Introduction

GN Nettest's aim in publishing this series of technical notes is to provide clear and correct information on relevant technical subjects.

This technical note is the fourth issue. It has been rewritten to give the reader basic information that is hard to find in other documents. It also forms a part of the material used in the training programs offered by GN Nettest.

We also wish to inform the reader about GN Nettest's credentials as one of the world's leading manufacturers of advanced telecommunications test and measurement instruments – credentials that result from our commitment to an intensive research programme. This research programme strives to bring our customers new equipment that combines the latest technology with cost-effectiveness and ease of operation.

When an instrument in our range has relevance to the topic discussed, we have included a brief description of that instrument.

January 1999
Issue 4

GN Nettest A/S

Kirkebjerg Allé 90
DK-2605 Brøndby
Denmark
Tel: +45 72 11 22 00
Fax: +45 72 11 22 10
E-mail: com@nettest.dk
Web: www.gnnettest.dk

Contents

1. Signalling

In any network, the definition of signalling is the exchange of information. In a telecommunication network, signalling is the exchange of information that relates to the establishment and control of connections, including management.

Today most transmission between telephone exchanges is digital, but in some cases signalling operates on specifications developed for analogue exchanges. The exchanges in these networks use Channel Associated Signalling (CAS). The CAS restricts signalling to the PCM link in which the telephone connections take place.

This means that the number of connections that the CAS signalling controls is equal to the capacity of the PCM link (30 in 2 Mbit/s systems and 24 in 1.5 Mbit/s systems). The CAS signalling also monopolises one time slot (channel) for signalling purposes in 2 Mbit/s systems.

Signalling System No. 7 uses a different method. It uses the same communication techniques as modern data networks: Common Channel Signalling (CCS).

If the data-network approach is used, the signalling for a number of connections takes place in a single time slot (channel). The same time slot can also transfer other required signalling information needed for operation of the network.

A number of features differentiate CCS signalling from CAS signalling:

- Signalling and speech can be sent on separate PCM links. This gives network designers the possibility to design robust networks that can withstand the failure of one or more PCM links.
- It has built-in error detection in the signalling, thereby enabling error correction. The CAS, however, only has the option, if there are errors, of dropping the connection, leaving reestablishment to the user.
- It can carry signalling for a large number of connections (> 1000) in a single time slot, thereby freeing time slots for connections.
- Using data network techniques, it can carry other service information – for example requests for number information, either from an operator (information) or through computers in the network (800 numbers, GSM location-register lookups or updates).

Thus, the designers of Signalling System No. 7 have given different user groups their sets of messages, depending on the needs of these user groups. The architecture of Signalling System No. 7 makes it easy to implement new messages for a new user group without affecting existing user groups in the system.

The basis for this description of Signalling System No. 7 is the ITU-T Q-series Recommendation, Helsinki Q3/93 (White Book).

2. The Signalling Network

The signalling network consists of a number of nodes interconnected by signalling links, with each link consisting of two PCM links (one for each direction). A number of links that interconnect two nodes directly are called a signalling link set. The topography of the network is such that there are at least two signalling paths and a maximum of eight signalling paths between any nodes in the network. This ensures that the network can survive the loss of one signalling path without customers being seriously affected. It also ensures that the nodes can split the traffic between the available signalling paths and thereby reduce the damage if there is a failure. In this context, failures include loss of signalling processors located at the nodes as well as loss of the physical link set.

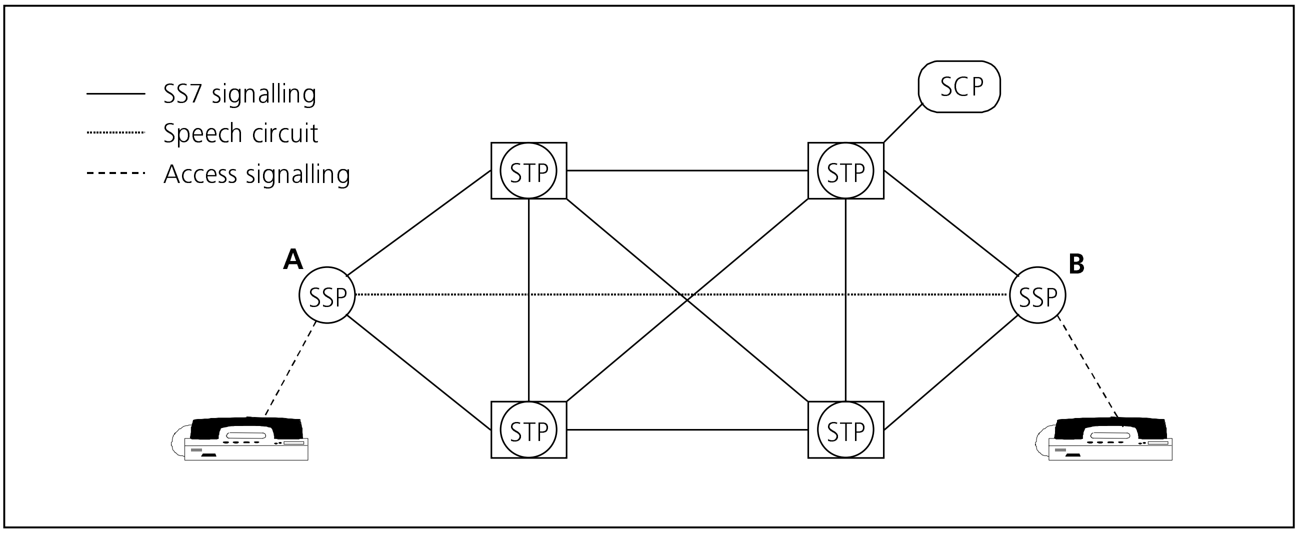


Fig. 2.1 ITU-T System No. 7 signalling network.

An **SSP** (Service Switching Point) is the node directly serving the subscribers – for example a telephone exchange for control of speech connections.

An **STP** (Signalling Transfer Point) is used for transfer of signalling messages between network nodes. An STP can be a stand-alone unit or include an SSP.

An **SCP** (Service Control Point) is used for control of intelligent network (IN) services.

An **SP** (Signalling Point) is the name of a network node (SSPs, STPs and SCPs are all SPs).

3. Signalling System No. 7 Levels

Signalling System No. 7 is not a large monolithic system. It is a layered system, in which each layer (level) contains a well-defined functionality, including the interface (functions and procedures).

Each level provides services to the level above and uses the services of the level below to obtain the functionality. This means that an entire level can be replaced without levels above or below having to be changed. More importantly, new functionality can be added to the topmost level, thereby implementing more functionality in the network.

This is the most important aspect of the Signalling System No. 7 levels, because the user can add new services to the network without affecting existing services, resulting in a dynamic network rather than a static one.

The four levels of Signalling System No. 7 are:

1. Signalling Data Link
The data link defines the characteristics (physical, electrical and functional) for the data transmission link. This data link transfers signals in both directions simultaneously.

2. Signalling Link
The signalling link defines the functions and procedures for transmitting information in one data link. The link level shares the task with the data link of ensuring reliable transmission between two signalling points.

3. Signalling Network
The signalling network level defines the functions for routing the signalling information in the signalling network, depending on the network's condition. The network level also defines functions for test and maintenance.

Levels 1-3 together are called the message transfer part (MTP).

4. User and Application Parts
The user level defines functions and procedures for different user parts. A user part can, for example, be the signalling set for telephone users.

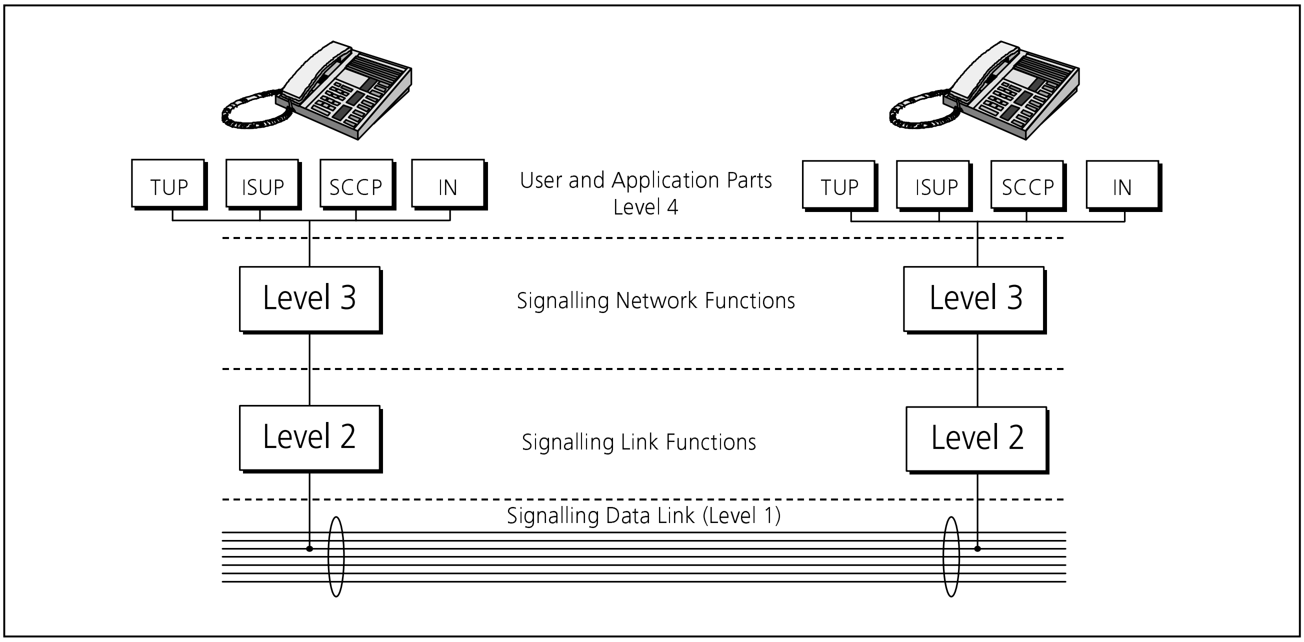

TUP
ISUP
SCCP
IN
User and Application Parts
Level 4
TUP
ISUP
SCCP
IN
Level 3
Signalling Network Functions
Level 3
Level 2
Signalling Link Functions
Level 2
Signalling Data Link (Level 1)

Fig. 3.1 Signalling System No. 7 levels.

3.1 OSI Reference Model

Signalling System No. 7 was developed before the creation of open-system architecture. The developers' aim was to define a signalling system, not a general-purpose communication system.

Signalling System No. 7 is a layered architecture. The layers are not in exact alignment with OSI.

Signalling System No. 7 defines a four-level architecture that corresponds with the four functional groupings. The signalling data link function provides the services expected of an OSI physical layer. The signalling link maps onto the OSI layer 2 data link. The signalling-network functions fall into the network layer of OSI. The MTP does not offer the complete OSI network service; it only provides a sequenced connectionless service to the user parts. Signalling System No. 7 combines the higher-layer OSI functions into a formless block called the user part.

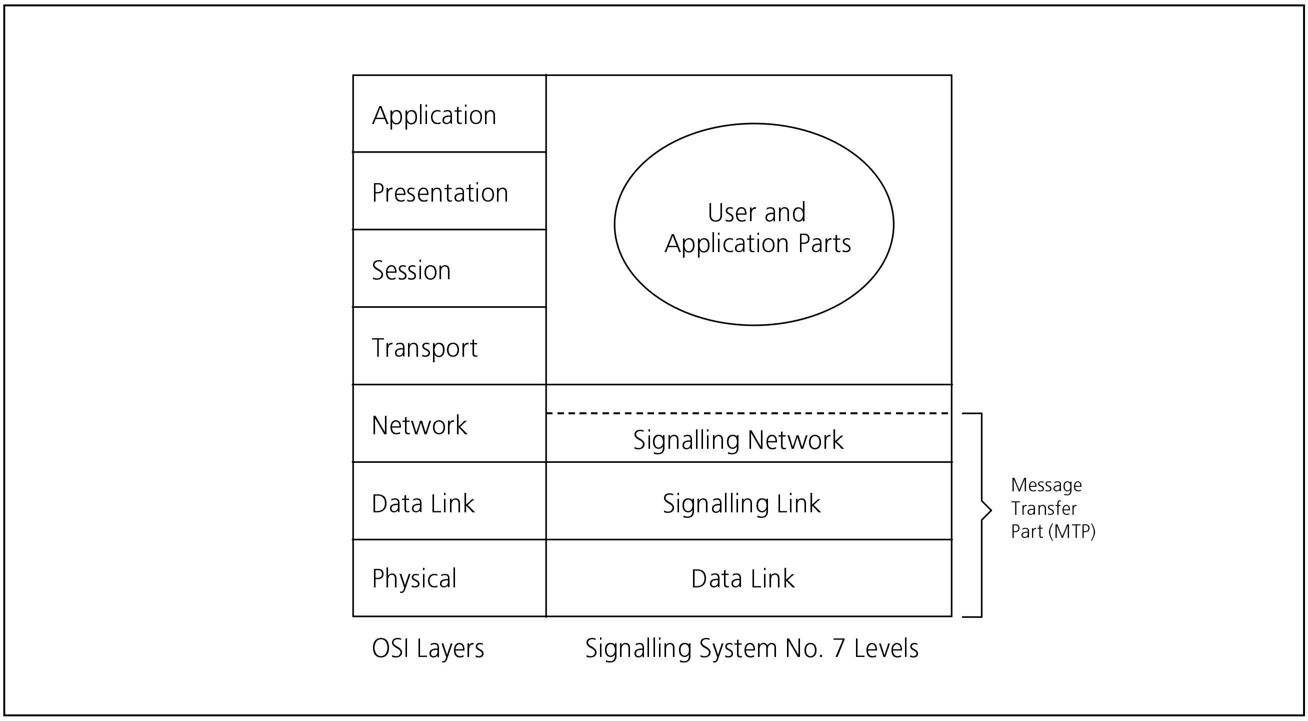


Fig. 3.2 Signalling System No. 7 and the ISO OSI model.

4. Signalling-data Link (Level 1)

In summary, level 1 has the means of sending a stream of bits of information from one point to another over a physical connection.

The requirements for the signalling-data link are defined in ITU-T Rec. Q.702. The standard signalling rate is 64 kbit/s, but many exceptions are permitted. Basically, any available channel can be used. A minimum of 4.8 kbit/s is specified for telephone signalling purposes.

Error-performance requirements are specified for the particular channel type. In general, the objective is a BER (Bit Error Rate) of less than 10^{-6}.

5. Signalling-link Functions (Level 2)

The signalling-link level provides a reliable transfer of signalling messages between two directly connected signalling points over one individual signalling data link. The link-level functions include:

- Delimiting of frames.
- Alignment of frames.
- Error detection.
- Error correction by retransmission.
- Initial alignment of data link.
- Error monitoring and reporting.
- Link-flow control.

These functions are usually modelled as a state-driven protocol machine. The activities of this machine are coordinated by the link-state control.

5.1 Basic Frame

The basic frame consists of an opening flag, information, checksum and a closing flag. In some implementations the closing flag is also the opening flag on the following frame. The flag is the bit sequence `01111110`. The transferred information in the frame is binary.

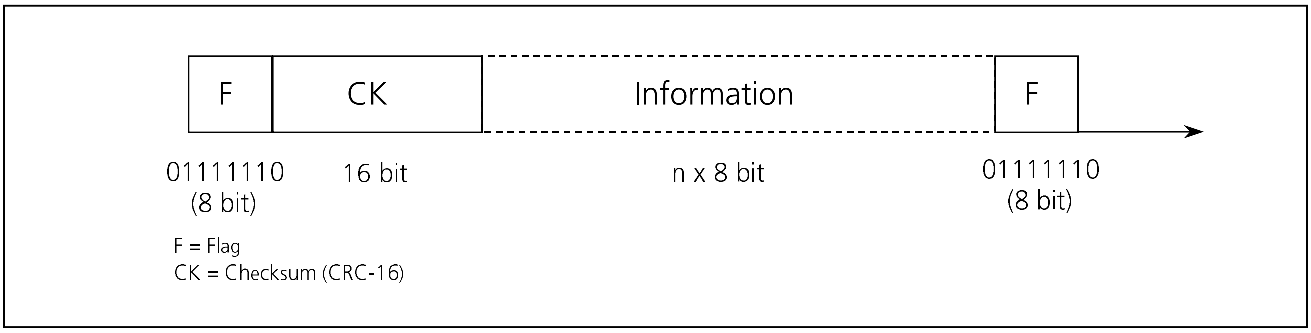


Fig. 5.1 Basic frame structure.

To prevent false flags in information and checksum, the transmitter performs bit stuffing on all bits between the flags: Whenever the transmitter has sent five one-bits, it will insert one zero-bit. The receiver will remove the zero-bit if it comes after five one-bits.

The 16-bit checksum is there to enable the receiver to detect changes in the frame during transmission. If that occurs, the receiver will disregard the frame.

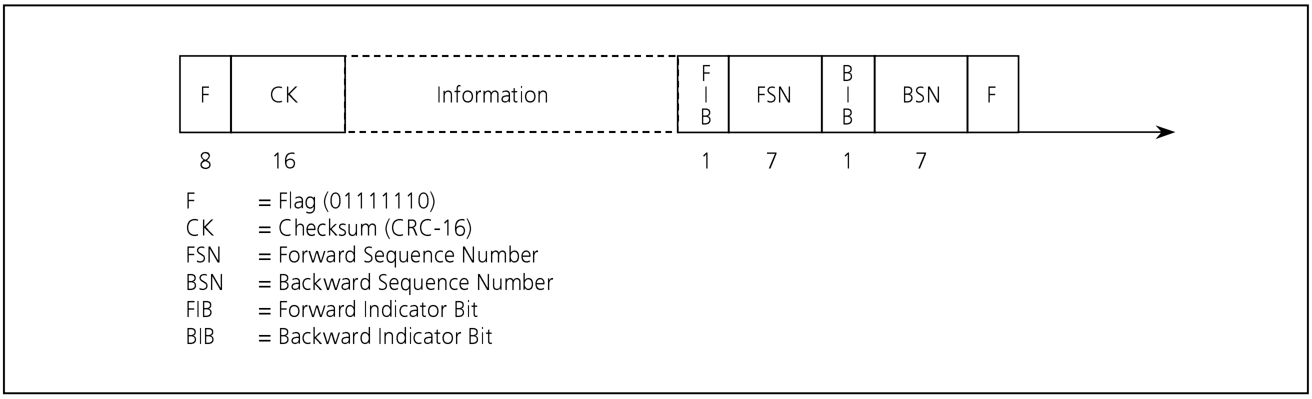
5.2 Message Types

Signalling System No. 7 transmits all frames (messages) as units. The system operates with the following three signal units (SUs):

1. Link Status Signal Unit (LSSU). The node uses the LSSU at link start-up or for handling severe errors on the link.
2. Message Signal Unit (MSU). The node uses the MSU for carrying signal information for user parts located at other nodes.
3. Fill-in Signal Unit (FISU).The node uses the FISU as an idle signal for error surveillance – for example when there is no information to transfer.

5.3 Error Correction

Error correction is only performed on MSUs. To enable the error correction between two nodes, four fields are present at the beginning of each frame: the backward sequence number (BSN), the backward indicator bit (BIB), the forward sequence number (FSN), and the forward indicator bit (FIB).



F = Flag (01111110)
CK = Checksum (CRC-16)
FSN = Forward Sequence Number
BSN = Backward Sequence Number
FIB = Forward Indicator Bit
BIB = Backward Indicator Bit

Fig. 5.2 Format of BSN, BIB, FSN and FIB.

