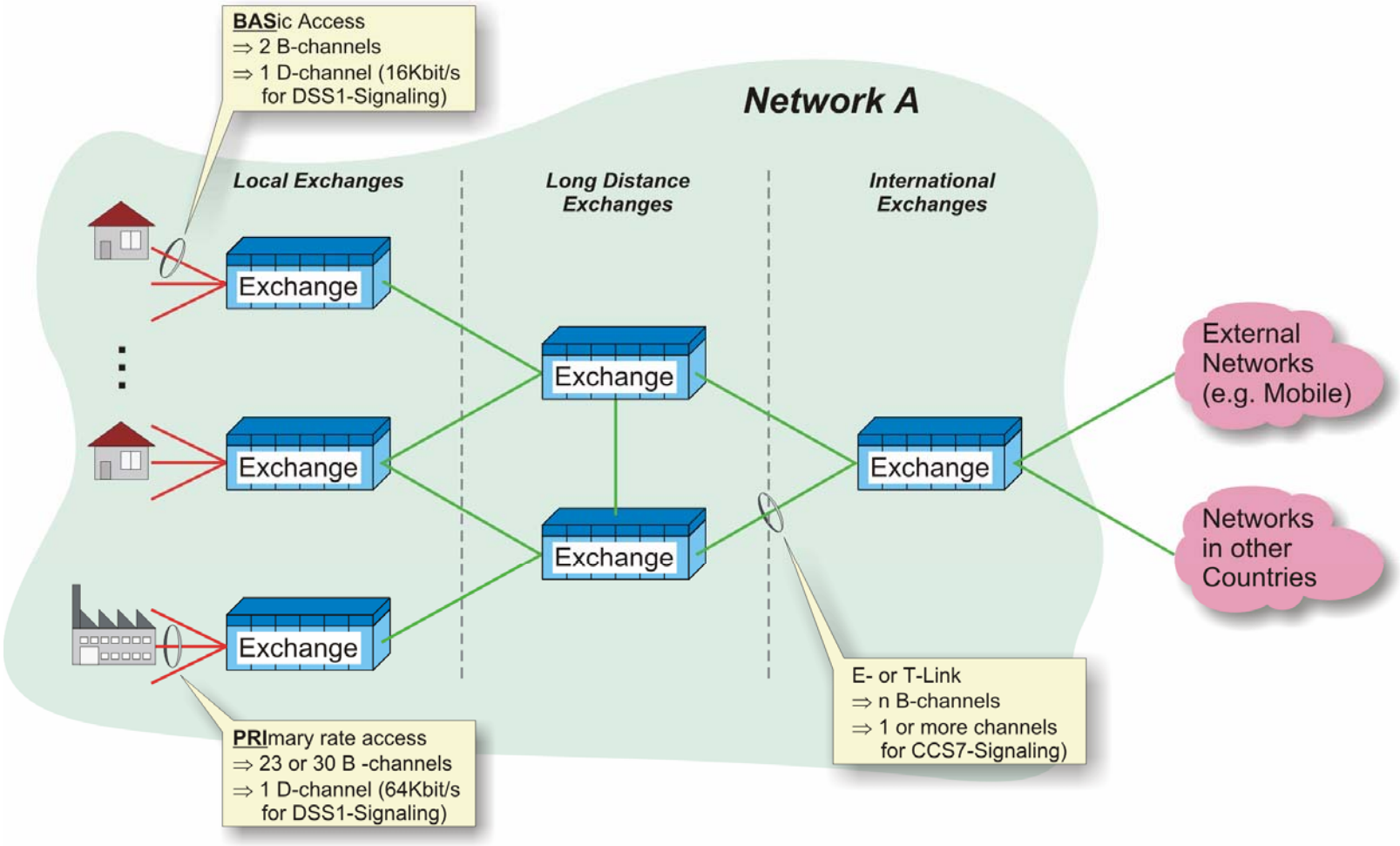
The Network Architecture in ISDN



The Network Architecture in ISDN

The figure illustrates the architecture of a typical ISDN / PSTN and the different interconnections towards users and foreign networks. The following specifics need to be emphasized:

- **Exchanges**
  The most important network elements are the exchanges which interconnect calling subscribers to one another. Exchanges are typically part of an overall hierarchy. The very exchanges that directly interconnect to the subscribers are called local exchange carriers (LEX) while other exchanges are responsible to route long distance calls or calls to external networks which may be inside or outside this country.
  The structure of an exchange will be illustrated on the following slides.

- **Basic Access Link**
  For residential subscribers, the typical choice is the provision of a basic access link (⇔ app. BAS) which offers two 64 kbit/s data channels for speech or data transmission plus one 16 kbit/s DSS1-signaling link (Digital Subscriber Signaling System No 1). The data channels are called B-channels while the signaling link is referred to as D-channel.

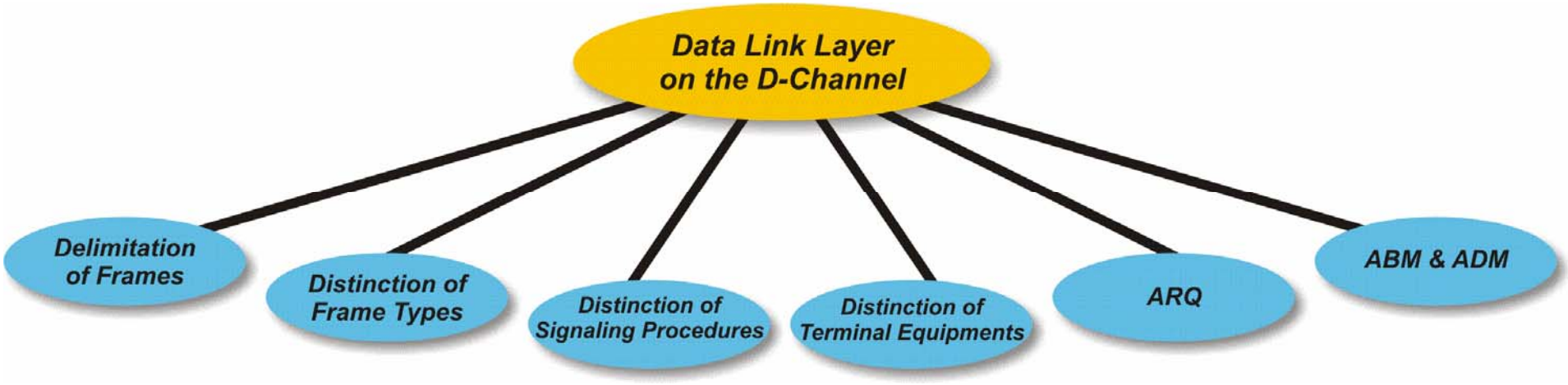
- **Primary Rate Access Link**
  For business subscribers which require more resources, ISDN offers a second type of access link called primary rate access link (abb. PRI). The primary rate access link offers 23 or 30 B-channels for data transfer and a 64 kbit/s D-channel for DSS1-signaling.

- **E- or T-Links**
  Between the exchanges, information transfer for both signaling information and data is performed on E- or T-links depending on the geographical location. E- and T-links are arranged in different hierarchy levels and offer throughput rates between 1.544 Mbit/s (⇔ T1-link) or 2.048 Mbit/s (⇔ E1-link) up to e.g. 139.264 Mbit/s (⇔ E4-link) in the plesiochronous digital hierarchy (PDH).

Note: Most remarkably about ISDN and CCS7 is the use of outband-signaling. Outband signaling relates to the fact that one timeslot is specifically designated (and wasted?) for the transfer of call control signaling information. Outband signaling has proven to be more efficient than inband signaling because not traffic resources are wasted during call setup and release.

