Common Channel Signalling System No. 7 (SS7)

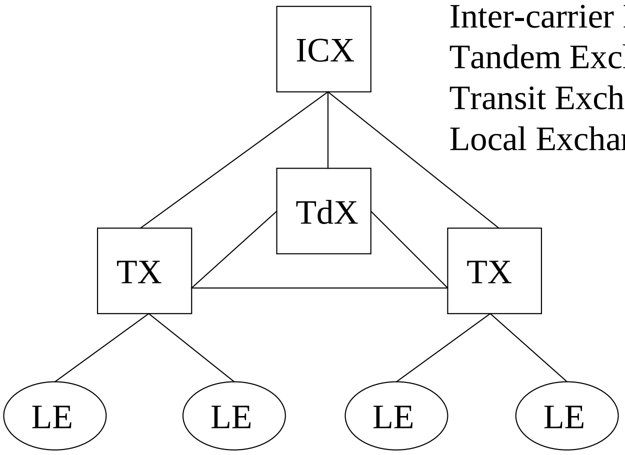
MSc in Software Development

Telecommunications Elective

Introduction

- Common Channel Signalling System No. 7 (SS7) is data communications network standard
- SS7 is intended to be used as a control and management network for telecommunication networks
- SS7 provides call management, data base query, routing, flow and congestion control functionality for telecommunication networks
- SS7 is specifically designed to support the functions of an Integrated Services Digital Network

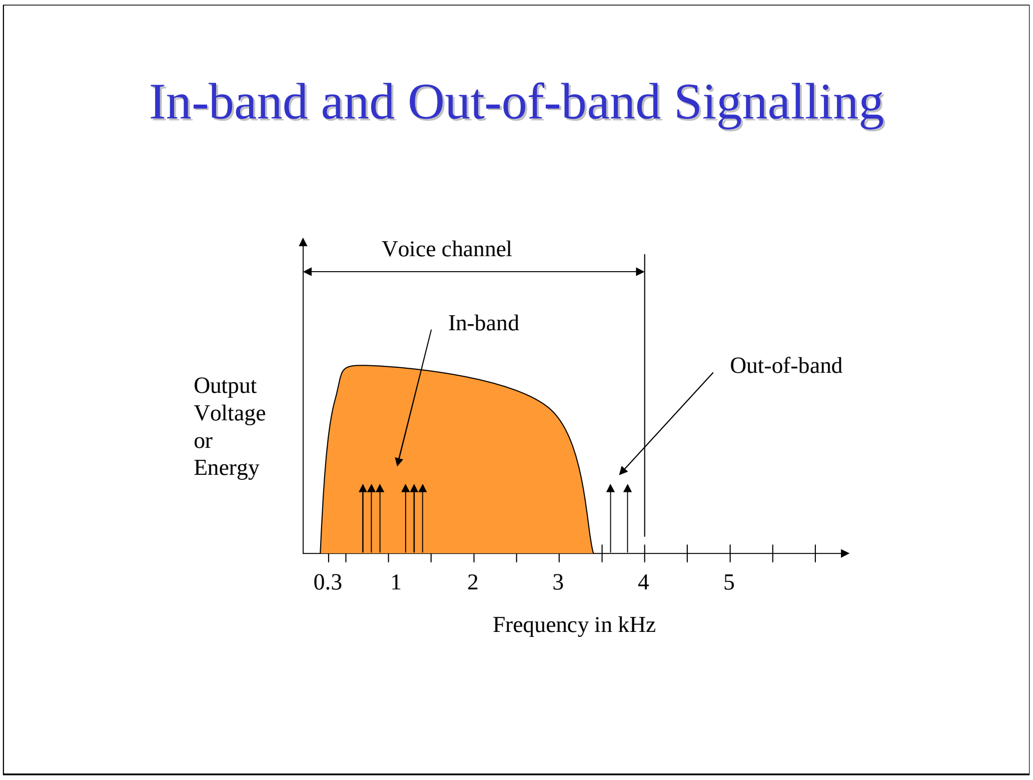
Hierarchy of Telephone Networks



Inter-carrier Exchange (ICX)
Tandem Exchange (TdX)
Transit Exchange (TX)
Local Exchange (LE)

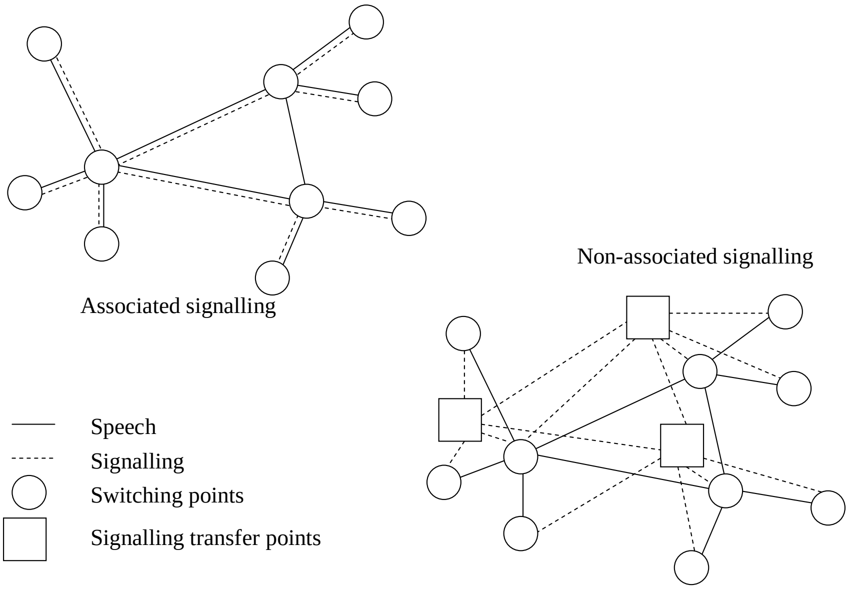
Signalling Transmission

- DC Signalling
  - On-Off type digital signals
- Tone Signalling
  - In-band or out-of-band signalling
- Digital Control Signals
  - similar to on-off signals but represent bit sequences
- Common Channel Signalling
  - digital signalling scheme between switches in the network



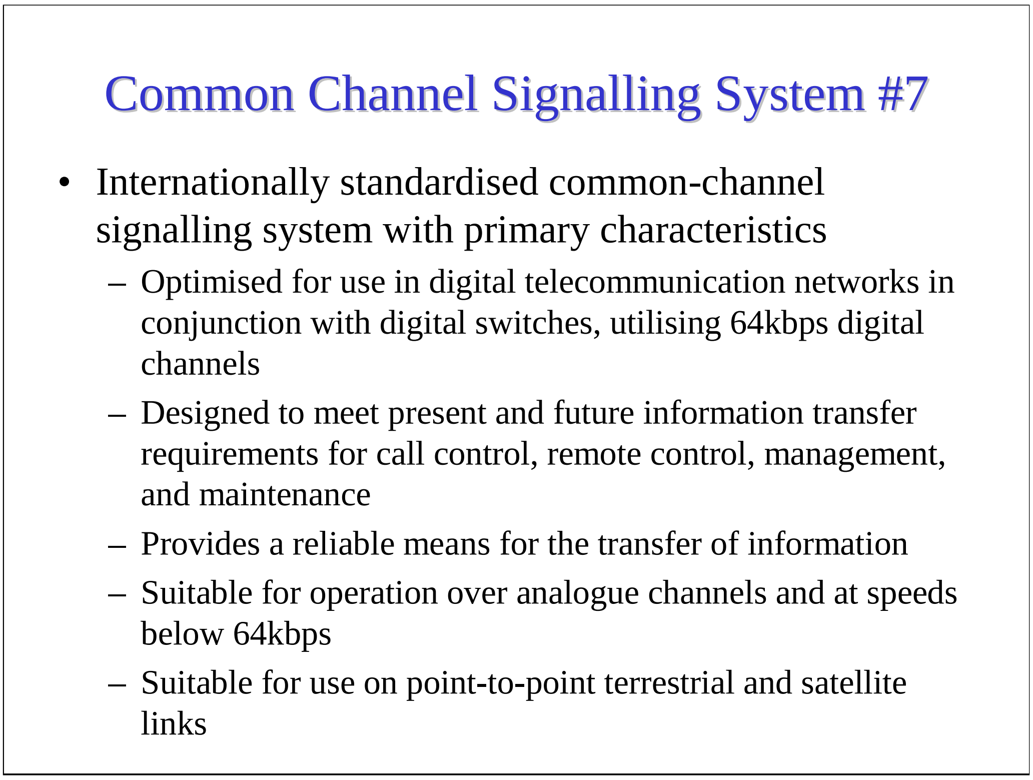
In-band and Out-of-band Signalling

Common Channel Signalling



As public network become more complex and provide a richer set of services, the drawbacks of in-channel signalling become more apparent. The information transfer rate is quite limited and with inband signalling only available if there are no voice signals on the circuit. Out-of-band signalling provides only a very limited bandwidth. With these limitations it is difficult to provide more complex control messages in order to manage the increasing complexity of evolving network technology. A more powerful approach is required. This approach is based on common channel signalling. In this approach the signalling path is physically distinct from the path for voice and other subscriber signals. The common channel can be configured with the bandwidth required to carry control signals for a rich variety of functions. With dropping costs for hardware this concept has become so attractive that it is being introduced in all public telecommunication networks. The control signals are messages passed between switches as wells as between a switch and the network management centre. Thus, the control-signalling portion of the network is a distributed computer network carrying short messages.

Two modes of operation are used, the *associated mode* and the *non-associated mode*. In the associate mode (shown above) the common channel closely tracks along the entire length of the inter-switch trunks. The non-associated mode is more complex, but more powerful; with this the network is augmented by additional nodes, known as signal transfer points. There is now no close or simple assignment of control channels to trunk groups. In effect, there are now two separate networks, with links between them so that the control portion of the network can exercise control over the switching nodes that carry the subscriber calls. This mode is used in ISDN and the control signalling architecture is called Common Channel Signalling System No. 7 (SS#7).



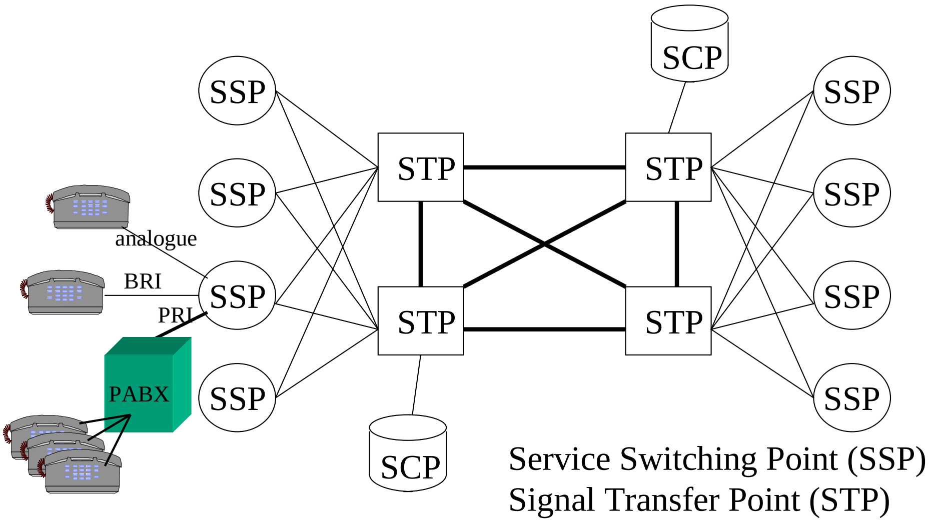
Common Channel Signalling System #7

- Internationally standardised common-channel signalling system with primary characteristics
  - Optimised for use in digital telecommunication networks in conjunction with digital switches, utilising 64kbps digital channels
  - Designed to meet present and future information transfer requirements for call control, remote control, management, and maintenance
  - Provides a reliable means for the transfer of information
  - Suitable for operation over analogue channels and at speeds below 64kbps
  - Suitable for use on point-to-point terrestrial and satellite links

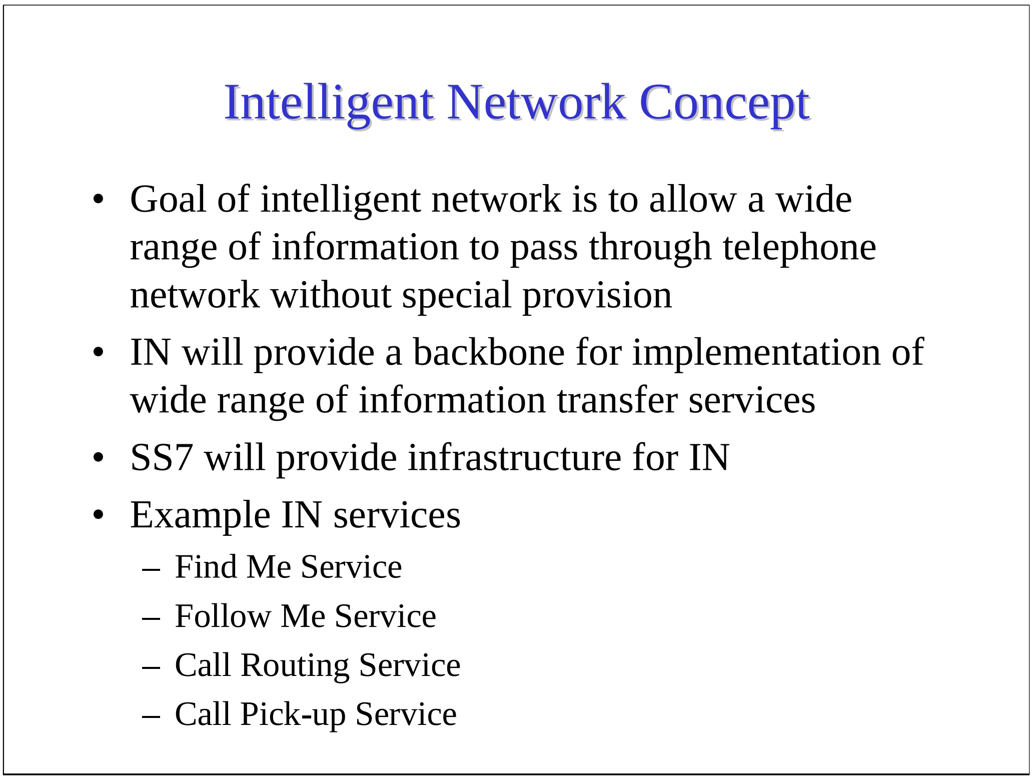
Common Channel Signalling System #7

- SS7 is based on a four level protocol layer architecture
- SS7 levels correspond to the OSI layer concept
- Since SS7 is older than the OSI RM, no immediate mapping between SS7 levels and OSI layers is possible
- SS7 protocol architecture defines packet-switched network

SS7 Network Model



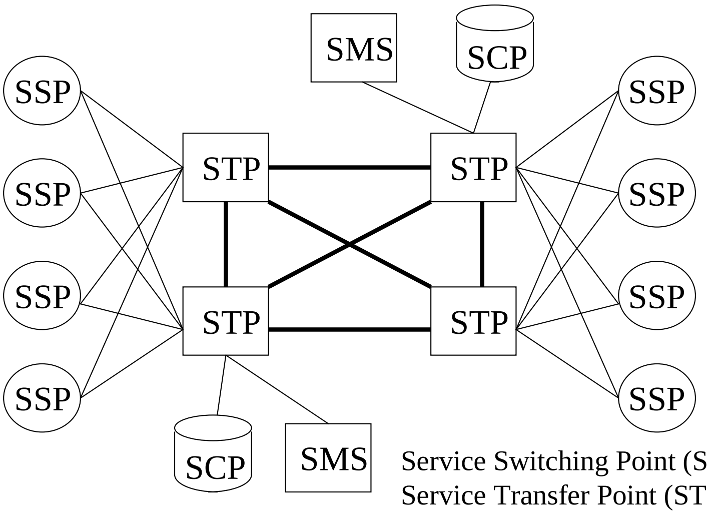
Service Switching Point (SSP)
Signal Transfer Point (STP)
Service Control Point (SCP)



Intelligent Network Concept

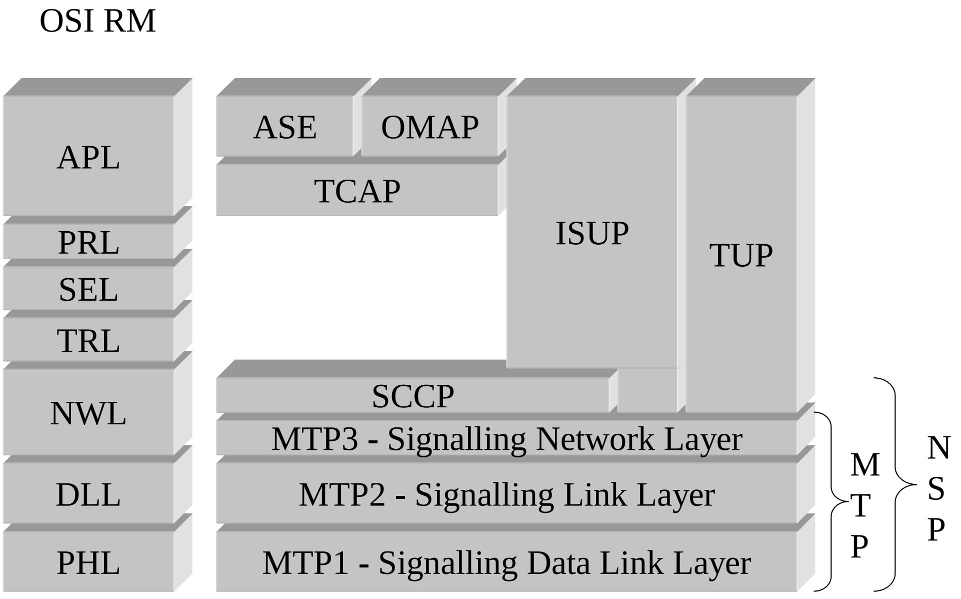
- Goal of intelligent network is to allow a wide range of information to pass through telephone network without special provision
- IN will provide a backbone for implementation of wide range of information transfer services
- SS7 will provide infrastructure for IN
- Example IN services
  - Find Me Service
  - Follow Me Service
  - Call Routing Service
  - Call Pick-up Service