The BSN and FSN contain a 7-bit value which is a number in the range 0-127. The transmitter side of the node increments the FSN for every MSU frame sent. When the transmitter increments the FSN beyond 127 it changes to 0. The transmitter uses the FSN as a label on every frame. The receiver in the opposite node uses the FSN to detect lost MSUs.

The receiver side of the node uses the BSN to acknowledge received MSUs. The node does this by setting the BSN equal to the FSN of the last correctly received MSU. Because of the size of the FSN and BSN, there is no need to acknowledge every MSU.

The transmitting side keeps copies of the MSUs that have been transmitted. These copies are kept until the receiving side has accepted them.

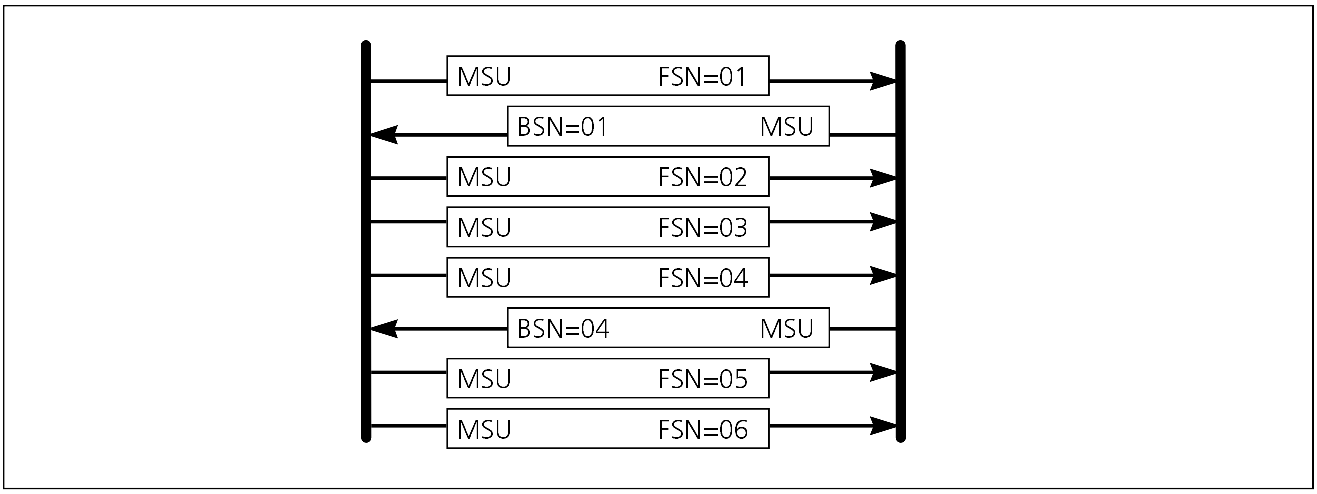


Fig. 5.3 Example of acknowledgement of correctly received MSUs.

When the receiver side detects a lost MSU, it inverts the BIB to request retransmission. The BSN assumes the value of the last accepted MSU.

Upon receipt of the request for retransmission, the receiver side retransmits the signalling messages, starting with the frame with an FSN value one higher than the received BSN, inverting the FIB to indicate the retransmission. When new frames are transmitted, no inversion of the FIB takes place.

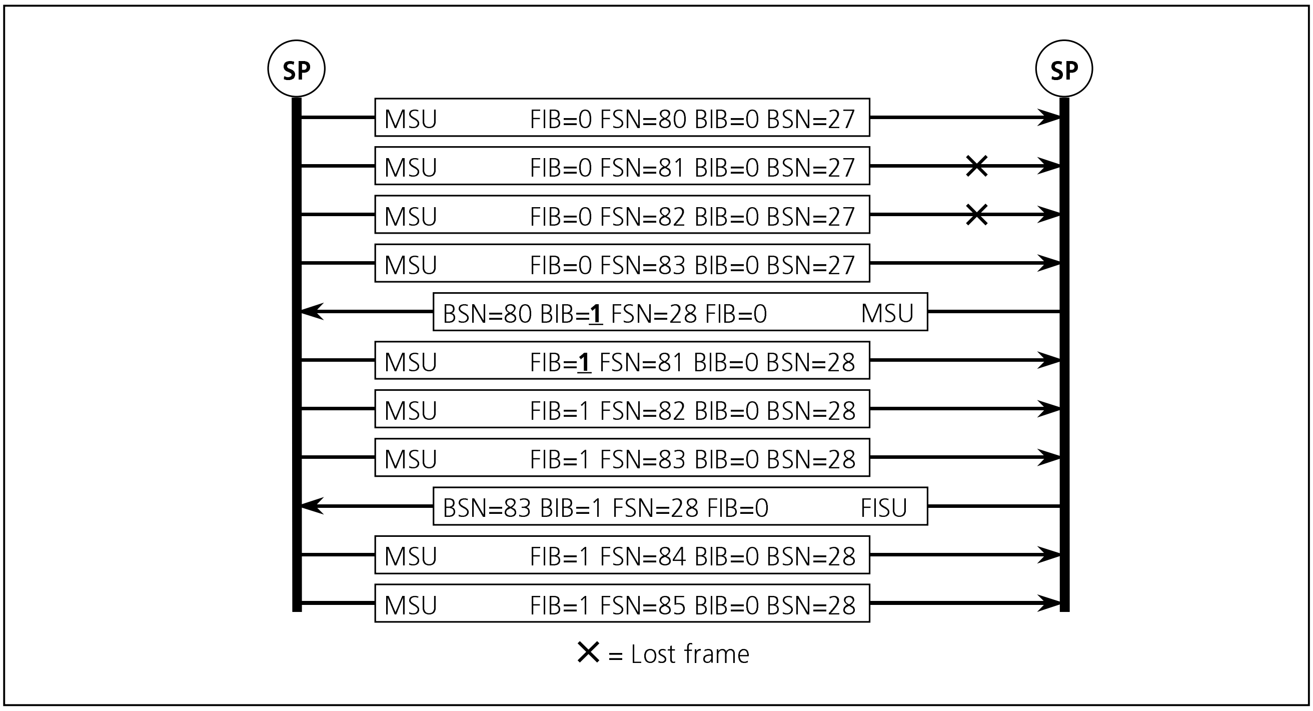

SP
SP
MSU FIB=0 FSN=80 BIB=0 BSN=27
MSU FIB=0 FSN=81 BIB=0 BSN=27
MSU FIB=0 FSN=82 BIB=0 BSN=27
MSU FIB=0 FSN=83 BIB=0 BSN=27
BSN=80 BIB=1 FSN=28 FIB=0 MSU
MSU FIB=1 FSN=81 BIB=0 BSN=28
MSU FIB=1 FSN=82 BIB=0 BSN=28
MSU FIB=1 FSN=83 BIB=0 BSN=28
BSN=83 BIB=1 FSN=28 FIB=0 FISU
MSU FIB=1 FSN=84 BIB=0 BSN=28
MSU FIB=1 FSN=85 BIB=0 BSN=28
✕ = Lost frame

Fig. 5.4 Example of request for retransmission due to lost MSU frames.

Fig. 5.4 shows a sequence of frames being sent. The receiver detects the error and requests retransmission by inverting the BIB. The transmitter transmits the frames that are not confirmed and informs the receiver by inverting the FIB. Finally, the receiver confirms the frames, and signalling continues normally.

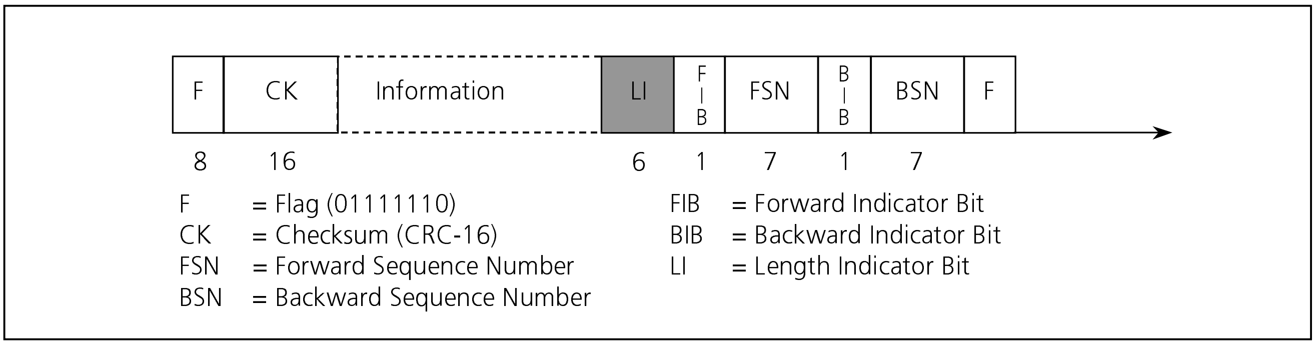
5.4 Preventive Cyclic Retransmission (PCR)

In systems that have long propagation delays – for example satellite systems – preventive cyclic retransmission of unacknowledged MSUs is used in order to reduce error-correction times:

1. If no new signal units are available for transmission, message-signal units which are available for retransmission are retransmitted cyclically.
2. If new signal units are available, the retransmission cycle (if any) must be interrupted and the signalling units transmitted with first priority.
3. Under normal conditions, when there are no message-signal units to be transmitted or cyclically retransmitted, fill-in signal units are sent continuously.

5.5 Length Indicator

The final mandatory information in the frame is the length indicator (LI). The LI contains information about how many bytes are contained in the information part of the frame and indicates the message type indirectly.



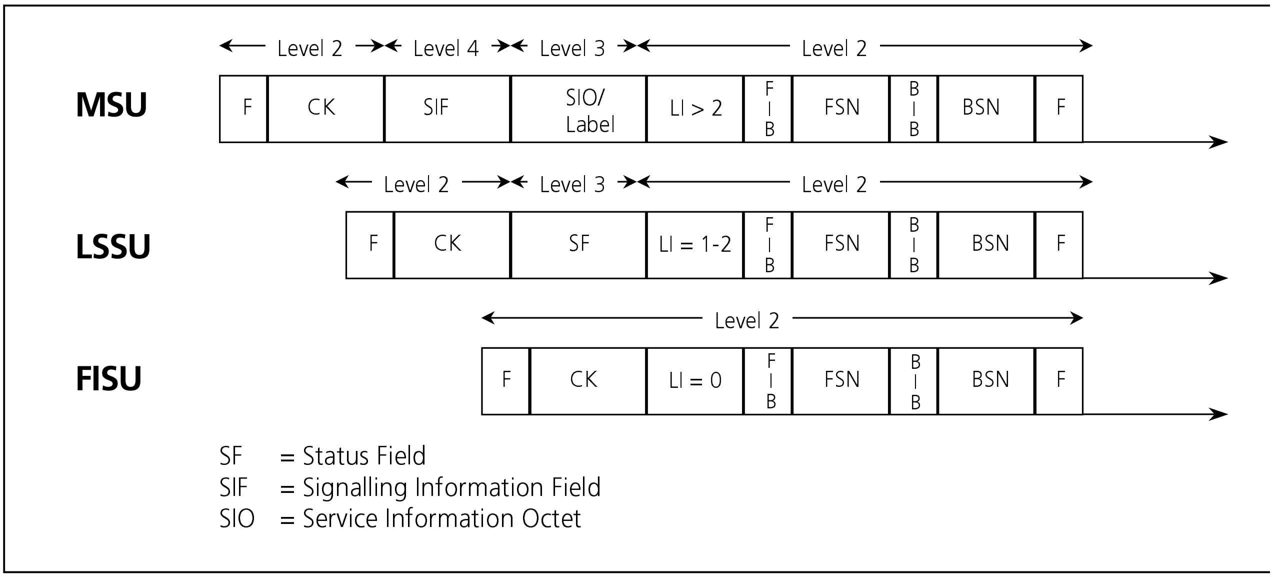
F = Flag (01111110)
CK = Checksum (CRC-16)
FSN = Forward Sequence Number
BSN = Backward Sequence Number
FIB = Forward Indicator Bit
BIB = Backward Indicator Bit
LI = Length Indicator Bit

Fig. 5.5 Format of length indicator.

The LI is a 6-bit field. Using 6 bits gives a number in the range 0-63, where:

- LI = 0 indicates a FISU.
- LI = 1 or 2 indicates an LSSU.
- LI > 2 indicates an MSU.

If the information is longer than 62 bytes, the LI has the value 63. Otherwise the LI contains the length of the information in the frame.



SF = Status Field
SIF = Signalling Information Field
SIO = Service Information Octet

Fig. 5.6 Format of signal-unit types.

5.6 Network Management (LSSU)

A vital component of the network management on the link level is the LSSU, which contains either a one-byte or two-byte information field. This field is used to indicate the sender's view of the actual status of the link. LSSUs have the highest priority of all signal units.

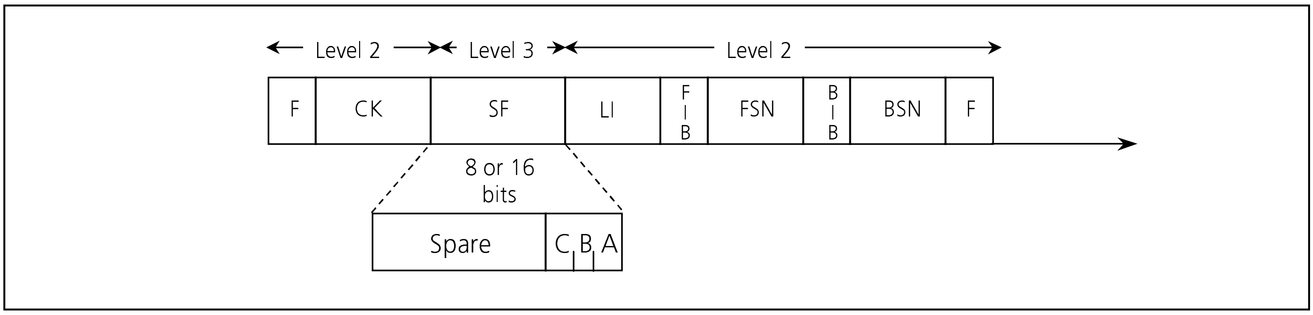


Fig. 5.7 Format of an LSSU.

Only the first three bits of the status field are used, with the remaining bits spare. The assigned values are:

Indication		C	B	A
Status "O"	– Out of alignment	0	0	0
Status "N"	– Normal alignment	0	0	1
Status "E"	– Emergency alignment	0	1	0
Status "OS"	– Out of service	0	1	1
Status "PO"	– Processor outage	1	0	0
Status "B"	– Busy	1	0	1

The OS status is sent when the link can neither transmit nor receive MSUs. The PO status is sent when the associated processor is out of service. Level 2 congestion is indicated by the B status.

5.6.1 Alignment

Link alignment is the process of synchronising the data link between two directly connected signalling points. It is applied initially at power-on time and during restoration following a link failure. Alignment is based on the compelled exchange of status information and a proving period to validate performance.

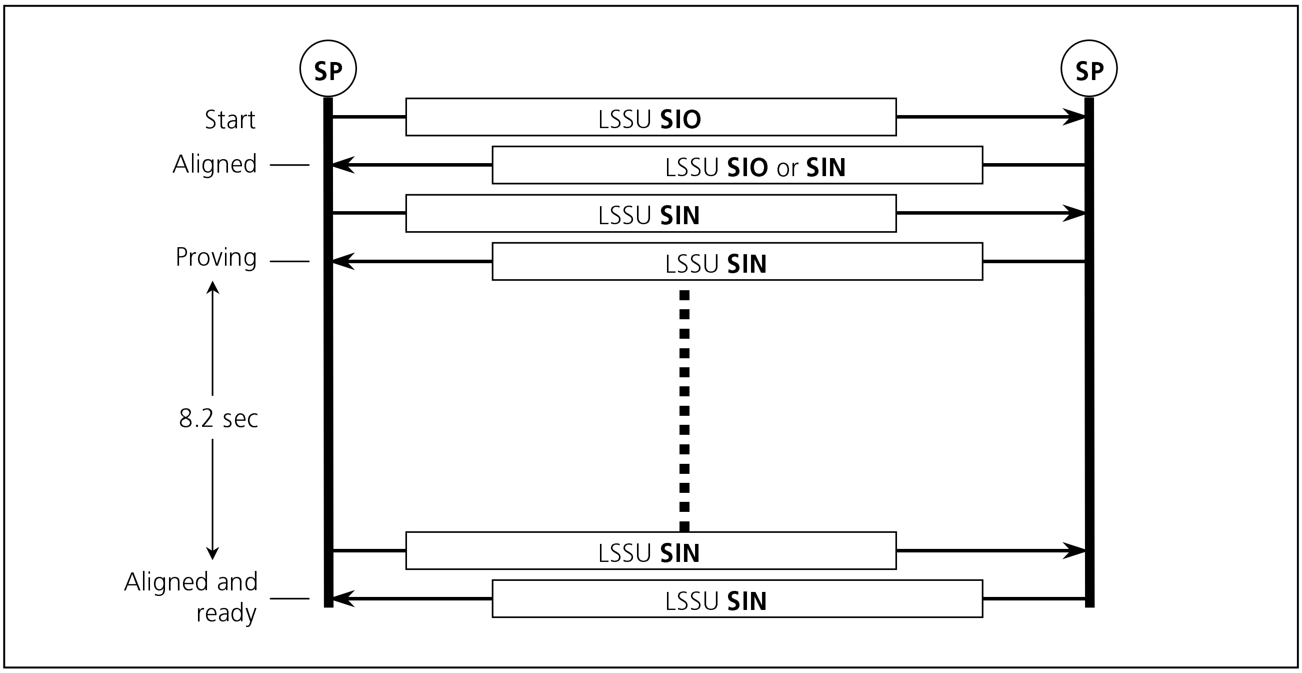


Fig. 5.8 Successful alignment of a link.

The normal, successful alignment procedure is illustrated in fig. 5.8. A signalling terminal begins by sending LSSUs carrying the **S**tatus **I**ndicator "O", which means out of alignment. This continues until the station receives an LSSU with either an "O" or an "N" (normal alignment) status. This indicates that the link is operational and that the station can achieve frame alignment. The two stations enter the proving phase where they repeatedly transfer LSSUs to each other while monitoring the error rate. The proving period is 2^{16} octet times for normal alignment and 2^{12} octet times for emergency alignment. This works out at 8.2 and 0.5 seconds at 64 kbit/s and 110 and 7 seconds at 4.8 kbit/s.

5.6.2 Error Monitoring (SUERM)

To support the objective of a reliable, responsive, and efficient data-link service, the Signalling System No. 7 link mechanism incorporates an error-monitoring function. A responsive error-monitoring system is obtained by using an up-down counter. Receipt of an erroneous signal unit causes the counter to step up by one count. Receipt of 256 error-free signal units causes the counter to step down by one count. If the counter reaches its maximum limit of 64, an alarm is triggered and the network level is notified.

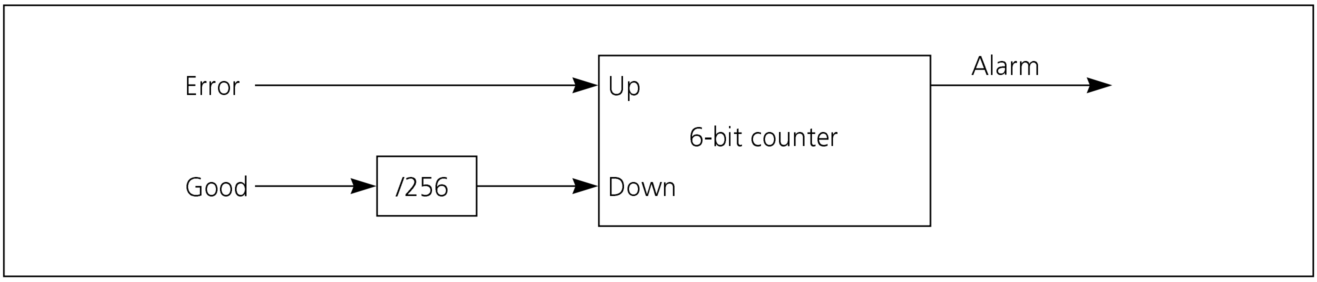


Fig. 5.9 SUERM counter.