The Data Link Layer on the D-Channel (Layer 2)

- **Tasks and Functions**



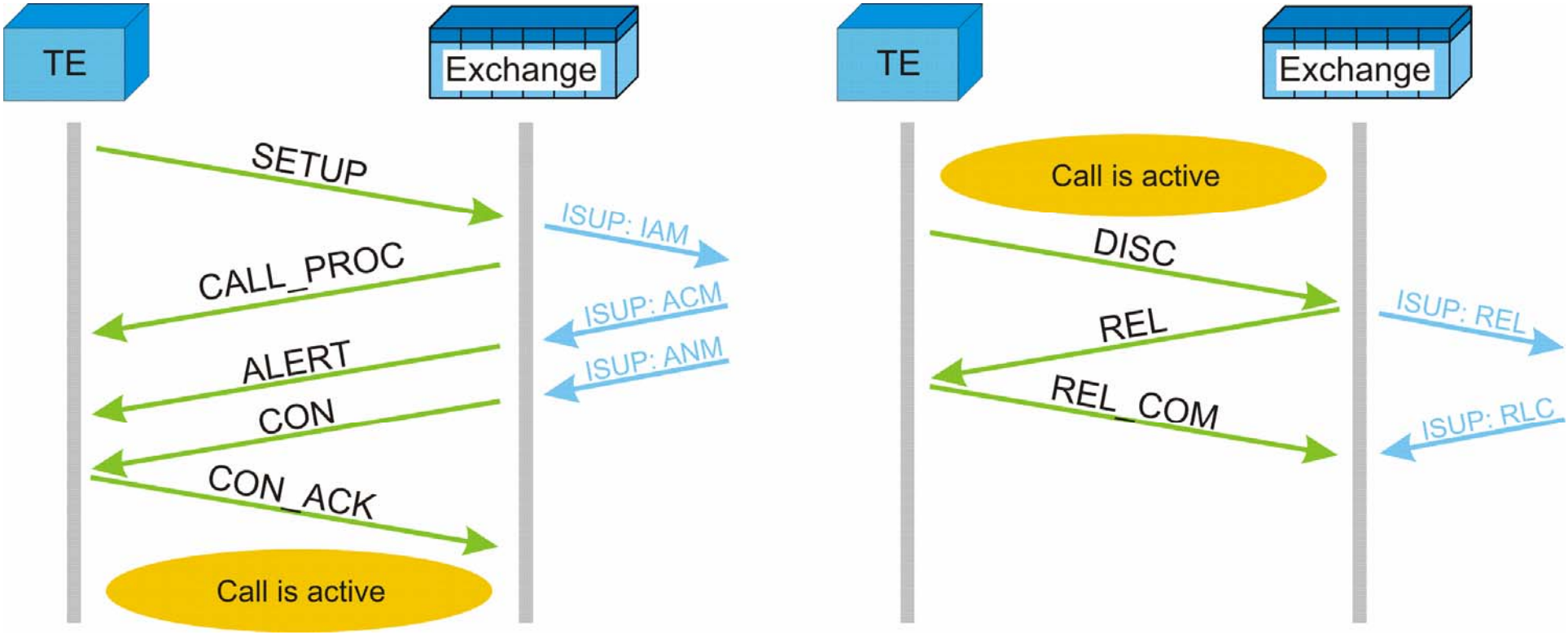
The Data Link Layer on the D-Channel (Layer 2)

Tasks and Functions

Note that most of the listed tasks and functions generally relate to the data link layer, not only on the ISDN D-channel.

- **Delimitation of Frames**
  One of the typical functions of the data link layer is the delimitation of consecutive signaling messages through specific bit sequences, called flags. In the ISDN-environment, there are start and end flags which are encoded with '0111 1110'$_{bin}$ / 7E$_{hex}$.
- **Distinction of Frame Types**
  Different frame types serve different functions. Through the assignment of different bit patterns for frame identification, the data link layer is able to provide a wide range of frame types which serve different tasks and functions (e.g. information transfer, connection management, supervision).
- **Distinction of Signaling Procedures**
  There may be signaling procedures related to e.g. layer 2-management, call control or packet data transmission on the D-channel (⇔ SAPI).
- **Distinction of Terminal Equipments**
  The data link layer provides means to distinguish the LAPD messages from and to the different terminal equipments through a numbering scheme (⇔ TEI).
- **ARQ (Automatic Repeat Request)**
  ARQ is another term for acknowledged mode operation. When ARQ applies, each information frame is numbered and needs to be acknowledged by the receiving peer.
- **ABM & ADM (Asynchronous Balanced Mode and Asynchronous Disconnected Mode)**
  The LAPD-protocol offers to modes of operation: connection-less and connection oriented. The default is connection-less which in case of LAPD automatically also means unacknowledged operation. Special signaling procedures are required to change the operation mode to connection-oriented in which each information frame needs to be acknowledged by the peer.

Basic Call Setup through Q.931 Signaling



Basic Call Setup through Q.931 Signaling

The figure illustrates a user originating call setup procedure between the terminal equipment and the exchange.

⇒ The procedure is initiated by the terminal equipment sending a SETUP-message to the exchange. This message contains the called party directory number plus a description of which bearer channel is requested (e.g. speech or data, 9.6 kbit/s, 64 kbit/s, ...).

⇒ The exchange will process this request internally. If everything appears to be correct and if sufficient information is available to process the call through CCS7 towards its destination, the exchange will reply a CALL_PROC-message (Call Proceeding) towards the terminal equipment.

⇒ Note that processing through CCS7 is done by the exchange sending an ISUP: IAM-message (Initial Address Message) towards the next exchange on the way to the dialed destination.

⇒ When the terminal at the peer is ringing, the exchange receives an ISUP: ACM-message (Address Complete) from the previous exchange. It will relay this information through an ALERT-message (Alerting) towards the calling terminal equipment. Consequentially, the calling terminal generates a ringing tone towards the user.

⇒ When the called party answers the call, the exchange receives an ISUP: ANM-message (Answer) from the previous exchange. It will relay this information as CON-message (Connect) towards the calling terminal equipment.

⇒ The calling terminal equipment confirms the successful call establishment by sending a CON_ACK-message (Connect Acknowledge) to the exchange. The call is now active.

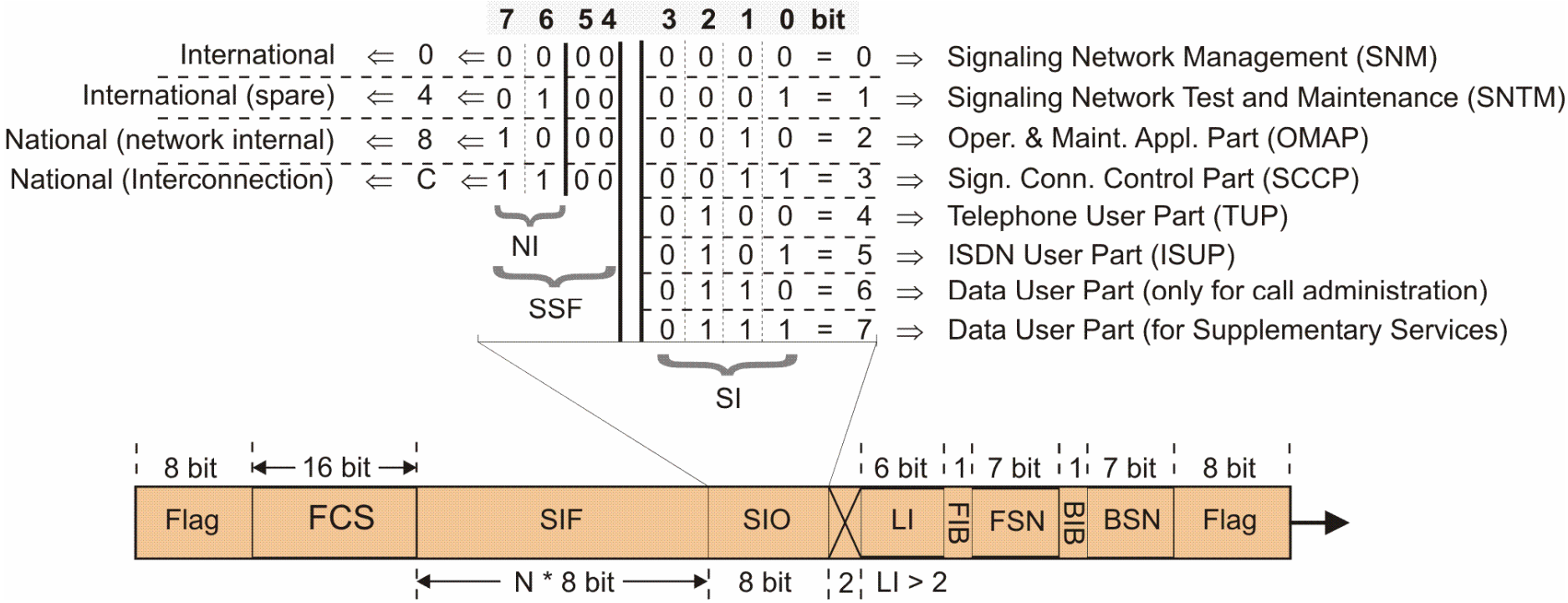
⇒ In our example, the calling party is also initiating the termination of the call. To do so, the terminal equipment sends a DISC-message (Disconnect) to the exchange. Note that this DISC-message must not be mistaken for the LAPD: DISC-message.

