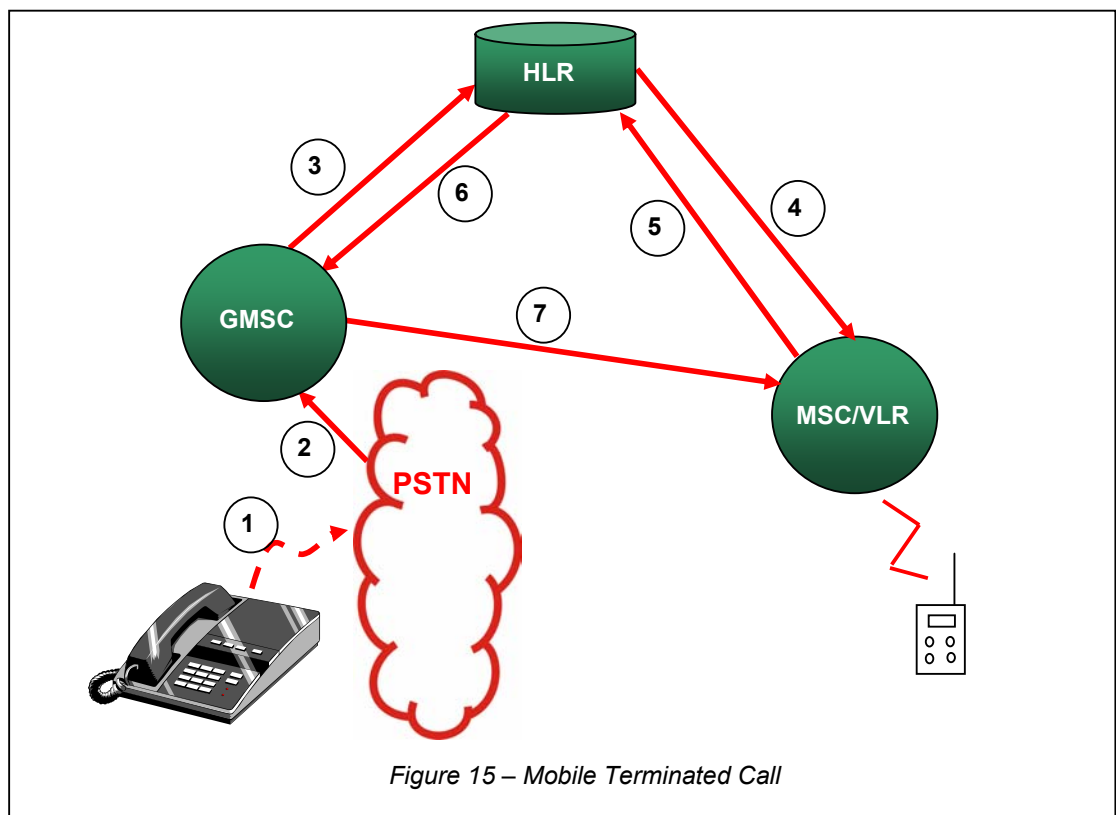


Figure 14 – Typical mobile network architecture

Key

- BSS Base-station sub-system. Includes BTS and BSC. Communicates with MSC using BSS-MAP (Over connection oriented SCCP)
- VLR Visitor Location Register. Stores information for mobile subscribers visiting cells managed by this MSC
- HLR Home Location register. Stores information for each subscriber, independent of location.
- GMSC Gateway MSC - inter-working between the mobile and fixed network or between different mobile networks
- AuC Authentication Centre
- EIR Equipment Identity Register (for identification of lost or stolen MS)

MAP provides the capability for all of the above elements to inter-work, each exchange of information taking place in a MAP service. Figure 15 shows how a mobile terminated call is routed.



