# SS7

- ITU-T Common Channel Signalling System No. 7 (CCSS7, CCS7, CCS, CCS#7, C7, SS7 …)
- At present the dominant inter-exchange signalling system in digital networks (PSTN, ISDN, PLMN)
- SS7 is in effect a robust, high-performance packet switched network, intended for secure transmission of signalling messages
- ITU-T Q.700-series Recommendations

Channel-associated signalling (CAS)

Old form of signalling (has mostly been replaced by SS7)
Signalling occurs in-band on voice channels

signalling possible   *signalling not possible*

circuit switched connection
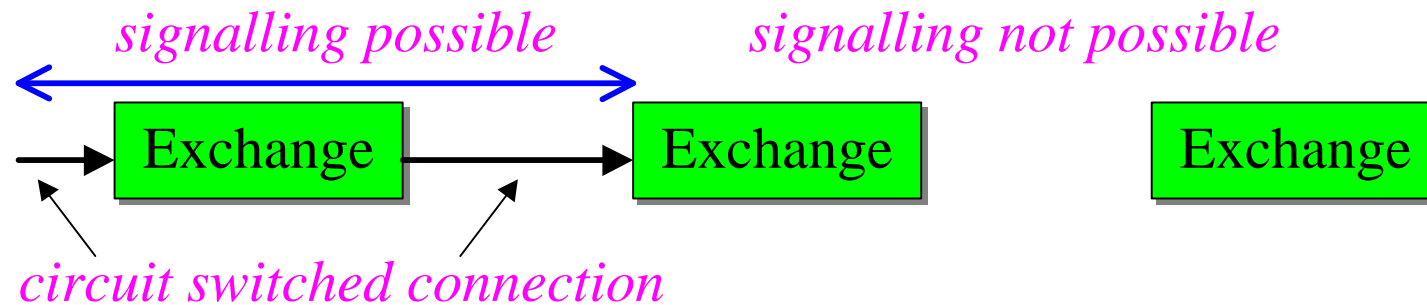
Before a circuit switched connection exists, end-to-end
signalling between originating and terminating local
exchanges (or to/from databases) is not possible

Common channel signalling (CCS)

Modern form of signalling (SS7 is based on this method)

Signalling occurs out-of-band on dedicated channels

signalling possible anywhere anytime

```
      ┌───────────┐        ┌───────────┐        ┌───────────┐
  ───►│ Exchange  │───────►│ Exchange  │        │ Exchange  │
      └───────────┘        └───────────┘        └───────────┘
```

Uses a separate packet-switched signalling network which is not related to circuit switched connections

End-to-end signalling between originating and terminating local exchanges (or to/from databases) is possible anytime

Common channel signalling (CCS)

Faster call setup times - compared to in-band signalling using multi-frequency (MF) signalling tones

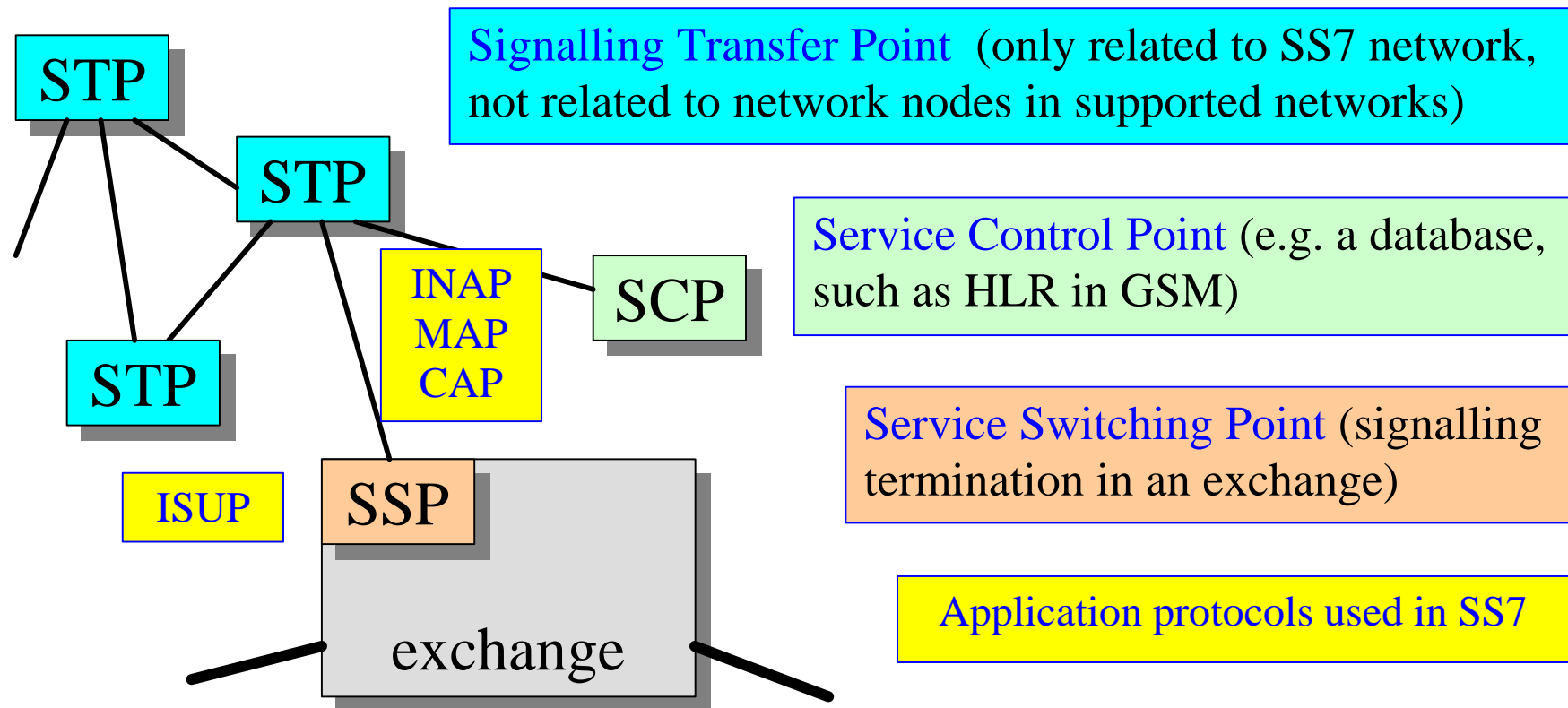More efficient use of voice circuits

Support for Intelligent Network (IN) services which require signalling to network elements (e.g., database systems) without the use of circuit switched connections

Support for ISDN-type supplementary services which require end-to-end signalling between terminals (or local exchanges)

Improved control over fraudulent network usage

Signalling points (SP) in SS7

Every SP is identified by a signalling point code (SPC)

STP

STP

Signalling Transfer Point (only related to SS7 network, not related to network nodes in supported networks)

STP

INAP
MAP
CAP

SCP

Service Control Point (e.g. a database, such as HLR in GSM)

Service Switching Point (signalling termination in an exchange)
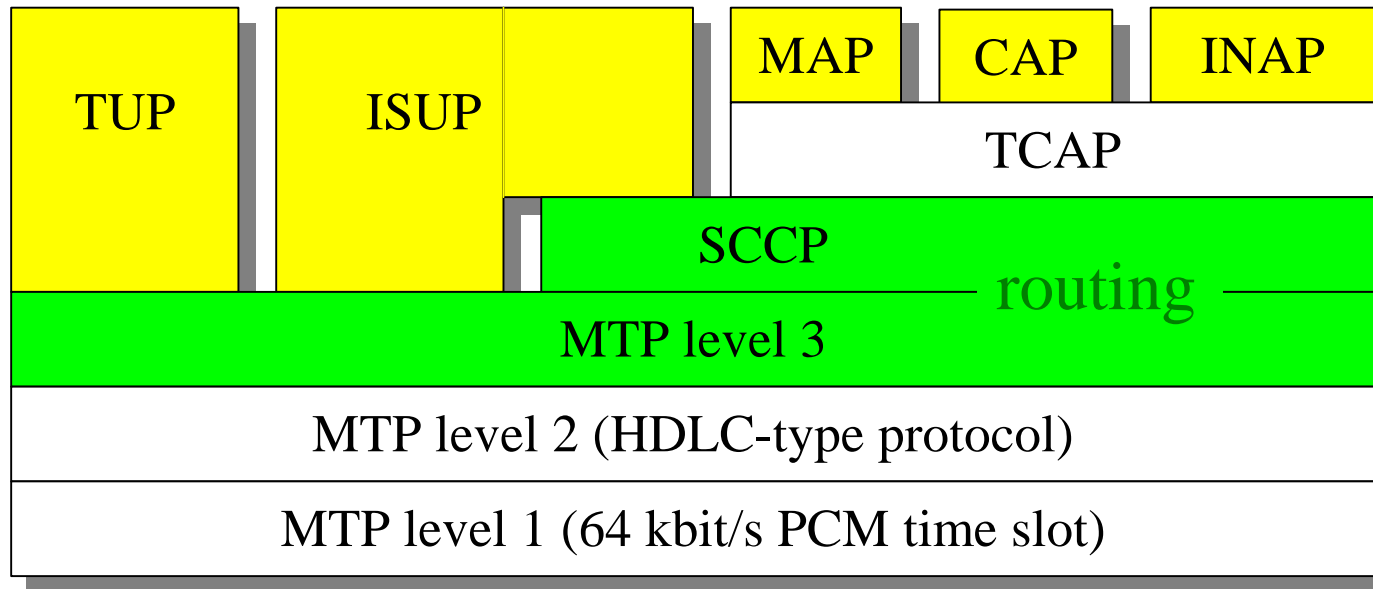
ISUP