⇒ The exchange forwards the termination request to the next exchange through an ISUP: REL-message (Release) and replies a Q.931: REL-message (Release) to the terminal equipment.

⇒ The terminal equipment confirms the release of the resources by sending a REL_COM-message (Release Complete) to the exchange.

⇒ The following exchange will also confirm the call termination by sending an ISUP: RLC-message (Release Complete) to the serving exchange.

The Message Signal Unit (MSU)



The Message Signal Unit (MSU)

⇒ The MSU is the only signal unit which is used to convey higher layer information between two CCS7-peers. This data is placed into the SIF (Signaling Information Field) which has to have a length of a multiple of 8 bit after stuffing bits have been withdrawn. Note that the maximum length of the SIF is limited to 272 octets.

⇒ The header fields of the MSU equal those of the FISU with one important exception: The length indication is > 2. That is, any signal unit with a length indication > 2 is considered to be an MSU.

Note that the maximum SIF-length to be indicated through the 6 bit long LI-field is 63 octets although SIF-lengths up to 272 octets are legitimate. Therefore, a length indication LI = 63_{dec} indicates a SIF-length of 63 octets up to 272 octets. If the SIF-length exceeds 63 octets the absolute length of the SIF needs to be determined by the receiving party through counting the number of octets to the next flag and considering the FCS.

⇒ Between the header and the SIF there is the 8 bit long SIO (Service Information Octet).

⇒ Bit 0 – 3 of the SIO form the SI (Service Indicator). This SI indicates to which higher layer protocol (⇔ called the “user part”) the information in the SIF is destined. The figure illustrates the coding of SI for the various user parts.

⇒ Bit 4, 5, 6 and 7 of the SIO are called SSF (Sub-Service Field). In that respect, bit 4 and 5 of the SIO are spare bits which are encoded with ‘00’$_{bin}$. Note that these spare bits may be used for instance to indicate the relative priority of a national MSU (implementation option).

⇒ Bit 6 and 7 of the SIO form the NI (Network Indicator). Most importantly, the NI indicates whether an MSU is national or international. In both cases, two options exist. Further details about the use of the NI-field will be provided in a later section.

⇒ Behind the SIO there is the SIF (Signaling Information Field) with a maximum length of 272 octets. The SIF carries routing information for that MSU at its top (called routing label (later section)) and it carries the actual data which in turn consists of signaling information from higher layers.

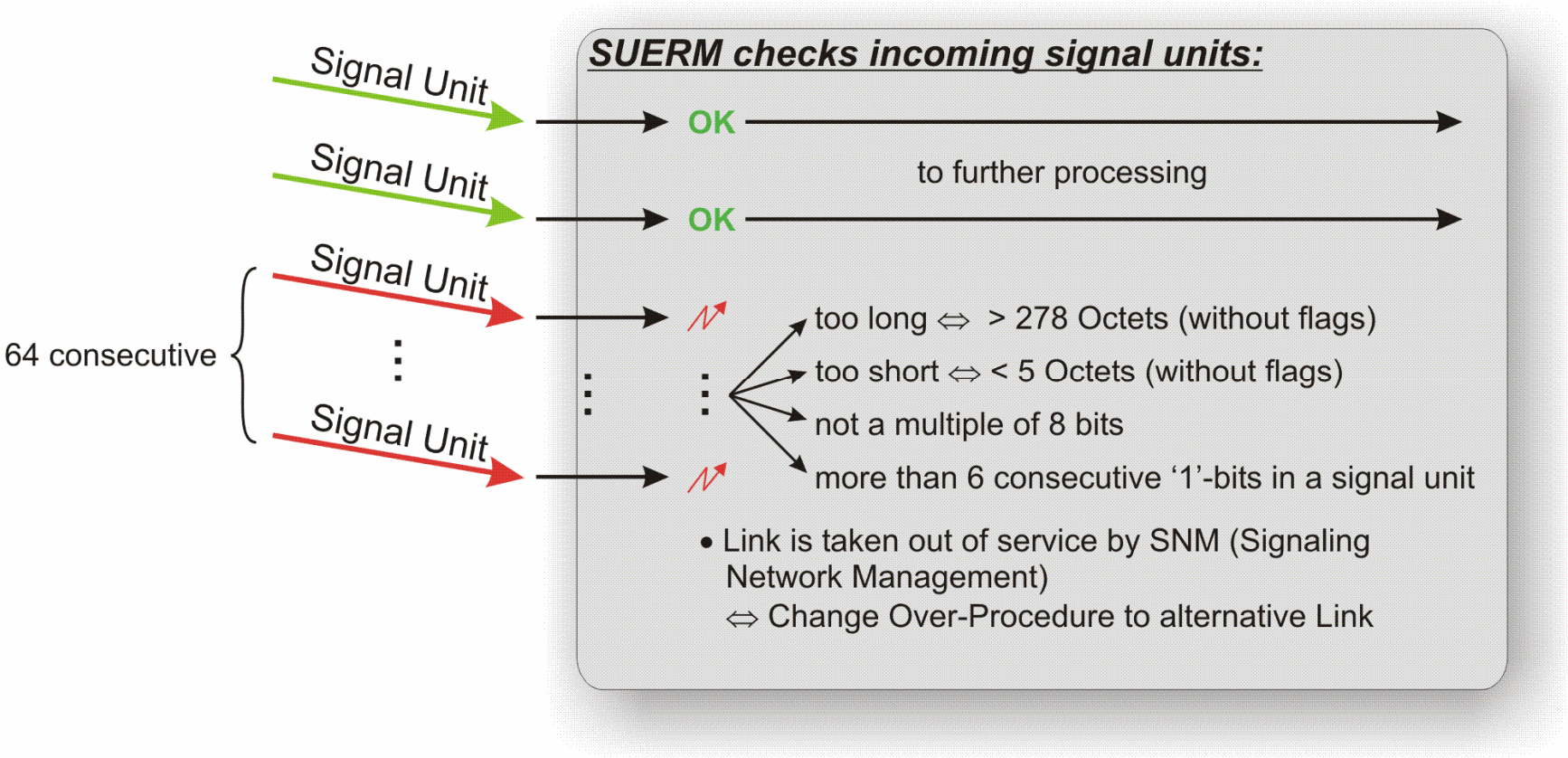
Accordingly, there is a maximum number of 268 octets of higher layer signaling data in one MSU. If the higher layer PDU (Protocol Data Unit) is longer, segmentation over more than one MSU is required and needs to be controlled by that higher layer.

⇒ Behind the SIF there is a 16 bit long FCS just like for the FISU.

⇒ The MSU ends with the end flag which usually is the start flag of the following signal unit.

[ITU-T Q.703 (2.2)]

The Signal Unit Error Rate Monitor (SUERM)



The Signal Unit Error Rate Monitor (SUERM)

⇒ On the previous slides, signal units were checked with respect to random bit errors that may have occurred during transmission. Another problem that may occur is an unstable link that entirely garbles the transferred signal units.

⇒ For instance, it may be impossible to determine the end of a signal unit because the end flag is missing. Another error may be that additional bits have been stuffed into the transmitted signal units.

⇒ In all of these cases, the CRC-check won't be able to detect a problem. That is the reason why the SUERM has been introduced as mandatory part of the MTP 2.