IN Network based on SS7



Service Switching Point (SSP)
Service Transfer Point (STP)
Service Control Point (SCP)
Service Management System (SMS)

SS7 Protocol Architecture


OSI RM
APL
PRL
SEL
TRL
NWL
DLL
PHL
ASE
OMAP
TCAP
ISUP
TUP
SCCP
MTP3 - Signalling Network Layer
MTP2 - Signalling Link Layer
MTP1 - Signalling Data Link Layer
MTP
NSP

Abbreviations

MTP - Message Transfer Part

SCCP - Signalling Connection Control part

NSP - Network Service Part

ISUP - ISDN User Part

TUP - Telephone User Part

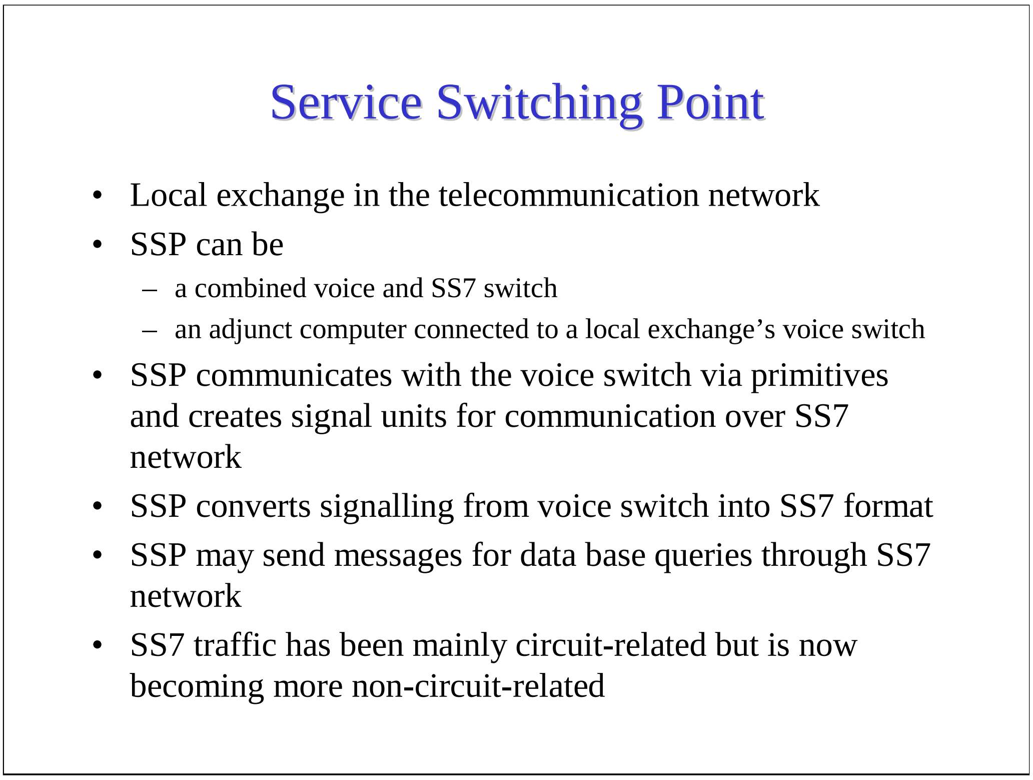
TCAP - Transaction Capabilities Application Part

ASE - Application Service Entities

OMAP - Operations and Maintenance Application Part

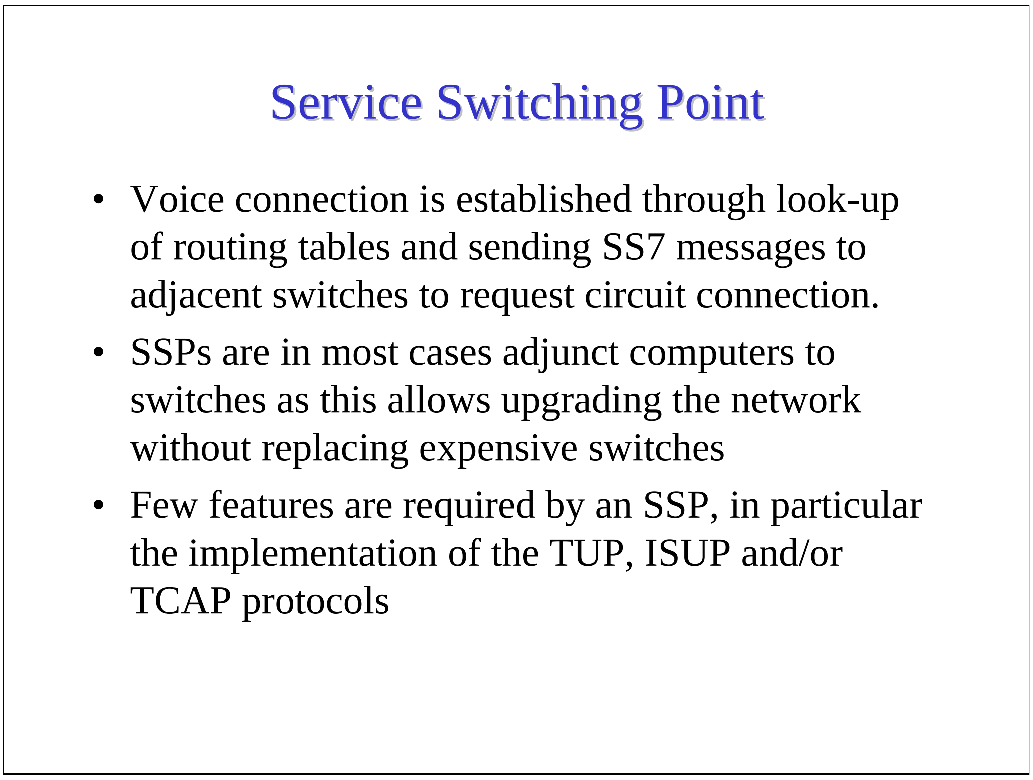
ITU-T SS7 Specifications

Q.700 - Q.709	Message Transfer Part (MTP)
Q.710	PBX Applications
Q.711 - Q.716	Signalling Connection Control Part (SCCP)
Q.721 - Q.725	Telephone User Part (TUP)
Q.730	ISDN Supplementary Services
Q.741	Data User Part (DUP)
Q.761 - Q.766	ISDN User Part (ISUP)
Q.771 - Q.775	Transaction Capabilities Application Part (TCAP)
Q.791 -Q.795	Monitoring Operations, and Maintenance
Q.780 - Q.783	Test Specifications



Service Switching Point

- Local exchange in the telecommunication network
- SSP can be
  - a combined voice and SS7 switch
  - an adjunct computer connected to a local exchange’s voice switch
- SSP communicates with the voice switch via primitives and creates signal units for communication over SS7 network
- SSP converts signalling from voice switch into SS7 format
- SSP may send messages for data base queries through SS7 network
- SS7 traffic has been mainly circuit-related but is now becoming more non-circuit-related

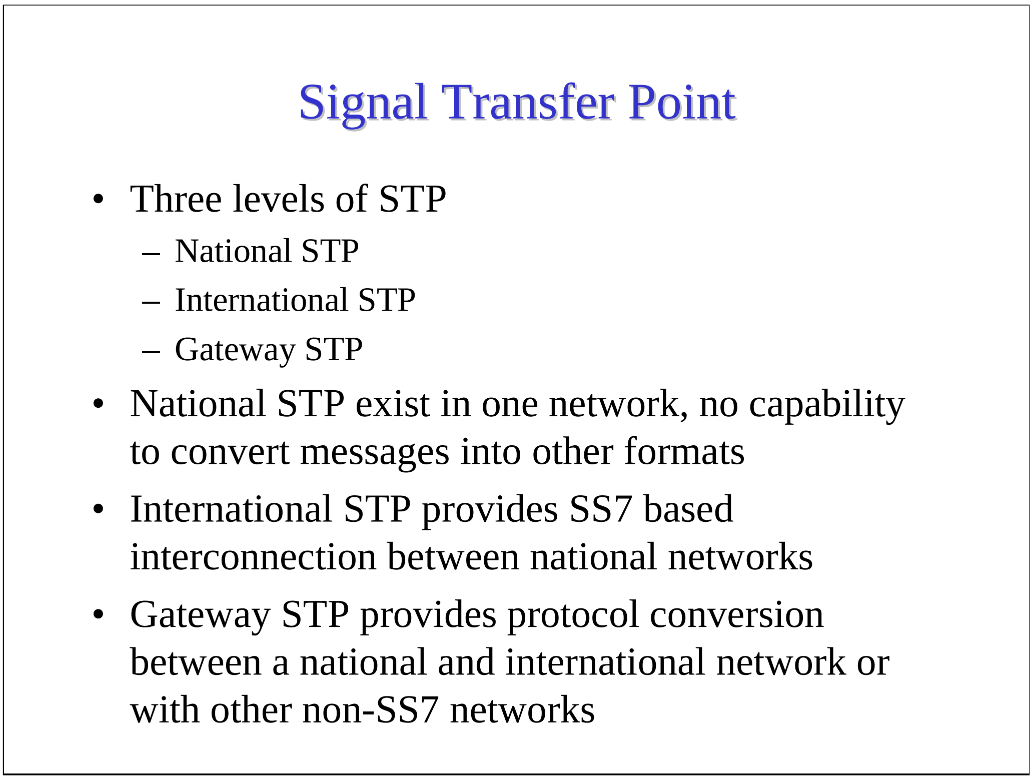


Service Switching Point

- Voice connection is established through look-up of routing tables and sending SS7 messages to adjacent switches to request circuit connection.
- SSPs are in most cases adjunct computers to switches as this allows upgrading the network without replacing expensive switches
- Few features are required by an SSP, in particular the implementation of the TUP, ISUP and/or TCAP protocols

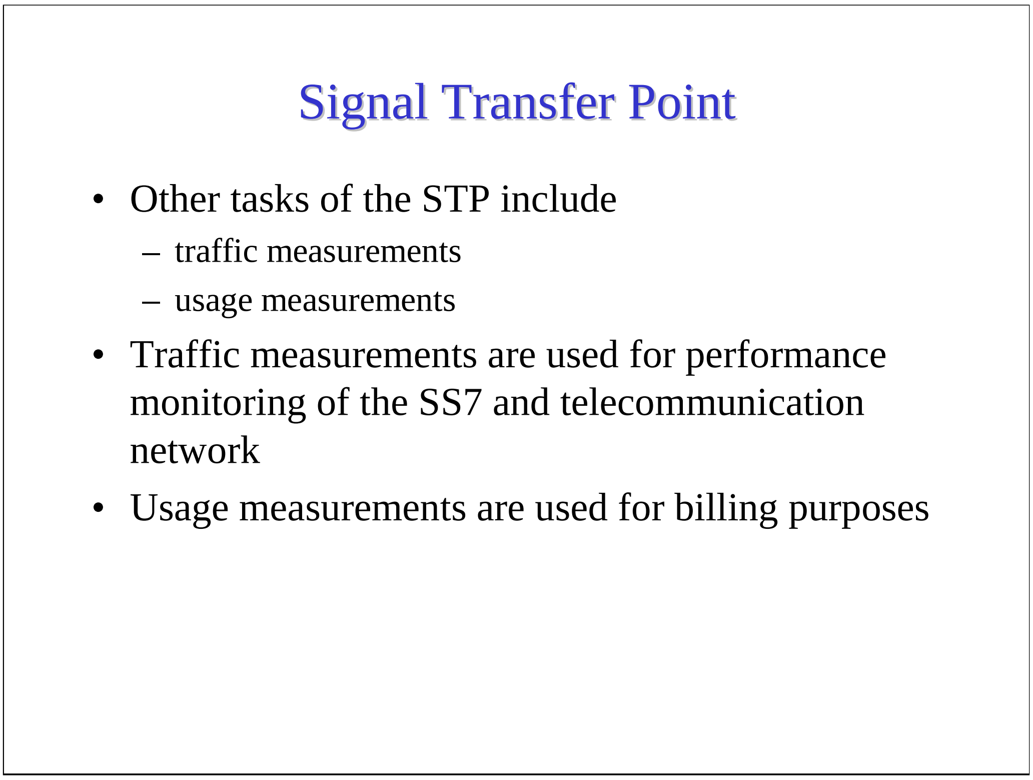
Signal Transfer Point

- SS7 messages travel from one SSP to another through the services of a Signal Transfer Point (STP)
- The STP acts as a router for SS7 messages
- STP does not usually originate SS7 messages
- STPs are typically adjunct computers to tandem voice switches, rarely an STP is a stand-alone system
- STP exchange information in form of packets related to either call connections or database queries



Signal Transfer Point

- Three levels of STP
  - National STP
  - International STP
  - Gateway STP
- National STP exist in one network, no capability to convert messages into other formats
- International STP provides SS7 based interconnection between national networks
- Gateway STP provides protocol conversion between a national and international network or with other non-SS7 networks



Signal Transfer Point

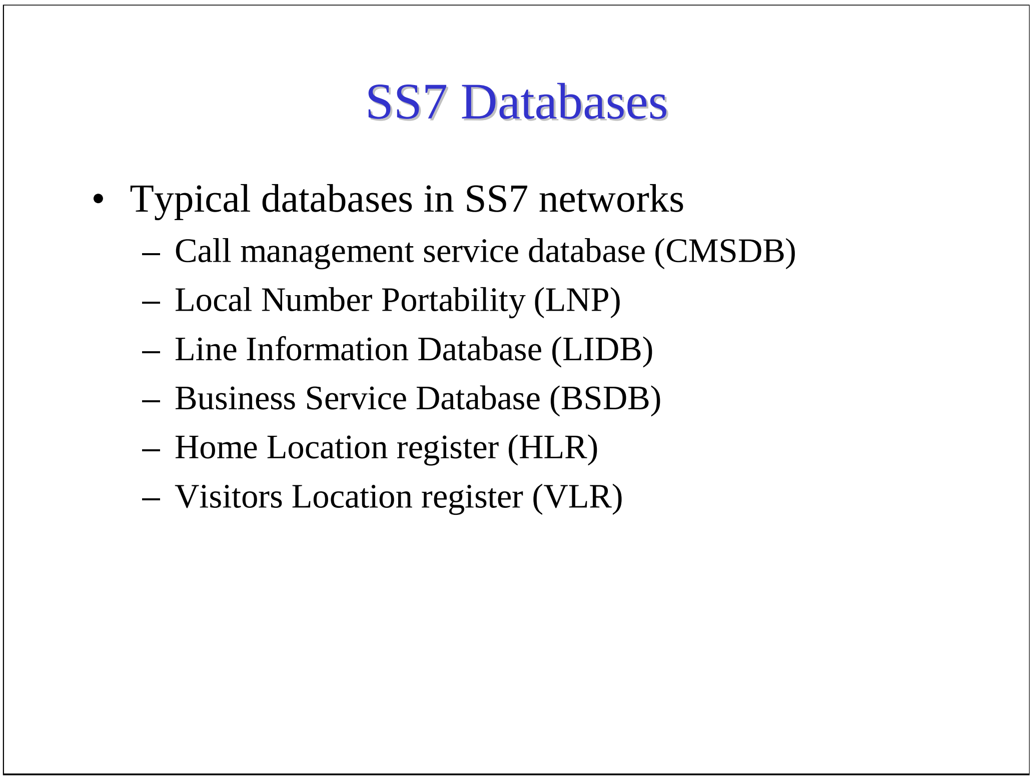
- Other tasks of the STP include
  - traffic measurements
  - usage measurements
- Traffic measurements are used for performance monitoring of the SS7 and telecommunication network
- Usage measurements are used for billing purposes

Service Control Point

- SCP serves as interface to a telephone company’s database
- Database store information about
  - subscriber’s services
  - routing of special service numbers
  - calling card validation and fraud protection
  - advanced intelligent network features for service creation
- SCP is a computer used as a front-end to a data-base

Service Control Point

- Communication between SCP and mainframe/mini-computer that hosts the database is via X.25 links
- Alternatively, SCP and STP can be integrated and the database resides then in the SCP
- Communication with database either by SS7 to X.25 protocol conversion of by primitives in the case of STP/SCP integration
- Database considered application entity and protocol to access database is TCAP