SSP

exchange

Application protocols used in SS7

Significance of SSP and SCP

During the processing of a circuit switched call, an SSP (Service Switching Point) in an exchange may be triggered to retrieve various switching related information (number analysis, time, location, security, charging...) from an SCP

Thus, the SCP (Service Control Point) provides information necessary for advanced call-processing capabilities

The usage of SSP and SCP depends on which IN (Intelligent Network) features a network operator has implemented (and which IN features the user has subscribed to).

Protocol layers ("levels") of SS7

MTP - Message Transfer Part
SCCP - Signalling Connection Control Part
UP - User Part   AP - Application Part

Application protocols in SS7

TUP (Telephone User Part) – is being replaced by ISUP

ISUP (ISDN User Part) – for all signalling related to management of circuit switched connections

MAP (Mobile User Part) – for transactions between exchanges (MSC, GMSC) and databases (HLR, EIR, AuC...) in mobile networks

INAP (Intelligent Network Application Part) – for IN applications in fixed networks

CAP (CAMEL Application Part) – for extended IN functionality in mobile networks

CAMEL = Customised Applications for Mobile networks Enhanced Logic

MTP functions

MTP level 1 (signalling data link level):
   Physical transmission in a 64 kbit/s PCM time slot.

MTP level 2 (signalling link level):
   HDLC-type frame-based protocol for flow control, error control (using ARQ), and signalling network supervision and maintenance functions.

MTP level 3 (signalling network level):
   Used for routing in the signalling network (OPC $\Leftrightarrow$ DPC) between SPs with level 4 users (see SIO at level 2).
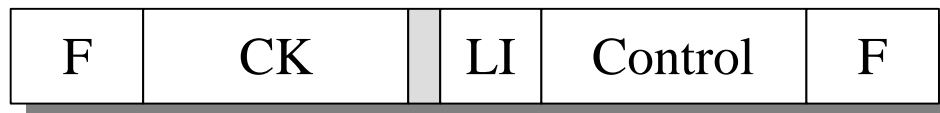
MTP level 2 frame formats

MSU (Message Signal Unit)

F	CK	SIF	SIO		LI	Control	F

Level 3 signalling message

LSSU (Link Status Signal Unit)

F	CK	SF		LI	Control	F

FISU (Fill-In Signal Unit)

F	CK		LI	Control	F

Network:
National network(s)
International network

User part:
TUP
ISUP
SCCP
Network management

MTP level 2 frames

MSU (Message Signal Unit):
- Contains signalling messages (User Part ? $\Leftrightarrow$ SIO)
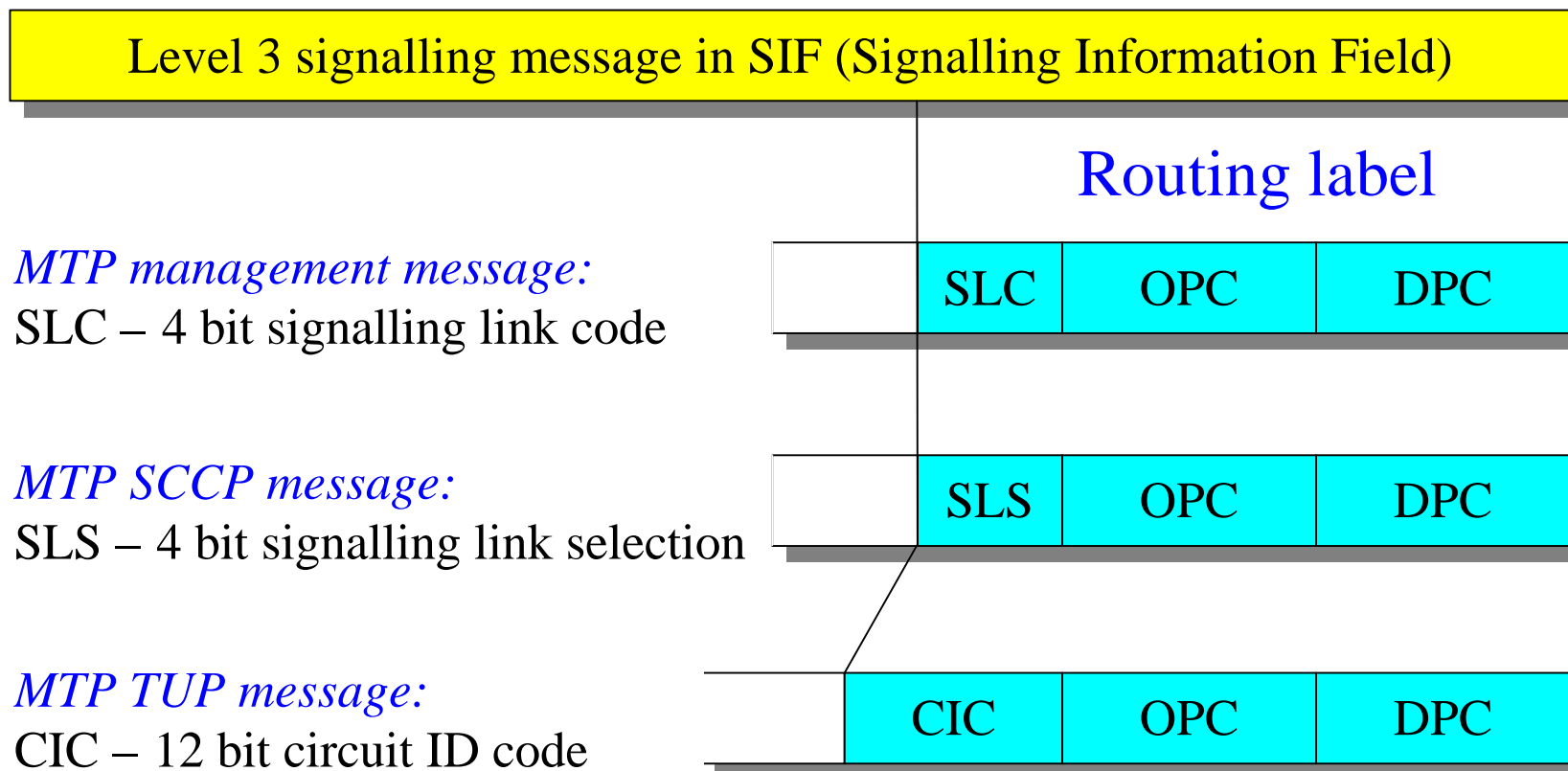- The received frame is MSU if LI > 2 (number of octets)