⇒ The SUERM will prove every incoming signal unit with respect to consistency. Consistency relates to following characteristics:

- **Is the signal unit too long or too short? The maximum length of a signal unit without flags is 278 octets and the minimum length without flags is 5 octets**
- **Are there sequences of more than six '1'-bits in the bit stream before the stuffed '0'-bits have been deleted?**
- **Is there a multiple of 8 bit between the start flag and the end flag after the stuffed '0'-bits for signal unit delimitation have been deleted?**

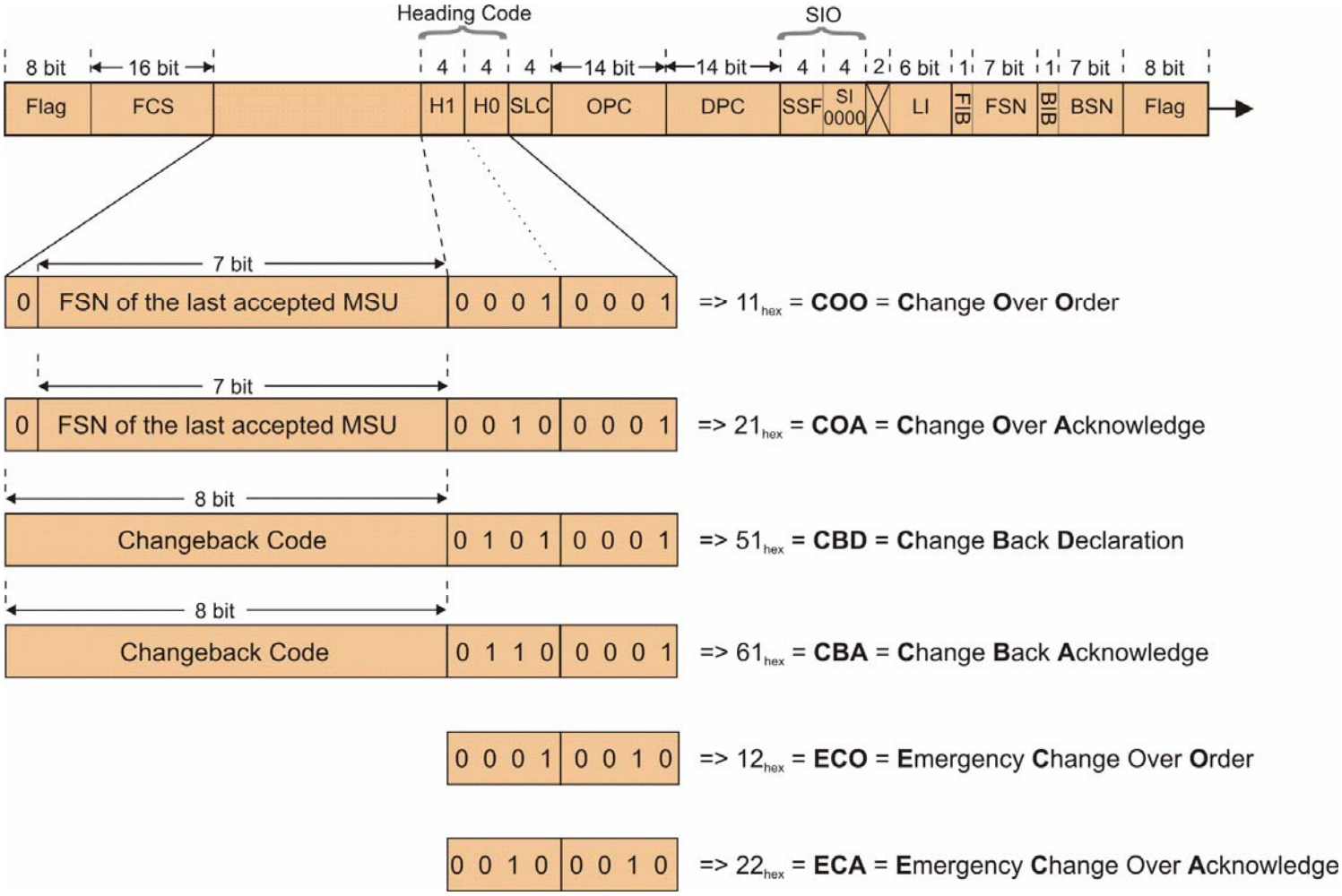
⇒ Whenever 64 consecutive signal units are found in error by the SUERM, the SUERM will take two actions:

- The SUERM will take that CCS7-link out of service. This is done through the transmission of an LSSU-SIOS signal unit to the peer CCS7-entity.
- The SUERM will inform the SNM-layer (Signaling Network Management) that the CCS7-link is out of operation.

Consequentially, the SNM-layer will perform a "Change Over" of the CCS7-signaling traffic from the faulty link to the alternative link through the COO-procedure (Change Over Order procedure) which will be dealt with in the next chapter.

[ITU-T Q.703 (4.1), (10.2)]

(1) Format, Meaning and Use of SNM-Messages



(1) Format, Meaning and Use of SNM-Messages

COO (Change Over Order)
The COO-message is used by SNM to automatically divert CCS7-traffic from a congested, blocked or erroneous CCS7-link to an alternative CCS7-link. The SLC-field in the routing label contains the identification of the very link that is unavailable. The data field includes the FSN of the last MSU that was correctly received from the CCS7-entity to which the COO-message is sent (and which therefore does not need to be retransmitted).

COA (Change Over Acknowledge)
The COA-message acknowledges the reception of the COO-message and the change over operation. The data part contains the FSN of the last accepted MSU from the perspective of the CCS7-entity which sends the COA-message (hence the FSN's in the COO and the COA will be different). Note that the CCS7-entity which sends the COA-message may instead send an ECA-message, if the FSN of the last correctly received MSU cannot be determined.

CBD (Change Back Declaration)
The CBD-message is used by SNM to redirect the diverted CCS7-signaling traffic back to a restored CCS7-link. The routing label contains the SLC of the very CCS7-signaling link which has been restored. The change back code contains a random number to be allocated by the transmitting CCS7-entity. The same change back code shall be used by the responding peer in the CBA-message.

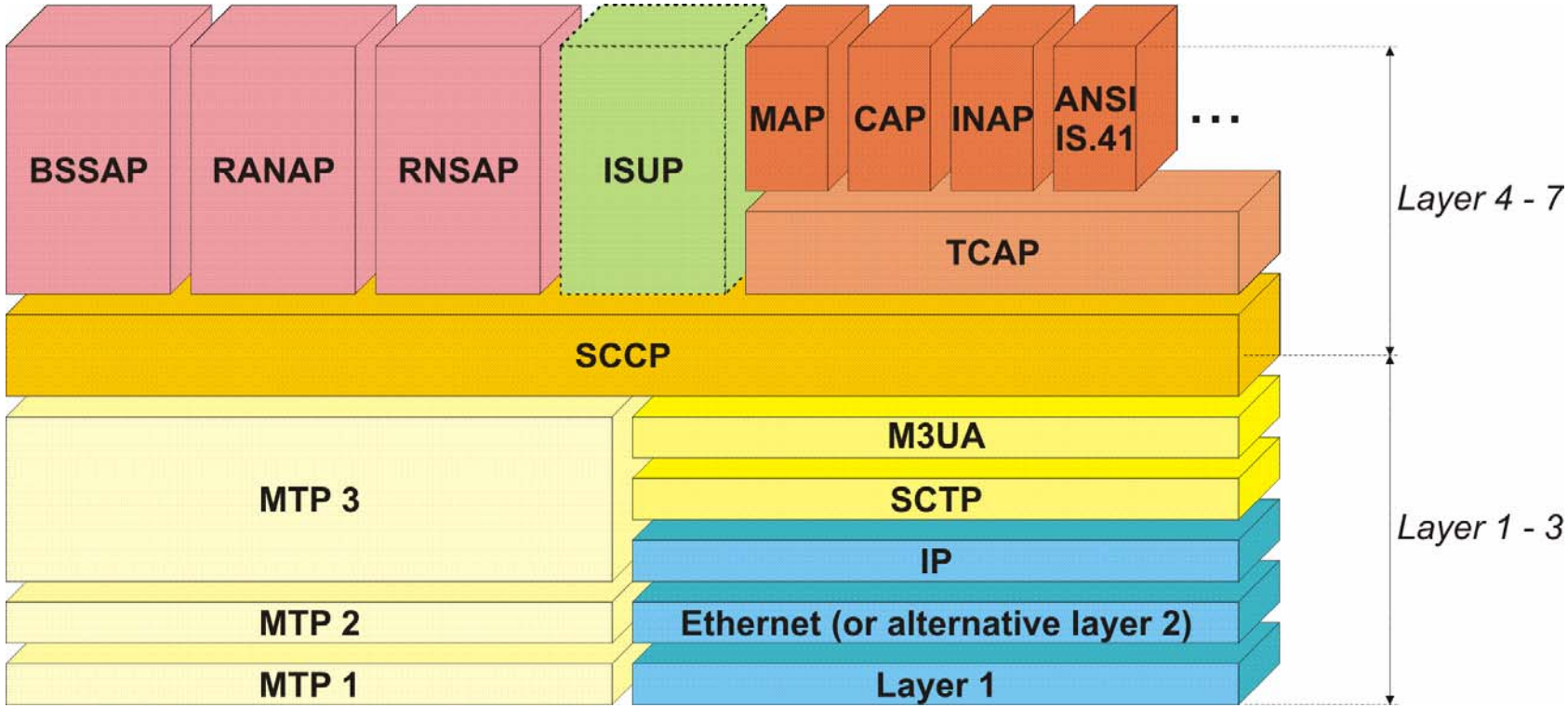
CBA (Change Back Acknowledge)
The CBA-message acknowledges the reception of the CBD-message and the execution of the change back operation.