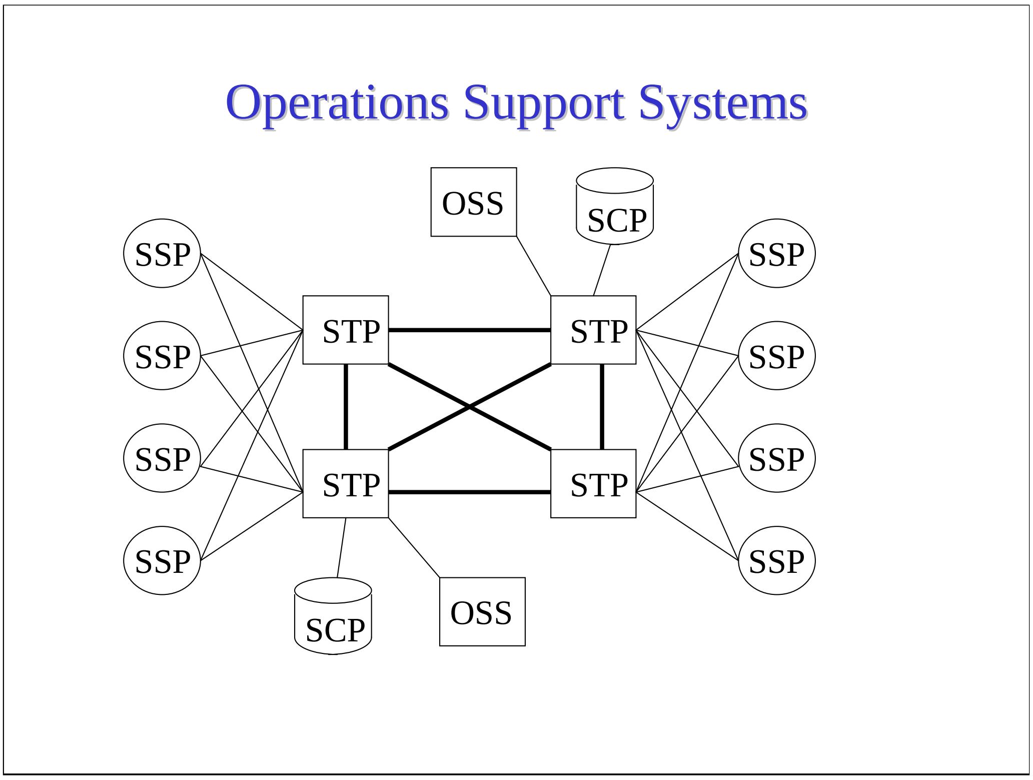
SS7 Databases

- Typical databases in SS7 networks
  - Call management service database (CMSDB)
  - Local Number Portability (LNP)
  - Line Information Database (LIDB)
  - Business Service Database (BSDB)
  - Home Location register (HLR)
  - Visitors Location register (VLR)

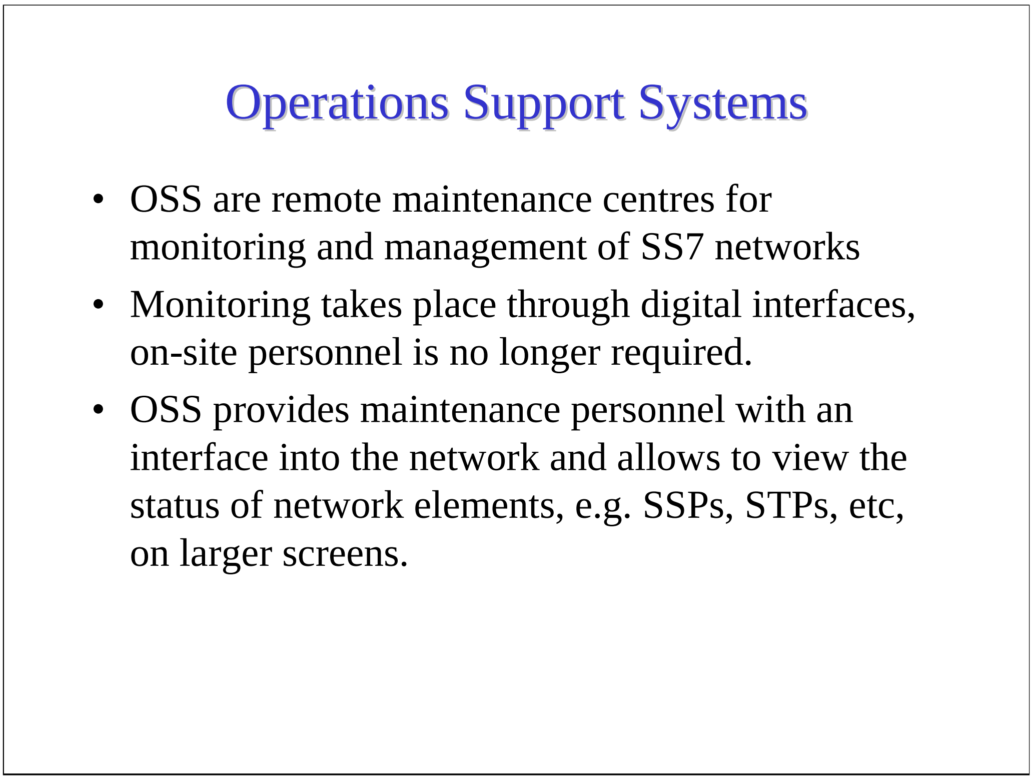
CMSDB - provides information relating to call processing, network management, and call smapling (for traffic measurement). Call processing provides routing information for special purpose nubers such as 1800, 1850, 1890, etc. Additionally, the database provide billing information. Network management functionality is sued for congestion control.

LIDB - provides information regarding subscribers such as calling card service, third-party billing instructions, and originating line number screening. Billing is the mst important feature of this database. In addition security features such as calling card PIN numbers are stored in this database.

BSDB - provides information relating to a large private customers private network such as call processing, management and other related functions. The purpose of this database is to allow larger corporation to set-up their own virtual private networks by using portions of the public network to interconnect their PBX systems.



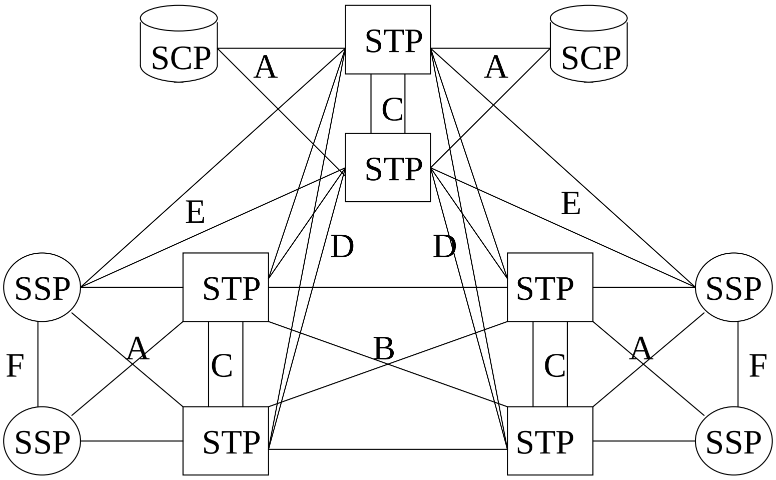
Operations Support Systems

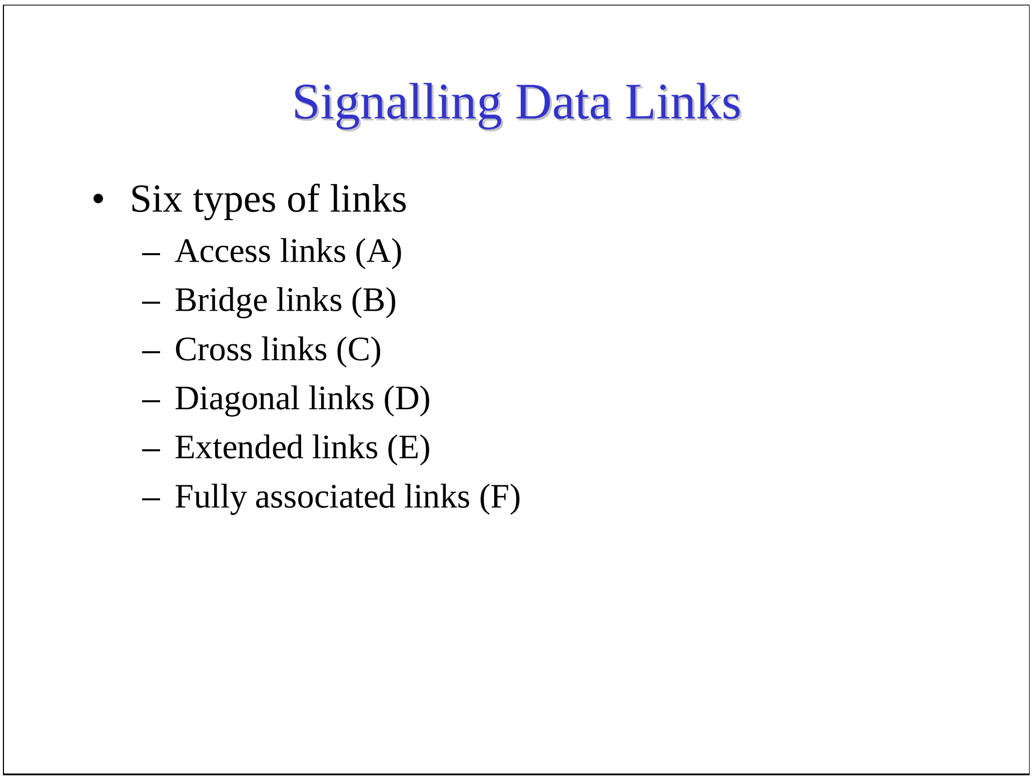


Operations Support Systems

- OSS are remote maintenance centres for monitoring and management of SS7 networks
- Monitoring takes place through digital interfaces, on-site personnel is no longer required.
- OSS provides maintenance personnel with an interface into the network and allows to view the status of network elements, e.g. SSPs, STPs, etc, on larger screens.

Signalling Data Links





Signalling Data Links

- Six types of links
  - Access links (A)
  - Bridge links (B)
  - Cross links (C)
  - Diagonal links (D)
  - Extended links (E)
  - Fully associated links (F)

Links

- Access links
  - are used between SSP and STP or SCP and STP
  - always two A links, one to each of the home STP pairs
  - Maximum of 16 A links int one STP
- Bridge links
  - connect mated STPs to other mated STPs at the same hierarchical level
- Cross links
  - Used to connect STP to its mate STP. STPs are always deployed in pairs to maintain redundancy in the network
  - Not used for routing, up to 8 C links between paired STPs

Links

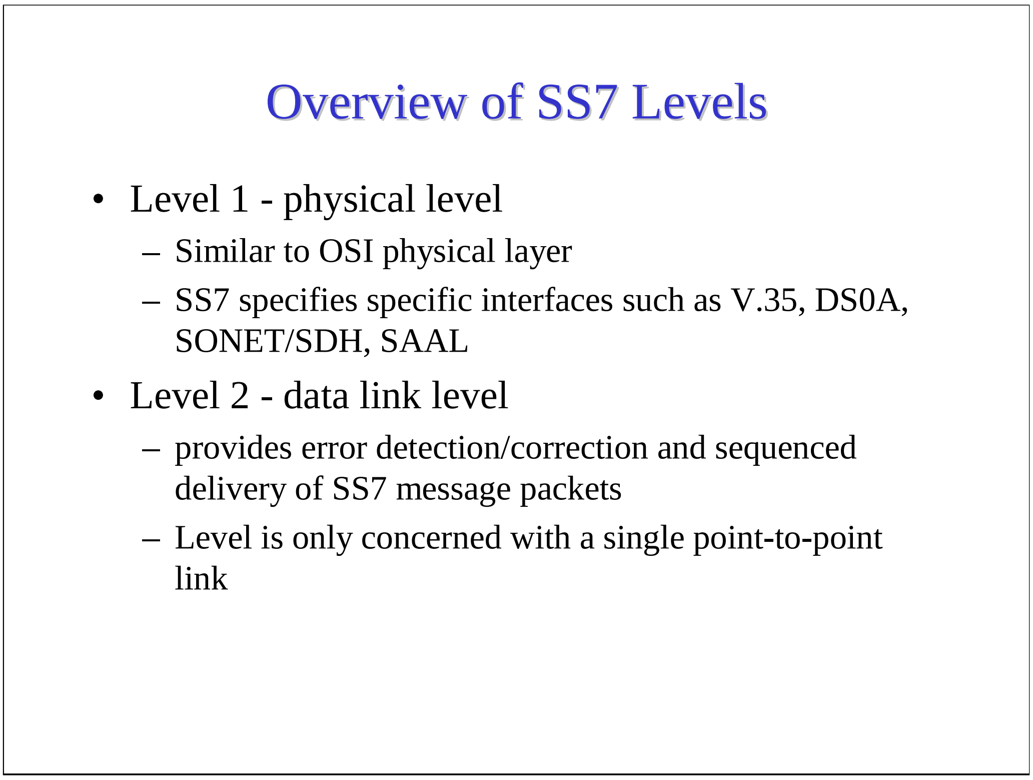
- Diagonal links
  - used to connect mated STP pairs from one hierarchical level to another mated STP pair at a higher level
  - Max. of 8 D links between mated STP pairs
- Extended links
  - used to connect SSPs to remote STP pairs
  - used to diversify and create redundancy
- Fully associated links
  - used to route large amount of traffic between two SSPs
  - also used when an SSP cannot be connected directly to an STP

Physical Interfaces

- Interfaces used to connect signalling data links to network equipment
  - V.35
  - single channel in E1 line
  - High-speed interfaces/links
- Other interfaces are used to connect adjunct equipment such as terminals, modems, etc.
  - RS-232/V.24
  - RS-449

High-Speed Links

- PDH links of 1.544Mbps or 2.048Mbps or higher have been defined for SS7
- Recently SONET/SDH links with data rates 51.84Mbps, 155.52Mbps, 622.08Mbps, and 2.48832Gbps have been defined for SS7
- SONET/SDH links will use ATM cell transmission and switching
- When using ATM, the Signalling ATM Adaptation Layer (SAAL) will replace SS7 protocol layers MTP1 and MTP2



Overview of SS7 Levels

- Level 1 - physical level
  - Similar to OSI physical layer
  - SS7 specifies specific interfaces such as V.35, DS0A, SONET/SDH, SAAL
- Level 2 - data link level
  - provides error detection/correction and sequenced delivery of SS7 message packets
  - Level is only concerned with a single point-to-point link

Overview of SS7 Levels

- Level 3 - network level
  - three functions - routing, message discrimination, distribution
  - three network management functions - link management, route management, traffic management
- Level 4 - user parts
  - several different protocols - user part or application part
  - Call connection management is performed with user part, e.g. TUP, ISUP
  - Database access is performed by application part, e.g. TCAP, etc.
  - Other application parts are used such as MAP in mobile networks

Signal Units

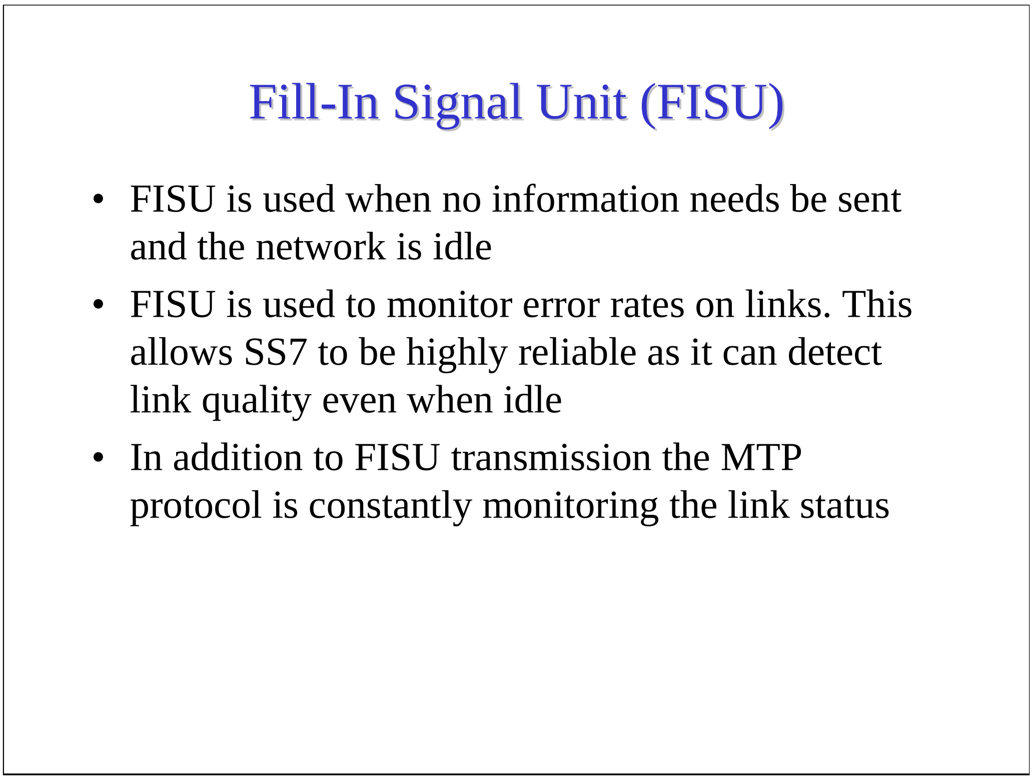
- Signal Units are the data packets that are sent in an SS7
- SS7 uses three types of signal units
- SS7 network management uses all three types of signal units whereas information is sent using only one type of signal unit
- SS7 is different to other types of data networks as it does not provide user-to-user data transmission but machine-to-machine data transmission
- Signal Units rely on the services of the MTP for routing, link control, and error control

Message Signal Unit (MSU)

- MSU carries SS7 information
- MSU consists of MTP protocol fields and two additional fields
  - Service indicator octet (SIO)
    - indicates type of protocol at level 4, e.g. TUP, ISUP, and type of standard, e.g. national, international.
  - Service information field (SIF)
    - used to carry control information as well as level 3 routing label. SIF can be up to 272 octets and is used by all level 4 protocols

Link Status Signal Unit (LSSU)

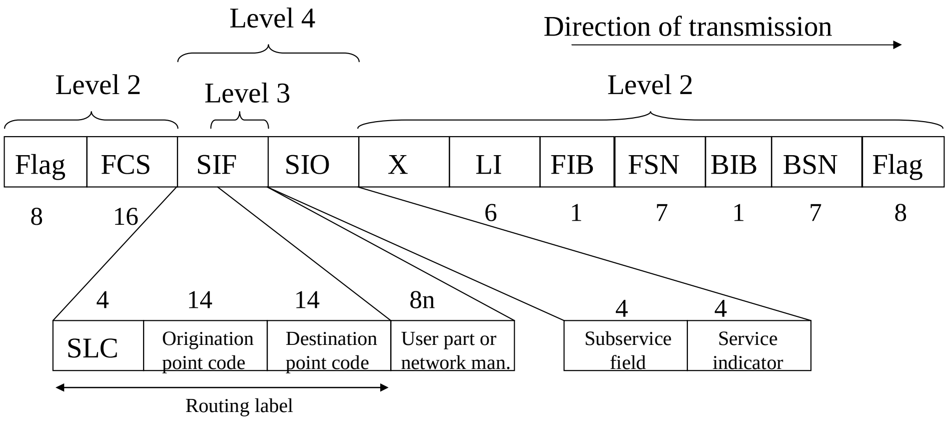
- Used to carry link status information
- Used by level 3 at one node to transmit link status information to its adjacent node
- LSSU only used on single point-to-point links, never through the network
- No information traffic is carried on a link when LSSU are sent



Fill-In Signal Unit (FISU)

- FISU is used when no information needs be sent and the network is idle
- FISU is used to monitor error rates on links. This allows SS7 to be highly reliable as it can detect link quality even when idle
- In addition to FISU transmission the MTP protocol is constantly monitoring the link status

Message Signal Unit



Level 4

Direction of transmission

Level 2

Level 3

Level 2

Flag FCS SIF SIO X LI FIB FSN BIB BSN Flag

8 16 6 1 7 1 7 8

4 14 14 8n

SLC

Origination point code

Destination point code

User part or network man.