LSSU (Link Status Signal Unit):
- Contains signalling messages for link supervision
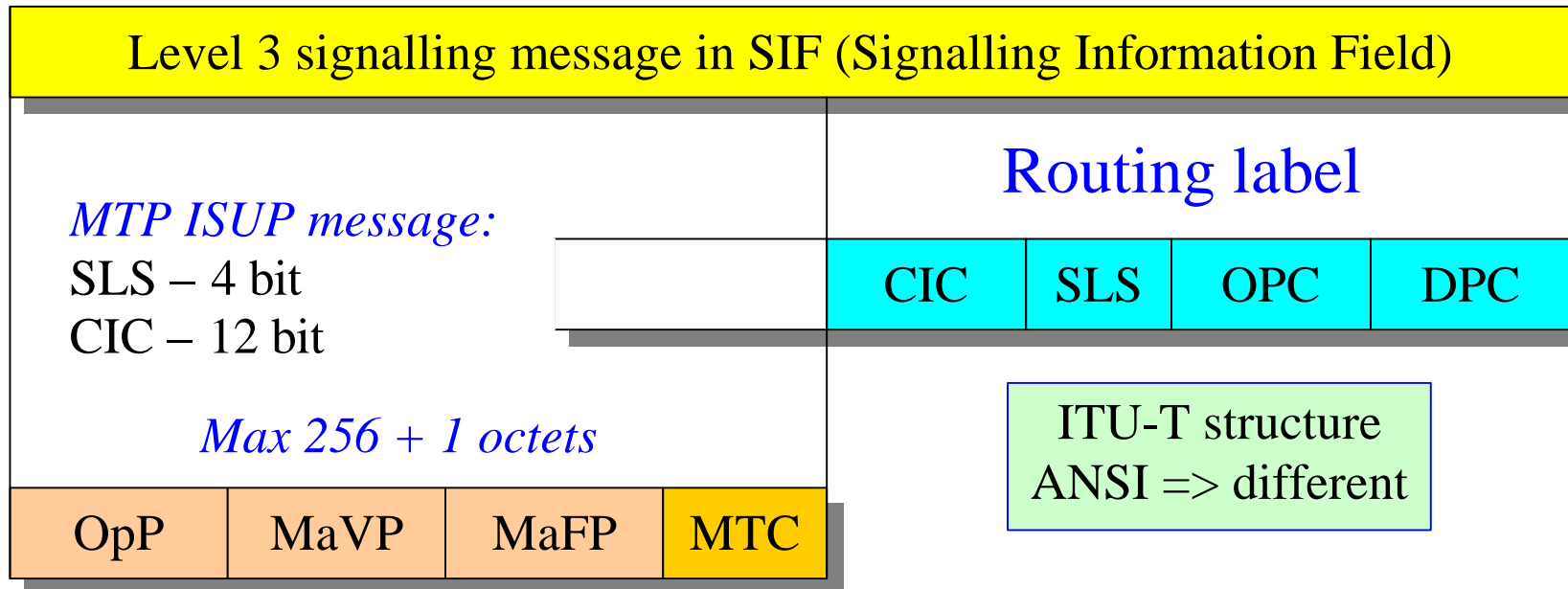- The received frame is LSSU if LI = 1 or 2

FISU (Fill-In Signal Unit):
- Can also be used to monitor quality of signalling link
- The received frame is FISU if LI = 0

Routing through SS7 network

Level 3 signalling message in SIF (Signalling Information Field)

Routing label

MTP management message:
SLC – 4 bit signalling link code

SLC	OPC	DPC

MTP SCCP message:
SLS – 4 bit signalling link selection

SLS	OPC	DPC

MTP TUP message:
CIC – 12 bit circuit ID code

CIC	OPC	DPC

Routing through SS7 network

Level 3 signalling message in SIF (Signalling Information Field)

Routing label

MTP ISUP message:
SLS – 4 bit
CIC – 12 bit

Max 256 + 1 octets

CIC	SLS	OPC	DPC

ITU-T structure
ANSI => different

OpP	MaVP	MaFP	MTC

MTC – Message Type Code (name of ISUP message)
MaFP – Mandatory Fixed Part (no LI, no parameter names required)
MaVP – Mandatory Variable Part (LI, no parameter names required)
OpP – Optional Part (LI and parameter names required)

Difference between SLS and CIC

SLS defines the signalling link used for transfer of signalling information.

CIC defines the circuit (used for a certain circuit switched connection) with which the ISUP message is associated.
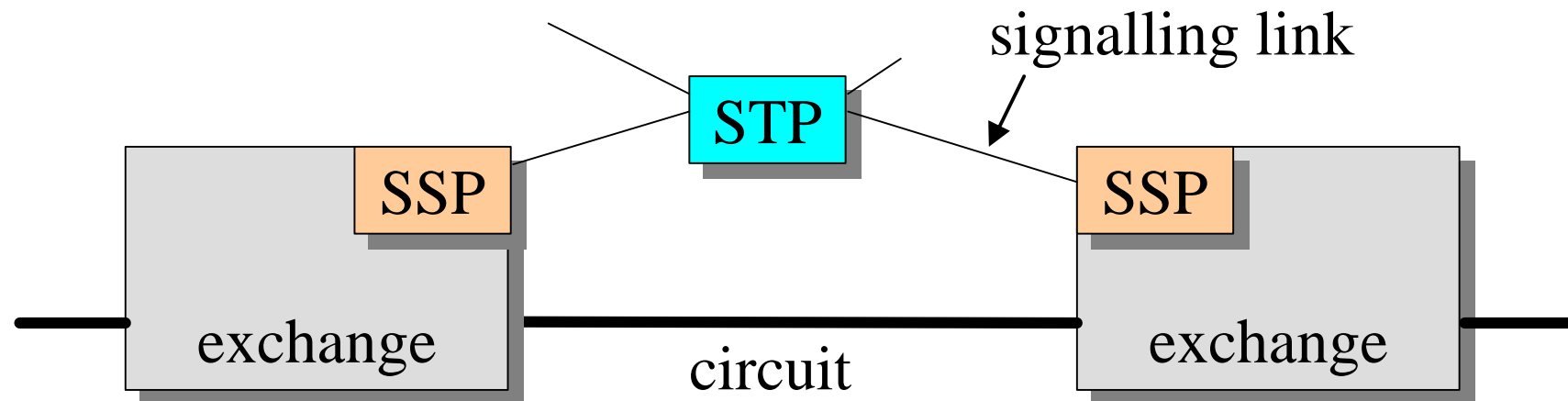
Role of DPC and OPC in SS7

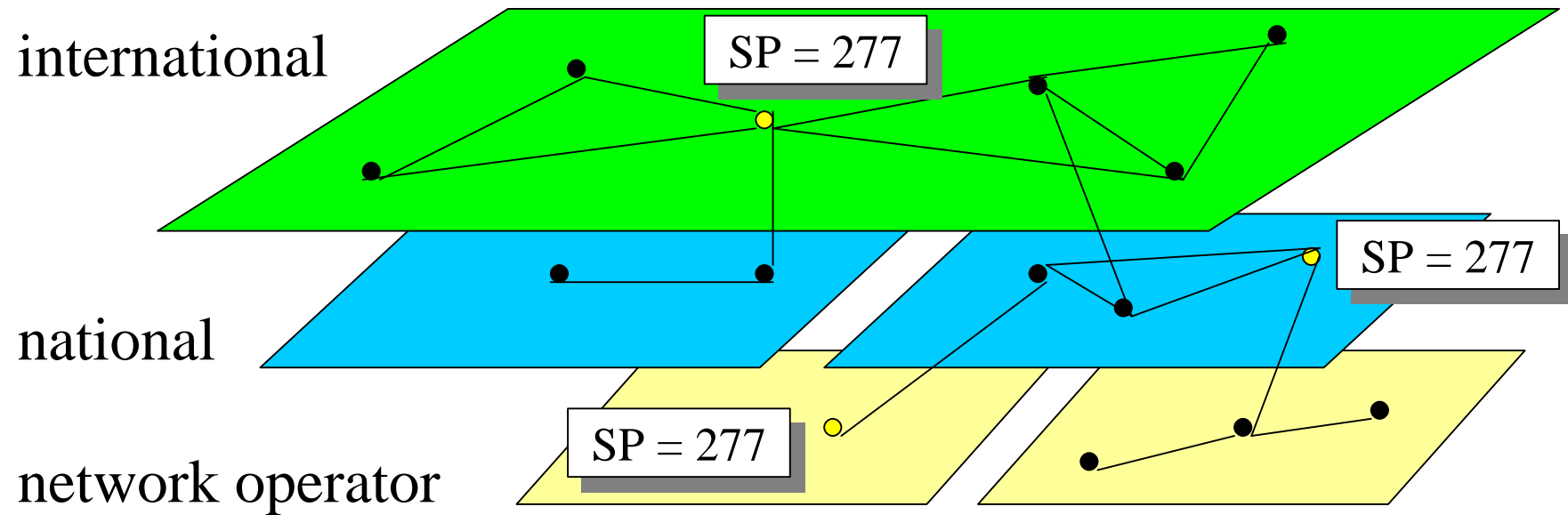*DPC – Destination Point Code* (14 bit ⇔ 16384 SPs)
- Global termination point of application transaction
- Key information for routing within SS7 network
- The DPC is inserted by the originating MTP "user".