ECO (Emergency Change Over Order)
The ECO-message is used instead of the COO-message to initiate a change over procedure, if the initiating peer is not able to determine the FSN of the last correctly received MSU (e.g. due to an internal software failure or due to congestion). Like the COO-message, the ECO-message contains the SLC of the faulty CCS7-link as part of the routing label. The receiving peer shall perform the change over procedure and continue to transmit MSU's starting with the first not yet transmitted MSU (hence it is left to higher layers to recover from possible MSU-losses).

ECA (Emergency Change Over Acknowledge)
The ECA-message is a correct response on a COO-message or an ECO-message, if the sending CCS7-entity is unable to determine the FSN of the last correctly received MSU (e.g. due to an internal software failure or due to congestion).

[ITU-T Q.704 (15)]

The SCCP in the CCS7-Protocol Stack



The SCCP in the CCS7-Protocol Stack

To allow for a quick overview of the SCCP in the CCS7-protocol environment, the figure on the graphics slide has been provided:

Underlying Protocols

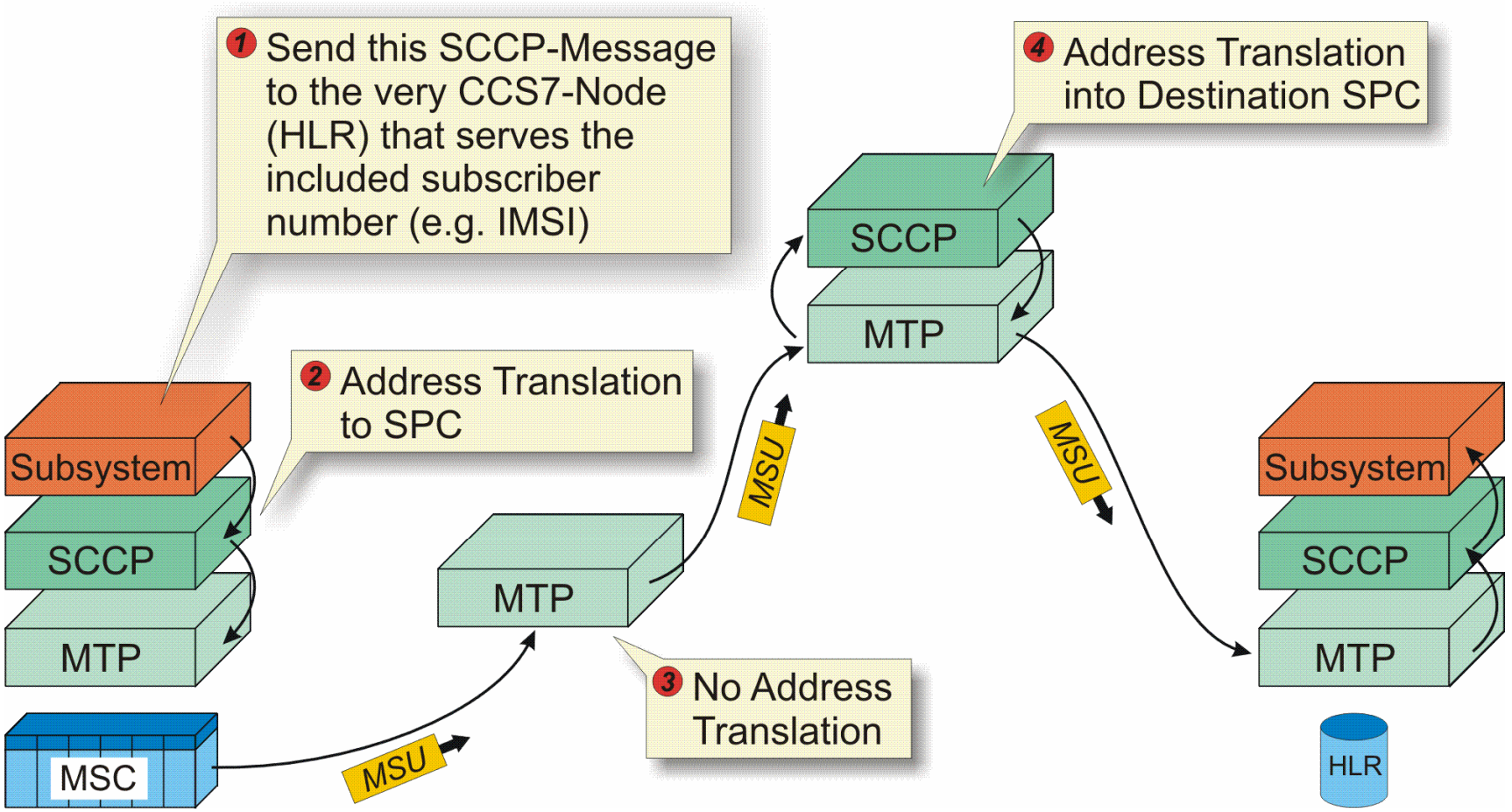
Traditionally and still predominantly, the SCCP uses the MTP 1 – 3 as underlying bearer. However, with the ever increasing availability of IP-networks, there was the demand to standardize an IP-based transport protocol suite for the SCCP.
This demand was suited by the IETF through the definition of the two protocols SCTP (Stream Control Transmission Protocol) and M3UA (MTP 3 User Adaptation Layer) which emulates the MTP 1 – 3 bearer towards the SCCP.

It is essential to fully comprehend that even the internet can now be used as bearer for the SCCP. And since the SCCP is the bearer for many applications like subscriber authentication in mobile networks or like intelligent networking, there is no more demand for an underlying CCS7-network for this and other sophisticated functions.

Application Protocols

Various different application protocols rely on the services that are offered by the SCCP. In GSM-networks, the communication between the MSC and the BSS's is achieved through the BSSAP-protocol which resides on the SCCP. Likewise, UMTS introduces RANAP for the communication between MSC and RNC and RNSAP for the communication between RNC's.
In addition, the ISUP may use the services of the SCCP for call establishment and release. This method has been defined in addition to the pass-along method (which is the default method) and comes with the advantage that the path of the signaling messages is independent from the data path. Despite this advantage, ISUP is usually residing on top of the MTP and that is why ISUP on top of the SCCP is presented in dotted lines.
Last but not least to be mentioned are all protocols that themselves require the dialog and discussion services of the TCAP-protocol. Those are namely the MAP-protocol (Mobile Application Part), the CAP-protocol (Camel Application Part), the INAP-protocol (Intelligent Network Application Part) and the IS.41-protocol which is comparable to MAP but which is used in North American mobile networks.