4 4

Subservice field

Service indicator

Routing label

BIB = Backward indicator bit
BSN = Backward sequence number
FCS = Frame check sequence
FIB = Forward indicator bit
FSN = Forward sequence number

LI = Length indicator
SIF = Signal information field
SIO = Service information octet
SLC = Signalling link code

Link Status Signal Unit

Direction of transmission →

Flag	FCS	SF	X	LI	FIB	FSN	BIB	BSN	Flag
8	16	8 or 16	2	6	1	7	1	7	8

BIB = Backward indicator bit
BSN = Backward sequence number
FCS = Frame check sequence
FIB = Forward indicator bit
FSN = Forward sequence number

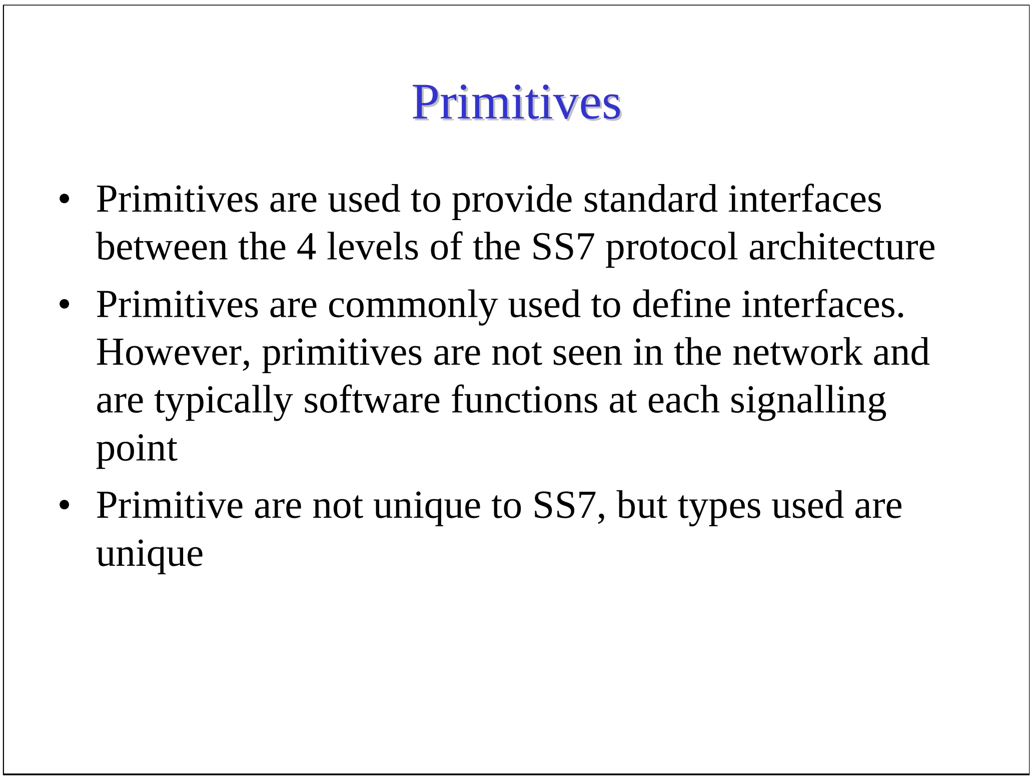
LI = Length indicator
SF = Status field

Fill-In Signal Unit

Direction of transmission →

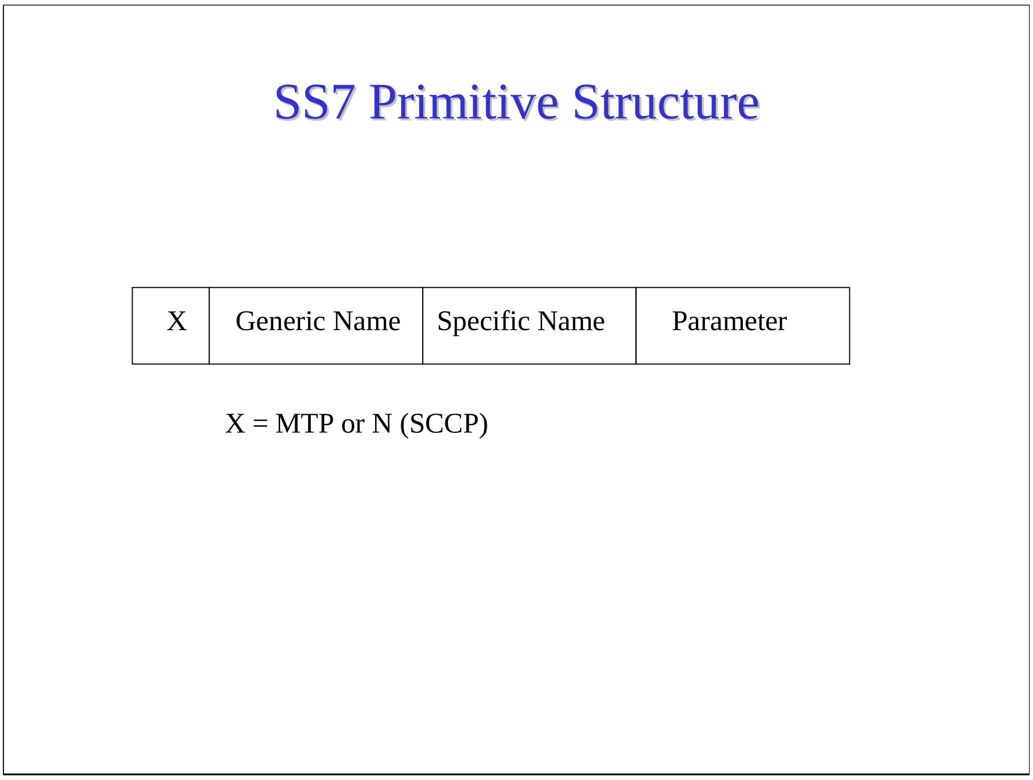
Flag	FCS	X	LI	FIB	FSN	BIB	BSN	Flag
8	16	2	6	1	7	1	7	8

BIB = Backward indicator bit
BSN = Backward sequence number
FCS = Frame check sequence
FIB = Forward indicator bit
FSN = Forward sequence number
LI = Length indicator



Primitives

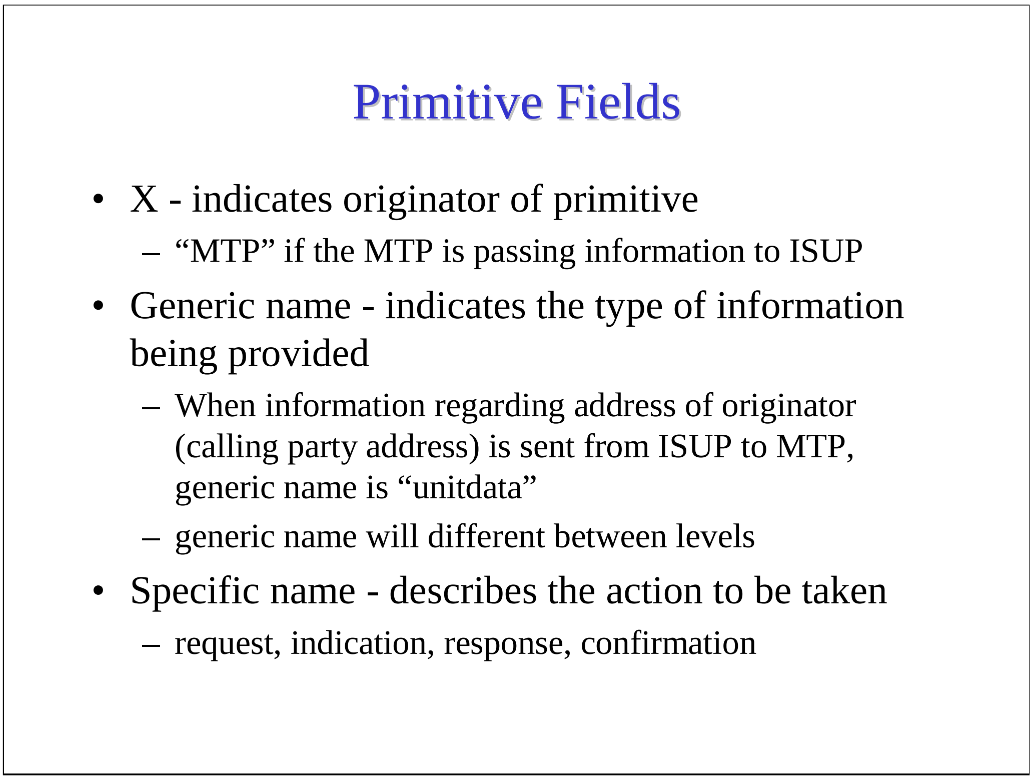
- Primitives are used to provide standard interfaces between the 4 levels of the SS7 protocol architecture
- Primitives are commonly used to define interfaces. However, primitives are not seen in the network and are typically software functions at each signalling point
- Primitive are not unique to SS7, but types used are unique



SS7 Primitive Structure

X	Generic Name	Specific Name	Parameter

X = MTP or N (SCCP)



Primitive Fields

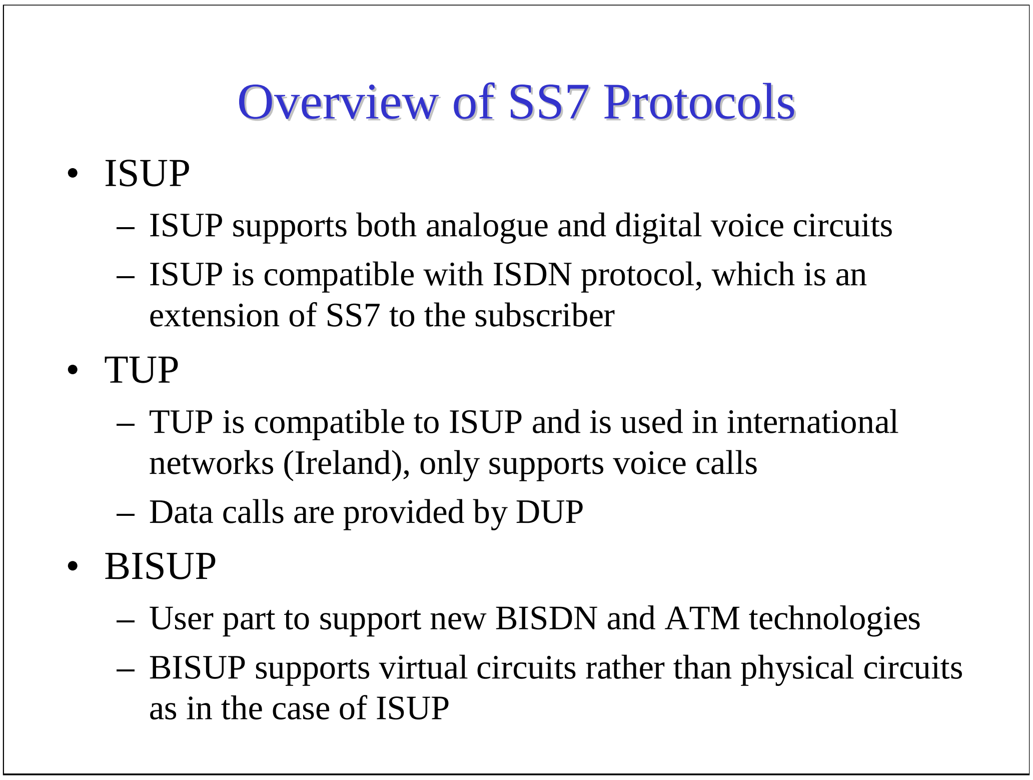
- X - indicates originator of primitive
  - “MTP” if the MTP is passing information to ISUP
- Generic name - indicates the type of information being provided
  - When information regarding address of originator (calling party address) is sent from ISUP to MTP, generic name is “unitdata”
  - generic name will different between levels
- Specific name - describes the action to be taken
  - request, indication, response, confirmation

Overview of SS7 Protocols

- Message Transfer Part (MTP)
  - Divided into 3 levels with similar functionality to OSI layer 1 to 3
  - Level 1 is the physical link interface
  - Level 2 provides link management and error control similar to other DLC protocols such as HDLC, LAPB/D, etc
  - Level 3 provide 4 functions - message routing, message discrimination, message distribution, and network management

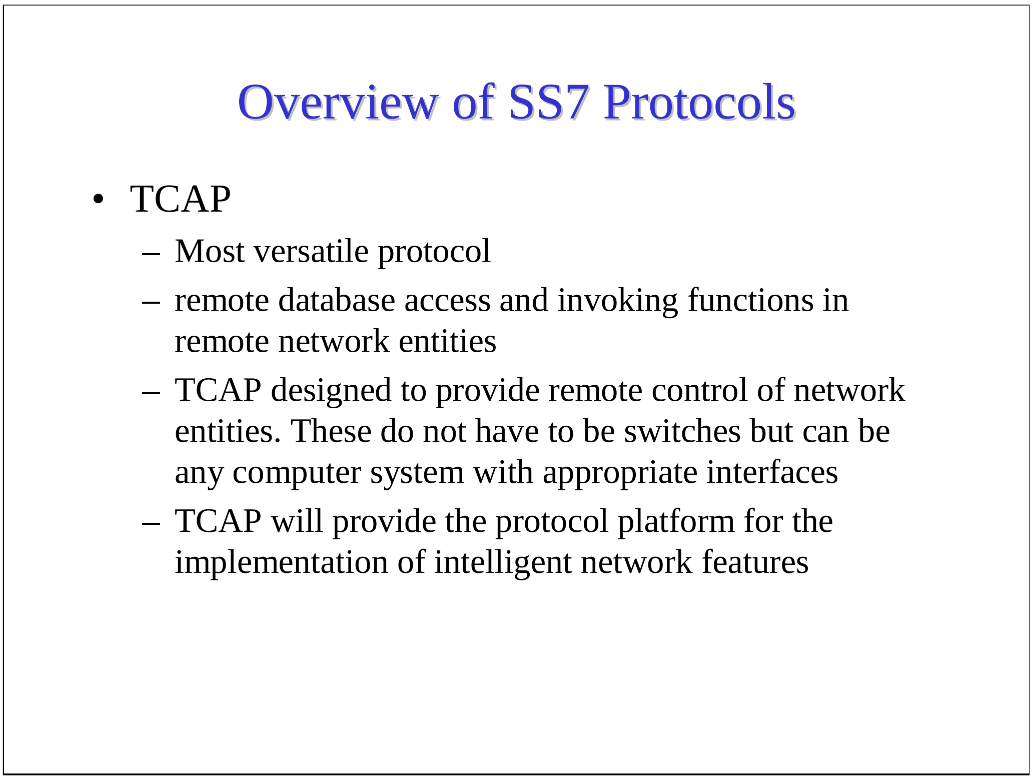
Overview of SS7 Protocols

- SCCP
  - so far only used with TCAP although ISUP may use SCCP too
  - SCCP provides means for end-to-end routing
  - SCCP uses more extensive addressing than MTP
- ISUP
  - circuit-related protocol used for establishing and maintaining connections throughout a call
  - ISUP is associated only with voice or data calls and does not support broadband technologies such as Frame Relay or ATM
  - BISUP will provide these new technologies



Overview of SS7 Protocols

- ISUP
  - ISUP supports both analogue and digital voice circuits
  - ISUP is compatible with ISDN protocol, which is an extension of SS7 to the subscriber
- TUP
  - TUP is compatible to ISUP and is used in international networks (Ireland), only supports voice calls
  - Data calls are provided by DUP
- BISUP
  - User part to support new BISDN and ATM technologies
  - BISUP supports virtual circuits rather than physical circuits as in the case of ISUP



Overview of SS7 Protocols

- TCAP
  - Most versatile protocol
  - remote database access and invoking functions in remote network entities
  - TCAP designed to provide remote control of network entities. These do not have to be switches but can be any computer system with appropriate interfaces
  - TCAP will provide the protocol platform for the implementation of intelligent network features