OPC – Originating Point Code (14 bit)
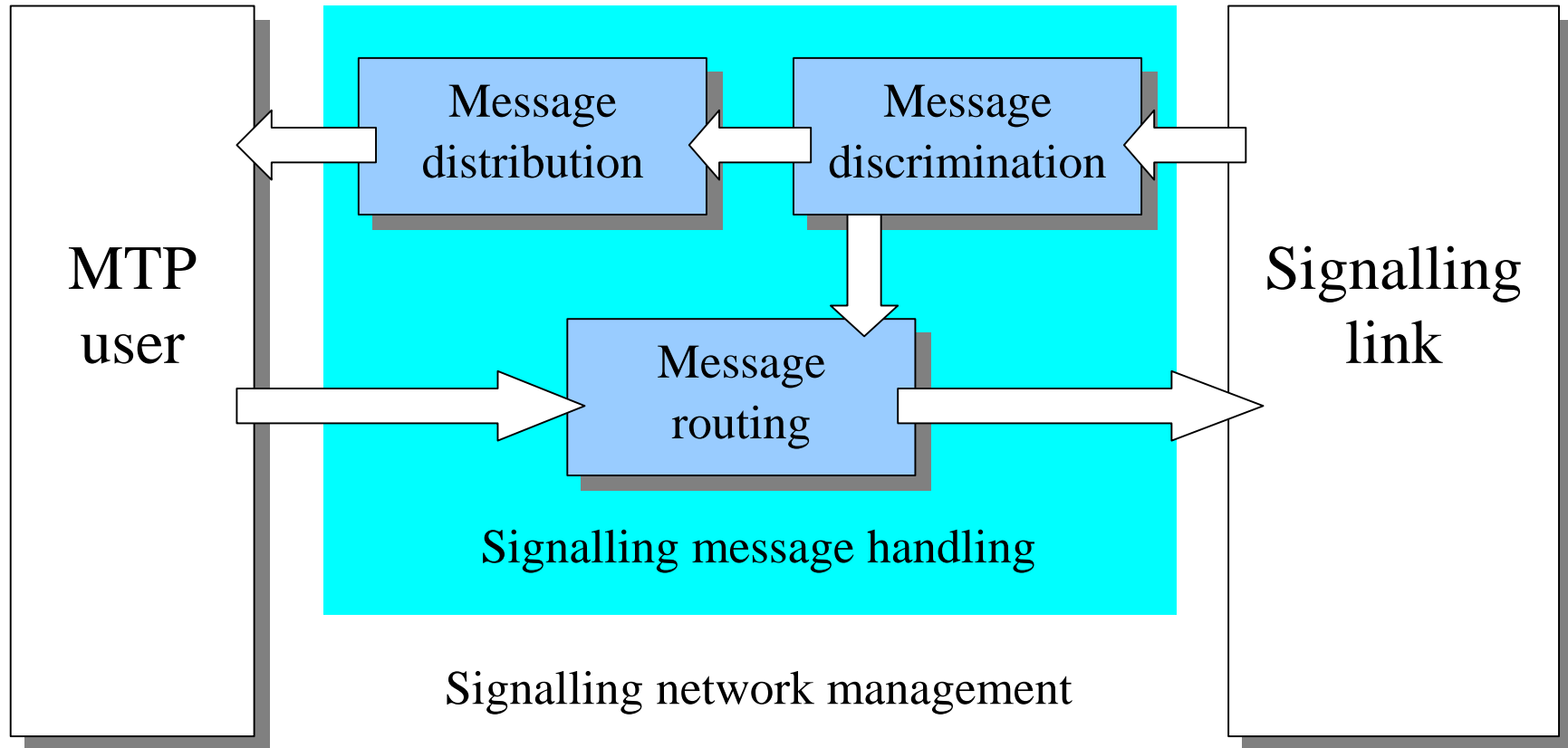- Global originating point of application transaction

The "network indicator" in the SIO octet determines whether the DPC or OPC is an international, national, or network dependent SP identifier.

Same signalling point codes can be reused at different network levels

international

SP = 277

SP = 277

national

SP = 277

network operator

Signalling network functions

MTP user

Message distribution

Message discrimination

Signalling link

Message routing

Signalling message handling

Signalling network management

ISUP
Integrated Services User Part

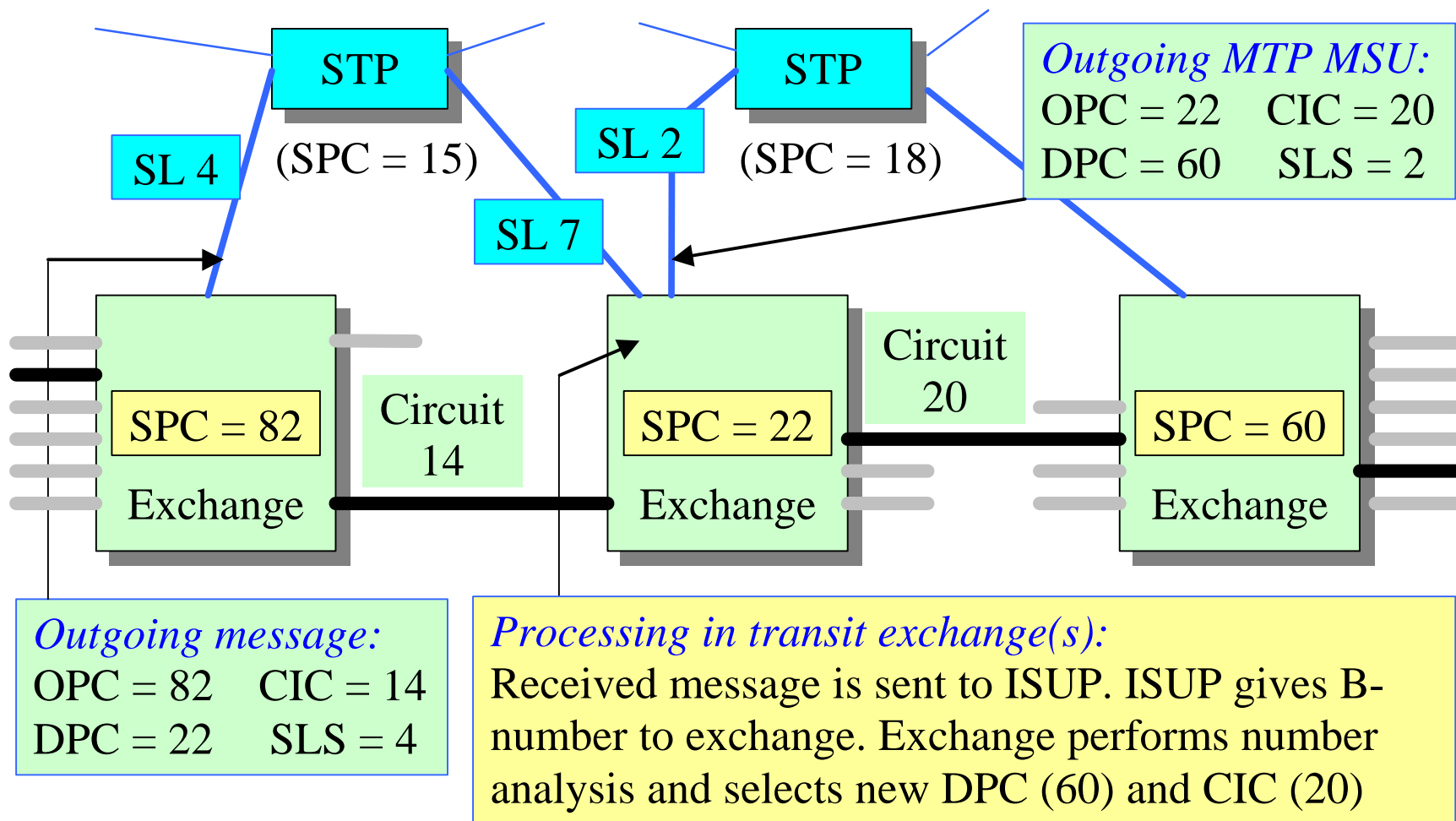**Essential for circuit-switching related signalling**