Use of the SCCP for End-to-End Addressing

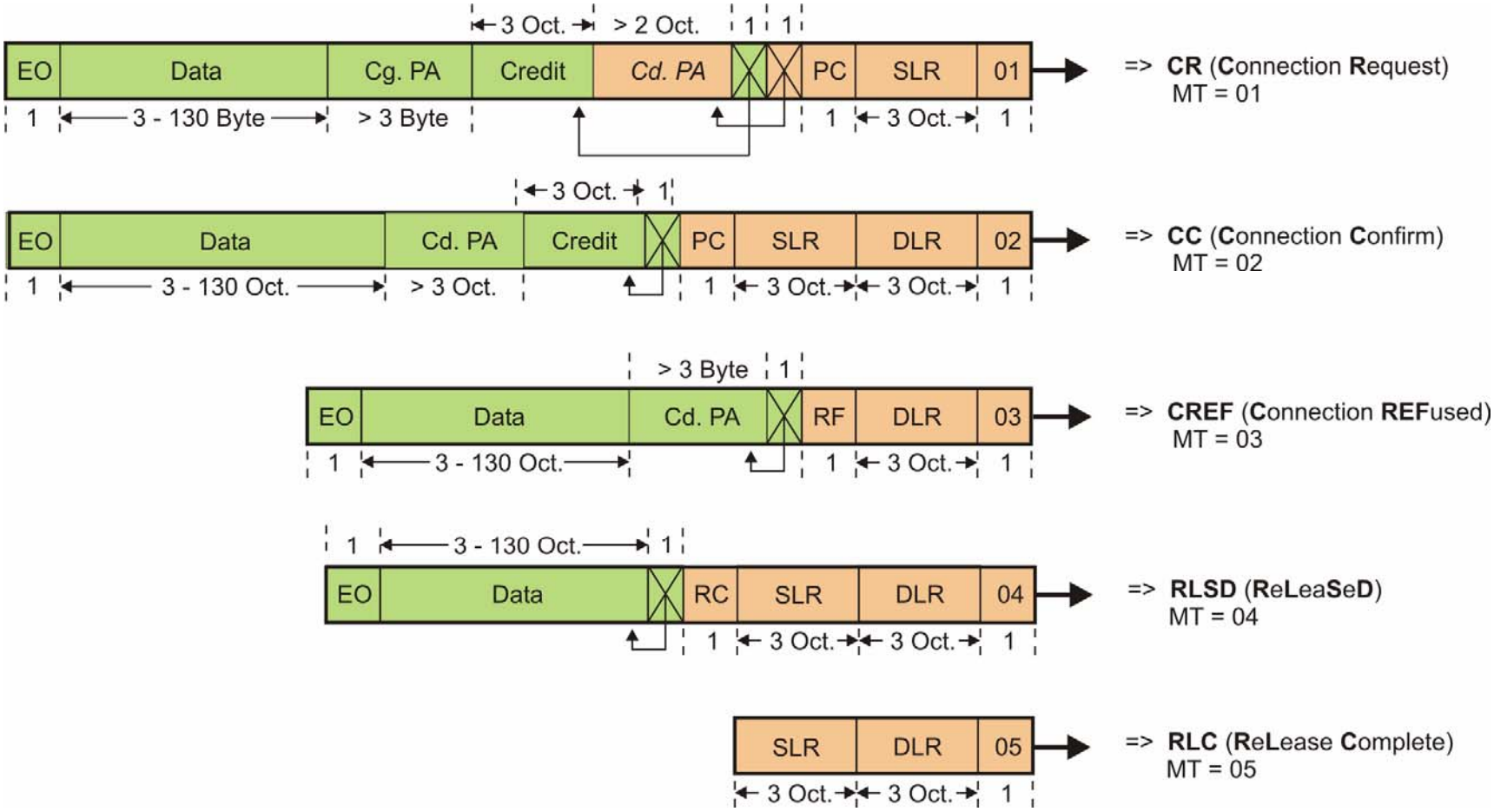


Use of the SCCP for End-to-End Addressing

To provide for end-to-end addressing between SCCP-applications around the world that have no knowledge of their SPC's, the SCCP is able to translate and process almost any kind of identification number in its 'called party address' information field.
Translation relates to the interpretation of the 'called party address' and its conversion into the SPC of the very CCS7-node on the shortest path to the final destination.
An example is illustrated on the graphics page:

1. The SCCP-subsystem receives a user data PDU from its application layer (from one of its subsystems, in this case from the MSC). As indicated, this PDU also contains routing information for the SCCP in the form of a subscriber identification number (e.g. IMSI).
2. The SCCP will perform its address translation function. As illustrated, the SCCP may not necessarily be able to translate the subscriber number into the SPC of the destination HLR. Still, the translation function will translate the provided subscriber identification number into the very CCS7-node with SCCP-layer that should be able to match the subscriber identification number to the SPC of the destination HLR.
3. In the intermediate CCS7-node without SCCP-layer, the MSU with the embedded SCCP-message is transparently routed through.
4. In the intermediate CCS7-node. With SCCP-layer, the SCCP-layer will evaluate the SCCP-address information (called party address) and translate it a second time after the MSC already did it before. This time, the translation of the subscriber identification number results in the SPC of the final destination HLR.

(1) Important SCCP-Message Types



(1) Important SCCP-Message Types

CR (Connection Request)
The CR-message is used by an SCCP-node to establish a virtual connection for a specific transaction towards another SCCP-node. The SLR (Source Local Reference) identifies the virtual connection in the transmitting SCCP-node, the PC (Protocol Class) identifies protocol class 2 or 3. C (Credit) will only be included in case of protocol class 3 and includes the window size. The Cg. PA (Calling Party) identifies the source of the message. The EO-octet is the EOC-octet (‘00’).

CC (Connection Confirm)
The CC-message confirms the establishment of a virtual connection which was initiated through the reception of a CR-message. The DLR (Destination Local Reference) identifies the virtual connection within the receiving SCCP-node, the SLR identifies the connection in the SCCP-node that sends the CC-message. The other parameters are explained under CR-message.

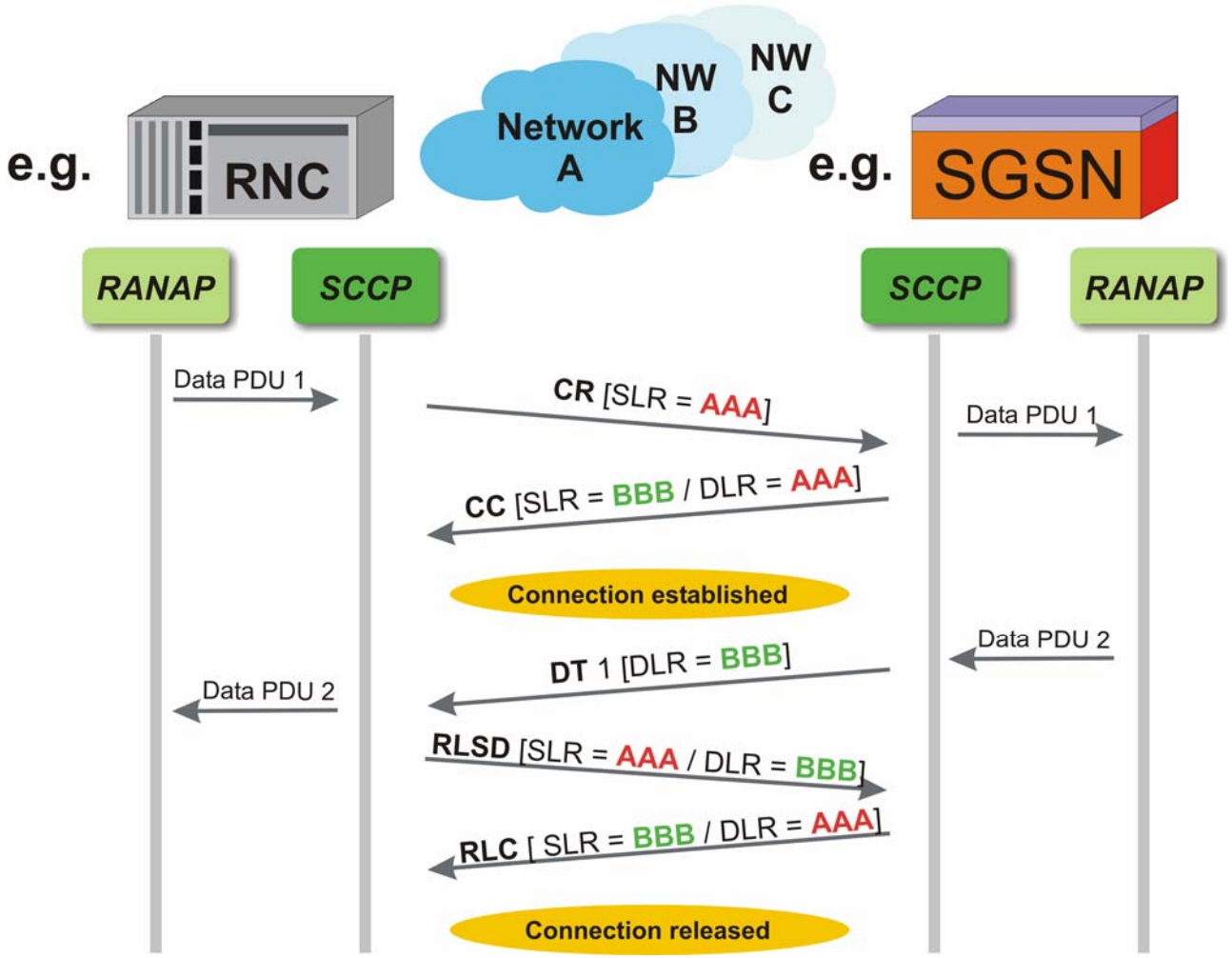
CREF (Connection Refused)
The CREF-message is used to reject the attempt for virtual connection establishment. RF (Refusal Cause) contains more information why the connection establishment is not done.