MTP Level 2

- Signalling Link Layer
- Provides error and link control on a point-to-point link between two adjacent nodes within an SS7 network
- Data transmission and link management is based on the three signal units
  - FISU
  - LSSU
  - MSU

MTP Level 2

- Functions include
  - Signal unit delimitation
  - Signal unit alignment
  - Signal unit error detection
  - Signal unit error correction
  - Signalling link initial alignment
  - Signalling link error monitoring
  - Flow control

MTP Level 2 - Operation

- FIB, FSN, BIB, and BSN implement flow and error control mechnisms typical for many layer 2 and layer 3 protocols
- MTP2 uses two types of error correction mechanisms (ARQ protocols)
  - Go-back-N with N = 127
  - Preventative Cyclic Retransmission (PCR)

Go-back-N ARQ

- Improves efficiency by adopting sliding-window flow control mechanism
- *N* denotes length of sliding window
- RR denotes ACK, REJ denotes NACK
- Principle
  - When a frame in error is received, destination sends a REJ and discards erroneous frame and all future frames until the one a frame is correctly received
  - Upon receipt of REJ, transmitter must retransmit erroneous frame and all frames that where sent in the meantime

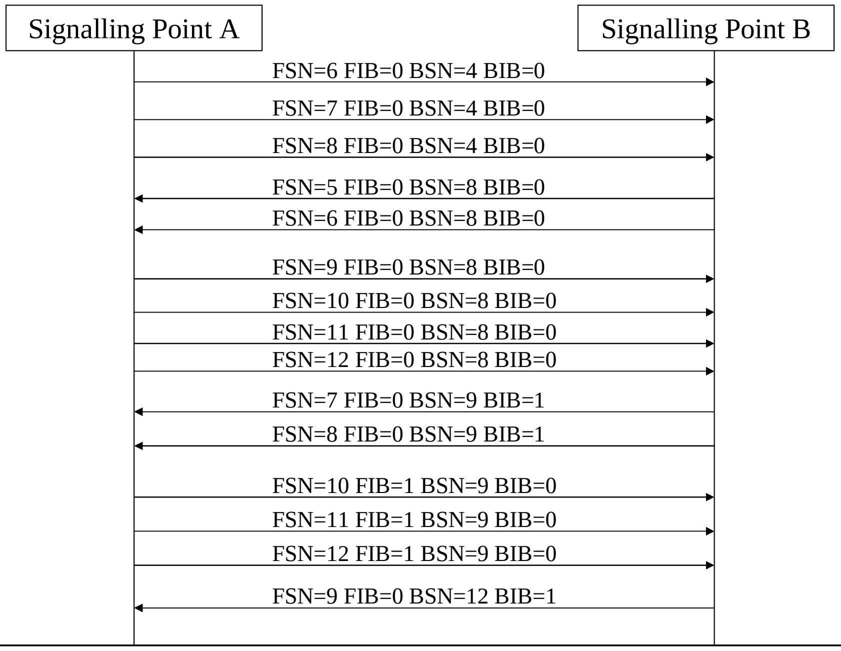
Go-back-N ARQ Operation

- Damaged Frame received
  - A transmits frame *i*. B detects error but has received *(i-1)* correctly. B sends REJ *i*, A retransmits *i* and all subsequent frames
  - Frame i was lost in transit. A sends *(i+1)*, B receives out of order frame and sends REJ i.
  - Frame i is lost. A does not send more frames and B receives nothing and does not send RR or REJ. A timer at A expires and A sends RR frame with poll bit *P = 1*. B sends RR with next frame it expects and A resends frame *i*

Go-back-N ARQ Operation

- Damaged RR
  - B receives *i* and sends RR *(i+1)*, which is lost. A may receive an RR to a subsequent frame before timer expires → no error
  - A’s timer expires and transmits an RR as in the case before. If RR response from B fails, A will try again for a number of times and than initiates link reset
  - A receives a damaged REJ. A acts like in the case of damaged RR.

Basic Error Correction Method -Go-back-N



Signalling Point A

Signalling Point B

FSN=6 FIB=0 BSN=4 BIB=0

FSN=7 FIB=0 BSN=4 BIB=0

FSN=8 FIB=0 BSN=4 BIB=0

FSN=5 FIB=0 BSN=8 BIB=0

FSN=6 FIB=0 BSN=8 BIB=0

FSN=9 FIB=0 BSN=8 BIB=0

FSN=10 FIB=0 BSN=8 BIB=0

FSN=11 FIB=0 BSN=8 BIB=0

FSN=12 FIB=0 BSN=8 BIB=0

FSN=7 FIB=0 BSN=9 BIB=1

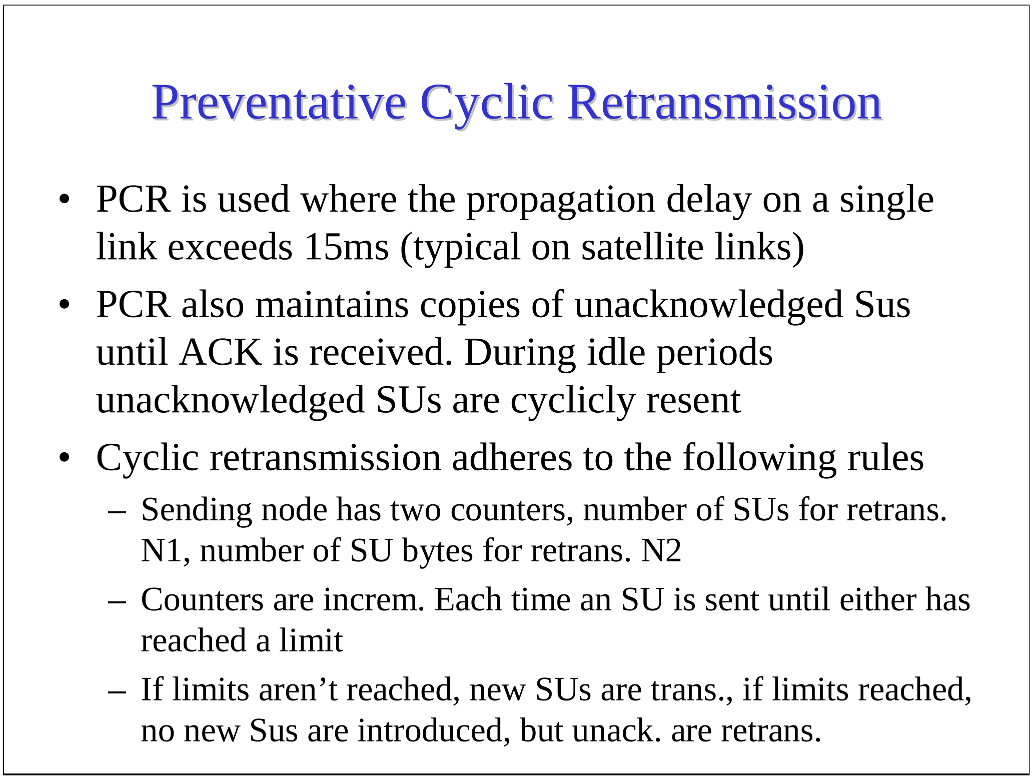
FSN=8 FIB=0 BSN=9 BIB=1

FSN=10 FIB=1 BSN=9 BIB=0

FSN=11 FIB=1 BSN=9 BIB=0

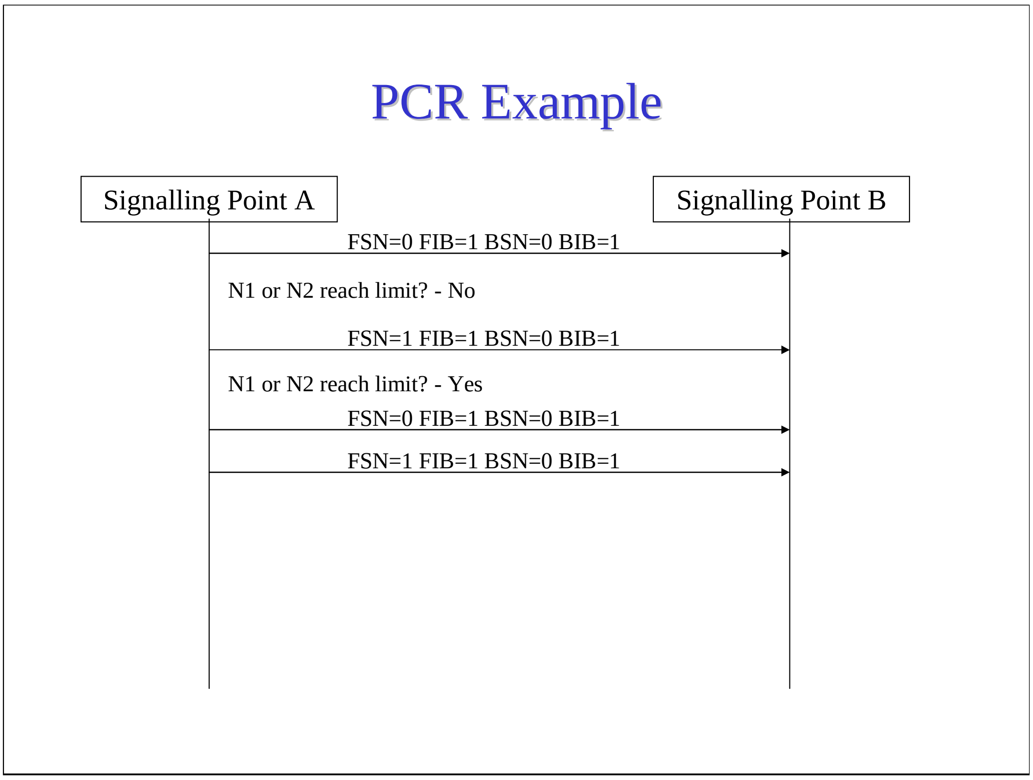
FSN=12 FIB=1 BSN=9 BIB=0

FSN=9 FIB=0 BSN=12 BIB=1



Preventative Cyclic Retransmission

- PCR is used where the propagation delay on a single link exceeds 15ms (typical on satellite links)
- PCR also maintains copies of unacknowledged Sus until ACK is received. During idle periods unacknowledged SUs are cyclicly resent
- Cyclic retransmission adheres to the following rules
  - Sending node has two counters, number of SUs for retrans. N1, number of SU bytes for retrans. N2
  - Counters are increm. Each time an SU is sent until either has reached a limit
  - If limits aren’t reached, new SUs are trans., if limits reached, no new Sus are introduced, but unack. are retrans.



PCR Example

Signalling Point A

Signalling Point B

FSN=0 FIB=1 BSN=0 BIB=1

N1 or N2 reach limit? - No

FSN=1 FIB=1 BSN=0 BIB=1

N1 or N2 reach limit? - Yes

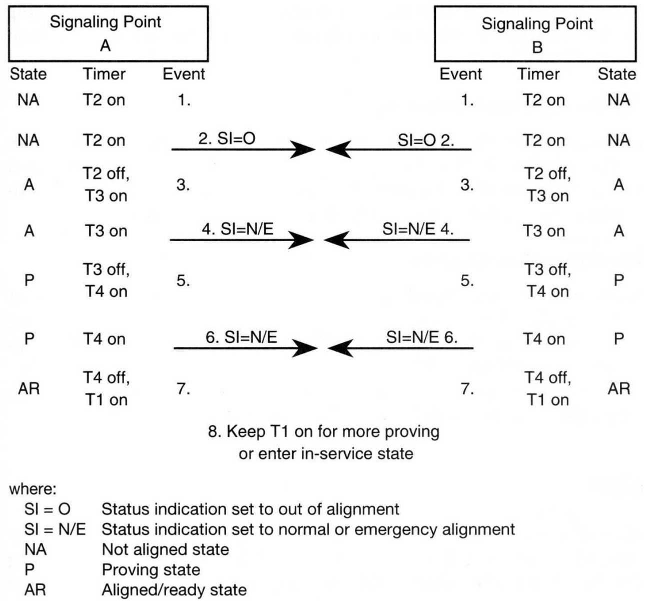
FSN=0 FIB=1 BSN=0 BIB=1

FSN=1 FIB=1 BSN=0 BIB=1

Signal Unit Alignment Procedure

- Used to activate and restore a signalling link
- Two proving periods available (chosen by MTP3)
  - normal proving
  - emergency proving
- Four alignment status indicators are used (coded in status field of LSSU)
  - O = out of alignment
  - N = normal alignment status
  - E = emergency alignment status
  - OS = out of service

SS7 Link Alignment - Example

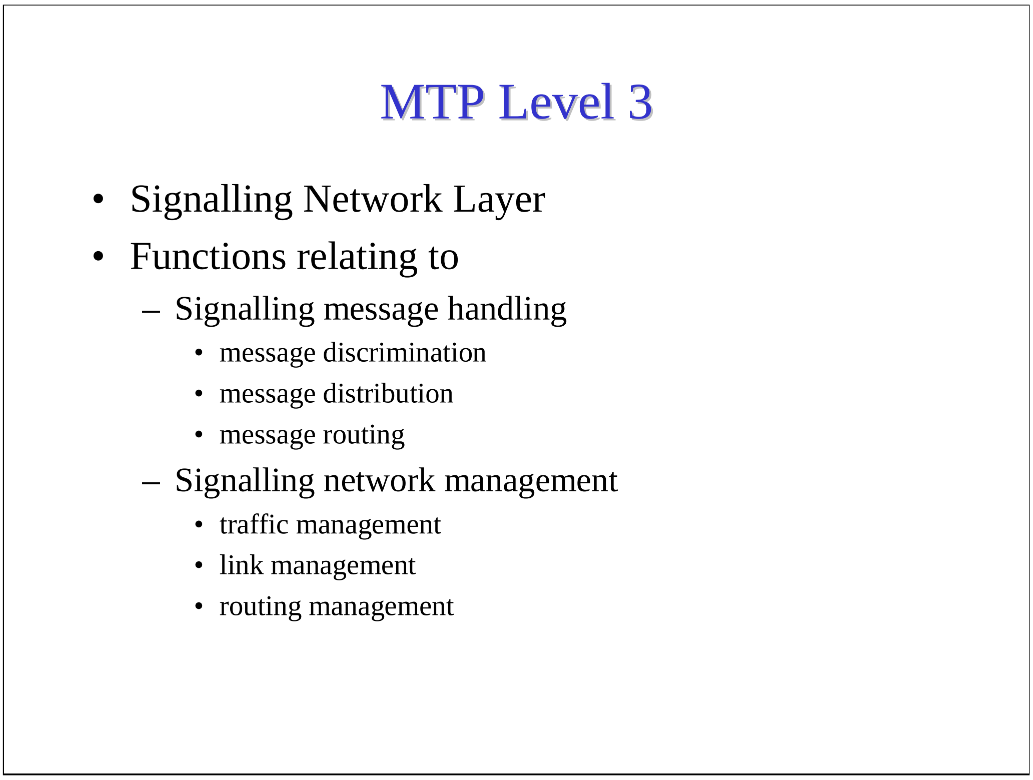


Signaling Point A						Signaling Point B	
State	Timer	Event			Event	Timer	State
NA	T2 on	1.			1.	T2 on	NA
NA	T2 on		2. SI=O →	← SI=O 2.		T2 on	NA
A	T2 off, T3 on	3.			3.	T2 off, T3 on	A
A	T3 on		4. SI=N/E →	← SI=N/E 4.		T3 on	A
P	T3 off, T4 on	5.			5.	T3 off, T4 on	P
P	T4 on		6. SI=N/E →	← SI=N/E 6.		T4 on	P
AR	T4 off, T1 on	7.			7.	T4 off, T1 on	AR

8. Keep T1 on for more proving
or enter in-service state

where:

SI = O	Status indication set to out of alignment
SI = N/E	Status indication set to normal or emergency alignment
NA	Not aligned state
P	Proving state
AR	Aligned/ready state



MTP Level 3

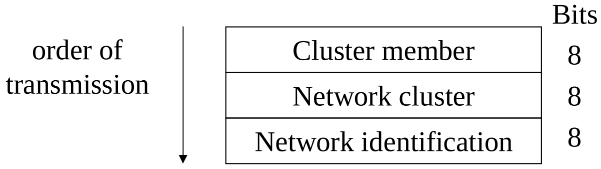
- Signalling Network Layer
- Functions relating to
  - Signalling message handling
    - message discrimination
    - message distribution
    - message routing
  - Signalling network management
    - traffic management
    - link management
    - routing management

SS7 Identifiers and Numbering Scheme

- SS7 signalling points (nodes) are identified by a unique address, the *point code*
- Point code is transparent to entities outside the SS7 network
- Point code is placed inside MTP3 message and is used for routing between signalling points
- PC is hierarchical address consisting of
  - network identifier
  - network cluster
  - network cluster member

SS7 Identifiers and Numbering Scheme

- SS7 also utilises a subsystem number (SSN) to identify a particular entity within a node
  - 1800 number service, calling card module, ISUP, etc
- SS7 also supports the *global title* (GT) identifier. This could be dialled digits of a telephone number.
- Best GT is combination of PC + SSN