This is also called a "leaky bucket" because each error event causes a large increase in the main counter that can slowly leak away as good blocks are received.

6. Signalling Network Level Functions (Level 3)

The third level of Signalling System No. 7 provides the functions and procedures for controlling the transfer of messages between the nodes of the signalling network. The signalling network levels build their routing and management functions on top of the underlying signalling link. Using these links, the network level ensures a reliable transfer of messages even when there is a link or node failure.

The level 3 functions are divided into two basic categories: signalling-message handling and signalling-network management.

Signalling-message handling ensures that messages originated by a user part at a signalling point are delivered to the corresponding user part at the specified destination. The message-handling function includes discrimination, distribution and routing.

Signalling-network management includes the functions necessary to reconfigure the network if there is a failure and to execute traffic-flow control when necessary. Network management includes traffic management, link management and route management.

6.1 Service Information Octet (SIO)

In message signal units (MSUs), the service information octet (SIO) is used to perform message distribution. This octet is divided into a four-bit service indicator (SI) and a four-bit subservice field. This subservice field is further divided into a two-bit network-indicator code and two bits that are spare if the indicator code is `00` or `01`, or are available for national use if the indicator code is `10` or `11`.

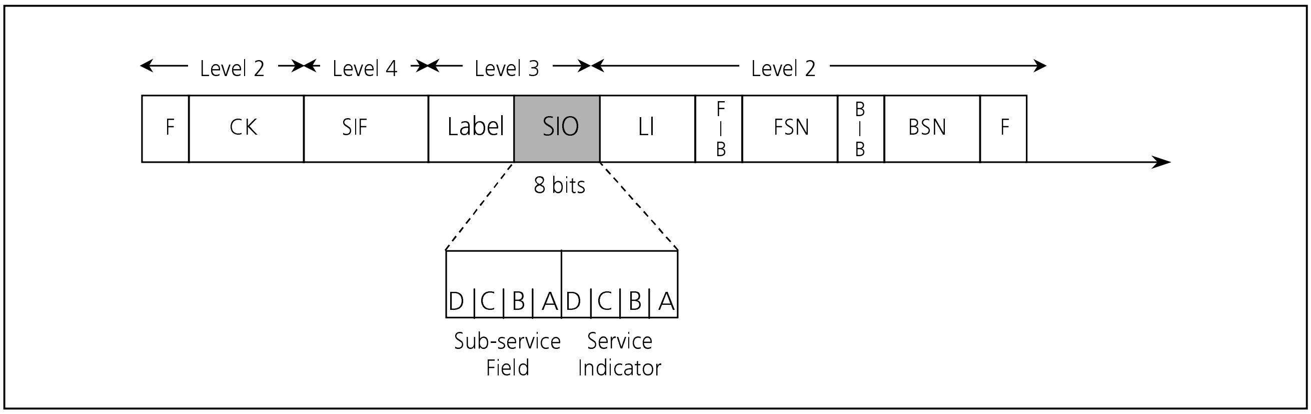


Fig. 6.1 SIO format.

Bit assignment for the **S**ervice **I**ndicator (SI) is:

Indication	D C B A	Hex
Signalling-network management messages (SNM)	0 0 0 0	0
Signalling-network testing and maintenance messages (SNT)	0 0 0 1	1
Spare	0 0 1 0	2
Signalling connection control part (SCCP)	0 0 1 1	3
Telephone user part (TUP)	0 1 0 0	4
ISDN user part (ISUP)	0 1 0 1	5
Data user part (call and circuit-related messages)	0 1 1 0	6
Data user part (facility registration and cancellation messages)	0 1 1 1	7
MTP testing user part	1 0 0 0	8
	1 0 0 1	9
Spare	to	
	1 1 1 1	F

The data user part is not implemented and the related ITU-T recommendations have been deleted.

Bit assignment for the sub-service field is:

Meaning	**D C B A**
International network	0 0 X X
Spare	0 1 X X
National network	1 0 X X
Reserved for national use	1 1 X X

The network indicator (bits D, C) provides for discrimination between international and national messages. They can also be used for discrimination, for example, between functionality in two national signalling networks with differing routing-label structures.

6.2 Routing Label

The "label" contains the routing information for delivery of MSUs from source to destination. It is used by both user messages and network-management messages. One of four different label types can be used, depending on the user part.

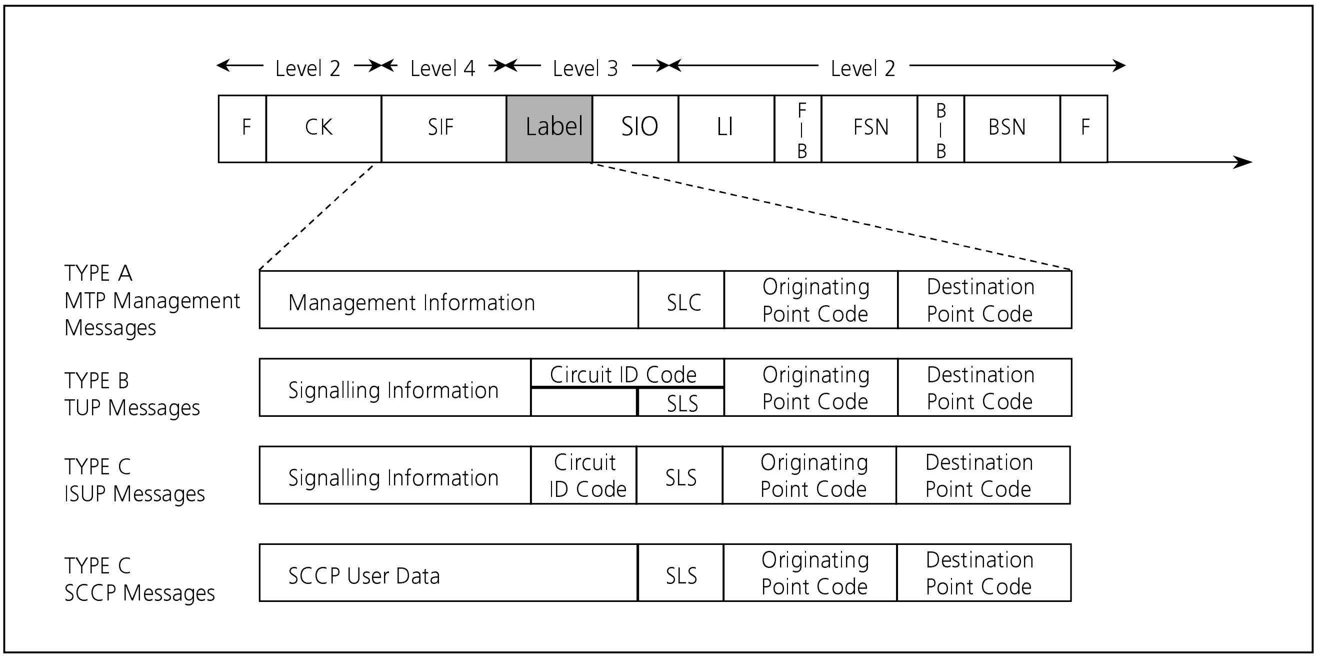


Fig. 6.2 Label types.

The destination point code (DPC) indicates the signalling point for which the message is intended. The originating point code (OPC) indicates the signalling point that is the source of the message.

For call-related or circuit-related messages, the circuit identification code (CIC) indicates the call or circuit to which the message is related. The four most significant bits of the CIC field are used to indicate the signal link selection (SLS). SLS indicates the signal link to be used if more than one link is used for signalling (load sharing).

For message transfer part management information, the signalling link code (SLC) is used to indicate the signalling route.

6.3 Heading Code

The heading code appears after the label in the signalling-information field. This "message header" is a single octet field that identifies the message group and then the message type within the group.

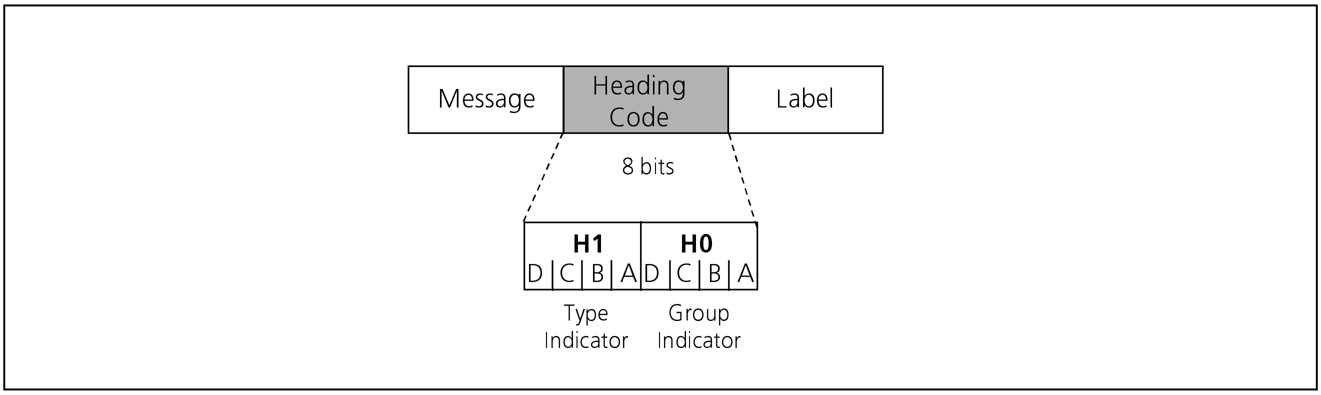


Fig. 6.3 Heading-code format.

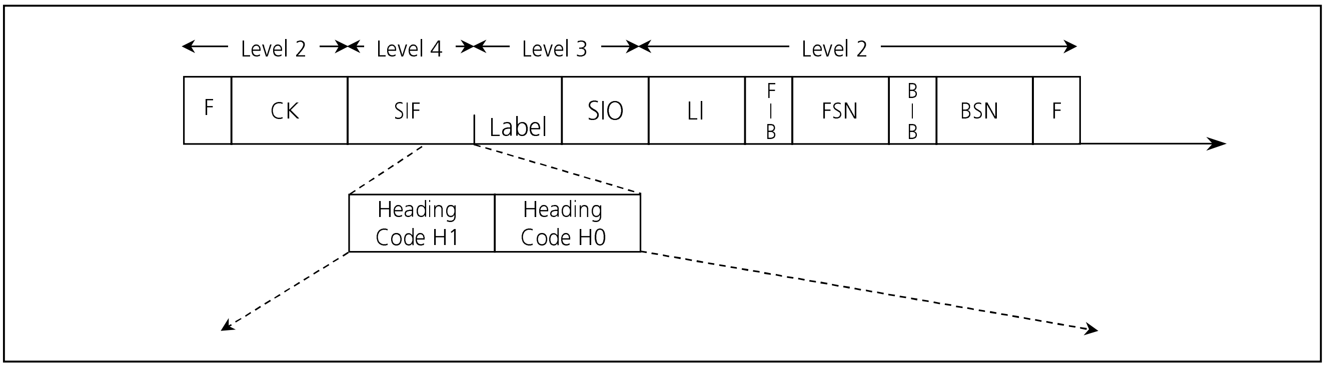
Groups and types are unique only within the message category. It is therefore necessary to process this field in conjunction with the SI field in order to determine the signalling-message format. For example, if the SI indicates a network-management message (SI code `0000`), the group indicator `0001` indicates a changeover message and the type indicator `0010` indicates a changeover acknowledgement signal.

6.4 Network Management (SNM)

Network management on the MTP level contains procedures for handling changeover and rerouting of messages.

A changeover from one link set to another is initiated when a signalling link is recognised as unavailable. This may be due to an excessive signal unit-error rate or other errors on the line. The limit of the error rate is decided by the SUERM counter (see the section "Error Monitoring (SUERM)"). The message group, signalling network management (SI = 0000), is used to transmit changeover messages.

The first field in a message indicates the message type with the heading codes H0 and H1. Fig. 6.4 shows the heading codes for signalling-network management messages.



Abbr.	Message	H1	H0
COO	Changeover order signal	1	1
COA	Changeover acknowledgement signal	2	
CBD	Changeback declaration signal	5	
CBA	Changeback acknowledgement signal	6	
ECO	Emergency changeover order signal	1	2
ECA	Emergency changeover acknowledgement signal	2	
TFP	Transfer prohibited signal	1	3
TFR	Transfer restricted signal	3	
TFA	Transfer allowed signal	5	
RST	Signalling route set test signal for prohibited destination	1	5
RSR	Signalling route set test signal for restricted destination	2	
LIN	Link inhibited signal	1	6
LUN	Link uninhibited signal	2	
LIA	Link inhibited acknowledgement signal	3	
LUA	Link uninhibited acknowledgement signal	4	
LID	Link inhibited denied signal	5	
LFU	Link forced uninhibited signal	6	
LLT	Link local inhibit test signal	7	
LRT	Link remote inhibit test signal	8	
TRA	Transfer restart allow signal	1	7
DLS	Signalling data link connector order signal	1	8
CSS	Connection successful signal	2	
CNS	Connection not successful signal	3	
CNP	Connection not possible signal	4	
UPU	User part unavailable	1	A

Fig. 6.4 Heading codes for signalling-network management messages.

The changeover procedure must ensure that signalling traffic carried by the unavailable signalling link is diverted to the alternative link as quickly as possible while avoiding message loss, duplication or mis-sequencing.

If a failure is detected, an MSU containing a changeover message will be transmitted on the alternative link.

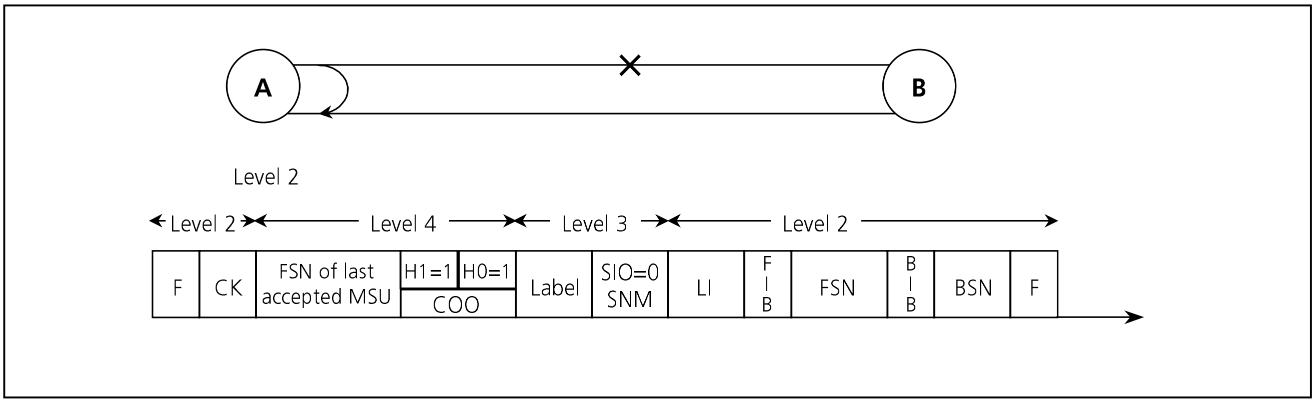


Fig. 6.5 Example of changeover and an MSU containing the changeover message.

When the changeover message in fig. 6.5 has been answered by a changeover acknowledgement, the messages in the retransmission buffer for the unavailable link are transferred to the alternative link and transmitted. When the link is in order, the signalling is transferred back to the original link set.

If the link set CB (in fig. 6.6) is unavailable, a forced rerouting has to be done by using the signalling transfer point D. In this case, messages may be lost because terminal A does not know what has been lost in link set CB (link-by-link signalling). When the signalling has been transferred to the alternative link set, a "transfer prohibited" message will be transmitted from terminal C to terminal A, and terminal A will start transmitting the link-status signal "out-of-service". When the link set is available again, a controlled rerouting back to the original link set will occur.

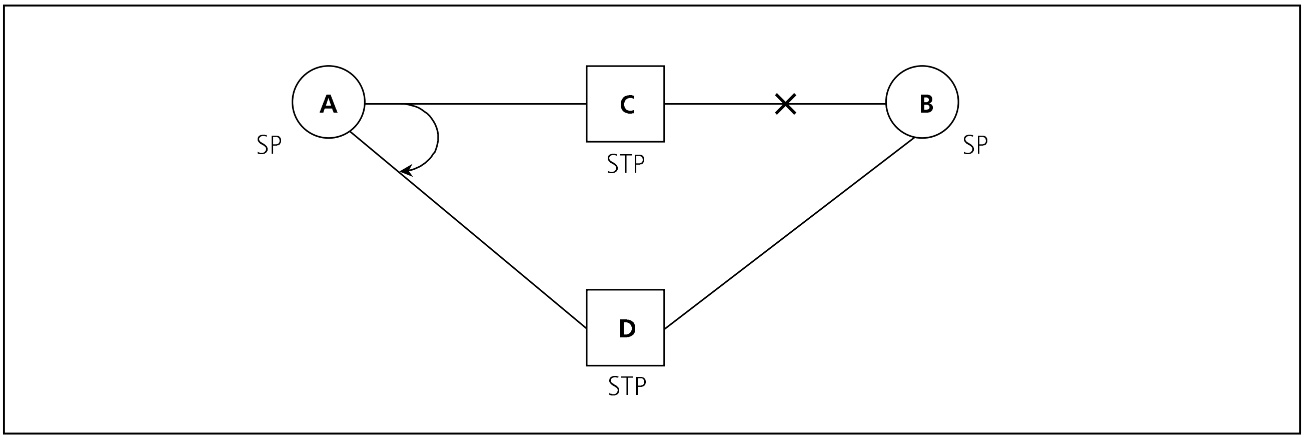
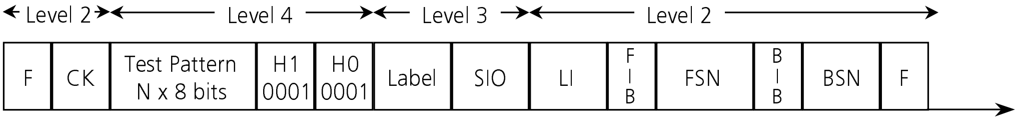


Fig. 6.6 Forced rerouting.

A failure in the signalling terminal may make it impossible for the corresponding end of the faulty signalling link to determine the forward-sequence number of the last accepted message. If this occurs, the emergency-changeover procedure is used. The procedure is the same as for normal changeover, except that the sequence number for the last accepted MSU is not in the emergency-changeover message and the transmission starts on the alternative link set without retransmission.

6.5 Network Testing (SNT)

In order to test the network, a signalling link-test message is specified. The user part for network testing is identified by `0001(1)` in the service indicator part of the service information octet. The test message has the structure shown in fig. 6.7.



F	CK	Test Pattern N x 8 bits	H1 0001	H0 0001	Label	SIO	LI	F I B	FSN	B I B	BSN	F

Fig. 6.7 Format of signalling-link test message.

7. User and Application Parts (Level 4)

7.1 Telephone User Part (TUP)

ITU-T has specified the international telephone user part but most countries have their own national versions. The messages are almost the same in the different versions but some messages may not be implemented, in particular national versions. The parameter fields in the messages are coded differently in the various versions and will therefore not be described here. The messages and their formats and codes described here are based on ITU-T Recommendation Q.723.