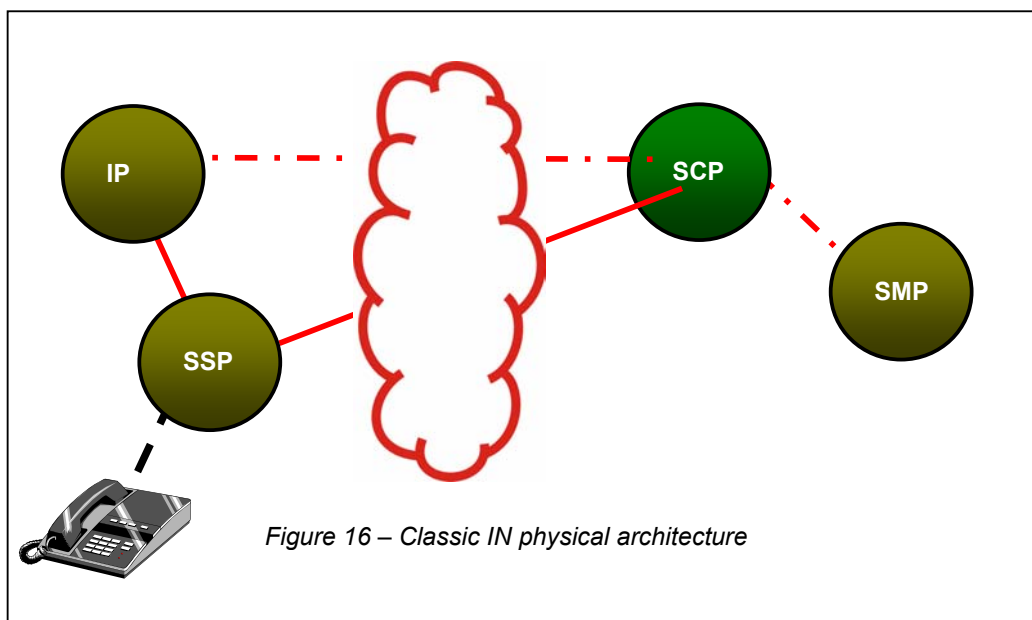
The stages of the mobile terminated call are controlled by the SS7-MAP protocol as follows:

- 1 The calling subscriber dials the mobile subscriber.
- 2 The mobile network prefix digits cause the call to be routed to the mobile network gateway MSC
- 3 The gateway MSC uses information in the called address digits to locate the mobile subscribers HLR
- 4 The HLR has already been informed of the location (VLR address) for the mobile subscriber and requests a temporary routing number to allow the call to be routed to the correct MSC.
- 5 The MSC/VLR responds with a temporary routing number that will be valid only for the duration of this call.
- 6 The routing number is returned to the GMSC
- 7 The call is made using standard ISUP (or similar) signalling between the GMSC and the visited MSC.

Intelligent Networking Application Part (INAP)

The intelligent network architecture extracts some of the intelligence traditionally embedded within the SSP, giving an open and defined interface to rapidly create services in a multi-vendor environment.

Figure 16 shows the classic IN physical architecture.



The SSP (Service Switching Point) is the point of subscription for the service user, and is responsible for detecting special conditions during call processing that cause a query for instructions to be issued to the SCP.

The SCP (service Control Point) validates and authenticates information from the service user (such as PIN information), processing requests from the SSP and issuing responses.

The IP (Intelligent Peripheral) provides additional voice resources to the SSP for playing back standard announcements and detecting DTMF tones when gathering information from the user.

The SMP (Service Management Point) provides the administration of the service.

In an IN system, the service user interacts with the SSP (by dialling the called party number). During the processing of the call, if certain pre-set conditions are met the SSP determines that this is an IN call and contacts the SCP to determine how the call should continue. The SCP can optionally obtain further caller information by instructing the IP to play back announcements and to detect tones (DTMF) from the user, for example to collect PIN information. The SCP instructs the SSP on how the call should continue, modifying call data as appropriate to any subscribed services.

The IN standards present a conceptual model of the Intelligent Network that model and abstract the IN functionality in four planes:

The *Service Plane* (SP) Uppermost, describes services from the users perspective. Hides details of implementation from the user

The *Global Functional Plane* (GFP) contains Service Independent Building Blocks (SIBs), reusable components to build services