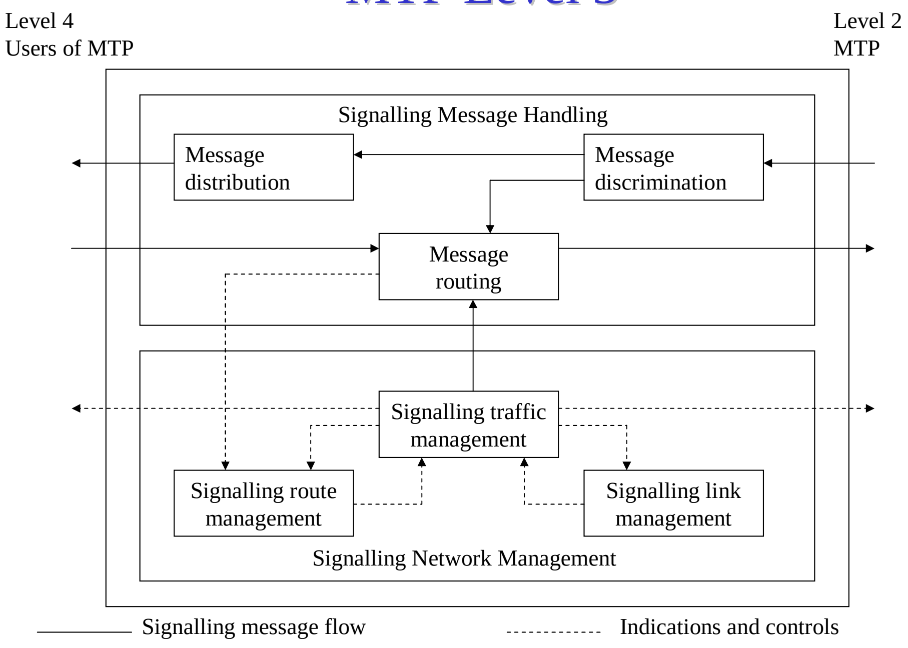


order of transmission

	Bits
Cluster member	8
Network cluster	8
Network identification	8

Format of signalling PC

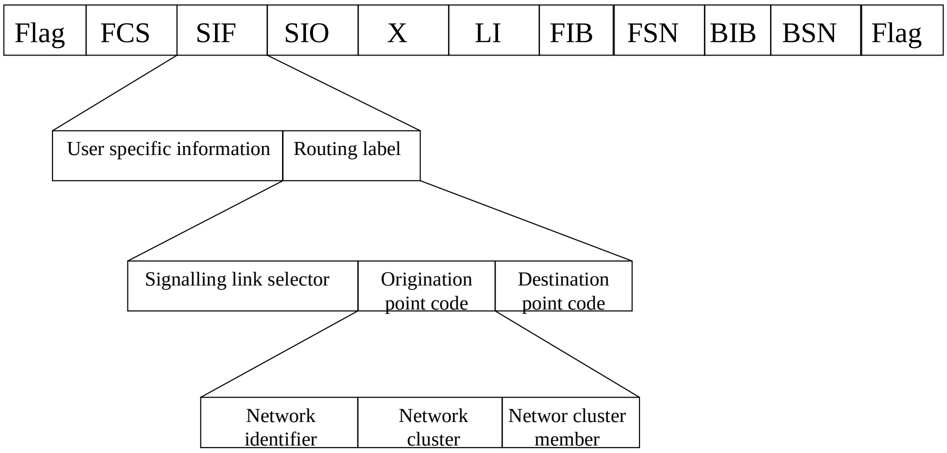
MTP Level 3


Level 4
Users of MTP
Level 2
MTP
Signalling Message Handling
Message distribution
Message discrimination
Message routing
Signalling traffic management
Signalling route management
Signalling link management
Signalling Network Management
Signalling message flow
Indications and controls

Signalling Message-handling Functions

- Message discrimination
  - determines upon PC if message is destined for this node (→ distribution) or other node (→ routing)
- Message distribution
  - passes message to appropriate application within node. Recipient is identified by Service Indicator Octet (SIO)
- Message routing
  - passes message to an appropriate link based on PC in the routing label. It also uses the Signalling Link Selection (SLS) field to determine which link in the link set to use

Routing Label



Flag	FCS	SIF	SIO	X	LI	FIB	FSN	BIB	BSN	Flag

User specific information	Routing label

Signalling link selector	Origination point code	Destination point code

Network identifier	Network cluster	Networ cluster member

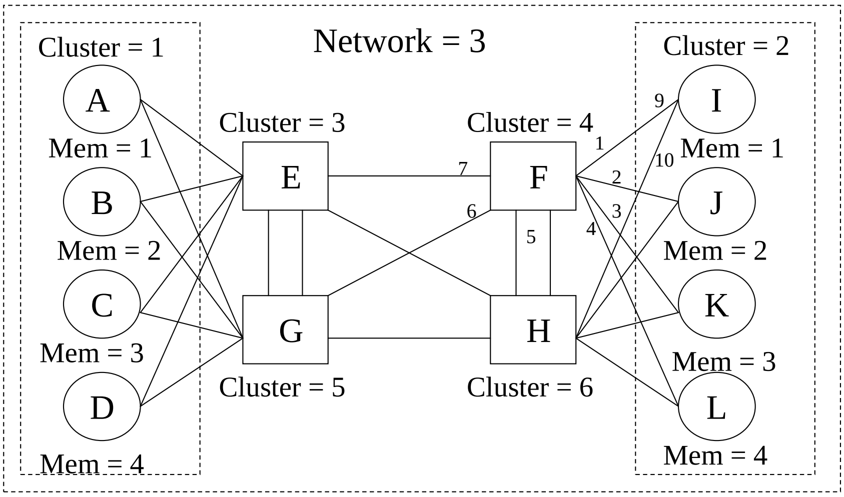
Signalling Link Selection

- Used to perform load sharing among links between adjacent signalling point by appropriately selecting links within a link set or among link sets
- 5-bit SLS is coded $X_1X_2X_3X_4X_5$, where X_i is either 0 or 1
- The LSB identifies the link set and the other 4 bits the link. If only one link set is used, the LSB is ignored
- Load sharing is achieved at each signalling point by rotating bits one position to the right within the SLS
- Bit rotation is not used for call control establishment messages and database queries as they require more than one SU and information has to be received in sequence.

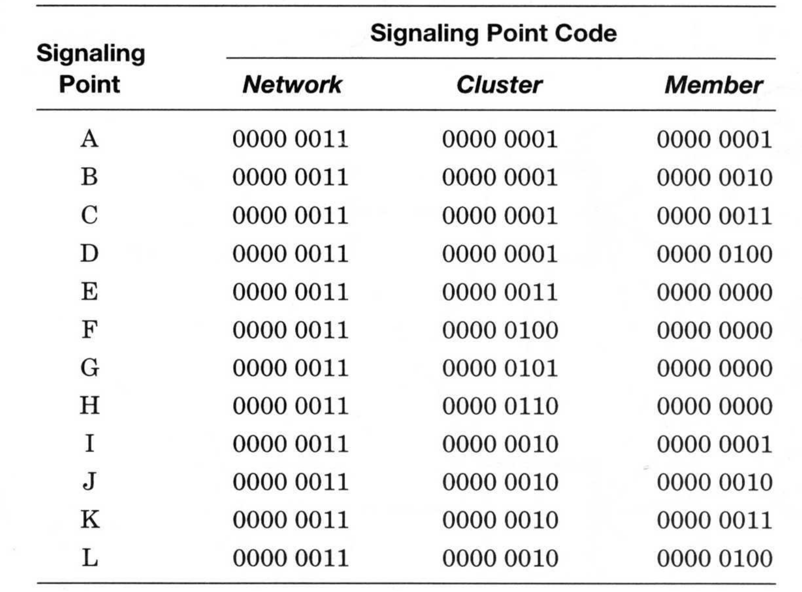
Routing in SS7 Networks

- Routing is based on the destination point code (DPC)
- Two approaches to routing
  - whole DPC is examined
  - part of DPC is examined → smaller routing tables
- Structure and contents of SS7 routing tables is not defined in standards. Approach is to design tables and software according to routing needs

SS7 Numbering Plan

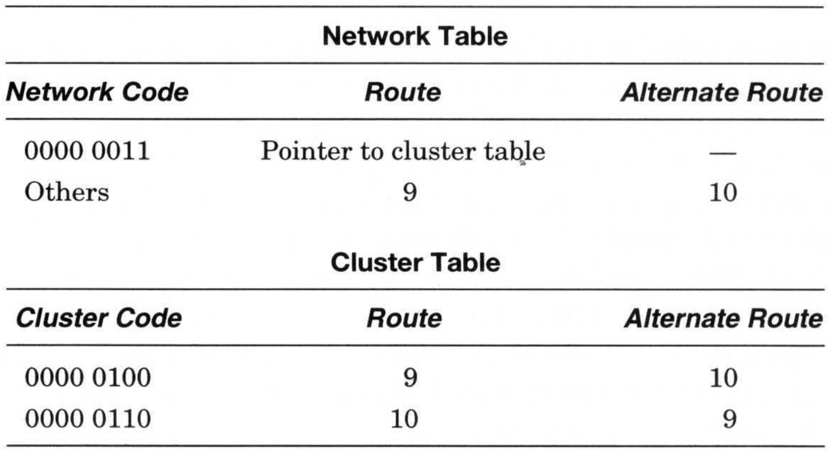


Address Table for Topology



Signaling Point	Signaling Point Code		
	Network	*Cluster*	*Member*
A	0000 0011	0000 0001	0000 0001
B	0000 0011	0000 0001	0000 0010
C	0000 0011	0000 0001	0000 0011
D	0000 0011	0000 0001	0000 0100
E	0000 0011	0000 0011	0000 0000
F	0000 0011	0000 0100	0000 0000
G	0000 0011	0000 0101	0000 0000
H	0000 0011	0000 0110	0000 0000
I	0000 0011	0000 0010	0000 0001
J	0000 0011	0000 0010	0000 0010
K	0000 0011	0000 0010	0000 0011
L	0000 0011	0000 0010	0000 0100

Routing Tables for Signalling Point I



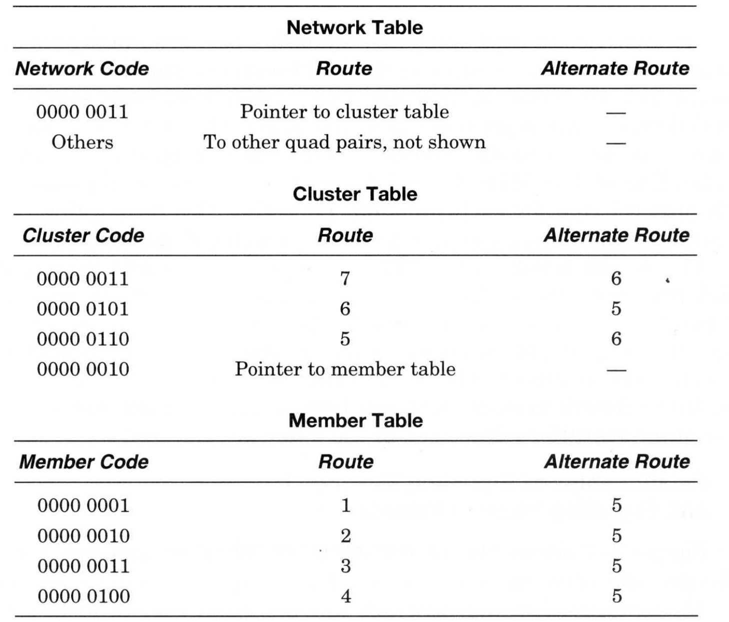
Network Table

Network Code	*Route*	*Alternate Route*
0000 0011	Pointer to cluster table	—
Others	9	10

Cluster Table

Cluster Code	*Route*	*Alternate Route*
0000 0100	9	10
0000 0110	10	9

Routing Tables for Signalling Point F



Network Table

Network Code	*Route*	*Alternate Route*
0000 0011	Pointer to cluster table	—
Others	To other quad pairs, not shown	—

Cluster Table

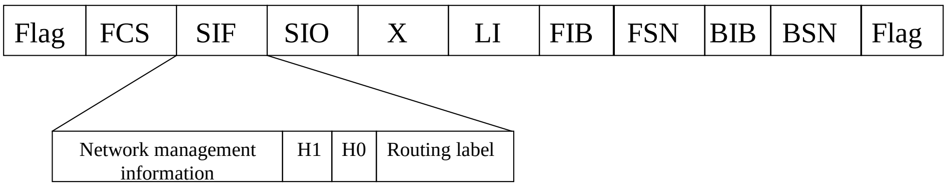
Cluster Code	*Route*	*Alternate Route*
0000 0011	7	6
0000 0101	6	5
0000 0110	5	6
0000 0010	Pointer to member table	—

Member Table

Member Code	*Route*	*Alternate Route*
0000 0001	1	5
0000 0010	2	5
0000 0011	3	5
0000 0100	4	5

Singalling Network Management Functions

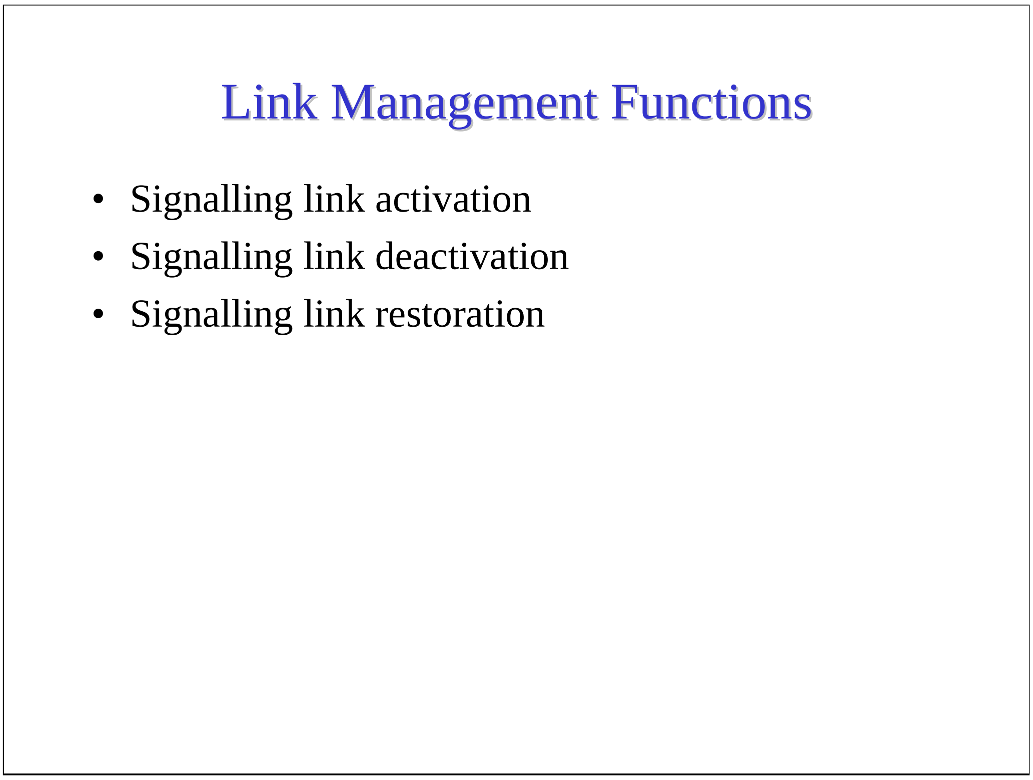
- Three categories
  - Signalling traffic management
  - Signalling link management
  - Signalling route management
- Network management messages use MSU



Flag	FCS	SIF	SIO	X	LI	FIB	FSN	BIB	BSN	Flag

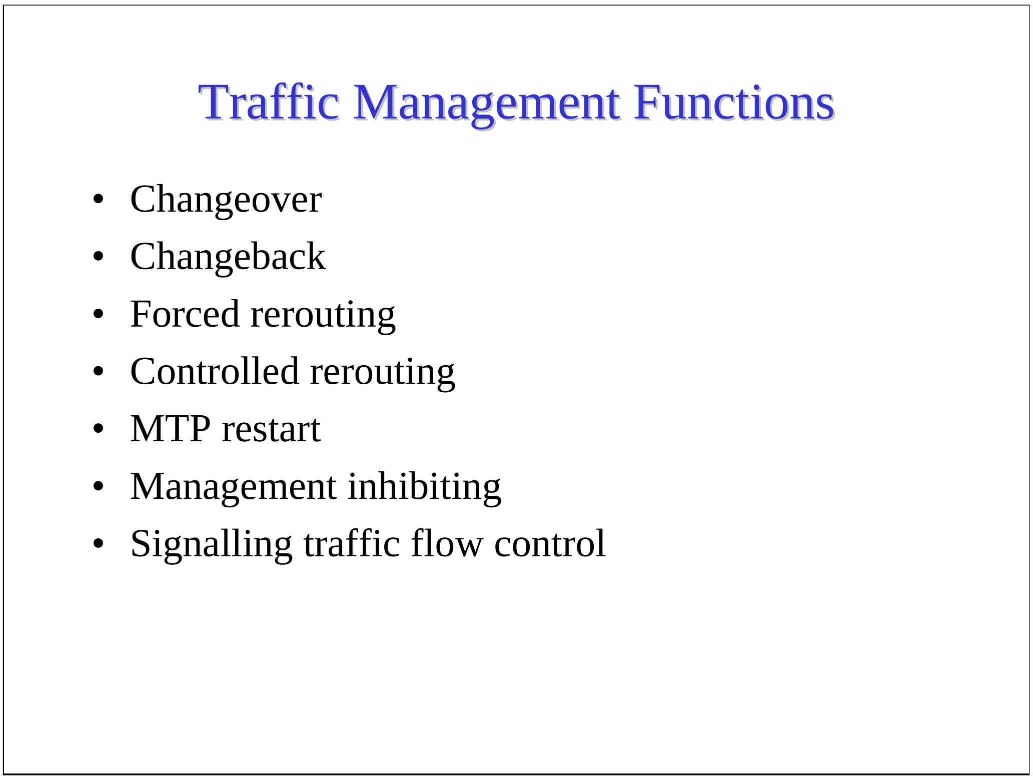
Network management information	H1	H0	Routing label