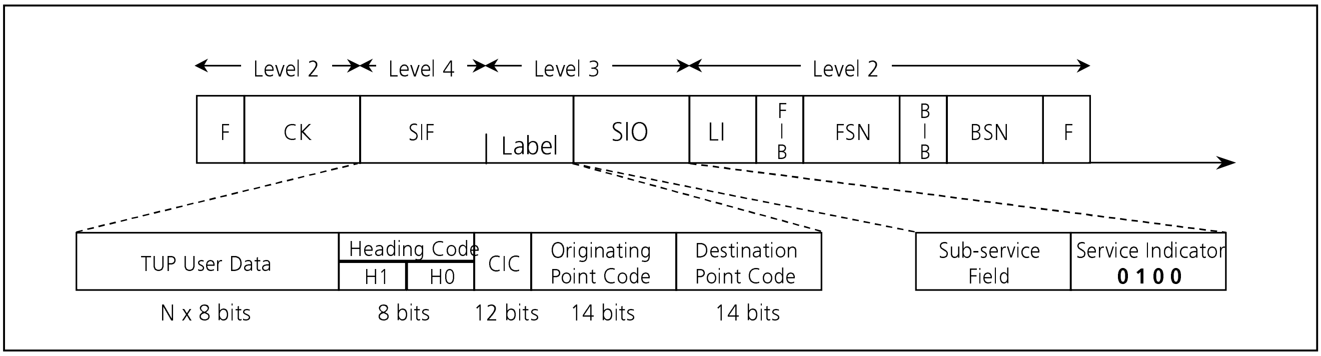


Fig. 7.1 Basic format of MSU containing a TUP message.

The service information octet (SIO) indicates that the message belongs to a telephone user part with the bit pattern `0100` (4 Hex) in the service indicator.

The label contains destination point code, originating point code and circuit identification code.

For 2 Mbit/s systems the circuit identification code is coded as follows:

The five least significant bits are a binary representation of the actual time slot assigned to the speech circuit. The remaining bits are used, where necessary, to identify one among several systems interconnecting an originating point and a destination point.

The label is followed by the heading codes H0 and H1. H0 indicates to which message group the message belongs, and H1 indicates the name of the message inside the group.

Message		**H1**	**H0**
Forward Address Messages			1
IAM	Initial address message	1	
IAI	Initial address message with additional information	2	
SAM	Subsequent address message	3	
SAO	Subsequent address message with one signal	4	
Forward Setup Messages			2
GSM	General forward setup information message	1	
COT	Continuity signal	3	
CCF	Continuity failure signal	4	
Backward Setup Request Messages			3
GRQ	General request message	1	
Successful Backward Setup Messages			4
ACM	Address complete message	1	
CHG	Charging message	2	

Message	H1	H0
Unsuccessful Backward Setup Messages		5
SEC Switching equipment congestion signal	1	
CGC Circuit group congestion signal	2	
NNC National network congestion signal	3	
ADI Address incomplete signal	4	
CFL Call failure signal	5	
SSB Subscriber busy signal	6	
UNN Unallocated number signal	7	
LOS Line out of service signal	8	
SST Send special information tone signal	9	
ACB Access barred signal	A	
DPN Digital path not provided signal	B	
MPR Misdialled trunk prefix	C	
EUM Extended unsuccessful backward setup-information message	F	
Call Supervision Messages		6
ANU Answer signal, unqualified	0	
ANC Answer signal, charge	1	
ANN Answer signal, no charge	2	
CBK Clear back signal	3	
CLF Clear forward signal	4	
RAN Reanswer signal	5	
FOT Forward transfer signal	6	
CCL Calling party clear signal	7	
Circuit Supervision Messages		7
RLG Release guard signal	1	
BLO Blocking signal	2	
BLA Blocking acknowledgement signal	3	
UBL Unblocking signal	4	
UBA Unblocking acknowledgement signal	5	
CCR Continuity check request signal	6	
RSC Reset circuit signal	7	
Circuit Group Supervision Messages		8
MGB Maintenance-oriented group blocking message	1	
MBA Maintenance-oriented group blocking acknowledgement message	2	
MGU Maintenance-oriented group unblocking message	3	
MUA Maintenance-oriented group unblocking acknowledgement message	4	
HGB Hardware-failure-oriented group blocking message	5	
HBA Hardware-failure-oriented group blocking acknowledgement message	6	
HGU Hardware-failure-oriented group unblocking message	7	
HUA Hardware-failure-oriented group unblocking acknowledgement message	8	
GRS Circuit group reset message	9	
GRA Circuit group reset acknowledgement message	A	
SGB Software-generated group blocking message	B	
SBA Software-generated group blocking acknowledgement message	C	
SGU Software-generated group unblocking message	D	
SUA Software-generated group unblocking acknowledgement message	E	
Circuit Network Management Messages		9
ACC Automatic congestion control information message	1	

Fig. 7.2 shows how the different messages in the telephone user part can be used during a normal call.

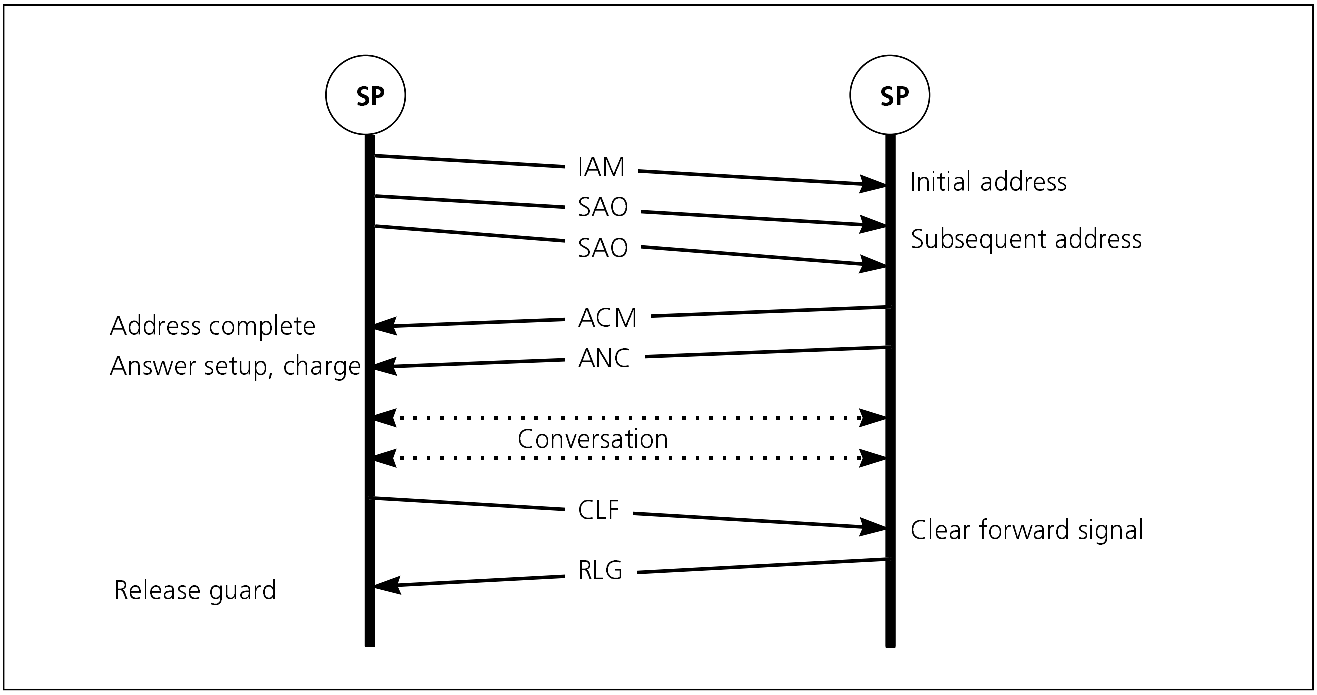


Fig. 7.2 Example of a TUP call.

7.2 ISDN User Part (ISUP)

The ISDN user part (ISUP) is the Signalling System No. 7 protocol which provides the signalling functions required to support basic bearer services and supplementary services for voice and non-voice applications in an Integrated Services Digital Network (ISDN).

The ISUP is described in ITU-T Recommendations Q.761 to Q.764. In addition, the ITU-T Rec. Q.767 describes an ISUP to be used for international signalling.

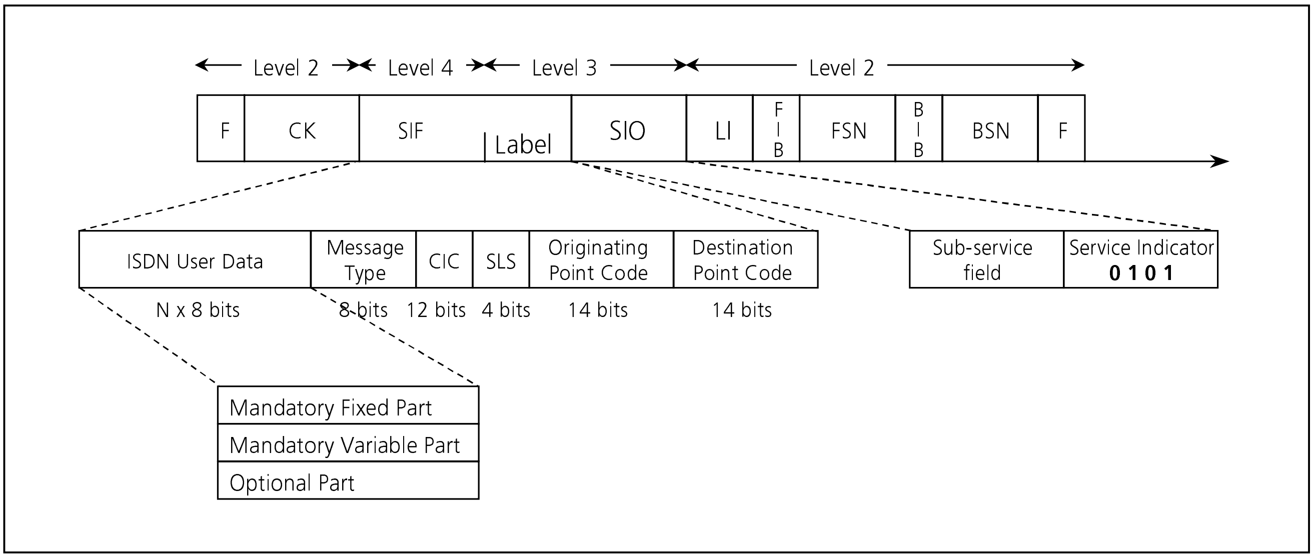


Fig. 7.3 MSU containing an ISDN message.

An ISUP message contains the following information:

- Routing label.
- Message type.
- Mandatory fixed part.
- Mandatory variable part.
- Optional part.

The service information octet indicates that the message belongs to an ISDN user part with the bit pattern `0101` (5 Hex) in the service indicator.

The label contains destination point code, originating point code and circuit identification code. For 2 Mbit/s systems, the circuit identification code is coded as follows:

The five least significant bits are a binary representation of the actual number of the time slot which is assigned to the speech circuit. The remaining bits are used where necessary to identify one among several systems interconnecting an originating point and a destination point.

The label is followed by an octet indicating the message type. The message-type code gives a unique definition of the function and format of each ISUP message.

Abbr.	**Message**	**Code**
ACM	Address complete	06
ANM	Answer	09
BLA	Blocking acknowledgement	15
BLO	Blocking	13
CCR	Continuity check request	11
CFN	Confusion	2F
CGB	Circuit group blocking	18
CGBA	Circuit group blocking acknowledgement	1A
CGU	Circuit group unblocking	19
CGUA	Circuit group unblocking acknowledgement	1B
CON	Connect	07
COT	Continuity	05
CPG	Call progress	2C
CQM	Circuit group query	2A
CQR	Circuit group query response	2B
DRS	Delayed release	27
FAA	Facility accepted	20
FAC	Facility	33
FAR	Facility request	1F
FOT	Forward transfer	08
FRJ	Facility rejected	21
GRA	Circuit group reset acknowledgement	29
GRS	Circuit group reset	17
IAM	Initial address	01
IDR	Identification request	36
INF	Information	04
INR	Information request	03
IRS	Identification response	37
LPA	Loop-back acknowledgement	24
NRM	Network resource management	32
OLM	Overload	30
PAM	Pass along	28
REL	Release	0C
RES	Resume	0E
RLC	Release complete	10
RSC	Reset circuit	12
SAM	Subsequent address	02
SGM	Segmentation	38
SUS	Suspend	0D
UBA	Unblocking acknowledgement	16
UBL	Unblocking	14
UCIC	Unequipped CIC	2E
UPA	User part available	35
UPT	User part test	34
USR	User-to-user information	2D

Below are short descriptions of each message type:

Address Complete Message (ACM). Sent in the backward direction to indicate that all the required address signals have been received.

Answer Message (ANM). Sent in the backward direction to indicate that the call has been answered and that metering or measurement of call duration can start.

Blocking Message (BLO). Only for maintenance. Sent in order to cause an engaged condition of a circuit for subsequent outgoing calls.

Blocking Acknowledgement Message (BLA). Sent in response to a blocking message to indicate that the circuit has been blocked.

Call Progress Message (CPG). Sent in either direction during the setup or active phase of the call, indicating that an event has occurred which is of significance and which should be relayed to the originating or terminating access.

Circuit Group Blocking Message (CGB). Sent to cause an engaged condition for a group of circuits for subsequent outgoing calls.

Circuit Group Blocking Acknowledgement Message (CGBA). Sent in response to a circuit group blocking message to indicate that the requested group of circuits has been blocked.

Circuit Group Query Message (CQM). Sent to request the far end to give information about the state of all circuits in a particular range.

Circuit Group Query Response Message (CQR). Sent in response to a circuit group query message to indicate the state of the circuits.

Circuit Group Reset Message (GRS). Sent to release an identified group of circuits.

Circuit Group Reset Acknowledgement Message (GRA). Sent is response to a circuit group reset message to indicate that the requested group of circuits has been reset.

Circuit Group Unblocking Message (CGU). Sent to cancel the engaged condition for a group of circuits.

Circuit Group Unblocking Acknowledgement Message (CGUA). Sent in response to a circuit group unblocking message to indicate that the requested group of circuits has been unblocked.

Charge Information Message (CIM). Sent for accounting and/or charging purposes.

Confusion Message (CFN). Sent in response to any message the exchange does not recognise.

Connect Message (CON). Sent in the backward direction to indicate that the required address signals have been received and the call has been answered.

Continuity Message (COT). Sent to request continuity checking equipment to be attached.

Continuity Check Request Message (CCR). Sent in the forward direction to indicate whether or not there is continuity on the preceding circuit(s).

Delayed Release Message (DRS). Sent to indicate that the calling or called party has been disconnected.

Facility Accepted Message (FAA). Sent in response to a facility request message to indicate that the requested facility has been invoked.

Facility Reject Message (FRJ). Sent in response to a facility request message to indicate that the request for the facility has been rejected.

Facility Request Message (FAR). Sent to request activation of a facility.

Forward Transfer Message (FOT). Sent in the forward direction when the outgoing international exchange operator requires help from an operator at the incoming international exchange.

Identification Request Message (IDR). Sent to request an action regarding the malicious call identification supplementary service.

Information Message (INF). Sent to convey information in association with the call.

Information Request Message (INR). Sent to request information in association with a call.

Initial Address Message (IAM). Sent in the forward direction to initiate seizure of an outgoing circuit and to transmit the number and other information related to the routing and handling of the call.

Loop Back Acknowledgement Message (LPA). Sent in the backward direction in response to a continuity check request message to indicate that a loop has been connected.

Network Resource Management Message (NRM). Sent in order to modify network resources associated with a certain call. The message is sent along an established path in any direction in any phase of the call.

Overload Message (OLM). Sent in the backward direction in response to an initial address message on non-priority calls to invoke a temporary trunk blocking.

Pass Along Message (PAM). Sent to transfer information between two signalling points.

Release Message (REL). Sent to indicate that the circuit is being released.

Release Complete Message (RLC). Sent in response to a release message to indicate that the circuit has been released and brought into the idle condition.

Reset Circuit Message (RSC). Sent to release a circuit.

Resume Message (RES). Sent to indicate that the called or calling party, having been suspended, is reconnected.

Segmentation Message (SGM). Sent in either direction to convey an additional segment of an overlength message.

Subsequent Address Message (SAM). Sent in the forward direction to convey additional called-party number information.

Suspend Message (SUS). Sent to indicate that the called or calling party has been temporarily disconnected.

Unblocking Message (UBL). Sent to indicate that the engaged condition of a circuit is to be released.

Unblocking Acknowledgement Message (UBA). Sent in response to an unblocking message to indicate that the circuit has been unblocked.

Unequipped CIC Message (UCIC). Sent when an unequipped circuit identification code is received.

User Part Available Message (UPA). Sent in either direction as a response to a user part test message, to indicate that the user part is available.

User Part Test Message (UPT). Sent in either direction to test the status of a user part marked as unavailable for a signalling point.

User to User Information Message (USR). A message used to transfer user to user signalling independently of call control messages.

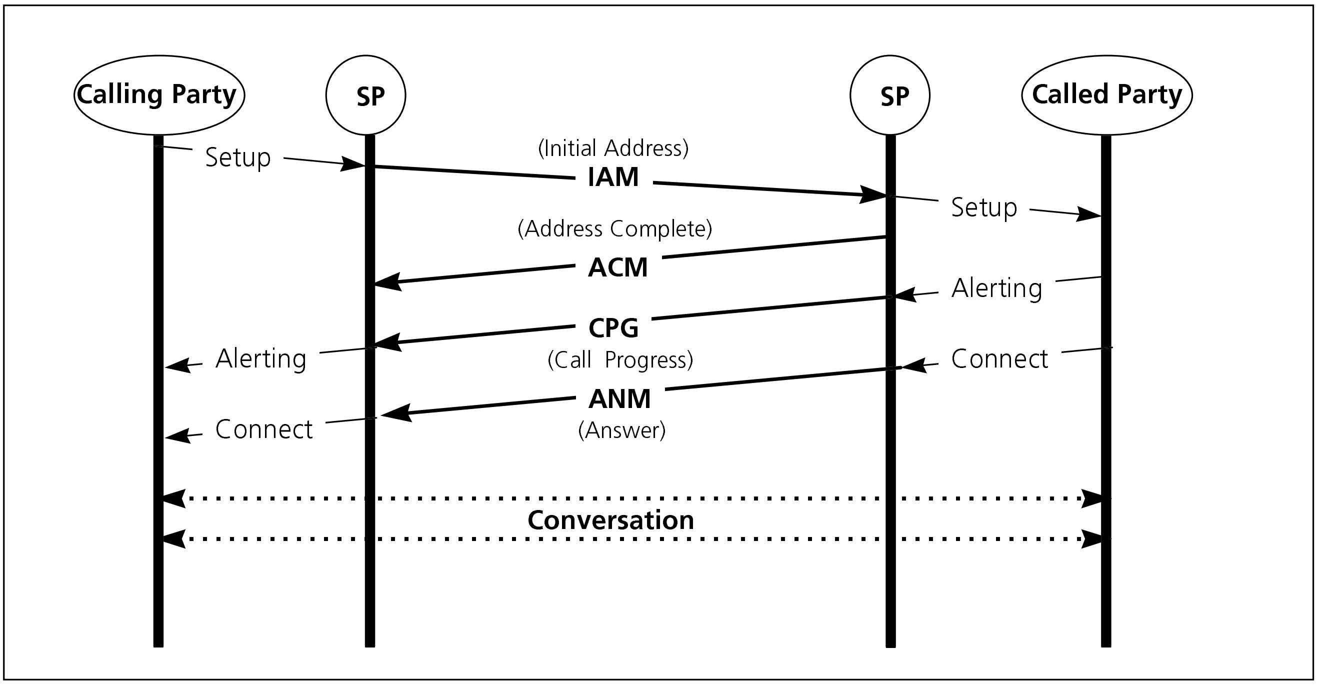


Fig. 7.4 Example of an ISUP call from an ISDN subscriber.