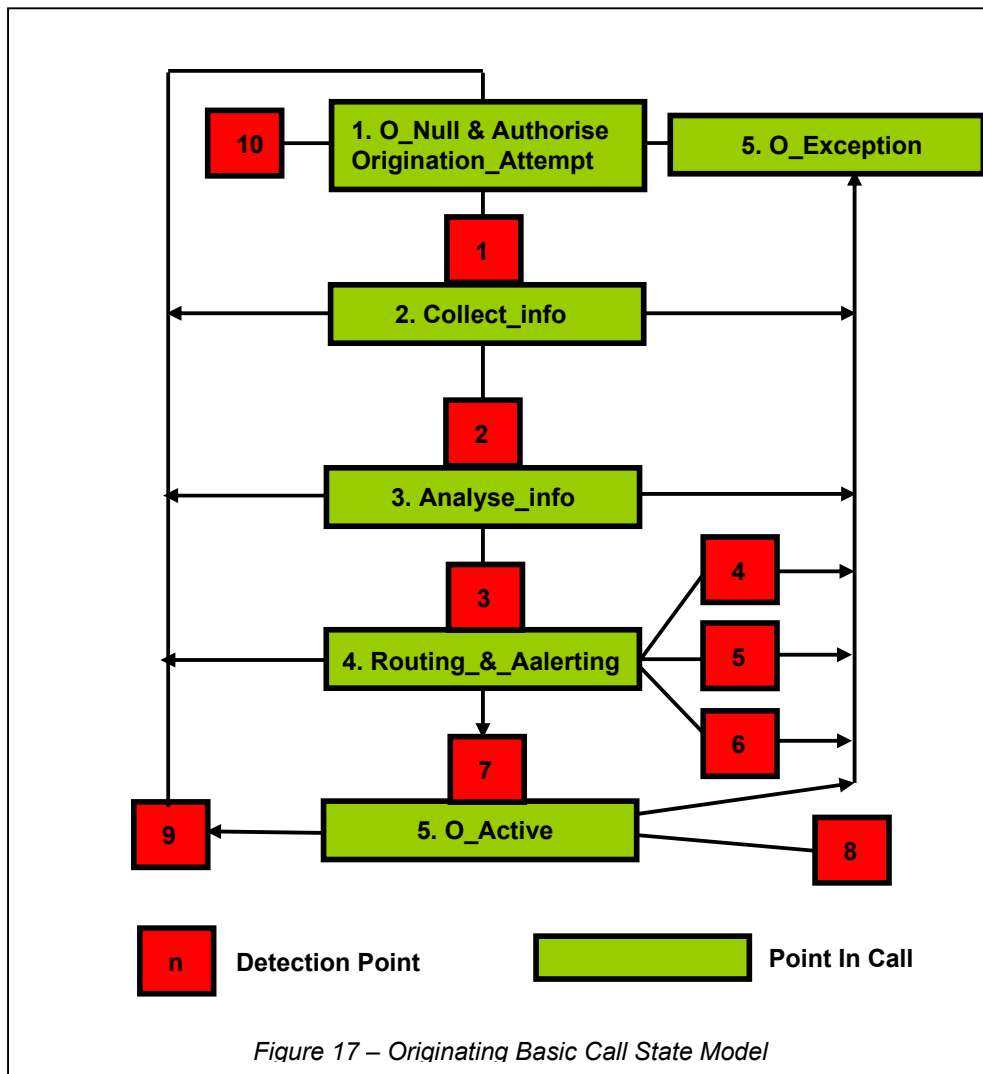
The *Distributed Functional Plane* (DFP) models the functionality in terms of units of network functionality, known as *Functional Entities* (FEs). The basis for IN execution in the DPF is the IN *Basic Call State Model*.

The *Physical Plane* (PP) Real view of the physical network.

The IN standards specify a vendor independent standard *Basic Call State Model* (BCSM) defining call processing states and events. Trigger Detection Points are pre-defined in both *the Originating Basic Call State Model* OBCSM and the *Termination Basic Call State Model* (TBCSM), with non-interruptible sequences of processing being termed Points-In-Call (PIC). Figure 17 shows the Originating Basic Call State Model.