H0/H1 fields identify type of network management message



Link Management Functions

- Signalling link activation
- Signalling link deactivation
- Signalling link restoration



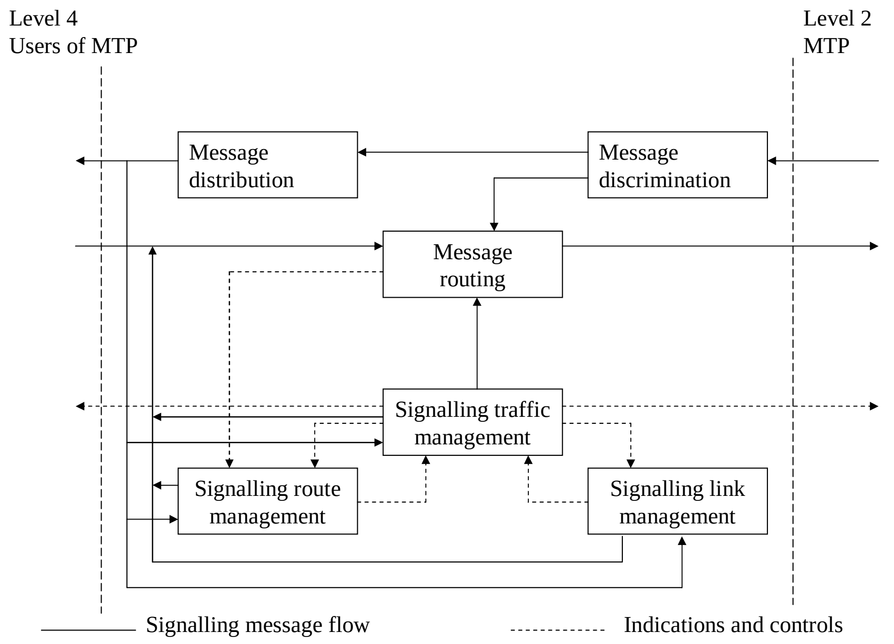
Traffic Management Functions

- Changeover
- Changeback
- Forced rerouting
- Controlled rerouting
- MTP restart
- Management inhibiting
- Signalling traffic flow control

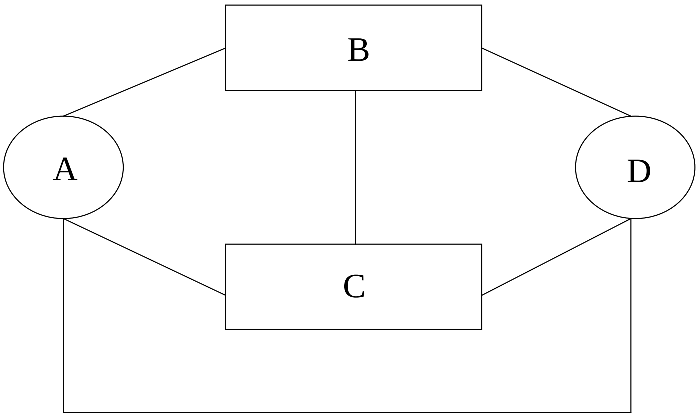
Routing Management Functions

- Transfer-prohibit procedure
- Transfer-restrict procedure
- Transfer-controlled procedure
- Transfer-allowed procedure
- Signalling-route-set-test procedure
- Singalling-route-set-congestion-test procedure

Relationship of functions within MTP3



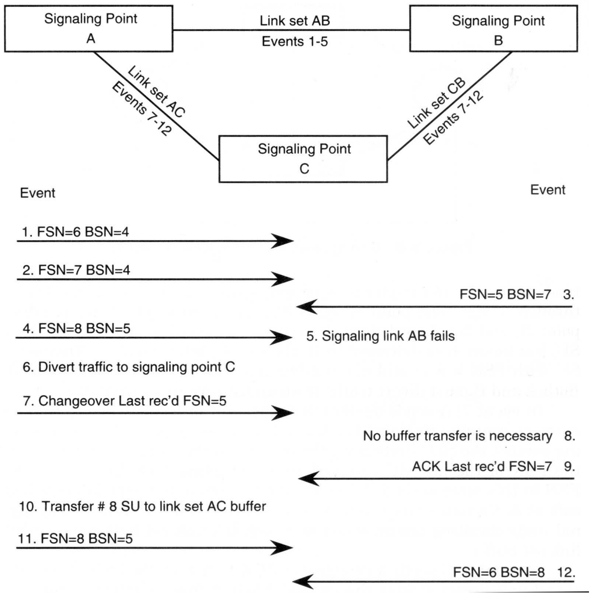
Changeover/Changeback



Changeover/Changeback

- Changeover is where signalling traffic is changed from an unavailable link to an alternative link
  - new link parallel to old link; traffic diversion from AF to another link
  - New link is through another route, but route passes through STP at far end of old link (STP B). Diversion is from link set AF to AC and CF
  - New link is through another route and route does not passes through STP at far end of old link (STP B). Diversion is from link set AB, BF to link set AC and CF
- Changeback is the opposite operation to changeover and switches the signalling traffic back from the alternative route to the main route

Changeover Operation - Example



1. FSN=6 BSN=4

2. FSN=7 BSN=4

FSN=5 BSN=7 3.

4. FSN=8 BSN=5

5. Signaling link AB fails

6. Divert traffic to signaling point C

7. Changeover Last rec'd FSN=5

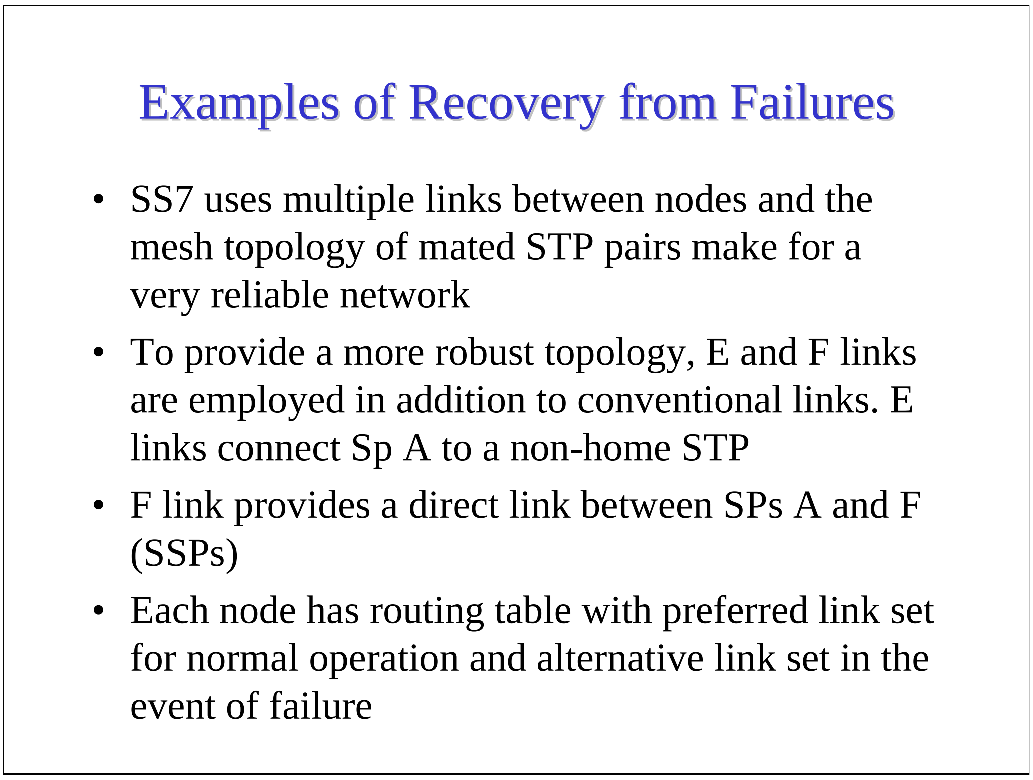
No buffer transfer is necessary 8.

ACK Last rec'd FSN=7 9.

10. Transfer # 8 SU to link set AC buffer

11. FSN=8 BSN=5

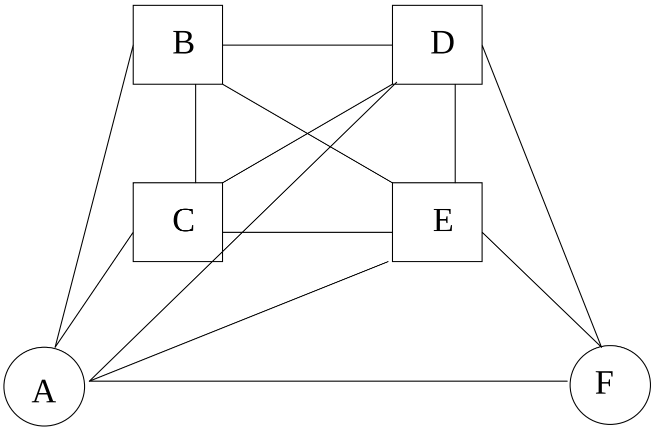
FSN=6 BSN=8 12.



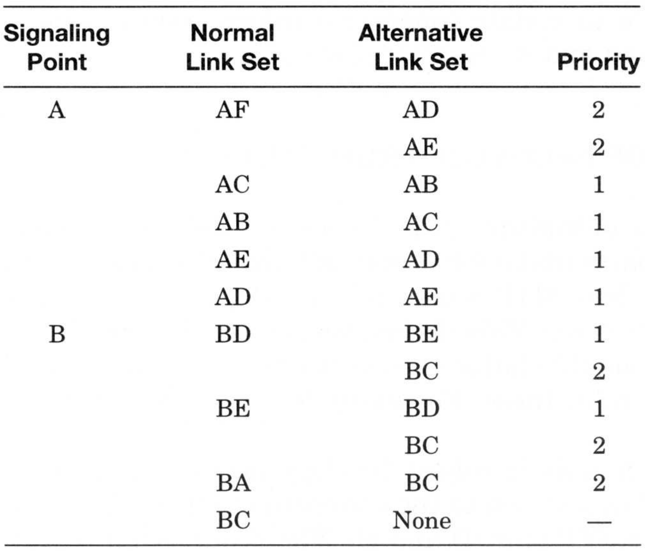
Examples of Recovery from Failures

- SS7 uses multiple links between nodes and the mesh topology of mated STP pairs make for a very reliable network
- To provide a more robust topology, E and F links are employed in addition to conventional links. E links connect Sp A to a non-home STP
- F link provides a direct link between SPs A and F (SSPs)
- Each node has routing table with preferred link set for normal operation and alternative link set in the event of failure

Model for Alternate Link Sets

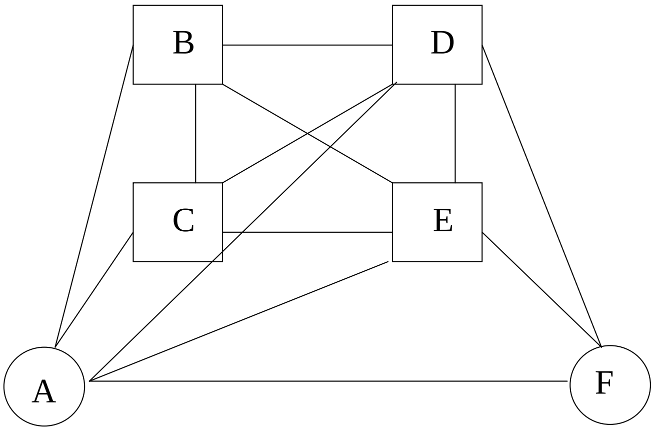


Normal and Alternative Link Set Table

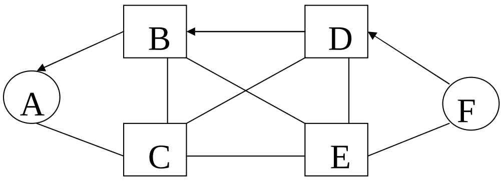


Signaling Point	Normal Link Set	Alternative Link Set	Priority
A	AF	AD	2
		AE	2
	AC	AB	1
	AB	AC	1
	AE	AD	1
	AD	AE	1
B	BD	BE	1
		BC	2
	BE	BD	1
		BC	2
	BA	BC	2
	BC	None	—

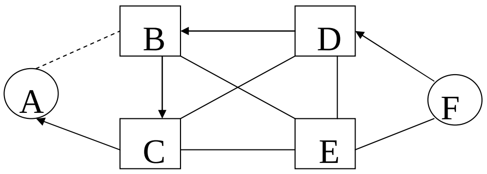
Failure of Access Links or Switches



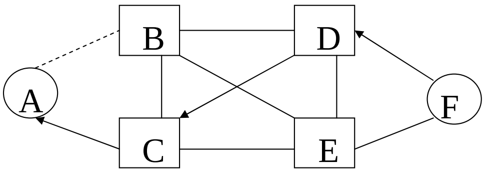
Initial and Final Traffic Diversion



Normal traffic flow from F to A

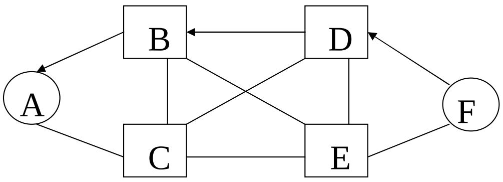


Diverted traffic flow from F to A when AB link fails

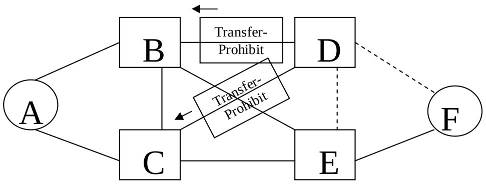


STP B informs STP D (and E) to divert traffic

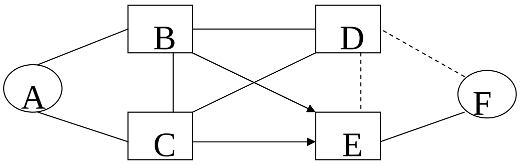
Transfer-prohibit Procedure



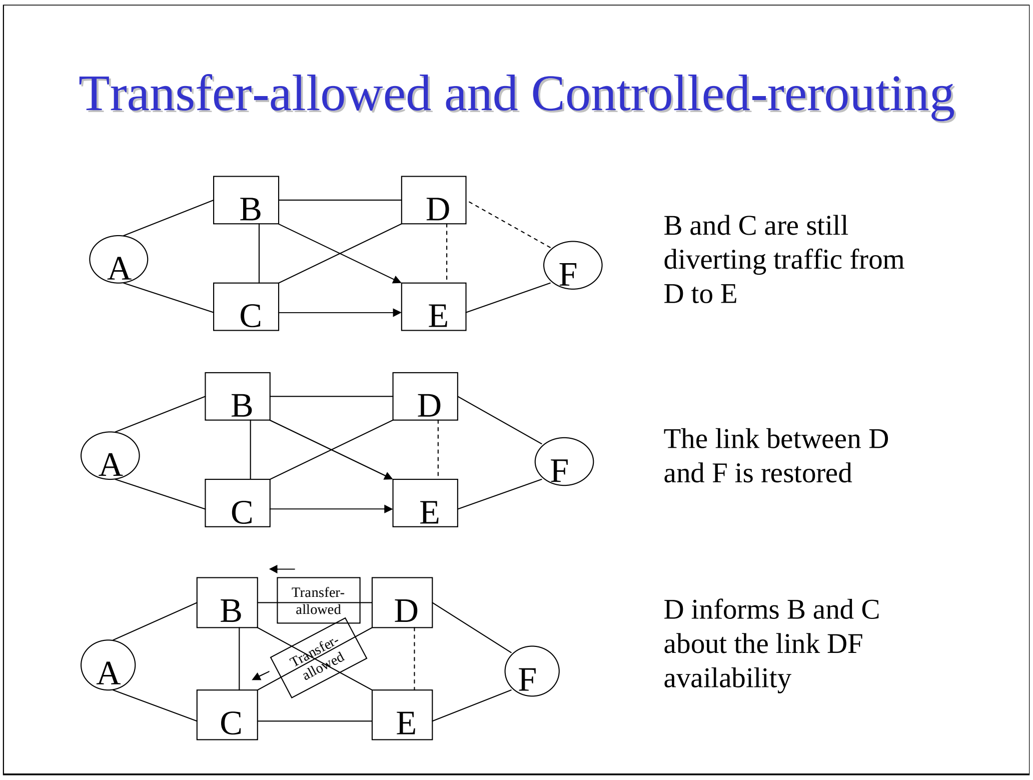
Normal traffic flow from F to A



D notes loss of links and sends transfer-prohibit messages



B and C divert traffic from D to E



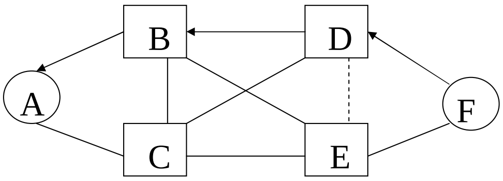
Transfer-allowed and Controlled-rerouting