Features:

1) Establishment / release of circuit switched connections

2) End-to-end signalling between two exchanges (for this purpose SCCP + ISUP is used) see Bhatnagar, p.77

3) General (non-user-related) circuit management

Example: ISUP during connection setup

before circuit switched connection exists (number analysis needed)

STP (SPC = 15)

SL 4

SL 2

SL 7

STP (SPC = 18)

Outgoing MTP MSU:
OPC = 22   CIC = 20
DPC = 60   SLS = 2

SPC = 82
Exchange

Circuit 14

SPC = 22
Exchange

Circuit 20

SPC = 60
Exchange

Outgoing message:
OPC = 82   CIC = 14
DPC = 22   SLS = 4

Processing in transit exchange(s):
Received message is sent to ISUP. ISUP gives B-number to exchange. Exchange performs number analysis and selects new DPC (60) and CIC (20)
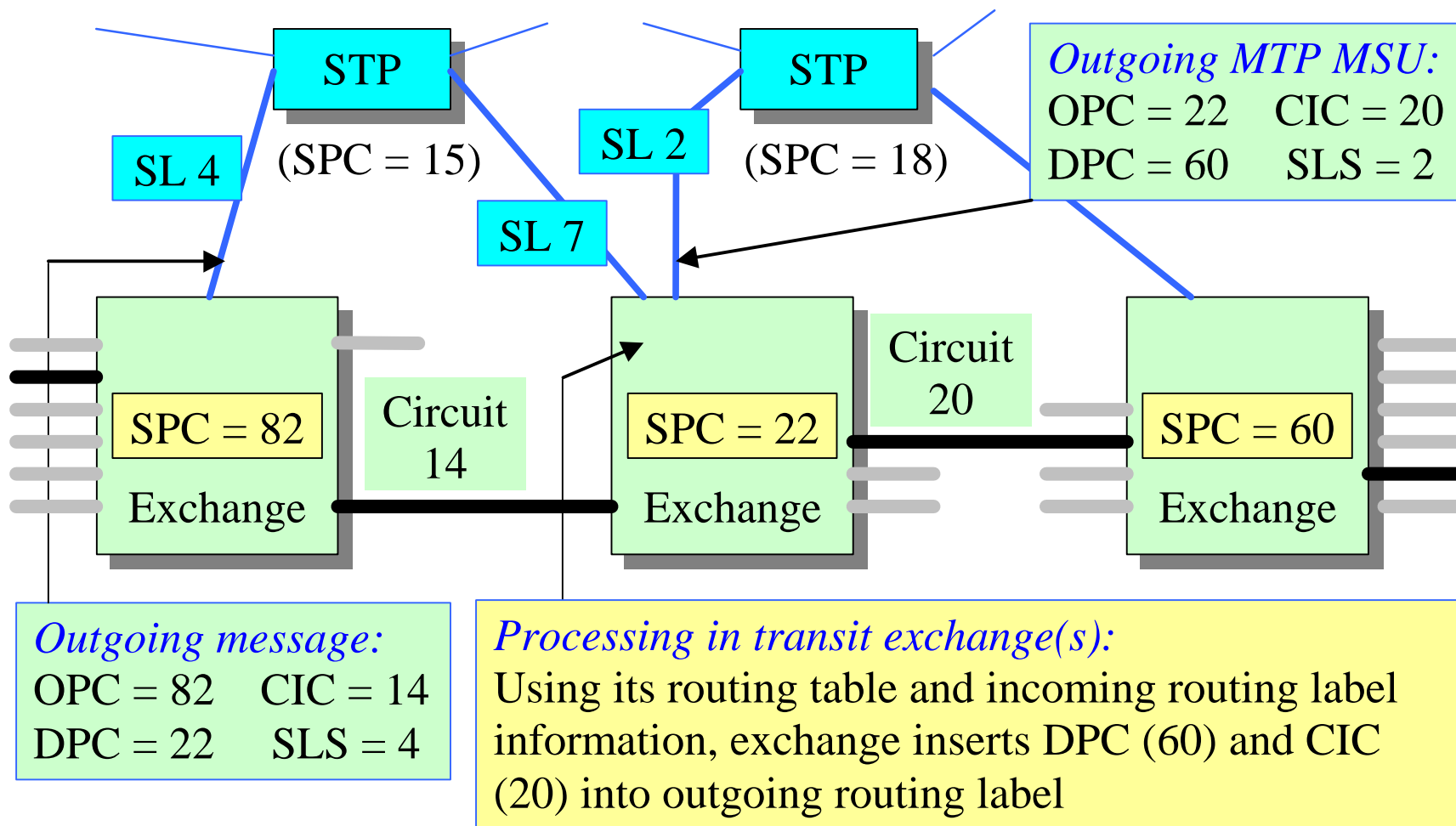
MTP + ISUP in SS7

- The routing capability of MTP is rather limited (entirely based on signalling points).

- Exchanges perform the routing through the network(s) during the establishment of circuit switched connections on an exchange-to-exchange basis, using the dialed digits (and generating routing tables for further use).
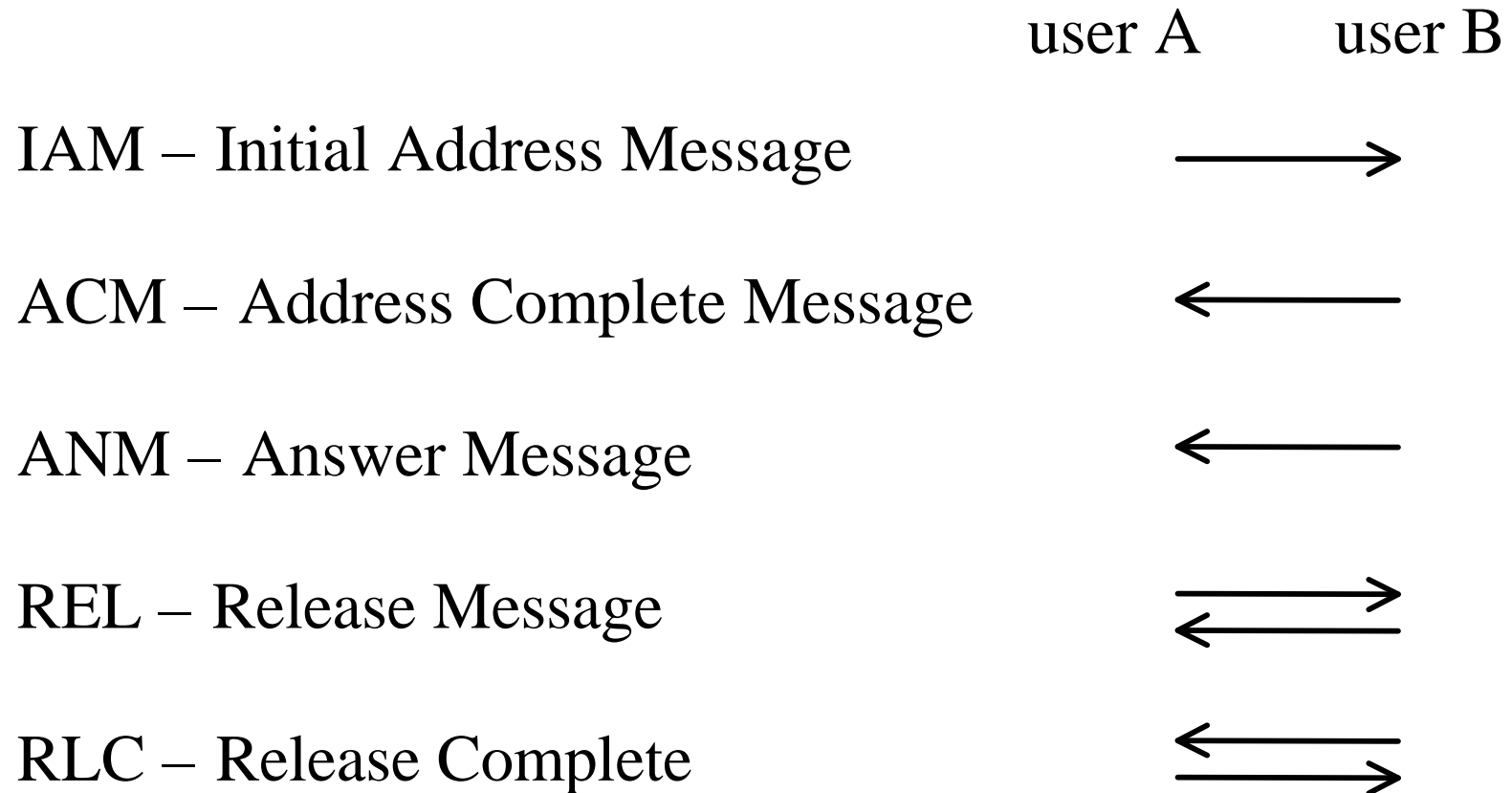
+358   9   4512343