A normal call becomes an 'IN call' if a special condition is recognised during the call handling; recognition of such a condition 'triggers' a query to an external control component (SCP). This recognition takes place at pre-defined *Detection Points* DP in the call handling, which may be armed (active) or not armed (inactive). DPs may be armed statically for a long period to implement a particular IN service, or armed dynamically to report particular events and errors. The detection points defined for the OBCSM are shown below

DP	Name	Function
1	Origination_attempt_authorized	Call setup is recognized and authorized
2	Collected_Information	Pre-defined number of dialed digits is collected
3	Analyzed_Information	Dialed digits are analyzed
4	Route_Select_Failure	Routing failed : no free channel, dialed number not available, network overload
5	O_Called_Party_Busy	Destination busy
6	O_NO_Answer	Caller does not answer in predefined time, Service Logic specifies the "no answer time" for SSP
7	O_Answer	Called subscriber answers: SSP receives e.g. an ANM
8	O_Mid_Call	Signal (hook flash, F-key) recognized during call
9	O_Disconnect	A or B side hangs up
10	O_Abandon	Call set-up discontinued by the A-side



A similar model exists for the terminating half of a call.

Once a detection point is reached and trigger criteria is met, depending on the service being invoked and the trigger point configuration, communication is established between the IN Functional Entities that need to exchange information in order to implement the service. Detection point processing may either suspend call processing and await further instructions or continue and simply issue a notification. The first information element conveyed in an IN session is normally an *InitialDP*, this conveys information relating to the service that is being invoked, the subscriber identity and any other data required in the processing of the service.

The Intelligent Network Application Part (INAP) provides a communication ability between the Functional Entities that exist in the Distributed Functional plane, transmitting operations peer-to-peer using the lower layer TCAP protocol in a similar way to the mobile phone protocols MAP and IS41. Each FE equates to a SCCP sub-system.

Figure 18 shows a possible implementation of a free-phone service using INAP, where the communication is shown between the *Service Switching Function*, SSF and the *Service Control Function*, SCF. The SSF normally resides within the SSP and the SCF within the SCP, although the IN standards do not enforce any particular physical location for each functional entity. The dialled free-phone number is sent to the SCF in an InitialDP for translation to a number suitable for routing through the network. This is sent back to the SSF in a Connect information element, with a request for notification of answer and disconnect, to enable the SCF to calculate the call duration for charging.