Each message contains one or several parameter fields. The names and codes of the parameters are given in the following table.

Abbr.	Parameter Name	Hex Code
ACCDELINF	Access delivery information	2E
ACCTR	Access transport	03
ACL_	Circuit state indicator	26
BCLIN_	Backward call indicators	11
CALNO	Called party number	04
CAUSE	Cause indicators	12
CDIVINF	Call diversion information	36
CGSM_	Circuit group supervision message indicators	15
CHISINF	Call history information	2D
CLGNO	Calling party number	0A
CLGPC_	Calling party category	09
CNTIN_	Continuity indicators	10
COMPINF	Message compatibility information	38
CONNO	Connected number	21
CR	Connection request	0D
CREF	Call reference	01
CSI_	Circuit state indicator	26
CUGIC	Closed user group interlock code	1A
ECHO_INF	Echo control information	37
EOP	End of optional parameters	00
FACIN_	Facility indicators	18
FOCIN_	Forward call indicators	07
GE	Generic notification	2C
GENDI	Generic digit	C1
GENNO	Generic number	C0
HLC	High layer compatibility	34
INFIN_	Information indicators	0F
IRQIN_	Information request indicators	0E
LOCNUM	Location number	3F
MCIDREQ	MCID request indicators	3B
MCIDRES	MCID response indicators	3C
MLPPPRE	MLPP precedence	3A
NATCI_	Nature of connection indicators	06
NSFAC	Network specific facilities	2F
OBCIN_	Optional backward call indicators	29
OFCIN_	Optional forward call indicators	08
ORC	Original called number	28
PC_	Signalling point code	1E
PCOMINF	Parameter compatibility information	39
PDELCOUN	Propagation delay counter	31
RDGNO	Redirecting number	0B
REDIN_	Redirection information	13
REDNO	Redirection number	0C
Remoteop	Remote operations	40
RG&ST	Range & status	16
RNUMRP	Redirection number restriction	40
SERVACT	Service activation	33
SIGNPC	Signalling point code	1F
SIGNPC	Signalling point code	2B
SUBNO	Subsequent number	05
TNS	Transit network selection	23
TRMRQ_	Transmission medium requirement	02
TRMRQP	Transmission medium requirement prime	3E
TRMUSED	Transmission medium used	35
USRIN	User-to-user information	20
USRSI	User service information	1D
USRSIP	User service information prime	30
UUIN_	User-to-user indicators	2A

7.3 Signalling Connection Control Part (SCCP)

SCCP supplements the message transfer part by providing both connectionless and connection-oriented network services for the transfer of circuit-related and non-circuit-related information. SCCP can control logical signalling connections. It can also transfer signalling data across the network, with or without use of logical connections.

The combination of MTP and SCCP is called Network Service Part (NSP). NSP meets the requirements for layer 3 services as defined in the OSI reference model.

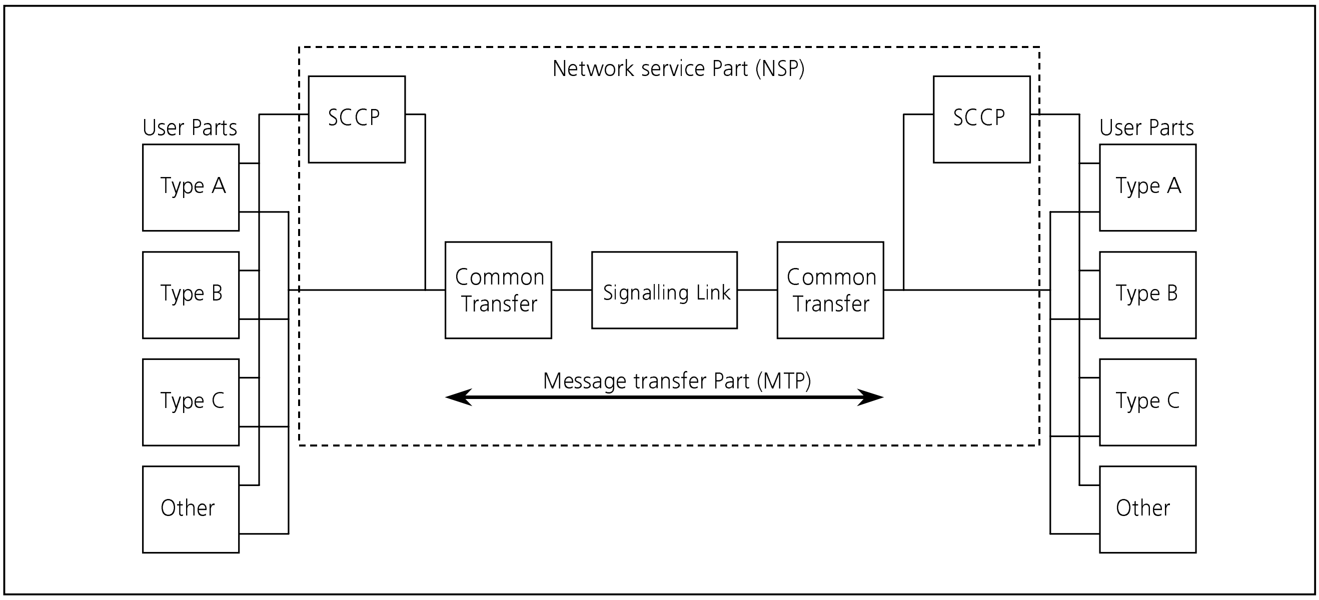


Fig. 7.5 Functional diagram for SCCP.

SCCP services are divided into two groups:

- Connection-oriented services.
- Connectionless services.

For connection-oriented services, two types of connections can be used:

1. Temporary signalling connections, with the connection initiated and controlled by the service user. This can be compared with dialled telephone calls.
2. Permanent signalling connections, established and controlled by the local operation and maintenance centre. These connections can be compared with leased lines.

For transferring the data, four different protocol classes are defined: Two for connectionless services and two for connection-oriented services. The four classes are as follows:

Class 0: Basic Connectionless Class.
Data are transported independently of each other and may therefore be delivered out of sequence. This corresponds to a pure connectionless network service.

Class 1: Sequenced Connectionless Class.
In protocol class 1 the features of class 0 are complemented by a sequence control. By use of the signalling link selection field, the same link is selected for all messages in one call. This secures sequence control and is identical to the standard service provided by the MTP to the user parts.

The connectionless protocol classes 0 and 1 provide functions necessary to transfer one network service data unit (NSDU). The maximum length of an NSDU is restricted to 32 octets in the international network and 256 octets in the national network.

Class 2: Basic Connection-oriented Class.
In protocol class 2, bi-directional transfer of NSDUs is done by setting up a temporary or permanent signalling connection. This corresponds to a simple connection-oriented network service.

Class 3: Flow Control Connection-oriented Class.
In protocol class 3, the features of protocol class 2 are complemented by the inclusion of flow control, with its associated capability of expedited data transfer. Moreover, an additional capability of detecting message loss and mis-sequencing is included. In such circumstances, the signalling connection is reset and a corresponding notification is given by the SCCP to the higher layers.

7.3.1 Connection-oriented Data Transfer

Setup of logic connections is based on the exchange of references between two ends of the connection. These references are used in all later data transfers.

The calling SCCP (A) starts transmitting a connection request (CR) message. This CR contains data about protocol class, the called SCCP address (B) and a reference chosen by A. The CR can also contain A's address and user data.

B answers with a connection confirm (CC) containing the reference number from A, a reference number chosen by B and the selected protocol class. The CC can also contain user data. When exchange A receives the CC the data connection is established. In the following data-transfer period, SCCP A uses the reference number chosen by B and SCCP B uses the reference number chosen by A.

The disconnection of the logic connection is done when A transmits a released (RLSD) message which is answered with a release complete (RLC) message.

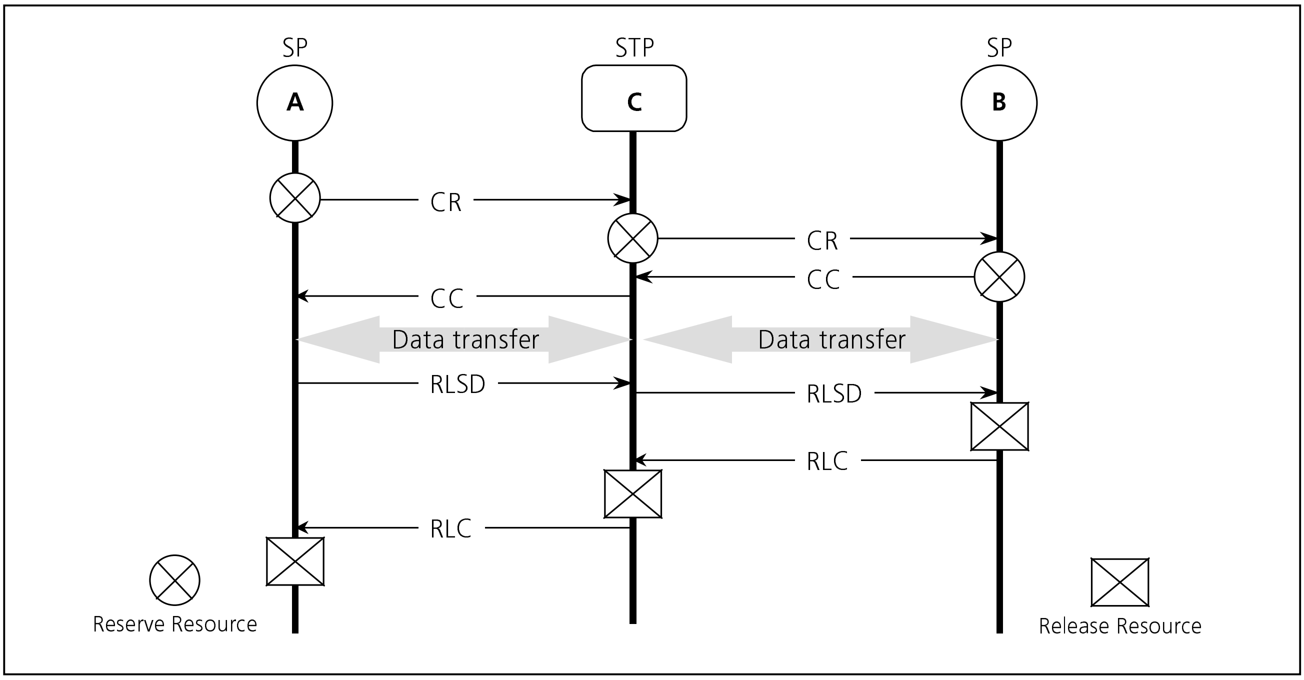


Fig. 7.6 Establishment and release of logical connection.

7.3.2 Connectionless Data Transfer

In this kind of data transfer, no reference numbers are exchanged or stored. The SCCP message, unit data (UDT), contains destination point code and originating point code. The destination point code is used for routing the message to the user, and the originating point code is used to return a message to the originating user. This returned message could either be an answer to the received UDT or a message from an SCCP in the selected route indicating that the message cannot be transferred. UDT also contains an indication as to whether the message has to be returned or not if it proves impossible to transfer the message to its destination point.

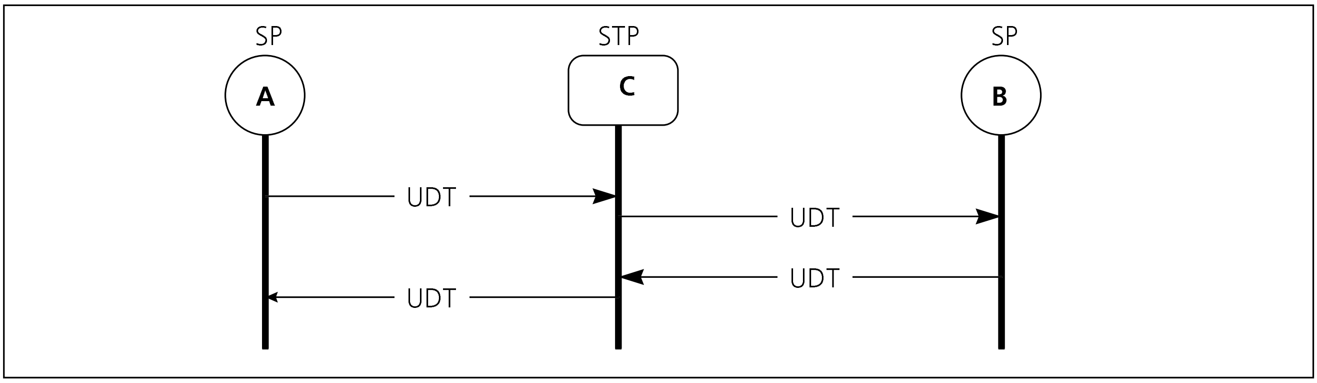


Fig. 7.7 Connectionless data transfer.

7.3.3 SCCP Format

An SCCP message contains the following information:

- Routing label.
- Message type.
- Mandatory fixed part.
- Mandatory variable part.
- Optional part which may contain fixed length and variable length fields.

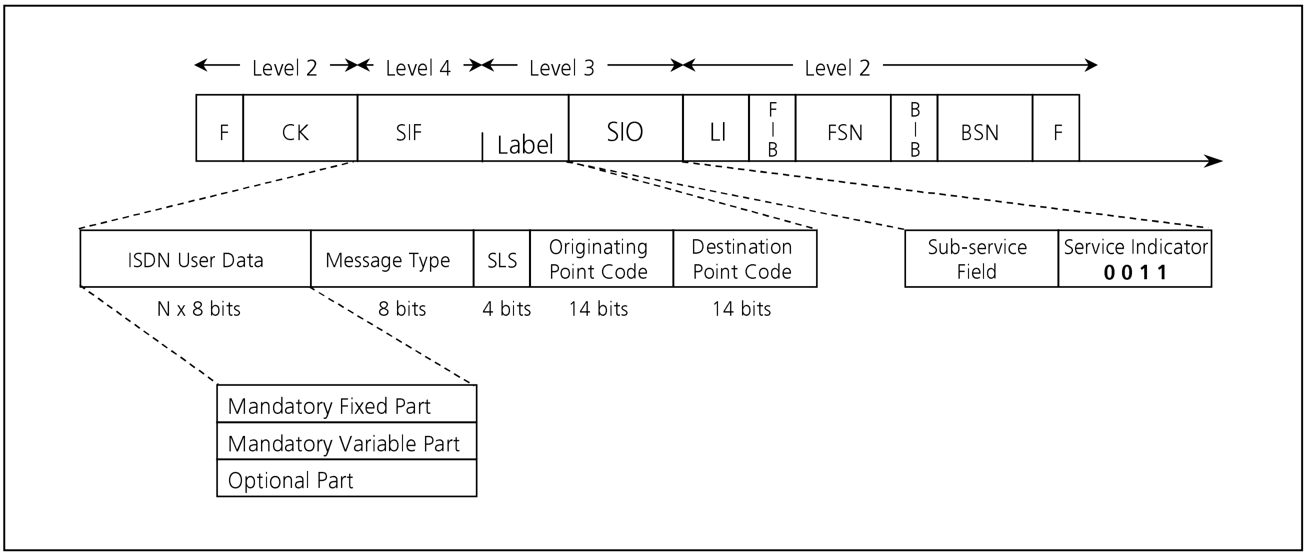


Fig. 7.8 Format of SCCP message.

The routing label has been discussed in the section "Routing Level".

Message Type.
The type code consists of a one-octet field. The message-type code gives a unique definition of the function and format of each SCCP message. Each message type can be used in different protocol classes, as shown in the following table.

Protocol class				Message type		Code
0	1	2	3			
		X	X	CR	Connection request	01
		X	X	CC	Connection confirm	02
		X	X	CREF	Connection refused	03
		X	X	RLSD	Released	04
		X	X	RLC	Release complete	05
		X		DT1	Data form 1	06
			X	DT2	Data form 2	07
			X	AK	Data acknowledgement	08
X	X			UDT	Unitdata	09
X	X			UDTS	Unitdata service	0A
			X	ED	Expedited data	0B
			X	EA	Expedited data acknowledgement	0C
			X	RSR	Reset request	0D
			X	RSC	Reset confirm	0E
		X	X	ERR	Protocol data unit error	0F
		X	X	IT	Inactivity test	10
X	X			XUDT	Extended unitdata	11
X	X			XUDTS	Extended unitdata service	12

Connection Confirm. Is sent by the called SCCP to indicate that the setup of the signalling connection has been carried out.

Connection Request. Is sent by the calling SCCP to request the setup of a signalling connection.

Connection Refused. Is sent by the called SCCP to indicate that the setup of a signalling connection has been refused.

Data Acknowledgement. Is used to acknowledge the receipt of data in protocol class 3 with flow control.

Data Form 1. Is used to pass SCCP user data between two SCCP nodes transparently.

Data Form 2. Is used to pass SCCP user data between two SCCP nodes transparently and to acknowledge received messages.

Expedited Data. Has the same function as data form 2 messages but can also bypass the flow-control mechanism that has been selected.

Expedited Data Acknowledgement. Is used to acknowledge an expedited data messa ge.

Extended Unitdata. Is used by the SCCP that wants to send data along with optional parameters in connectionless mode.

Extended Unitdata Service. Is used to indicate to the origination SCCP that an XUDT with optional parameters cannot be delivered to its destination.

Inactivity Test. May be sent periodically to check if the signalling connection is active at both ends.

Protocol Data Unit Error. Is sent on detection of any protocol error.

Released. Is sent to indicate that the transmitting SCCP wants to release the signalling connection.

Release Complete. Is sent in response to the released message to indicate that a released message has been received and that the signalling connection has been released.

Reset Confirm. Is sent to indicate that a release request has been received and that the reset procedure has been completed.

Reset Request. Is sent to indicate that the transmitting SCCP wants to initiate a reset procedure.

Unitdata. Is used by the SCCP to send data in connectionless mode.

Unitdata Service. Is used to indicate to the originating SCCP that a UDT cannot be delivered to its destination.

Parameter Fields.
Each SCCP message type has its own set of parameters. Fig. 7.9 shows which parameters are contained in each message.

Message	Parameter Field	Message type code	Destination local reference	Source local reference	Called party address	Calling party address	Protocol class	Segmenting/reassembling	Receive sequence number	Sequencing/segmenting	Credit	Release cause	Return cause	Reset cause	Error cause	Refusal cause	Data	Segmentation	Hop counter	End of optional parameter
CR	Connection request	M		M	M	O	M				O						O			O
CC	Connection confirm	M	M		O		M				O						O			O
CREF	Connection Refused	M	M		O											M	O			O
RLSD	Released	M	M	M								M					O			O
RLC	Release Complete	M	M	M																
DT1	Data Form 1	M	M					M									M			
DT2	Data Form 2	M	M							M							M			
AK	Data Acknowledgement	M	M						M		M									
UDT	Unitdata	M			M	M	M										M			
UDTS	Unitdata Service	M			M	M							M				M			
ED	Expedited Data	M	M														M			
EA	Expedited Data Ack.	M	M																	
RSR	Reset Request	M	M	M										M						
RSC	Reset Confirm	M	M	M																
ERR	Protected Data Unit Error	M	M												M					
IT	Inactivity Test	M	M	M			M			M	M									
XUDT	Extended Unitdata	M			M	M	M										M	O	M	O
XUDTS	Extended Unitdata Service	M			M	M							M				M	O	M	O

M = Mandatory field O = Optional field

Fig. 7.9 SCCP message types and parameters.