RLSD (Released)
Through the transmission of a RLSD-message, an SCCP-node initiates the termination of an existing SCCP-connection. RC (Release Cause) contains more information about the reason for release.

RLC (Release Complete)
The RLC-message is the response for a RLSD-message. It confirms the termination of an existing SCCP-connection.

[ITU-T Q.712 (1), ITU-T Q.713 (4)]

SCCP Connection-Oriented Operation Using SLR and DLR



SCCP Connection-Oriented Operation Using SLR and DLR

The figure illustrates through an example how the connection establishment in SCCP works and how it is based on the allocation of SLR (Source Local Reference) and DLR (Destination Local Reference).

SLR and DLR are unformatted numbers and have a length of 3 octets. The SLR of one peer is the DLR of the other peer.

- **Connection Establishment / Allocation of SLR and DLR**
  - ⇒ Whenever a peer (in this case the RNC on the left side) is required to establish an SCCP connection to another peer (in this case the SGSN on the right side), it will issue a CR-message to that peer. This CR-message contains the SLR = AAA as allocated by the RNC.
  - ⇒ When the receiving SGSN is willing and able to confirm the connection establishment request of the RNC, it will allocate its own SLR = BBB and transmit it within a CC-message back to the RNC. Note that the CC-message contains the DLR = AAA. That is: The SLR from the RNC's perspective is the DLR from the perspective of the MSC.
  - ⇒ With the reception of the CC-message by the RNC, the connection is established and higher layer data PDU's can be exchanged. Note that CR- and CC-messages may also contain data but the embedded PDU's must not exchange the maximum data field length of the CR- or CC-message because segmentation is not possible.
- **Data Transfer Phase**
  - ⇒ During the data transfer phase, each SCCP-node uses the SLR of the peer to transmit DT1-messages (or DT2-messages) to that peer which is related to a specific connection. The SLR of the peer is contained in the DT1-message (or DT2-message) as DLR.
  - ⇒ This allows the receiving peer to relate an incoming DT1-message (or DT2-message) to one out of many simultaneous connections.

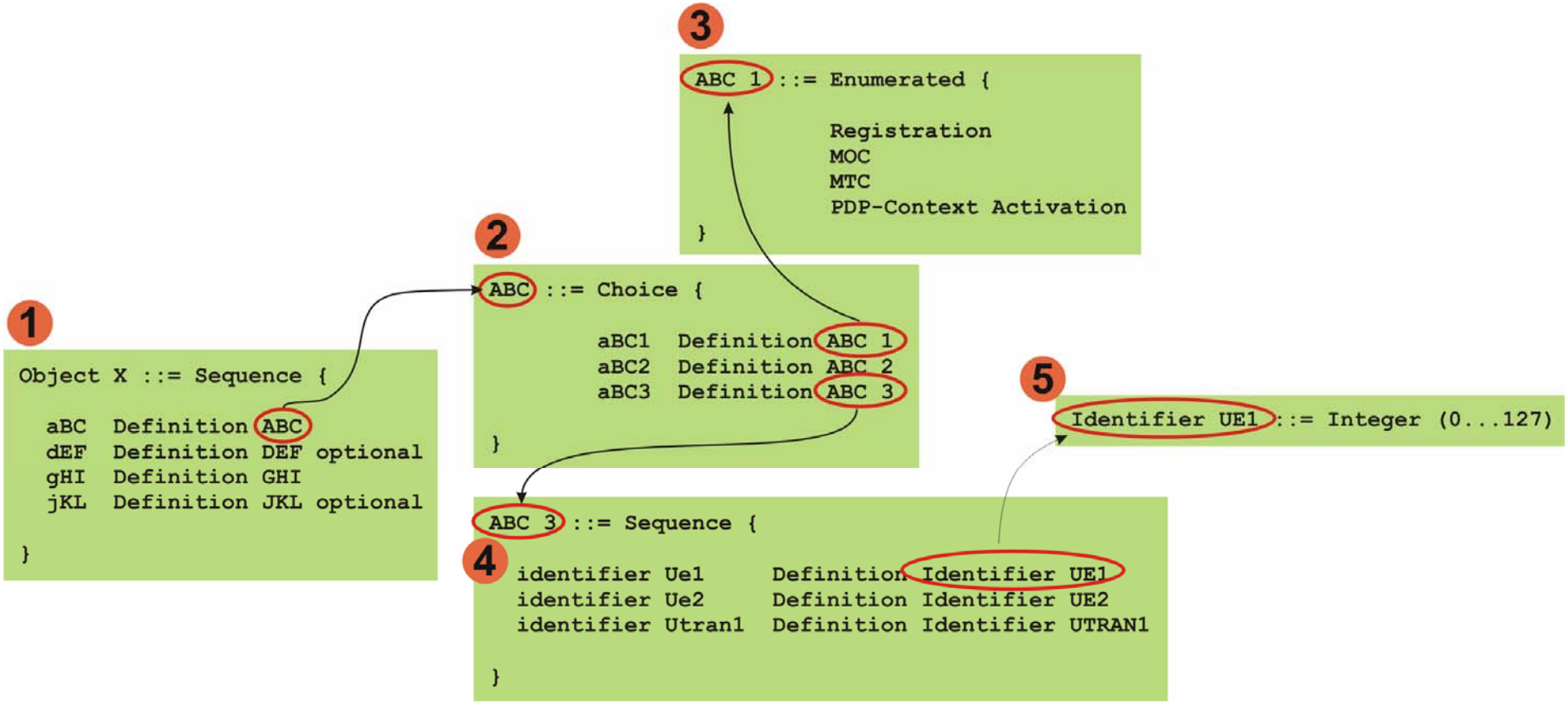
Note that neither DT1- nor DT2-messages contain the SLR from the perspective of the sender. To view both local reference numbers in one message, the CC-, RLSD- or RLC-message needs to be found in a recording file.

- **Connection Release / De-Allocation of SLR and DLR**
  - ⇒ When no more signaling data has to be transmitted (e.g. the call has been released by one user), one SCCP-node will initiate SCCP-connection release by sending a RLSD-message to its peer. In our example, the RNC initiates the connection release procedure.
  - ⇒ The requested peer shall reply with a RLC-message.

Consequentially, both local reference numbers are available again for the next connection.

Encoding of TCAP-Messages – Introducing ASN.1

- **ASN.1: Basic Encoding Rules (BER)**



Encoding of TCAP-Messages – Introducing ASN.1

: Basic Encoding Rules (BER)

Nested Information Elements
The most important hint for the interpretation of ASN.1 code is illustrated in the figure: ASN.1 uses a hierarchical description form. One information element is nested into another which again may be nested into another information element which …

ASN.1 Types
The figure illustrates only a fraction of the different description types that ASN.1 is using. For a complete listing please refer to the respective standards (see references underneath).

The Sequence Type
The sequence type describes which information elements together form an information element. In the figure, Object X (⇔ point (1)) consists of the IE's ABC, DEF, GHI and JKL. Note that DEF and JKL are indicated as being optional. The figure also illustrates that ABC3 (⇔ point (4)) is again a sequence of different identifiers.

The Choice Type
The choice type is a "one out of many" descriptor. In the example (⇔ point (2)), the IE ABC is a choice of either ABC1 or ABC2 or ABC3. Only one can be present as ABC in Object X.

The Enumerated Type
The enumerated type provides a simple identifier for something. In the figure (⇔ point (3)), ABC1 is either registration = 1 or MOC = 2 or MTC = 3 or PDP-Context-Activation = 4. Only one these values will be included in the message.