exchange ID

Country code   National region   Subscriber number
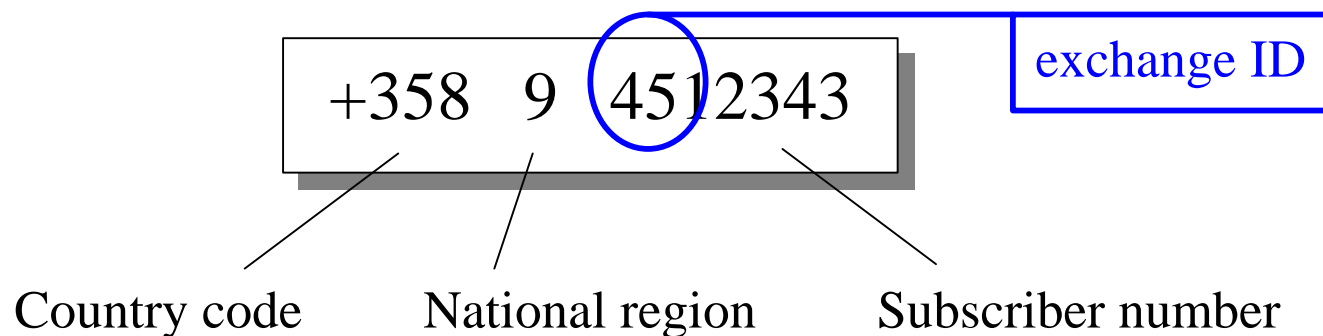
Example: ISUP for link-by-link signalling

when circuit switched connection already exists (no number analysis...)

STP
(SPC = 15)

STP
(SPC = 18)

SL 4

SL 2

SL 7

Outgoing MTP MSU:
OPC = 22   CIC = 20
DPC = 60   SLS = 2

SPC = 82

Exchange

Circuit
14

SPC = 22

Exchange

Circuit
20

SPC = 60

Exchange

Outgoing message:
OPC = 82   CIC = 14
DPC = 22   SLS = 4

Processing in transit exchange(s):
Using its routing table and incoming routing label information, exchange inserts DPC (60) and CIC (20) into outgoing routing label

Some basic ISUP messages

user A   user B

IAM – Initial Address Message $\longrightarrow$

ACM – Address Complete Message $\longleftarrow$

ANM – Answer Message $\longleftarrow$

REL – Release Message $\rightleftarrows$

RLC – Release Complete $\leftrightarrows$

Setup of a "call" using ISUP
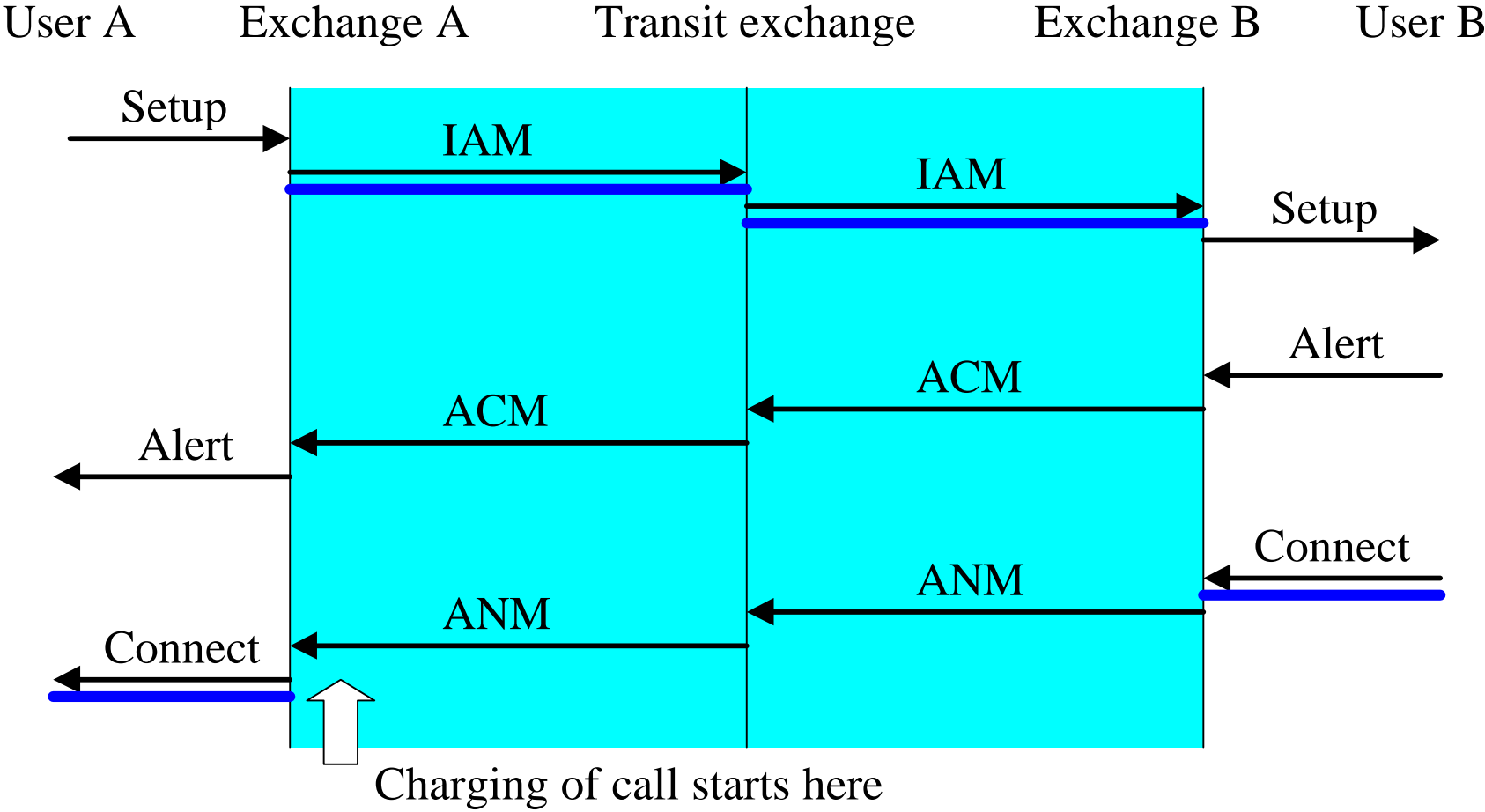
SCCP
Signalling Connection Control Part