A brief description of the parameter fields is given in the following.

End of Optional Parameters. A one-octet field containing only zeros.

Destination Local Reference. A three-octet field containing a reference number used to identify the connection section for outgoing messages.

Source Local Reference. A three-octet field containing a reference number used to identify incoming messages.

Called Party Address. This parameter field contains one octet for indicating the address type and a variable number of octets containing the actual address (see fig. 7.10). The address type indicates the type of address information contained in the address field. The actual address consists of any combination of the following elements:

- Signalling point code, represented by two octets.
- Subsystem number that identifies an SCCP user function, for example OMAP or ISDN-UP.
- Global title, for example dialled digits.

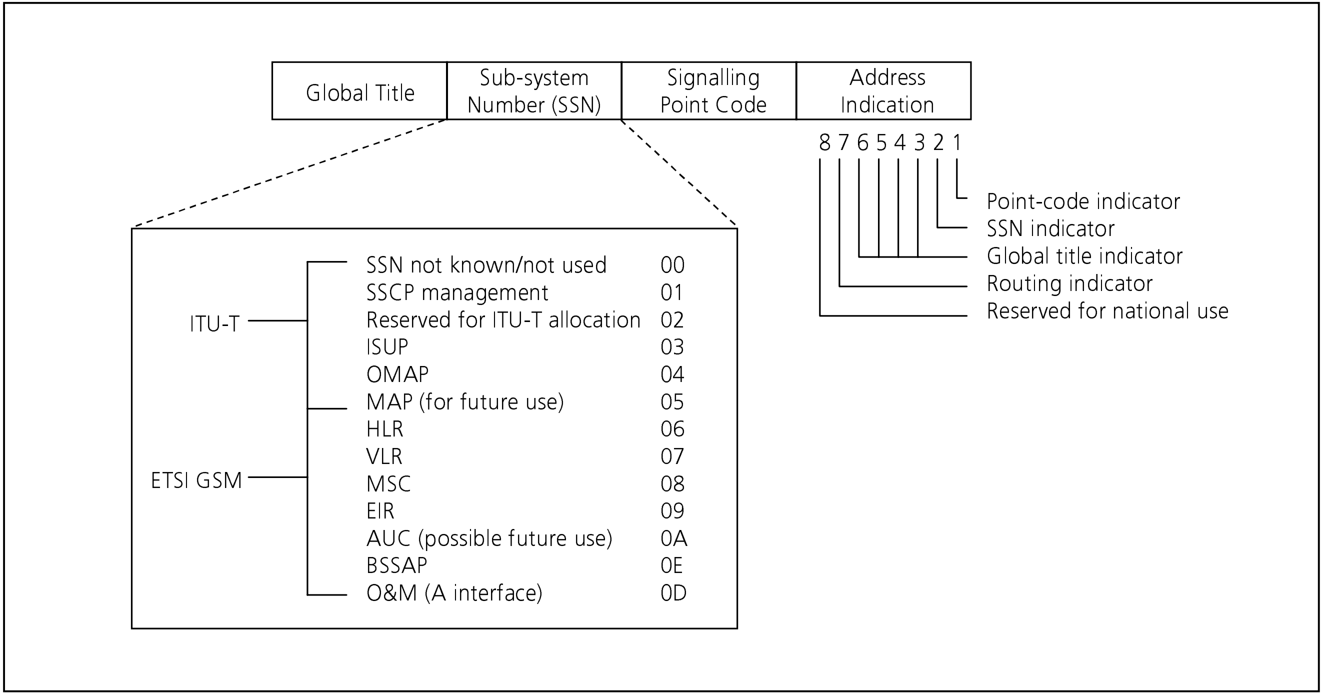


Fig. 7.10 Format of SCCP address field.

Calling Party Address. A variable length parameter with the same structure as the called party address.

Protocol Class. A one-octet field used to indicate the selected protocol class. Bits 1-4 are coded as follows:
Bit 4-1 = 0000 – Class 0.
Bit 4-1 = 0001 – Class 1.
Bit 4-1 = 0010 – Class 2.
Bit 4-1 = 0011 – Class 3.
When bits 1-4 indicate a connection-oriented protocol class (classes 2 and 3), bits 5-8 are spare.
When bits 1-4 indicate a connectionless protocol class (classes 0 and 1), bits 5-8 are used to specify message handling as follows:
Bits 8-5 = 0000 – No special options.
Bits 8-5 = 1000 – Return message on error.

Segmenting/Reassembling. More data is indicated by bit 1 as follows:

- Bit 1 = 0 – No more data.
- Bit 1 = 1 – More data.

Bit 1 is spare.

Receive Sequence Number. The receive number of the next expected message is contained in bits 2-8. Bits 2-8 are spare.

Sequencing/Segmenting. The first octet contains the send-sequence number in bits 2-8. Bit 1 is spare. The second octet contains the receive-sequence number in bits 2-8 and bit 1 indicates more data as follows:

- Bit 1 = 0 – No more data.
- Bit 1 = 1 – More data.

Credit. A one-octet field used in protocol classes that include flow-control functions (allowed window size).

Release Cause. The release cause field contains the reason for the release of the connection.

Return Cause. For unit data service messages, the return cause field is a one-octet field containing the reason for the message return.

Reset Cause. A one-octet field containing the reason for resetting the connection.

Error Cause. A one-octet field indicating the exact protocol error.

Release cause	Code
End-user originated	00
End-user congestion	01
End-user failure	02
SCCP-user originated	03
Remote procedure error	04
Inconsistent connection data	05
Access failure	06
Access congestion	07
Subsystem failure	08
Subsystem congestion	09
Network failure	0A
Network congestion	0B
Expiration of reset timer	0C
Expiration of receive inactivity timer	0D
Not obtainable	0E
Unqualified	0F
Spare	10 to FF

Refusal Cause. A one-octet field indicating the reason for the refusal on the connection.

Data. The data field is of variable length and contains the SCCP user data.

Hop Counter. Used in the XUDT and XUDTS messages to detect loops in the SCCP layer.

Segmentation. Used in the XUDT and XUDTS messages to indicate that an SCCP message has been segmented.

7.3.4 SCCP Management

The SCCP provides functions for managing the status of the SCCP subsystems. These functions are, for example, used to inform other subsystems of the status of an SCCP subsystem and to allow a co-ordinated change of status of SCCP subsystems. A brief description of the SCCP management messages is given below:

Message		Code
SSA	Subsystem allowed	01
SSP	Subsystem prohibited	02
SST	Subsystem status test	03
SOR	Subsystem out-of-service request	04
SOG	Subsystem out-of-service grant	05

Subsystem Allowed (SSA). Sent to involved destinations to inform them that a subsystem which was formerly prohibited is now allowed.

Subsystem Out-of-service Grant (SOG). Sent in response to a subsystem out-of-service request message to give information that the request has been accepted.

Subsystem Out-of-service Request (SOR). Is used to allow subsystems to go out of service without degrading the performance of the network.

Subsystem Prohibited (SSP). Is sent to involved destinations to inform SCCP management at these destinations of the failure of a subsystem.

Subsystem Status Test (SST). Is sent to verify the status of a subsystem that was marked prohibited.

7.4 Transaction Capabilities Application Part (TCAP)

The overall objective of the ITU-T specified transaction capabilities application part **(TCAP)** is to provide means for the transfer of information between nodes (exchanges and/or service centres), and to provide generic services to applications (distributed over the exchanges and service centres), while being independent of any of these. The currently specified applications using TCAP are OMAP, GSM MAP and INAP, which are described in more detail later.

The relation between TCAP, applications (TC users) and the ISO OSI model is shown in fig. 7.11.

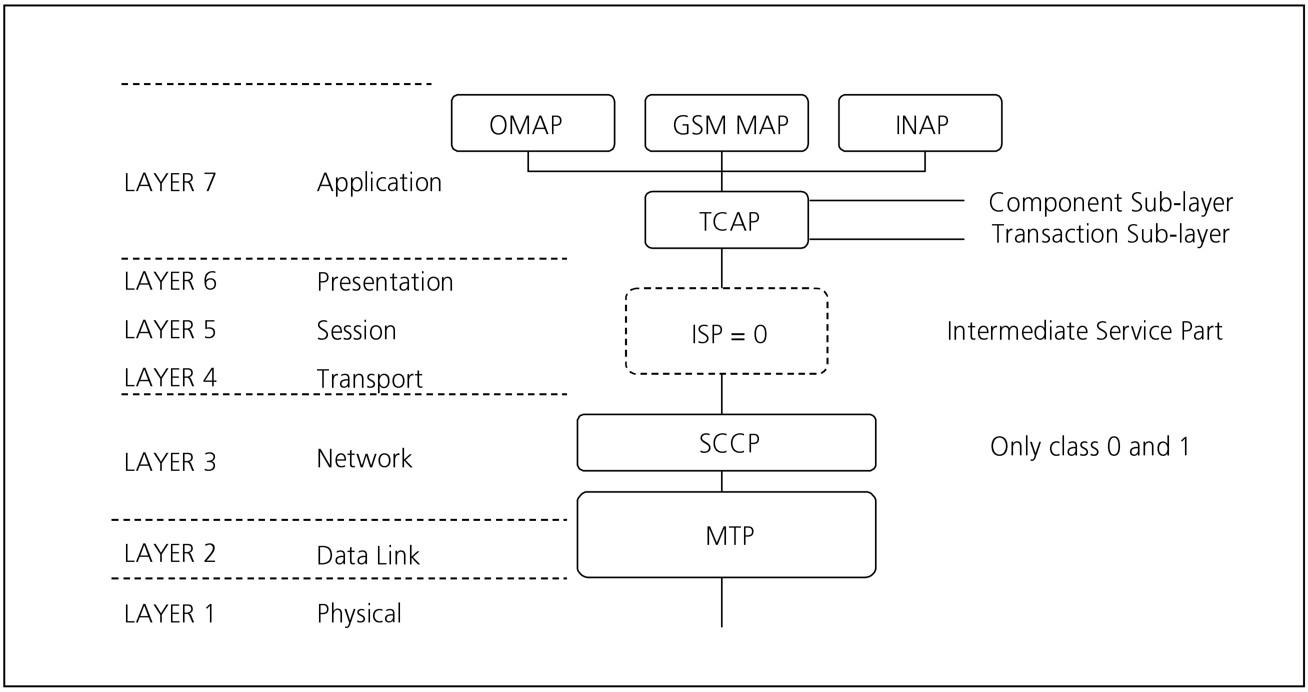


Fig. 7.11 Relation between INAP, OMAP, GSM, MAP, TCAP and the ISO OSI model.

ITU-T has only specified the use of SCCP class 0 and 1 (connectionless transfer) for the TCAP. This means that the Intermediate Service Part **(ISP)** is empty/not needed because no layer 4-6 functions are required for control of SCCP connections.

TCAP is divided into two sub-layers:

- **Component sub-layer** deals with components that are the application protocol data units (APDU) which convey remote operations and their responses.
- **Transaction sub-layer** deals with the exchange of messages containing components and, optionally, a dialogue portion between two TC users.

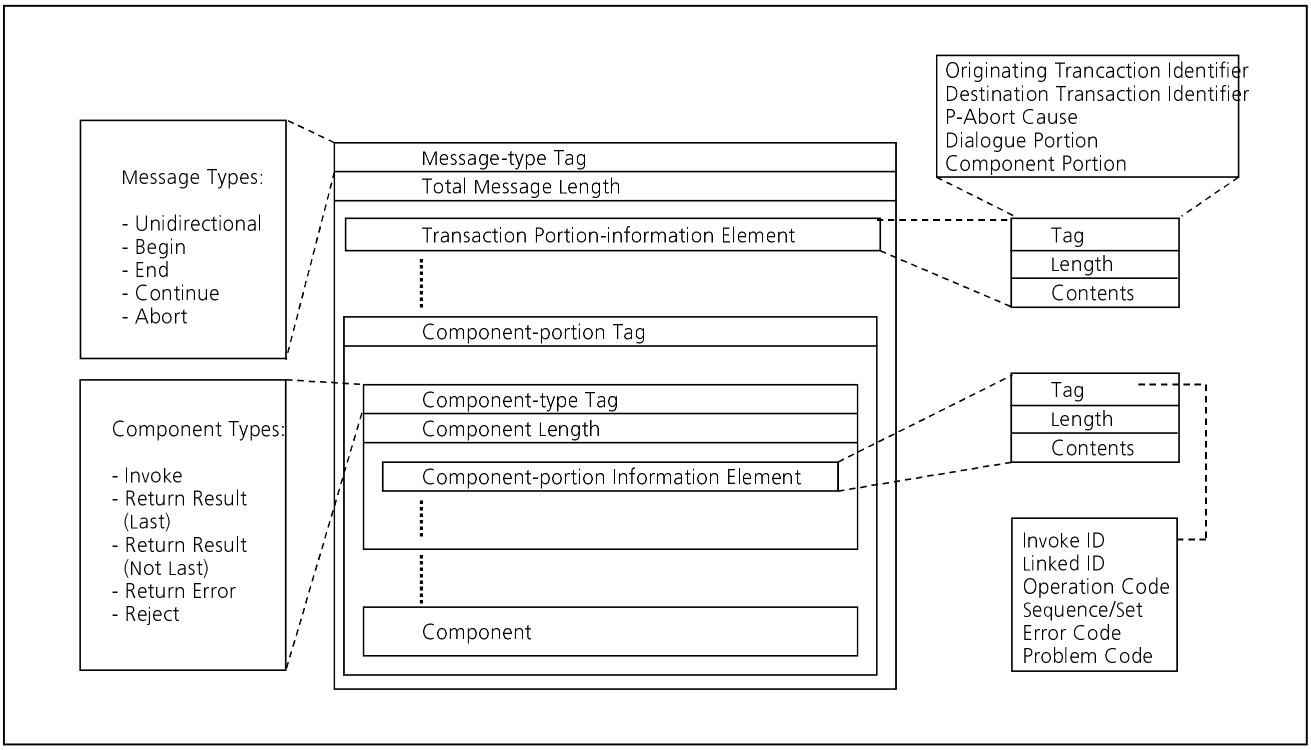


Fig. 7.12 TCAP message structure.

7.4.1 TCAP Transaction Sub-layer

Message-type tag		**Code**
- Unidirectional	(Used when there is no need to establish a transaction)	61
- Begin	(Initiate transaction)	62
- End	(Terminate transaction)	64
- Continue	(Continue transaction)	65
- Abort	(Terminate transaction in abnormal situation)	67

Transaction portion information-element tag		**Code**
- Originating transaction ID	(Transaction identity at originating end)	48
- Destination transaction ID	(Transaction identity at destination end)	49
- P-Abort cause	(Reason for abort by transaction sub-layer)	4A
- Dialogue portion	(Application context and user information that are not components, e.g. application protocol/subset/options to be used, passwords and identification of sub-processes)	6B
- Component portion	(Contains component portion, see component sub-layer)	6C

7.4.2 TCAP Component Sub-layer

Component-type tag		**Code**
- Invoke	(Request operation to be performed at remote end)	A1
- Return result (last)	(Successful completion of operation, contains last/only result)	A2
- Return error	(Reports unsuccessful completion of operation)	A3
- Reject	(Incorrect component received at remote end)	A4
- Return result (not last)	(Contains part of result of operation)	A7
Component portion information-element tag		**Code**
- Invoke ID	(Operation-reference number)	02
- Linked ID	(Reference number for an operation linked to another operation)	80
- Local operation	(Indicates the local operation to be invoked)	02
- Global operation	(Indicates the global operation to be invoked)	06
- Sequence	(Sequence of parameters accompanying a component)	30
- Set	(Set of parameters accompanying a component)	31
- Local err code	(Reason for unsuccessful completion of operation contained in the return	02
- Global err code	error component)	06
- Problem code	(Cause contained in the reject component)	80-83

The operation to be performed at the remote end depends on the TC user.

7.5 Operations, Maintenance and Administration Part (OMAP)

OMAP specifies procedures and protocols related to operations, maintenance and administration information. These procedures and protocols are associated with the application layer of the OSI reference model (layer 7).

Three groups of procedures are specified:

- Operations, maintenance and administration procedures for the signalling network.
- Operations, maintenance and administration procedures for exchanges.
- Operations, maintenance and administration procedures that are associated with the signalling network and exchanges.

7.6 GSM Mobile Application Part (MAP)

MAP (mobile application part) is specified by ETSI (European Telecommunications Standards Institute) for use in GSM networks (Global System for Mobile Communication) for the transfer of location and service information of the mobile subscribers, for example to allow an incoming call to a GSM mobile subscriber to be routed to the area in which the mobile is presently located.

More details on GSM and MAP can be found in GN Nettest Technical Note 6, GSM Global System for Mobile Communication.

7.7 Intelligent Network (INAP)

Intelligent network (IN) concentrates the intelligence for controlling telecommunications services in a small number of IN switches instead of spreading it throughout the network (as today), making it possible to introduce new services faster and independently of the switch vendors. A typical example of an IN architecture is shown in fig. 7.13.

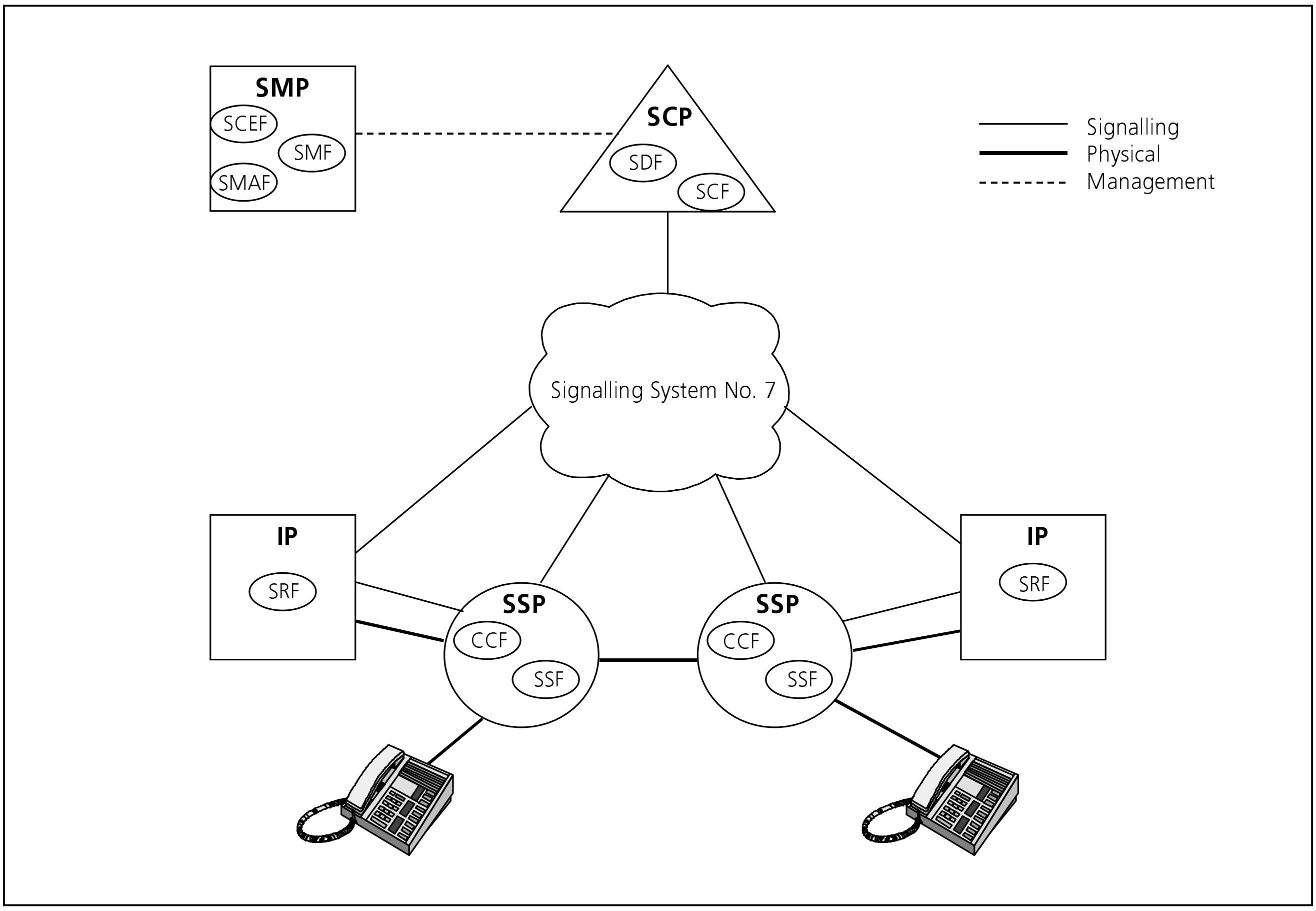


Fig. 7.13 IN architecture.