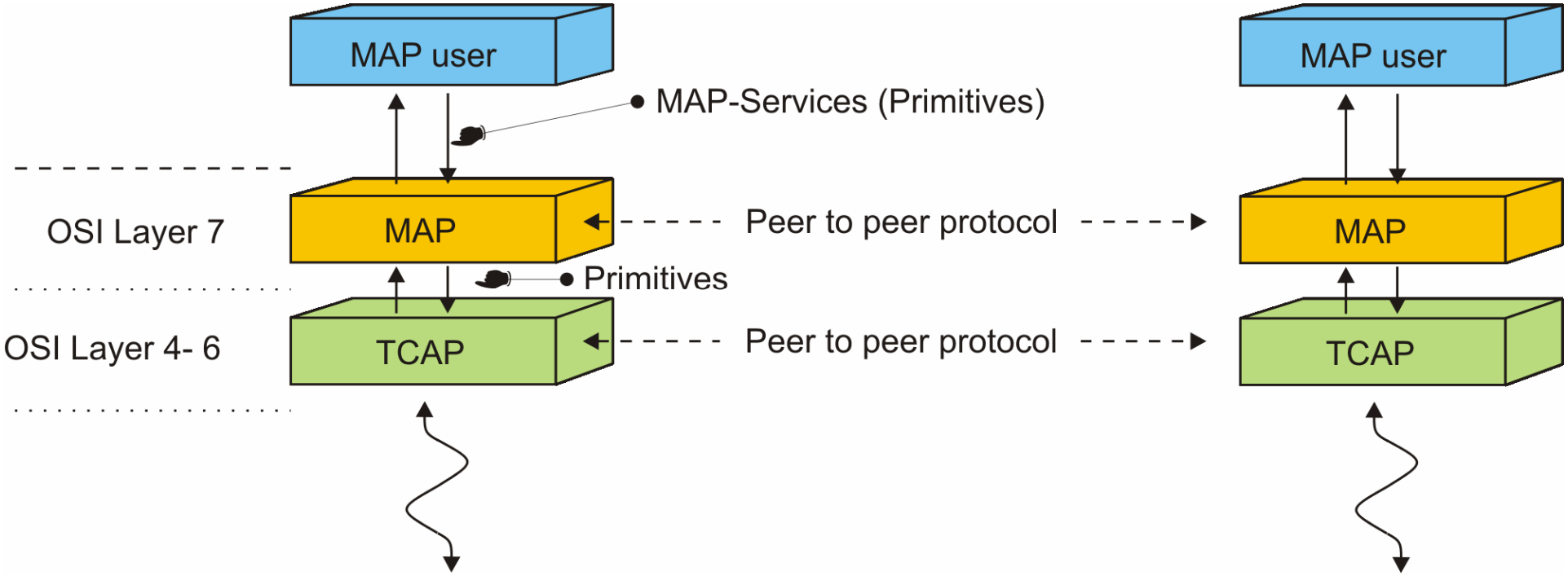
Value Assignment
In the figure (⇔ point (5)), IdentifierUE1 is assigned an integer value with a range between '0' and '127'$_{dec}$.

Note: ASN.1 encoding is used in various GSM- and UMTS-protocols like MAP, NBAP, RANAP and RNSAP but also by other protocols like H.248 for media gateway control or H.323 for multimedia call control.

[ITU-T X.680, X.681]

Communication between MAP and Application

- **General Aspects**



Communication between MAP and Application

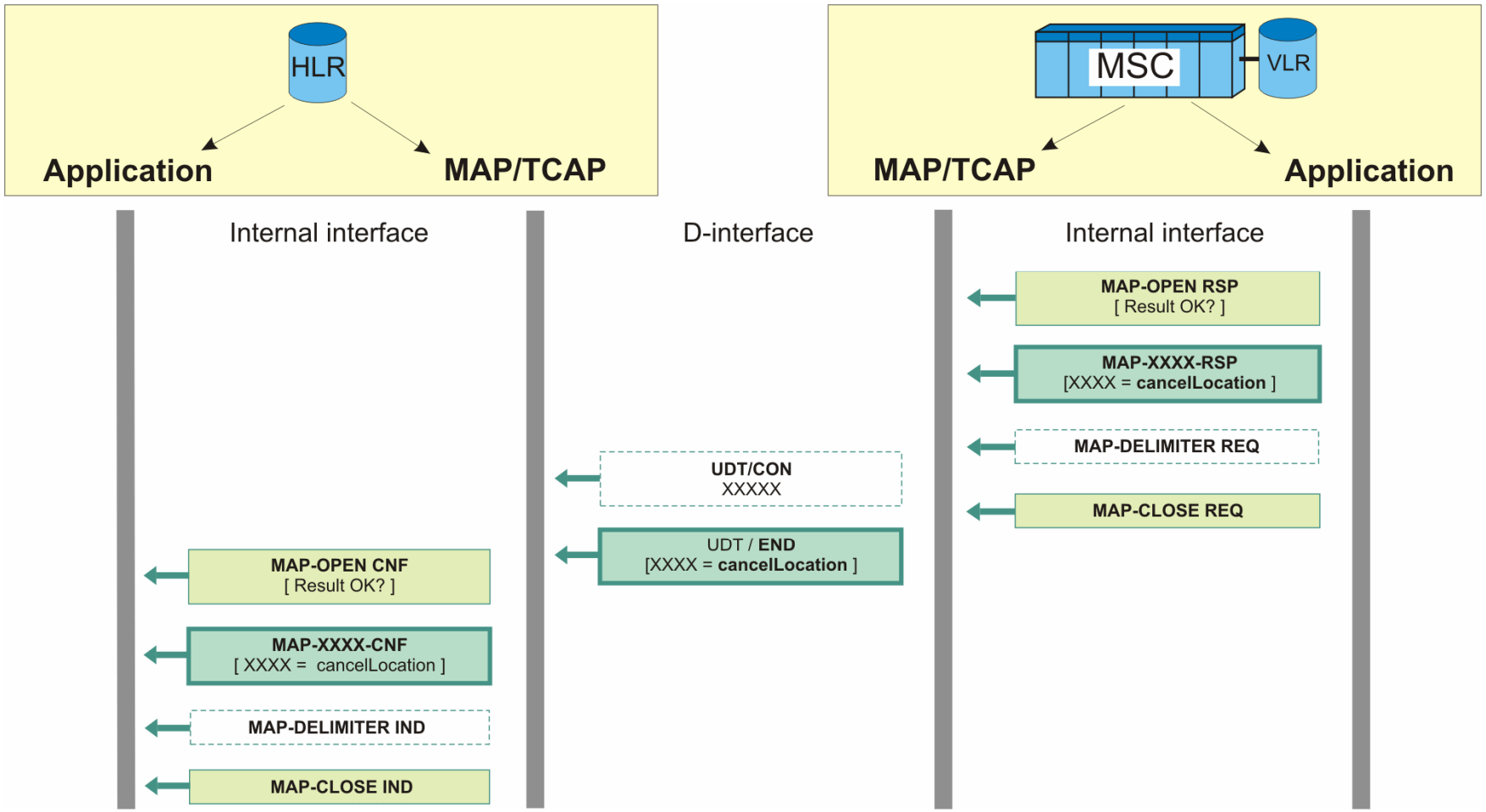
General Aspects

The communication between the MAP-layer in OSI-layer 7 and its application outside the OSI-reference is somewhat different to any other protocol that we have been dealing with yet.
As the figure illustrates, this communication is not horizontal but vertical. These vertical messages are in general called primitives. In the case of MAP they are called MAP-services.

Note that MAP distinguishes common and special MAP-services.

[3GTS 29.002 (7)]

(2) Example



(2) Example

- ⇒ After processing of the received indication, the VLR itself needs to invoke the transmission of a response TCAP-message towards the HLR. Accordingly, it will start the related MAP-operation by sending a MAP-OPEN-RSP primitive to MAP.
- ⇒ Afterwards, the related parameters for the component portion are conveyed to MAP in the MAP-XXXX-RSP primitive. The MAP-XXXX-RSP primitive is related to the MAP-XXXX-IND primitive through the Invoke-ID.
- ⇒ Whether or not a MAP-DELIMITER-REQ is sent to MAP, depends on whether the dialogue shall be finished through the upcoming response message or not. The MAP-DELIMITER-REQ will only be sent, if the dialogue shall not be finished (⇔ if a CON-message shall be sent).
- ⇒ In our case, the dialogue is indicated to be closed by the VLR sending a MAP-CLOSE-REQ primitive to MAP.
- ⇒ The reception of the MAP-CLOSE-REQ-primitive triggers the transmission of the TCAP: END-message towards the HLR. In turn, the reception of this TCAP-message by the HLR results in the transfer of a MAP-OPEN-CNF primitive by MAP towards the HLR-application. The received component follows in a MAP-XXXX-CNF-primitive.
- ⇒ The dialogue is terminated with the reception of the MAP-CLOSE-IND primitive.