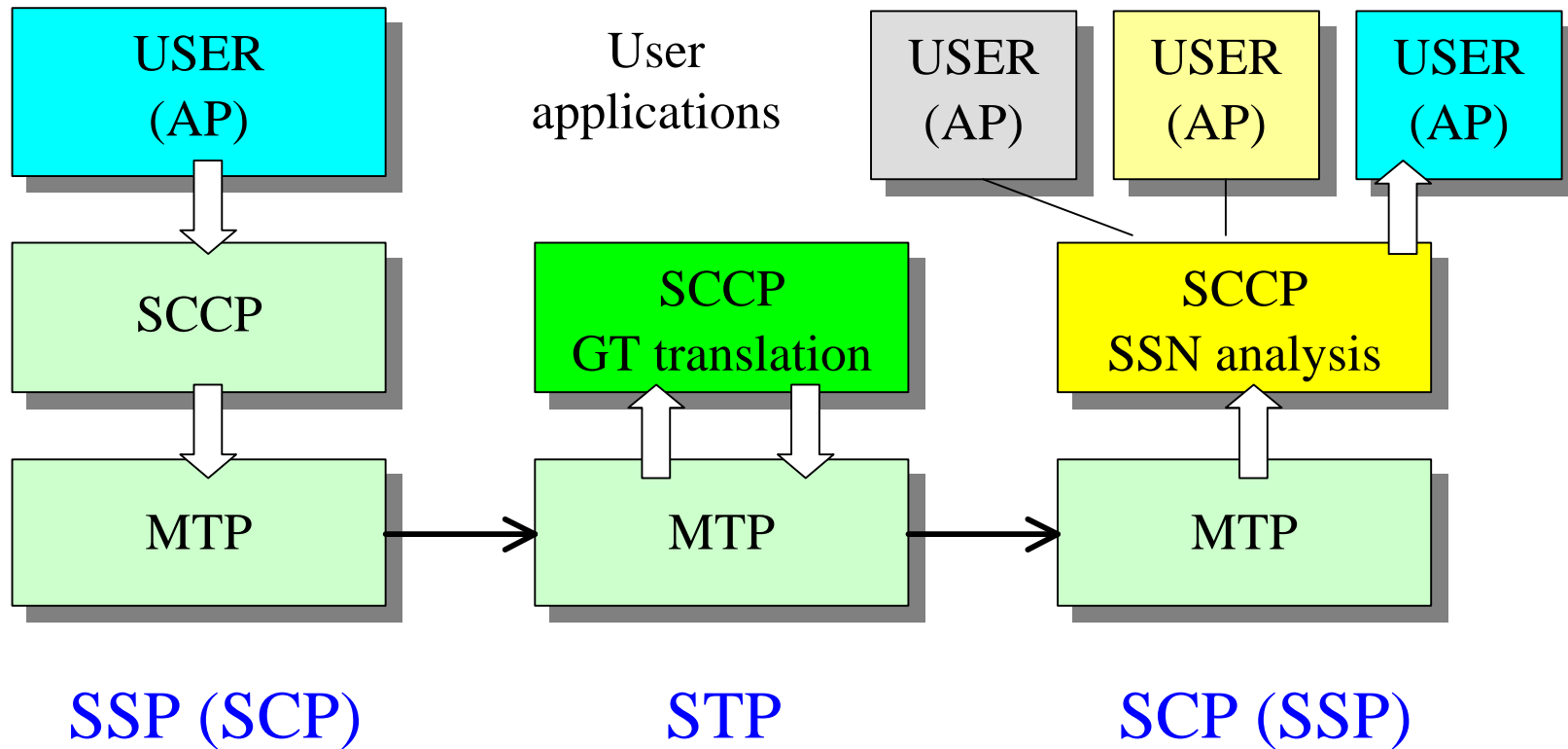**Essential for non-circuit-switching related signalling**

Features:

Layer 3 functionality

1) Essential for end-to-end signalling & database access

2) Global Title Translation (GTT) for enhanced routing

3) SubSystem Number (SSN) analysis at destination
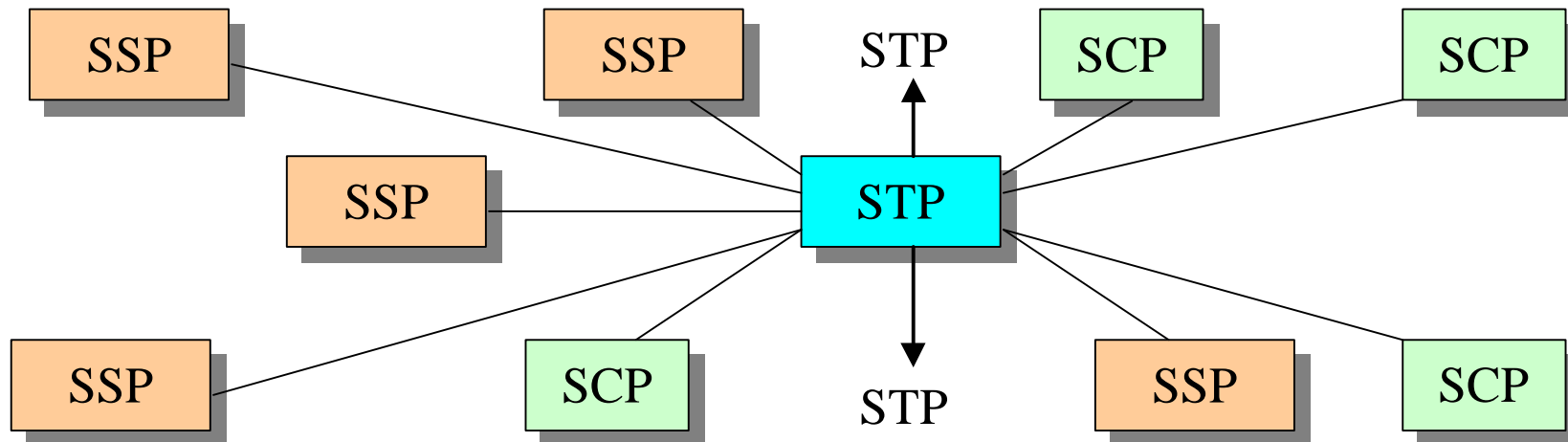
4) 4 Transport Service Classes
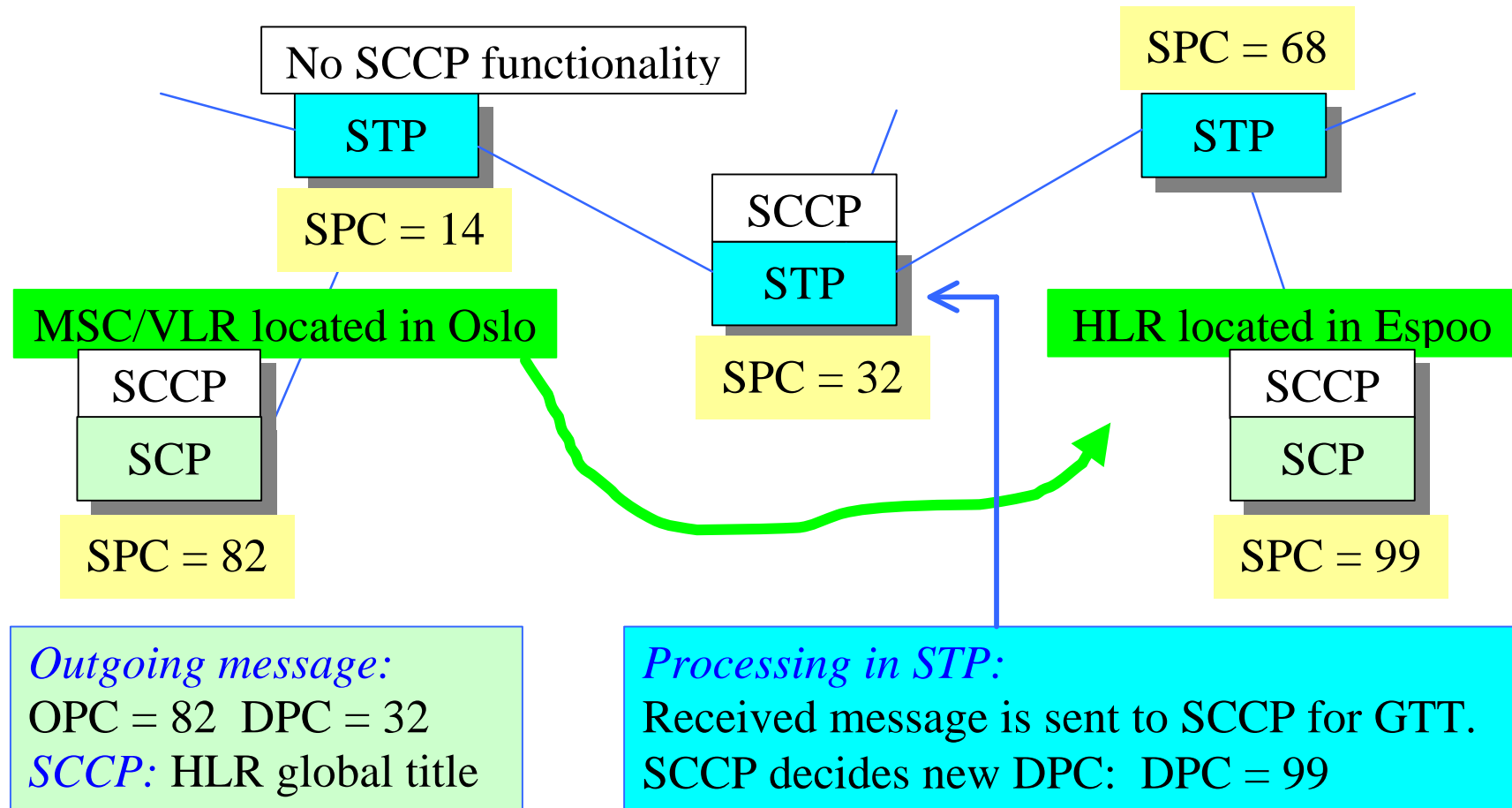
Layer 4 functionality

SS7 connection setup using SCCP

SS7 connection setup using SCCP

Global title translation (GTT) is usually done in an STP.