The service switching point **(SSP)** allows the users access to the IN capabilities. SSP contains a normal switch call control function **(CCF)** and a service switching function **(SSF)** that provides interaction to the SCP.

The service control point **(SCP)** contains the service logic programs via the service control function **(SCF)** that handle the IN service processing and customer concerned and/or network data via the service data function **(SDF)**.

The intelligent peripheral **(IP)** provides the special resources needed for supporting the IN services via the specialised resource function **(SRF)**, for example voice announcements, DTMF digit collection, speech-recognition devices, audio-conference bridge and protocol converters.

The service management point **(SMP)** performs service management control, service provision control and service deployment control via the service management function **(SMF)**. Examples of functions are database administration, network surveillance and testing, network-traffic management and network-data collection. The service creation environment function **(SCEF)** is used to define, develop and test new IN services. The service management access function **(SMAF)** provides selected users – such as service managers or some customers – with access to the SMP.

ITU-T has standardised the first set of IN capabilities: capability set 1 **(CS-1)**. CS-1 makes possible the provision of the services listed in the following table as well as other non-standardised services using the same capabilities.

ABD	Abbreviated dialling
ACC	Account card dialling
AAB	Automatic alternative billing
CD	Call distribution
CF	Call forwarding
CRD	Call rerouting distribution
CCBS	Completion of call to busy subscriber
CON	Conference calling
CCC	Credit card calling
DCR	Destination call routing
FMD	Follow-me diversion
FPH	Freephone
MCI	Malicious call identification
MAS	Mass calling
OCS	Originating call screening
PRM	Premium rate
SEC	Security screening
SCF	Selective call forward on busy / don't answer
SPL	Split charging
VOT	Televoting
TCS	Terminating call screening
UAN	Universal access number
UPT	Universal personal telecommunication
UDR	User-defined routing
VPN	Virtual private network

IN will evolve in the future. The next capability set (CS-2) from ITU-T is, among others, expected to cover mobility services and broadband ISDN (B-ISDN).

The intelligent network application protocol **(INAP)** supports the communication between the functional entities SCF, SSF, SRF and SDF (see fig. 7.13). INAP is a user of TCAP.

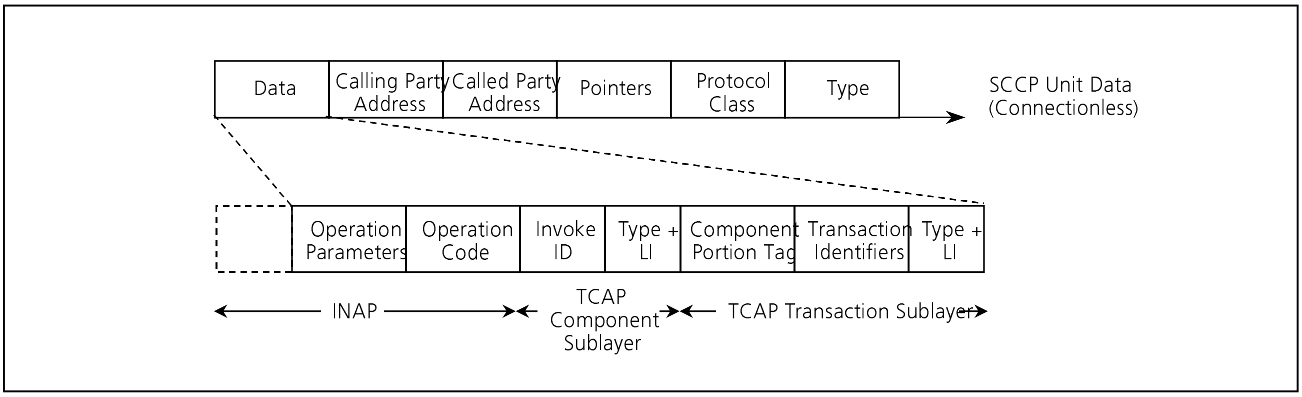


Fig. 7.14 SCCP/TCAP message structure for INAP information.

INAP operations for ITU-T CS-1:

INAP operations	
SCF - SSF operations:	
- Activate service filtering	- Activity test
- Activity test response	- Analysed information
- Analyse information	- Apply charging
- Apply charging report	- Assist request instructions
- Call gap	- Call information report
- Call information request	- Cancel (call information request)
- Cancel status report request	- Collected information
- Collect information	- Connect
- Connect to resource	- Continue
- Disconnect forward connection	- Establish temporary connection
- Event notification charging	- Event report BCSM[1]
- Furnish charging information	- Hold call in network
- Initial DP[2]	- Initial call attempt
- O_answer	- O_called_party_busy
- O_disconnect	- O_midcall
- O_no_answer	- Origination attempt authorised
- Release call	- Request notification charging event
- Request report BCSM event	- Request status report (poll resource status, monitor for change or continuous monitor)
- Reset timer	
- Route select failure	- Select facility
- Select route	- Send charging information
- Service filtering response	- Status report
- T_answer	- T_called_party_busy
- T_disconnect	- Term attempt authorised
- T_midcall	- T_no_answer
SCF - SRF operations:	
- Assist request instructions from srf	- Cancel announcement
- Collected user information	- Play announcement
- Prompt and collect user information	- Specialised resource report
SCF - SDF operations:	
- Query	- Query result
- SDF response	- Update confirmation
- Update data	

[1] BCSM = Basic call state model.

[2] DP = Detection point (in SSP).

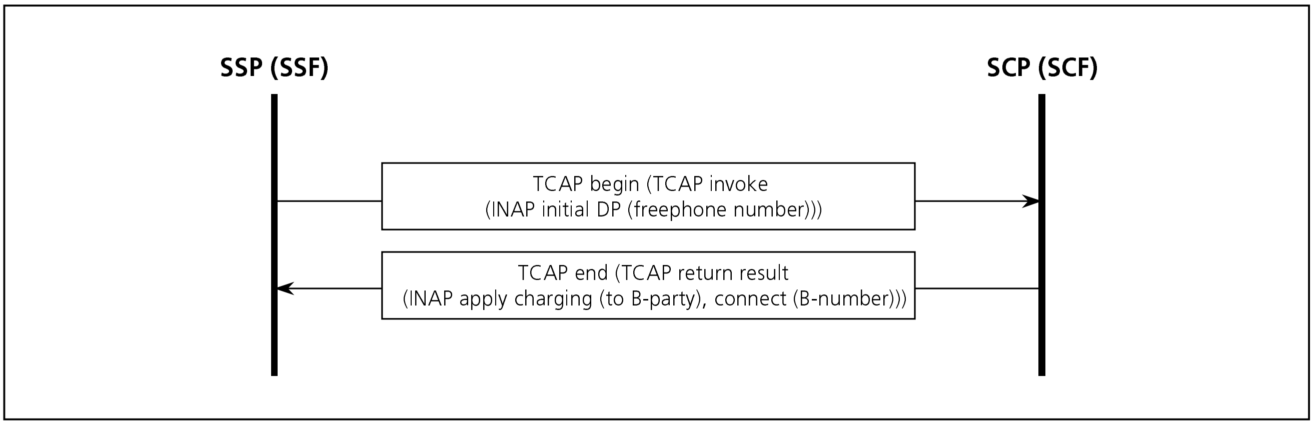

SSP (SSF)
SCP (SCF)
TCAP begin (TCAP invoke
(INAP initial DP (freephone number)))
TCAP end (TCAP return result
(INAP apply charging (to B-party), connect (B-number)))

Fig. 7.15 Signalling example: Freephone.

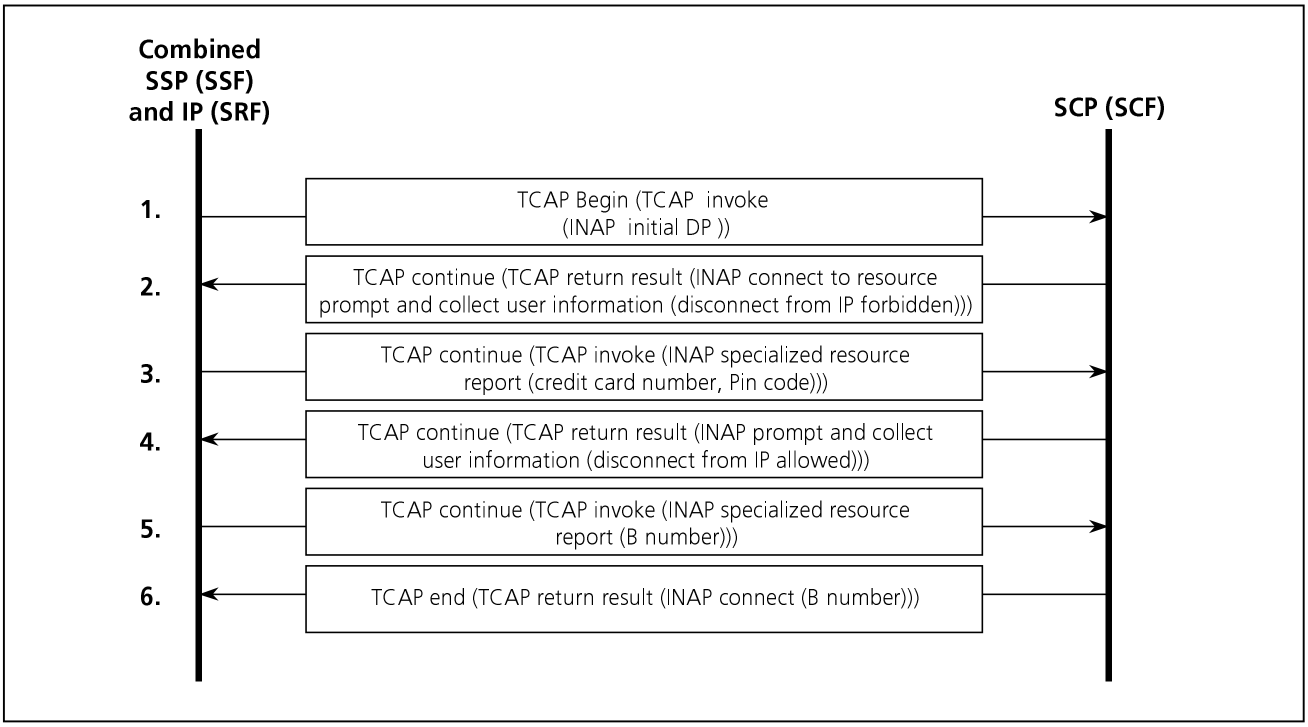

Combined SSP (SSF) and IP (SRF)
SCP (SCF)
1.
TCAP Begin (TCAP invoke (INAP initial DP))
2.
TCAP continue (TCAP return result (INAP connect to resource prompt and collect user information (disconnect from IP forbidden)))
3.
TCAP continue (TCAP invoke (INAP specialized resource report (credit card number, Pin code)))
4.
TCAP continue (TCAP return result (INAP prompt and collect user information (disconnect from IP allowed)))
5.
TCAP continue (TCAP invoke (INAP specialized resource report (B number)))
6.
TCAP end (TCAP return result (INAP connect (B number)))

Fig. 7.16 Signalling example: Credit-card calling.

1. SSP detects off-hook of a credit-card payphone.
2. SCP requests SSP to connect the payphone to a digit-collection device in IP and instructs the IP to collect the information keyed in by the user.
3. IP returns the collected credit-card number and pin code to SCP.
4. SCP requests the IP to collect more information from the user after verification of credit-card number and pin code.
5. IP returns the collected B number to SCP.
6. SCP instructs SSP to connect the call to the collected B number.

7.8 MTP Tester

The MTP tester is connected to the MTP as a user part, i.e. identified by a service indicator. It generates message signal units (MSUs) containing a serial number (and possible additional information) in the signalling information field (SIF). On receipt of these messages, a check is performed to verify that the messages are delivered in accordance with the defined performance criteria for that MTP. The MTP tester is controlled by the OMAP.

The service indicator coding for the MTP tester is: `1000` (8 Hex).

The heading codes for the MTP tester messages are listed in the following table.

Message	H1	H0
Test Control Messages		0
Test request message	0	
Test acceptance message	1	
Test refusal message	2	
Test termination request message	3	
Test termination acknowledge message	4	
Test Traffic Messages		1
Test traffic message	0	

The test-traffic message is formatted as indicated in fig. 7.17.

		BA		0	1	
Filler Octets	Serial Number	Spare	GPC	H1	H0	Label
m * 8	32	2	14	4	4	32

0< m <262

GPC: The point code of the tester initiating the test and generating the traffic.
Serial number: The serial number assigned to the message.
Filler octets: Additional octets of information, i.e. a time stamp.

Fig. 7.17 Format of test-traffic message.

8. Test and Maintenance

8.1 Multichannel Protocol Analyser MPA 7xxx

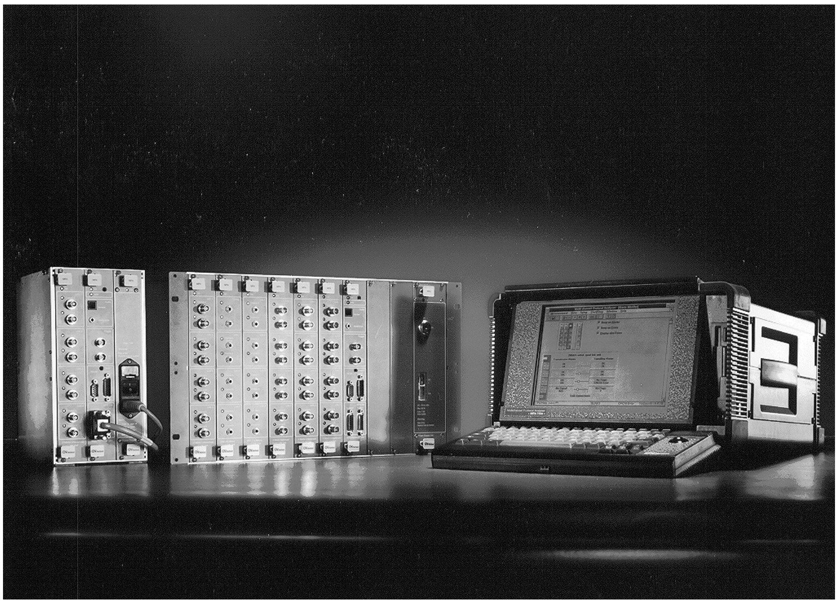


Fig. 8.1 GN Nettest Multichannel Protocol Analyser MPA 7100/7200/7300.

The MPA is designed for the installation testing, performance analysis, maintenance and troubleshooting of today's large, complex SS7 networks, with special focus on advanced services/protocols such as IN and GSM.

Typical applications:

Acceptance testing, detailed troubleshooting, daily maintenance, performance analysis.

- Up to 24 full duplex links in one instrument.
- User interface based on MS Windows® 95.
- Large (and expandable) processing capacity.
- Predefined "click-and-go" triggers and filters including complete call trace.
- Focus on GSM and IN protocols.
- Automatic recognition of signalling errors.
- User-defined result displays.
- Statistical counters.
- ODBC (Open Data Base Connectivity).

General description:

The Multichannel Protocol Analyser (MPA) is an easy-to-use multi-link test instrument for the detailed analysis of telecom digital signalling protocols, i.e. Signalling System No. 7 (SS7), particularly complex protocols such as IN (Intelligent Network) and GSM (Global System for Mobile Communications). The MPA is available as three different instrument types:

MPA 7100
Slimline portable unit able to handle four full duplex signalling links and using an external PC for data presentation.

MPA 7200
19" subrack able to handle up to 24 full duplex signalling links, also using an external PC for data presentation.

MPA 7300
Portable stand-alone instrument able to handle up to 16 full duplex signalling links and with built-in PC for data presentation. The instrument contains a 10.4" colour LCD display, a 3.5" floppy-disk drive, a keyboard (PC notebook type) and a trackball. The keyboard can be flipped up during transportation, covering the display. Socket for external mouse.

The user interface is based on MS Windows® 95. Up to 1 Gbyte of data can be stored. Five different line interfaces are available:

- 2 Mbit/s Unbalanced Quad Link Unit (BNC or 1.6/5.6).
- 2 Mbit/s Balanced Quad Link Unit.
- DS1 Quad Link Unit.
- DS0(A) Triple Link Unit.
- V.35 Quad Link Unit.

The MPA provides three main measurement functions: transmission alarm monitoring, protocol analysis, and statistics. The instrument can be controlled from a remote PC using standard communication interfaces and PC remote control programs, for example ReachOut.

Transmission alarm monitoring:
Transmission-link alarms are monitored on every line input on the MPA:

- 2 Mbit/s: No Signal, AIS (Alarm Indication Signal), No Frame, Distant Alarm.
- DS1: No Signal, AIS, Out of Frame, Yellow Alarm, CRC6 Error.
- V.35/DS0(A): No Data, No Octet, No Timing.

Alarms are sent immediately as they are recognised (the delay in the MPA is shorter than one second). An indication is also sent when an alarm ceases. Alarms can be time-stamped and stored in the memory.

Protocol analysis:
The basic function of the MPA is to record and display in real time the decoded signalling messages on one or more of its link interfaces. Decoding takes place using the protocol assigned to the link. Up to 10 different protocols may be in use simultaneously. The MPA works on full-rate as well as sub-rates and supports both split-rate and link load-sharing.

The MPA has two different modes of operation: Event mode and Sequence mode. Sequence mode is a sorted version of Event mode, with messages grouped according to call. The Sequence mode allows capture MAP, INAP, BSSAP and A-bis sequences as well as TUP and ISUP.

Graphical user interface (GUI):
Based on the MS Windows® 95/NT platform, the MPA's GUI is much like that for other Windows® applications. Its prime elements are the protocol, alarm and statistical windows, providing the user with a good overview of measurement status and results. Extensive use of schematic diagrams, flow charts and combo-boxes facilitates operation.

Storage:
Instrument configurations, measurement conditions, individual filters and measured data can all be stored for later use. The user's own favourite filters can be stored, for example. The Replay function permits a virtual repetition of the measurement back home in the office – even allowing decoding protocols and filters to be changed and conversion of the recorded measurement from simple Events into Sequences.