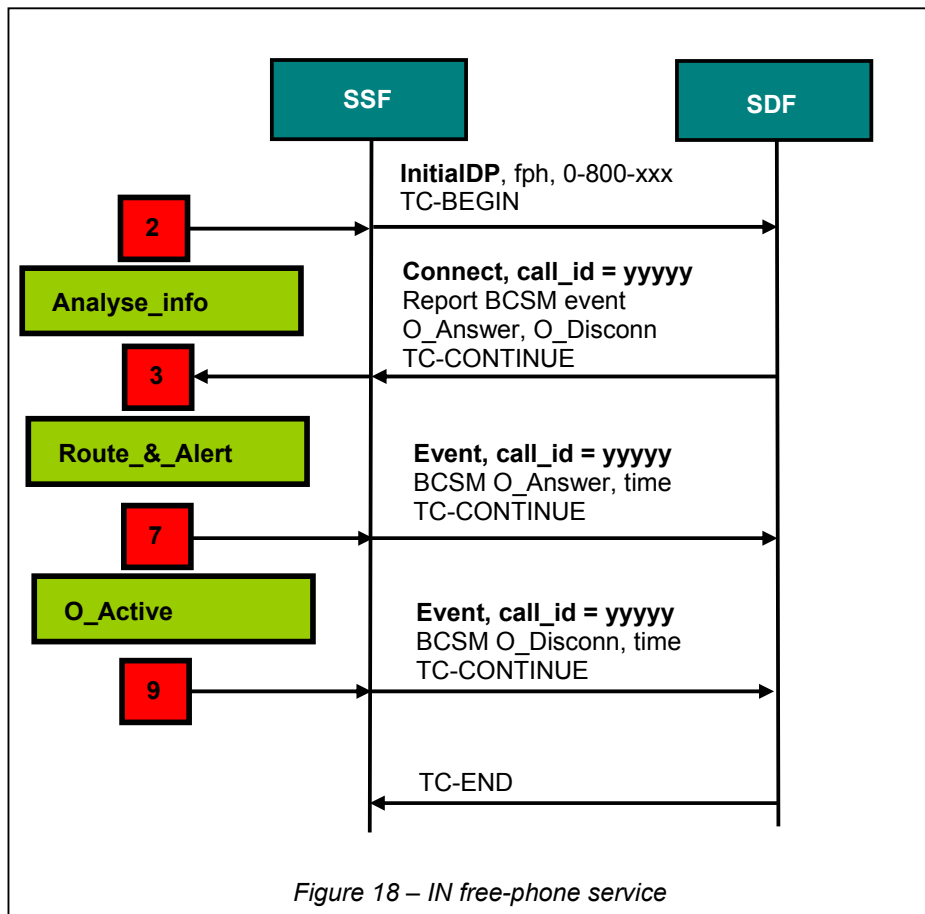


Figure 18 – IN free-phone service

The set of services and features that an IN system supports is referred to as a *Capability Set*. The current level of deployment of INAP is based around Capability Set 1 (CS1), which define single ended, single point of control services, where either the calling or called subscriber controls the INAP part of a call at any one time (but not both together). CS2, recently defined adds interaction between called and calling parties to enable far more complex services to be built.

Mobile/Wireless Intelligent Networking (CAMEL/WIN)

The functionality provided by the intelligent network is equally applicable to mobile/wireless networks, although the challenges of implementation are greater since this adds the complexity of mobility management to the task of implementing distributed IN services.

In Europe, extensions to the INAP protocol have provided capabilities known as CAMEL (Common Architecture for Enhanced Mobile Logic), in North America, this is being implemented by additions to the ANSI 41 protocol to provide WIN (Wireless IN) functionality.

SS7 Standards

SS7 is a global standard for telecommunications, able to support traditional telephony, mobile/wireless communication and advanced intelligent networking standards. There are two major geographic areas that set the SS7 standards, in Europe, the International Telecommunication Union ITU-T (formerly CCITT) specify SS7 operation with the Q.700 standards. ESTI also produce a similar set of pan-European standards published as ETS-xxx-xxx recommendations.

In North America, the American National Standards Institute (ANSI) publishes a similar set of ANSI T1.11x series SS7 standards; these also exist in a similar format in the Bellcore (Telcordia) Bellcore GR-246-CORE series standards. Although similar, the European and North American Standards do not provide inter-working.

Many countries adopt these standards for national use, or adapt them slightly for the needs of local operators. Hence there are a large number of national standards in existence, many refer directly to either the ITU-T or ANIS specifications and some re-iterate the text of these standards in a similar manner with some minor modifications. Major exceptions to this are the United Kingdom which uses a layer 4 protocol known as NUP (National User Part), France which uses a TUP based protocol known as SSUTR-2 and Japan which uses a standard that has features of both the European and American publications.

SS7 and IP Convergence

The proliferation of packet based protocols throughout the telephony industry has generated a need for the transmission of signalling information through an IP based. Much of the development work on methods to implement such information transport is still in its infancy, however, a number of standards are emerging, one of the more notable the work by the Internet Engineering Task Force, IETF, Sigtran group.

The IETF have specified a number of signalling transport protocols and inter-working layers that enable SS7 like information to be conveyed through IP networks. IP is a transport mechanism, whereas SS7 is a transport mechanism and network structure that provides user services, the IETF specifications provide a migration path that combines the structure of existing networks with the advantages of IP transport.

The SS7 protocols have a clearly defined transport protocol, the Message Transfer Part. The IETF Sigtran protocols effectively replace this with IP protocols and adaptation layers that present an interface to the existing SS7 upper layers (User Parts) that is identical to the existing MTP interface.

Initial IP implementations either relied on UDP (Unreliable Datagram Protocol) or TCP (transmission Control Protocol), both of which had shortfalls for use as a reliable telephony signalling transport. The IETF defined a new protocol, Simple Control Transmission Protocol, SCTP as the preferred alternative. Two layers may be run above SCTP in order to present an interface consistent with the SS7 standards, M2UA (MTP2 User Adaptation Layer) and M3UA (MTP3 User Adaptation Layer), which present a MTP2 and MTP3 interface respectively.

Figure 19 shows use of SCTP and M3UA in the construction of a SS7/IP *Signalling Gateway* SG. Such an architecture enables the SG to appear as a STP from both the SS7 and IP side, allowing individual nodes in the IP network to be addressed as individual point codes, or by ranges of circuit numbers, or SCCP global title.