Advantage: GTT functionality needed only in a few STPs with large packet handling capacity, instead of many SSPs (exchanges) and SCPs (databases) in the network.

Example: SCCP connection with GTT

No SCCP functionality

STP

SPC = 14

SPC = 68

STP

SCCP

STP

SPC = 32

MSC/VLR located in Oslo

SCCP

SCP

SPC = 82

HLR located in Espoo

SCCP

SCP

SPC = 99

Outgoing message:
OPC = 82 DPC = 32
SCCP: HLR global title

Processing in STP:
Received message is sent to SCCP for GTT.
SCCP decides new DPC: DPC = 99

MTP + SCCP

- SCCP $\Leftrightarrow$ can handle "global" routing in those cases where the terminating point DPC is not known

- GT (Global Title) translation in intermediate STP node(s) with SCCP functionality

- SSN (SubSystem Number) for distribution to the correct user (application part) $\Leftrightarrow$ SAP in OSI

In summary, routing capability of MTP + SCCP is much better than that of MTP alone

Four classes of service in SCCP

- Class 0: Basic connectionless class. Each information block (SCCP message) is transmitted from one SCCP user to another SCCP user independently.

- Class 1: Sequenced (MTP) connectionless class. All messages use the same SLS code.

- Class 2: Basic connection-oriented class. Virtual connections are set-up and released + same SLS code + segmentation & reassembly (SAR)

- Class 3: Flow-control connection-oriented class. VC control + same SLS codes + SAR + flow control
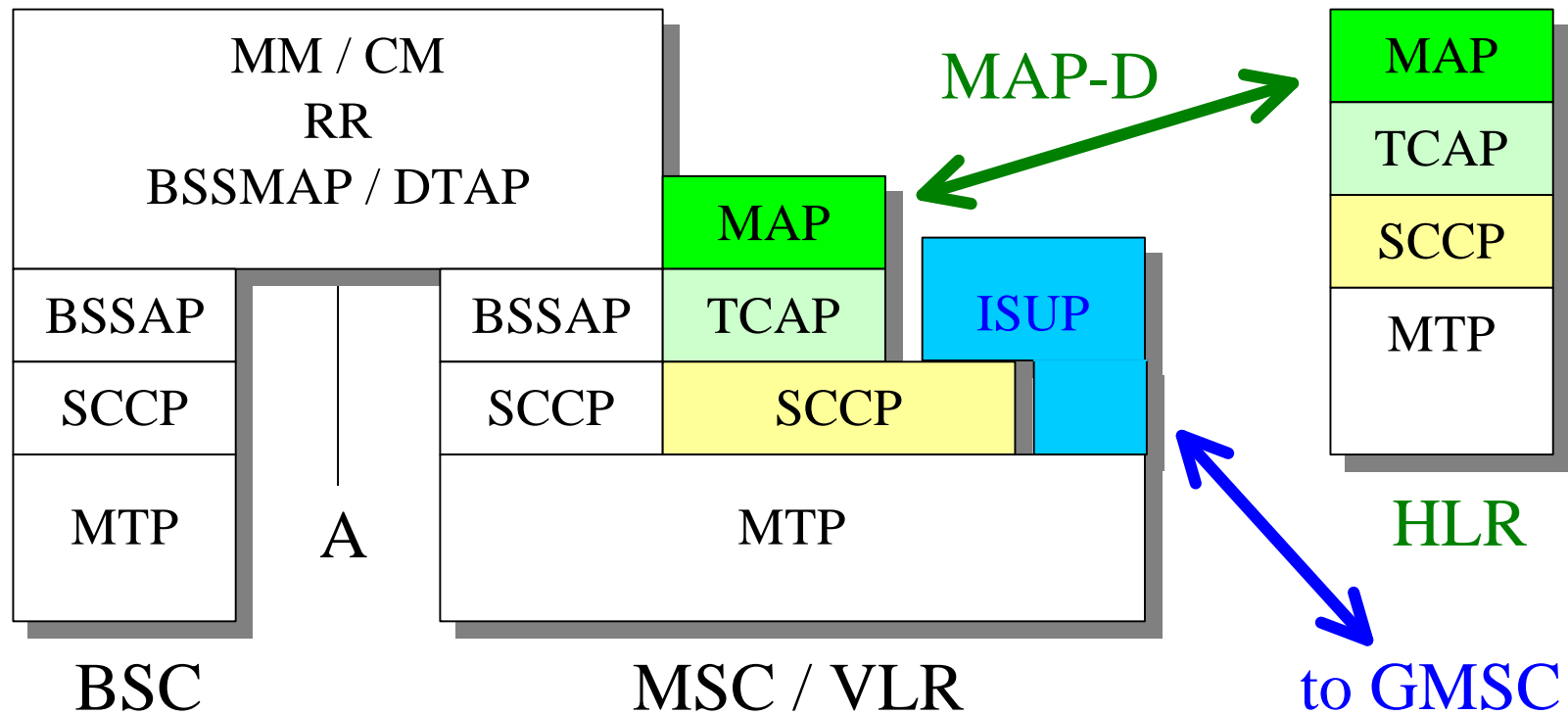
GSM /UMTS core network interfaces (1)
(UMTS: Circuit switched domain of core network)

MAP-B: Between MSC and its associated VLR.

The interface is "internal" and message transfer does not involve the signalling network. This interface is not standardised by ETSI or 3GPP.

MAP-C: Between Gateway MSC (GMSC) and HLR.

This interface is required for the establishment of mobile terminated calls. Through this interface the GMSC enquires the current user location from the HLR, and the HLR provides the MSC with a Mobile Subscriber Roaming Number (MSRN) necessary for setting up the circuit switched connection from the GMSC to the serving MSC (see case study 2 in GSM slides).

GSM /UMTS core network interfaces (2)

MAP-D: **Between VLR and HLR.**

This interface is involved both in CM (Connection Management) and MM (Mobility Management) applications.

CM: Through this interface the HLR asks the VLR to assign and return a roaming number (MSRN) which is used for the establishment of a mobile terminated call (see case study 2 in GSM slides).

MM: This interface may also be used during a Location Update between VLRs when the VLRs update the HLR (in other words the VLRs inform the HLR about changes in user location), or when the HLR deletes information in "old" VLR (see case study 1 in GSM slides).

GSM /UMTS core network interfaces (3)

MAP-E: **Between MSCs in a PLMN.**

> This interface is used during inter-MSC handover operations. (Note: in addition, the E interface involves ISUP)

MAP-F: **Between MSC and EIR.**

> This interface carries information for MS identity checking.

MAP-G: **Between two VLRs.**

> For instance, in case of an inter-VLR Location Update the "new" VLR may request the "old" VLR to provide relevant user information (see case study 1 in GSM slides).

GPRS /UMTS core network interfaces
(UMTS: Packet switched domain of core network)

Gc: **Between GGSN and HLR.**

Similar to MAP-C interface (see above).

Gf: **Between SGSN and EIR.**

Similar to MAP-F interface (see above).

Gn: **Between SGSN and GGSN.**

Gr: **Between SGSN and HLR.**

Gs: **Between SGSN and MSC/VLR.**

This interface is required when the user location information cannot be stored at the SGSN.

Further information on SS7

Tutorials:

Modarressi, Skoog: "SS7: a tutorial", *IEEE Comm. Magazine*, July 1990

Laitinen, Rantala: "Integration of IN services into GSM", *IEEE Comm. Magazine*, June 1995

Jabbari: "CCSS7 for ISDN and IN", *Proc. IEEE*, Feb. 1991

Books:

Bhatnagar: *Engineering networks for synchronization, CCS7, and ISDN*, IEEE Press, 1997

Van Bosse: *Signaling in telecommunication networks*, Wiley, 1998

Web tutorial:

www.iec.org/online/tutorials/ss7