Filters:
The MPA contains several independent filters for reducing the amount of data stored and/or displayed. All filters are logically represented by hierarchical layers, for example MTP, SNT, SNM, ISUP, SCCP etc. to allow filter criteria to be specified at individual layers. A special sequence filter allows the capture of whole sequences, simply by specifying for example Calling or Called, or IMSI number.

Remote operation:
The MPA can be controlled from a remote site using the PC software package "Reach Out". This can be used to achieve remote control via RS 232, a standard modem, LAN networks or the Internet.
For more advanced applications, the MPA also serves as the measuring probe in a TMN-based QUEST7 surveillance system.

Statistics:
The MPA offers statistical counting in three different areas: link activity, message types and alarms. The statistical function allows real-time monitoring of statistics and more advanced post-processing for the preparation of pre-defined graphs and reports. Time resolution can be set to any value between 1 minute and 2 hours.

Application software:
Optional software packages are available for various applications, for example the Call Data Recorder package. This generates a record containing relevant information for every call and stores it in an ODBC database. Such records include a time stamp, call duration, the called/calling numbers and other relevant parameters.

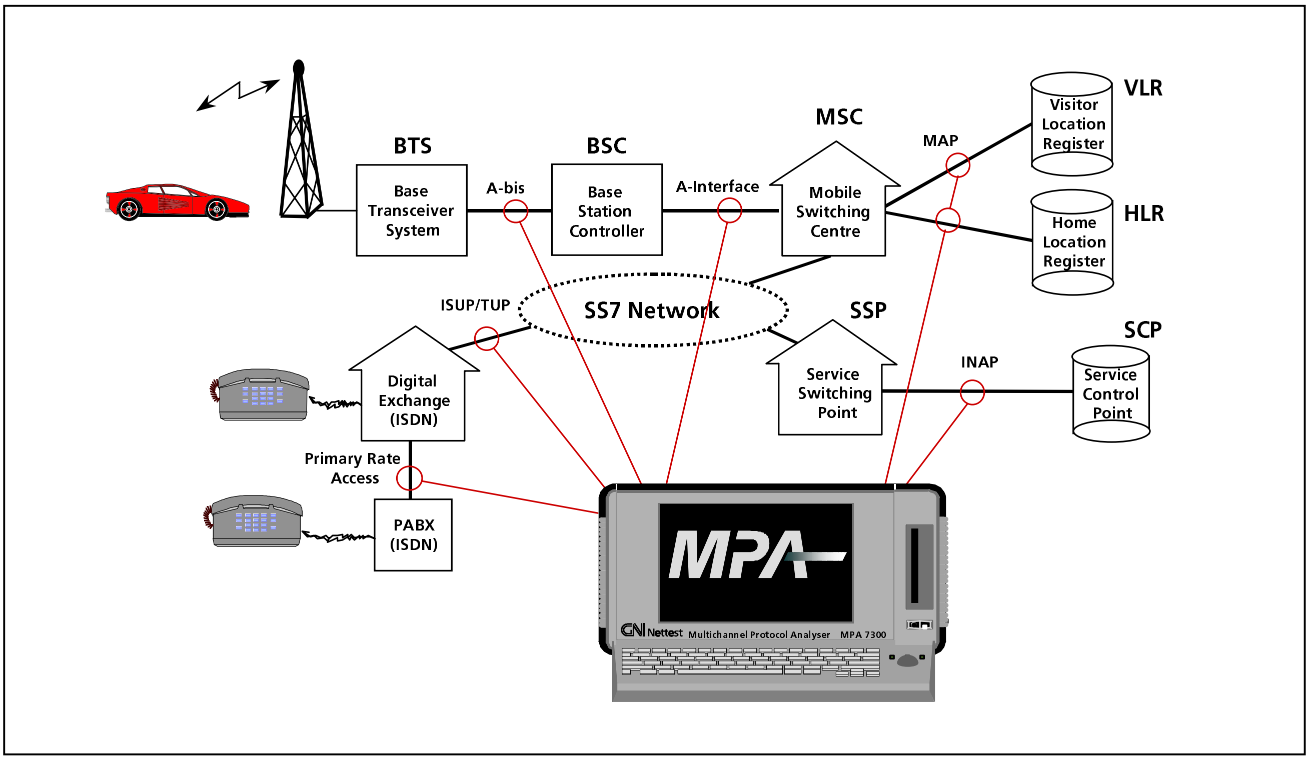


Fig. 8.2 Typical applications for the MPA 7100/7200/7300.

Acceptance testing:
Detailed comparison of the signalling protocol with the specification (message formats, message contents, signalling sequences), performed during the initial installation of the protocol and/or exchange type and when there is a major software update/release.

Detailed troubleshooting:
Detailed signalling analysis during fault-finding in the operation phase – for example tracing of specific calls, looking for specific cause values, analysis of data just before and after the occurrence of an error.

Daily maintenance:
Checking of link loads (number/ratio of MSUs and LSSUs) and quality (number/ratio of errored and re-transmitted MSUs).

Performance analysis:
Counting of message types per link/direction, for example number of error and blocking messages, or number of call attempts (IAM/IAIs), number of successful calls (ACMs) and number of unsuccessful call attempts (unsuccessful backward setup messages).

8.2 LITE 3000

The LITE 3000 is a multi-purpose, battery-powered instrument for field technicians. The instrument is a powerful tool for a wide range of applications, from fast first-aid troubleshooting to comprehensive, in-depth analysis of transmission and signalling problems. The addition of optional software modules expands the LITE 3000 from a full-featured transmission-line quality tester into an advanced signalling analyser.

8.2.1 Main Features of the LITE 3000:

- Fast troubleshooting.
- Simultaneous monitoring of both sides of a 2 Mbit/s PCM line.
- Powerful testing of framed Nx64 kbit/s and unframed 2 Mbit/s PCM systems.
- G.821, G.826 or M.2100 error-performance parameters.
- Test of GSM A-bis interface (option).
- Advanced all-layer signalling analysis options:
  - SS7 protocols incl. GSM A interface and MAP protocols.
  - GSM A-bis interface protocols.
  - ISDN protocols.
  - CAS and MF signalling.
  - Powerful signalling statistics.
  - MEASUREMENT_RESULT filter (A-bis).
- Propagation-time measurements.
- Drop-and-insert testing.
- Immediate LED indications.
- Large colour display.
- Fast and easy access to results.
- Easy intuitive operation.
- Automatic configuration to monitored line.
- Cost-effective.
- More than 10 hours of battery operation.

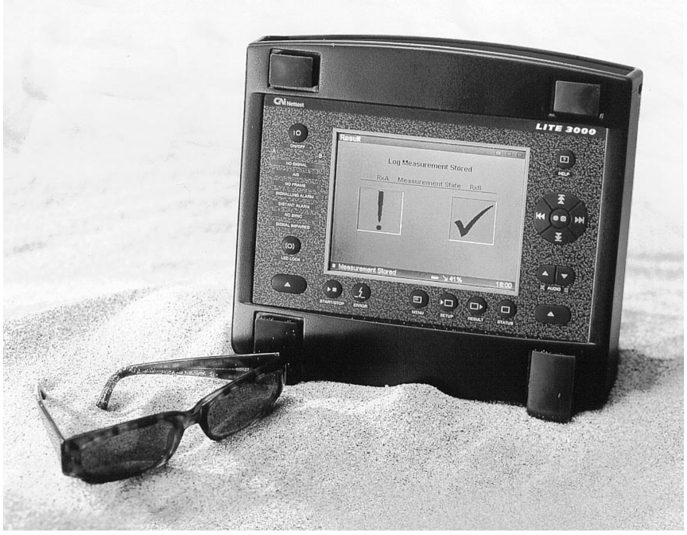


Fig. 8.3 GN Nettest LITE 3000.

8.2.2 General Description

The basic LITE 3000, with its two independent receivers and one transmitter, supports framed and unframed testing and monitoring. This makes it ideal for both in-service and out-of-service transmission-quality measurements. For fast troubleshooting, the LITE 3000 displays alarms and transmission-link status on LED indicators, as well as other relevant information, such as the level of the 2 Mbit/s signal and the frequency difference between the inputs. The instrument's two inputs permit immediate monitoring of the two sides of a PCM line and allow comparison of simultaneously recorded results.

With the SS7 signalling option added, the LITE 3000 becomes a powerful signalling analyser for SS7. An A-bis option tailors the LITE 3000 to test the A-bis interface of GSM networks. Equipped with GSM-specific SS7 protocols (A-interface and MAP protocols), it is converted into a comprehensive transmission tester and signalling analyser for GSM networks. With other options, it becomes a powerful signalling analyser ISDN protocols and for CAS and MF signalling. Easy-to-interpret signalling decodes and statistics make signalling analysis and acquisition of information on the current state of the network very straightforward tasks.

Results are easy to read and interpret on the large LCD display, with its colour coding and graphical symbols. Data can be printed direct to an external printer or exported to a PC via the remote interface. Presentation of transmission-error results as histograms facilitates error-tracing. The LITE 3000 may be operated remotely through an optional MS Windows® program.

With its auto-configuration feature, stored setups and intuitive man-machine interface, the LITE 3000 is quick to set up and very user-friendly in operation. The instrument's portability and robust design allow measurements to be taken at any suitable measuring point. It is powered by rechargeable and replaceable intelligent high-capacity NiMH batteries. These provide more than 10 hours of operation with PowerSave. The LITE 3000 can also be powered via an external mains adapter in long-term measurement operations.

8.2.3 Testing Transmission Quality

The basic LITE 3000 includes a wide range of 2 Mbit/s network transmission-quality applications. For example:

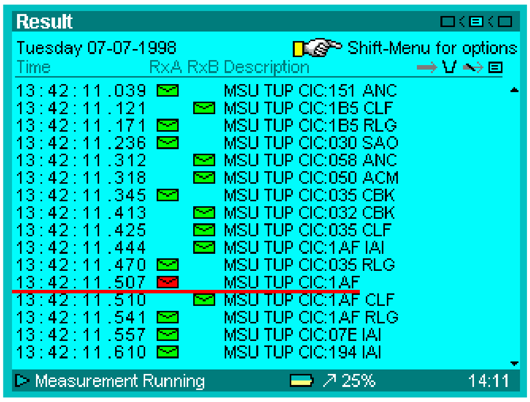
- First-aid troubleshooting and in-service monitoring, using the status monitoring facilities.
- Identification of synchronisation problems through slip measurements and input frequency deviation indication.
- Traffic-channel monitoring and usage analysis.
- Installation and conformance testing via comprehensive out-of-service BERT tests.
- Framed 2 Mbit/s testing for stress testing a network element through variation of the test signal.
- In-service and out-of-service error-performance measurements (G.821/G.826/M.2100).
- Nx64 kbit/s drop-and-insert measurements for in-service measurements of transmission quality.
- Propagation-time measurement for examination of delays in the network.
- Advanced in-service troubleshooting, examining errors and alarms with the event log.
- Audio Performance Test through generation of analogue traffic-channel contents.

8.2.4 SS7 Signalling Analysis in the LITE 3000

With the SS7 signalling option added, the LITE 3000 facilitates analysis of the ITU-T defined Signalling System No. 7 (SS7) between public exchanges, including high level TCAP-based protocols such as GSM. During installation or troubleshooting, the LITE 3000's event log provides valuable, detailed information on the signalling by collecting signalling messages from the connected SS7 signalling links. All layers of the protocol are decoded completely into mnemonics. The mnemonics can be translated to plain language and the use and possible values of the field are explained.

The LITE 3000 can present the recorded information in different ways:

The **Overview** presentation gives a one-line indication of each message. It is easy to see on which of the two inputs the message was detected. Intuitive colour indications highlight messages that could not be correctly decoded. A search facility makes it easy to find such messages. The overview presentation may be changed to contain a couple of lines per message, stating the most important information in the message.

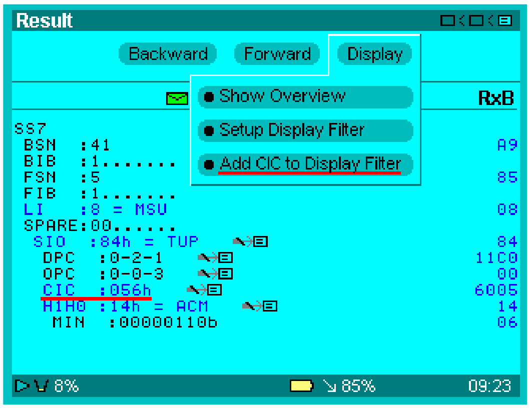


```
Tuesday 07-07-1998
Time              RxA RxB Description
13:42:11.039  🟩      MSU TUP CIC:151 ANC
13:42:11.121      🟩  MSU TUP CIC:1B5 CLF
13:42:11.171  🟩      MSU TUP CIC:1B5 RLG
13:42:11.236  🟩      MSU TUP CIC:030 SAO
13:42:11.312      🟩  MSU TUP CIC:058 ANC
13:42:11.318      🟩  MSU TUP CIC:050 ACM
13:42:11.345  🟩      MSU TUP CIC:035 CBK
13:42:11.413      🟩  MSU TUP CIC:032 CBK
13:42:11.425      🟩  MSU TUP CIC:035 CLF
13:42:11.444      🟩  MSU TUP CIC:1AF IAI
13:42:11.470  🟩      MSU TUP CIC:035 RLG
13:42:11.507  🟥      MSU TUP CIC:1AF
13:42:11.510      🟩  MSU TUP CIC:1AF CLF
13:42:11.541  🟩      MSU TUP CIC:1AF RLG
13:42:11.557  🟩      MSU TUP CIC:07E IAI
13:42:11.610  🟩      MSU TUP CIC:194 IAI
▷ Measurement Running        ↗ 25%        14:11
```

Fig. 8.4 The overview presentation of signalling.

The **High level** presentation displays most parts of the message, making it easy to identify the information carried in each message.

The **Detailed** presentation shows all parts of the message and its hexadecimal contents for detailed inspection and analysis.

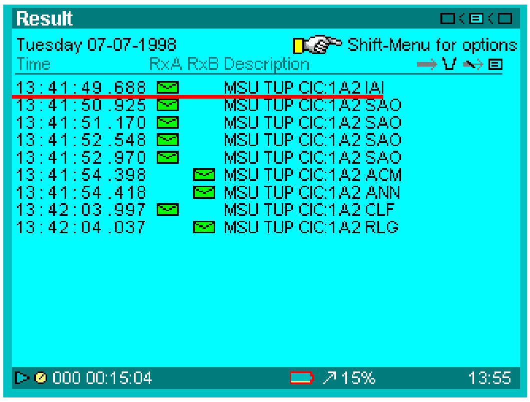


```
SS7
 BSN   :41                                 A9
 BIB   :1.......
 FSN   :5                                  85
 FIB   :1.......
 LI    :8 = MSU                            08
 SPARE:00......
  SIO   :84h = TUP                         84
   DPC   :0-2-1                          11C0
   OPC   :0-0-3                            00
   CIC   :056h                           6005
   H1H0 :14h = ACM                         14
    MIN   :00000110b                       06
▷ 8%                     ↘ 85%          09:23
```

8.5 The detailed presentation.

The SS7 messages are stored in the LITE 3000's memory and can be examined during or after the measurement. More than 20,000 messages can be stored. The instrument's filter facilities permit limitation of the information to be stored, minimising both the storage requirement and the time needed to retrieve data.

Filters can be applied to select the most essential information for storage and display. For ISUP type protocols the user can for example set a filter to see IAM messages only, giving a quick overview of calls on the line. Easy import of the OPC, DPC and CIC parameter value to display filters makes it straightforward to extract messages that belong to the same call. And a general 4 digit search facility allows extract of messages with containing the 4 digits. This may be used to identify messages with a particular called party or calling party number.



```
Result
Tuesday 07-07-1998                    Shift-Menu for options
Time          RxA RxB Description
13:41:49.688  🟩      MSU TUP CIC:1A2 IAI
13:41:50.925  🟩      MSU TUP CIC:1A2 SAO
13:41:51.170  🟩      MSU TUP CIC:1A2 SAO
13:41:52.548  🟩      MSU TUP CIC:1A2 SAO
13:41:52.970  🟩      MSU TUP CIC:1A2 SAO
13:41:54.398      🟩  MSU TUP CIC:1A2 ACM
13:41:54.418      🟩  MSU TUP CIC:1A2 ANN
13:42:03.997  🟩      MSU TUP CIC:1A2 CLF
13:42:04.037      🟩  MSU TUP CIC:1A2 RLG

▷ 000 00:15:04            ↗15%           13:55
```

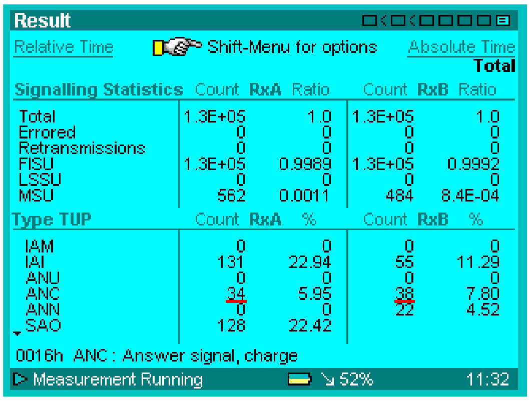
Fig. 8.6 Extract of messages for a call.

8.2.5 Signalling Statistics

The LITE 3000’s signalling statistics provide data on total traffic load and the quality of the signalling link.

The instrument can inform the user on the occurrence of and load from the different SS7 User Parts divided by the SIO value.

For network optimisation the SS7 ISUP and TUP message type statistics opens a vast range of possibilities for the user. Call completion in TUP protocols can be examined by comparing count of IAMs or IAIs on one side of the line with answer messages (ANC/ANN/ANU) on the other side of the line. Furthermore release cause statistics are available for ISUP type protocols.



Result

Relative Time   Shift-Menu for options   Absolute Time

Total

Signalling Statistics	Count RxA	Ratio	Count RxB	Ratio
Total	1.3E+05	1.0	1.3E+05	1.0
Errored	0	0	0	0
Retransmissions	0	0	0	0
FISU	1.3E+05	0.9989	1.3E+05	0.9992
LSSU	0	0	0	0
MSU	562	0.0011	484	8.4E-04

Type TUP	Count RxA	%	Count RxB	%
IAM	0	0	0	0
IAI	131	22.94	55	11.29
ANU	0	0	0	0
ANC	34	5.95	38	7.80
ANN	0	0	22	4.52
SAO	128	22.42		

0016h ANC : Answer signal, charge

▷ Measurement Running   ↘ 52%   11:32

Fig. 8.7 Signalling link and message type statistics.

8.2.6 Other Signalling Options

Other signalling options available for the LITE 3000:

- ISDN signalling analysis.
- GSM A-bis interface protocol signalling analysis.
- Detailed CAS and MF signalling analysis.

9. References

This Technical Note is based on the following ITU-T recommendations (dated Helsinki Q3/93):

Q.700	Introduction to ITU-T Signalling System No. 7.
Q.701-709	Message Transfer Part (MTP tester).
Q.710	Simplified message transfer part
Q.711-716	Signalling Connection Control Part (SCCP).
Q.721-725	Telephone User Part (TUP).
Q.730	ISDN supplementary services
Q.741	Data user part DUP
Q.750-754	Operations, Maintenance and Administration Part (OMAP).
Q.755	Signalling System No. 7 Protocol Tests (MTP tester).
Q.761-767	Integrated Services Digital Network User Part (ISUP).
Q.771-775	Transaction Capabilities Application Part (TCAP).
Q.780-783	Test specification.
Q.791	Monitoring and measurements.
Q.795	Operation, Maintenance and Administration part (OMAP).
Q.12xx	Intelligent Network Application Protocol (INAP).

In addition, the following ETSI specifications have been used:

GSM 09.02	Mobile Application Part (MAP).