B and C are still diverting traffic from D to E

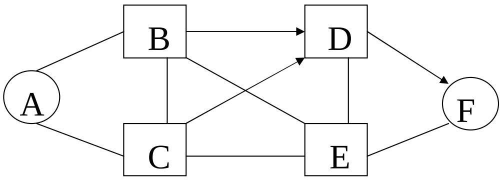
The link between D and F is restored

D informs B and C about the link DF availability

Transfer-allowed and Controlled-rerouting

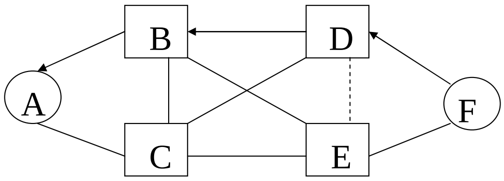


F returns to sending traffic to D

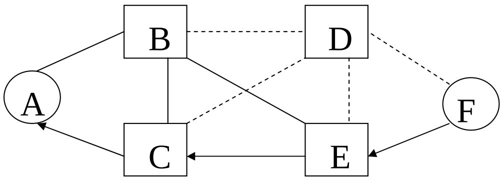


B and C resume their normal routing to D

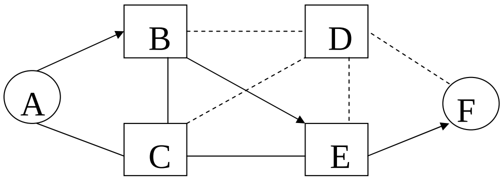
Failure of Multiple Links



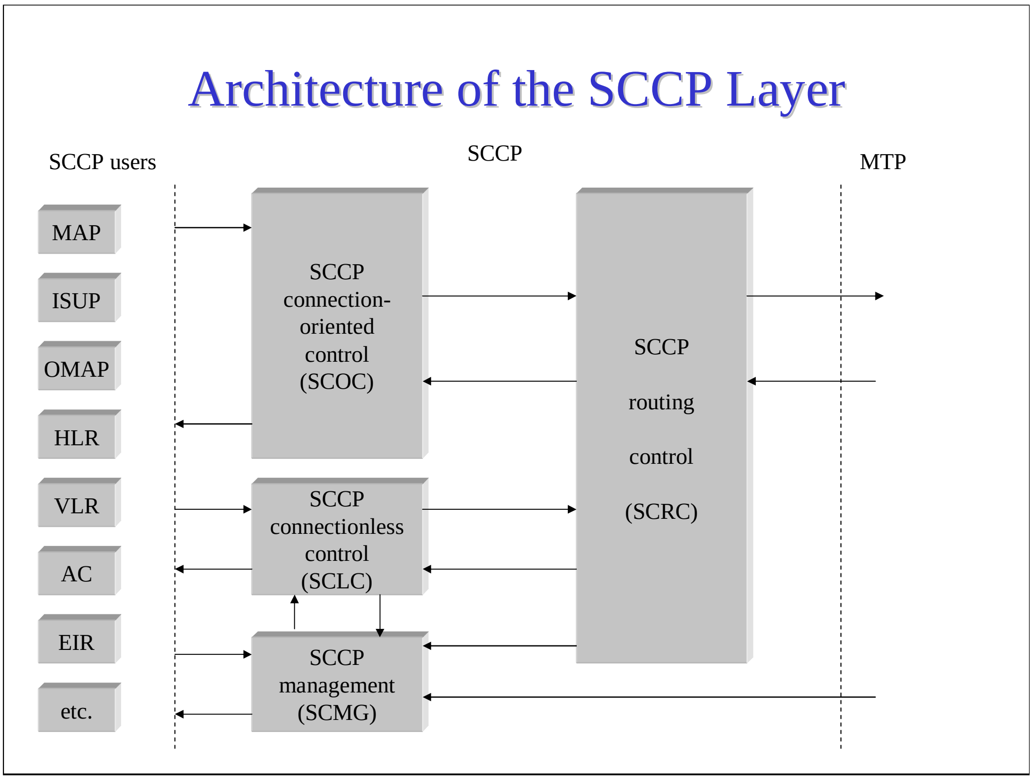
Traffic flow from F to A



STP B down; Traffic flow from F to A after STP B goes down



Traffic flow from A to F



Architecture of the SCCP Layer

SCCP users
SCCP
MTP
MAP
ISUP
OMAP
HLR
VLR
AC
EIR
etc.
SCCP connection-oriented control (SCOC)
SCCP connectionless control (SCLC)
SCCP management (SCMG)
SCCP routing control (SCRC)

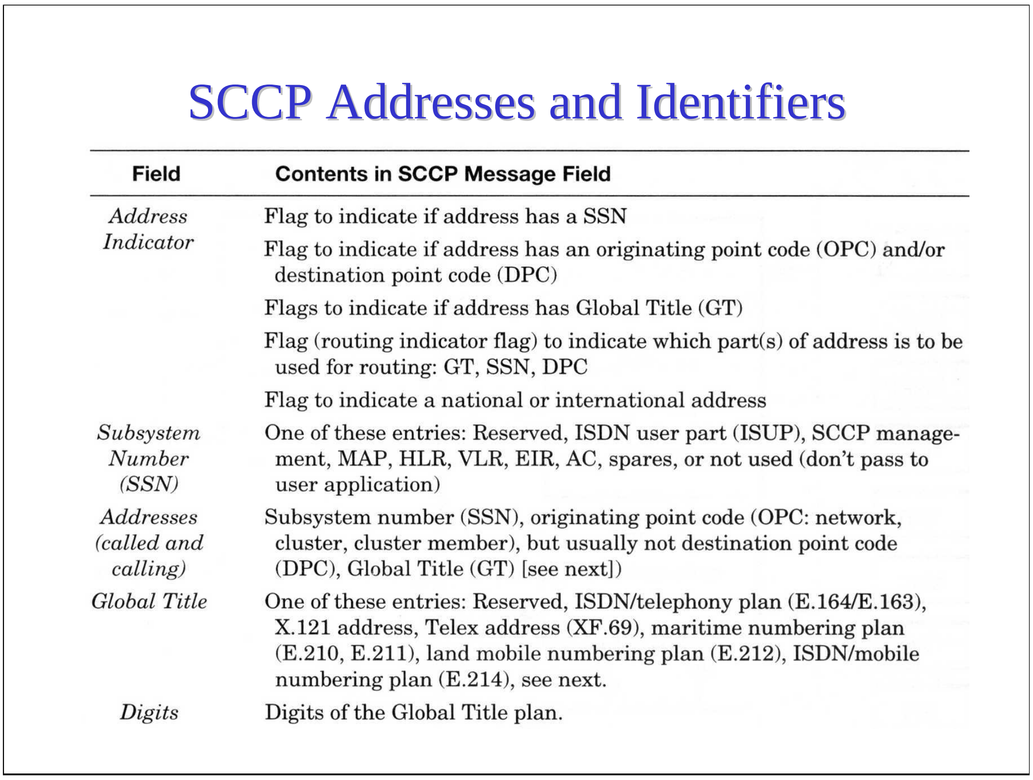
SCCP sits between the upper layers, which may consist of a wide variety of applications and user parts, such as ISUP, MAP, etc., an the lower layer, MTP3. SCCP is made up of four entities: SSCP routing control (SCRC), SCCP connection-oriented control (SCOC), SSCP connectionless control (SCLC), and SCCP management (SCMG).

SCRC is responsible for ttwo major operations: routing and address translation. Routing is performed internally by relaying the traffic to another user entity or to one of the three other SCCP entities. SCRC can translate different types of addresses, such as a global title to a destination point code.

SCOC is responsible for setting up a connection between two users of SCCP, transferring traffic between these users, and tearing down the connection. It supports several features, such as segmentation, sequencing, and flow control.

SCLC is responsible for transferring traffic between two users of SCCP but it does not create a connection. In addition, unlike SCOC, it has limited features.

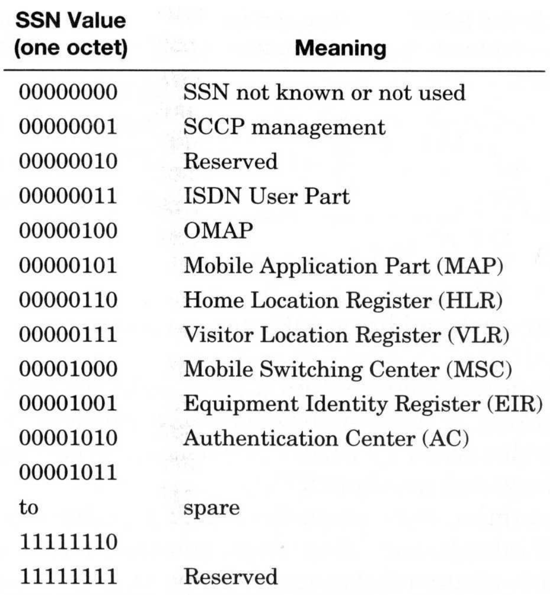
SCMG is used for management and status operations. Some of its primary functions are: coordinating the withdrawal of a subsystem (SSN), informing SCCP management about the status of an originating user or the status of a connection, and providing information about the type of traffic pattern a user is receiving.



SCCP Addresses and Identifiers

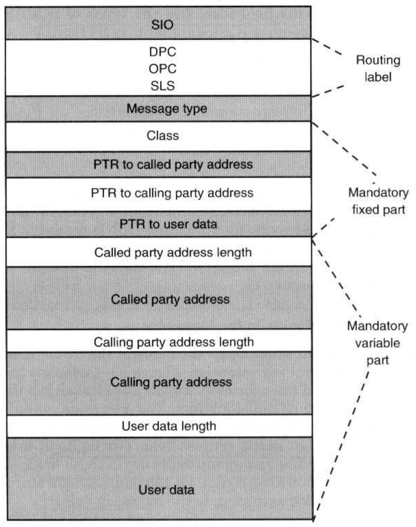
Field	Contents in SCCP Message Field
Address Indicator	Flag to indicate if address has a SSN Flag to indicate if address has an originating point code (OPC) and/or destination point code (DPC) Flags to indicate if address has Global Title (GT) Flag (routing indicator flag) to indicate which part(s) of address is to be used for routing: GT, SSN, DPC Flag to indicate a national or international address
Subsystem Number (SSN)	One of these entries: Reserved, ISDN user part (ISUP), SCCP management, MAP, HLR, VLR, EIR, AC, spares, or not used (don't pass to user application)
Addresses (called and calling)	Subsystem number (SSN), originating point code (OPC: network, cluster, cluster member), but usually not destination point code (DPC), Global Title (GT) [see next])
Global Title	One of these entries: Reserved, ISDN/telephony plan (E.164/E.163), X.121 address, Telex address (XF.69), maritime numbering plan (E.210, E.211), land mobile numbering plan (E.212), ISDN/mobile numbering plan (E.214), see next.
Digits	Digits of the Global Title plan.

Subsystem Numbers



SSN Value (one octet)	Meaning
00000000	SSN not known or not used
00000001	SCCP management
00000010	Reserved
00000011	ISDN User Part
00000100	OMAP
00000101	Mobile Application Part (MAP)
00000110	Home Location Register (HLR)
00000111	Visitor Location Register (VLR)
00001000	Mobile Switching Center (MSC)
00001001	Equipment Identity Register (EIR)
00001010	Authentication Center (AC)
00001011 to 11111110	spare
11111111	Reserved

SCCP Message Structure



SIO

DPC
OPC
SLS

Message type

Class

PTR to called party address

PTR to calling party address

PTR to user data

Called party address length

Called party address

Calling party address length

Calling party address

User data length

User data

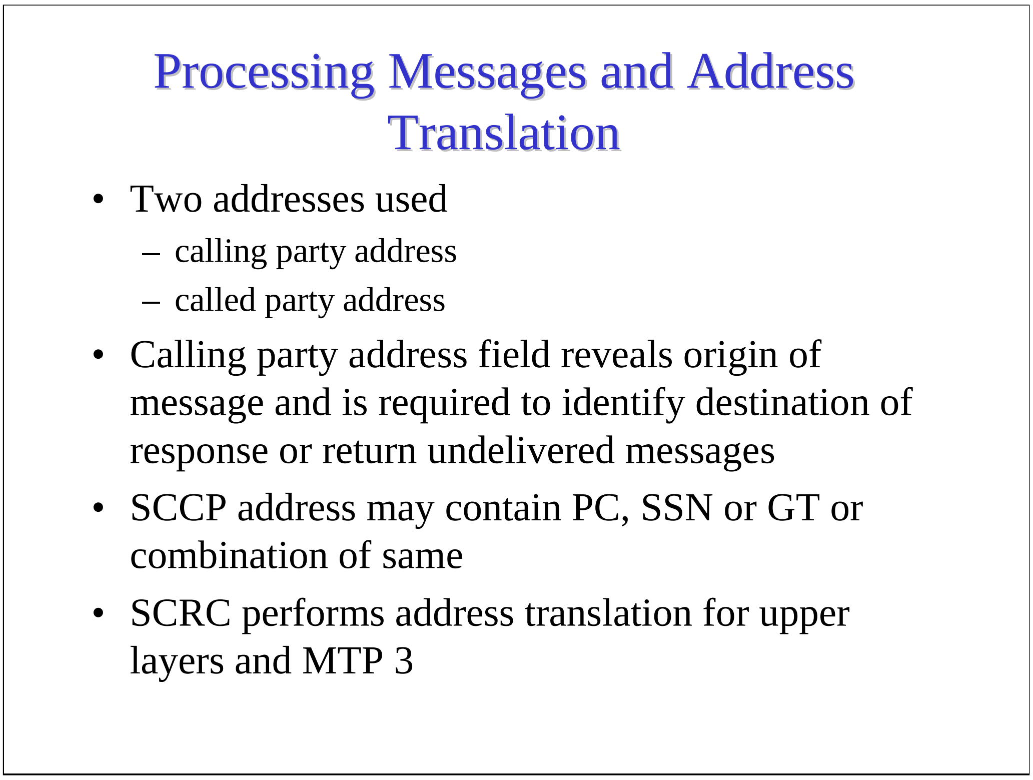
Routing label

Mandatory fixed part

Mandatory variable part

where:

DPC	Destination point code
OPC	Originating point code
PTR	Pointer
SIO	Signaling information octet
SLS	Signaling link selector

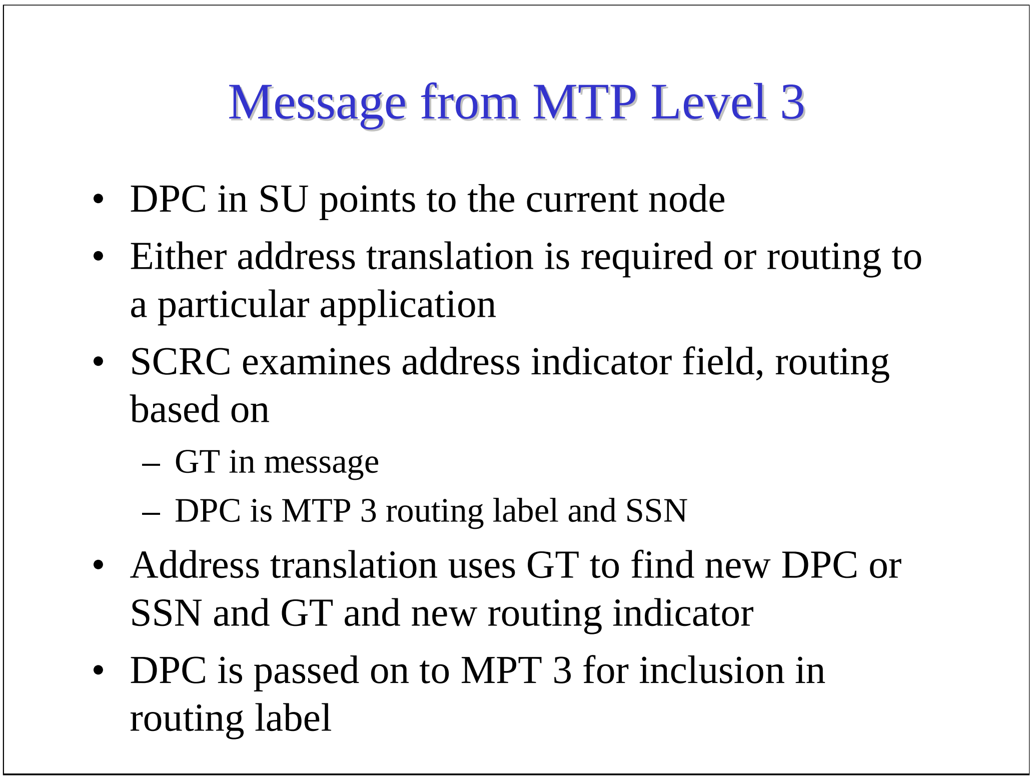


Processing Messages and Address Translation

- Two addresses used
  - calling party address
  - called party address
- Calling party address field reveals origin of message and is required to identify destination of response or return undelivered messages
- SCCP address may contain PC, SSN or GT or combination of same
- SCRC performs address translation for upper layers and MTP 3

Message Translation for Upper Layer

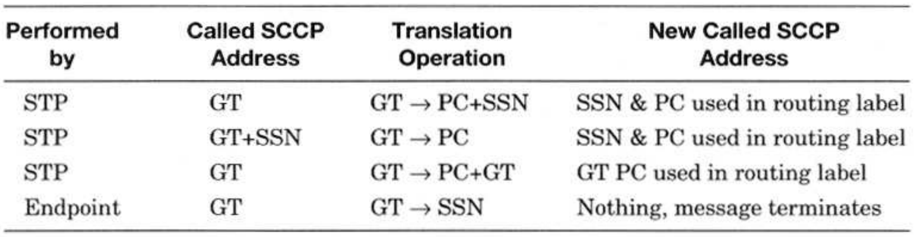
- SCRC receives message from user layer, address in forms
  - DPC
  - DPC + (SSN and/or GT)
  - GT
  - GT + SSN
- If DPC is not present, SCCP must derive it from GT (using mapping table setup by network engineers)
- If DPC = other node, message is passed to MTP 3 otherwise it is routed internally based on SSN



Message from MTP Level 3

- DPC in SU points to the current node
- Either address translation is required or routing to a particular application
- SCRC examines address indicator field, routing based on
  - GT in message
  - DPC is MTP 3 routing label and SSN
- Address translation uses GT to find new DPC or SSN and GT and new routing indicator
- DPC is passed on to MPT 3 for inclusion in routing label

Common SCCP Translation

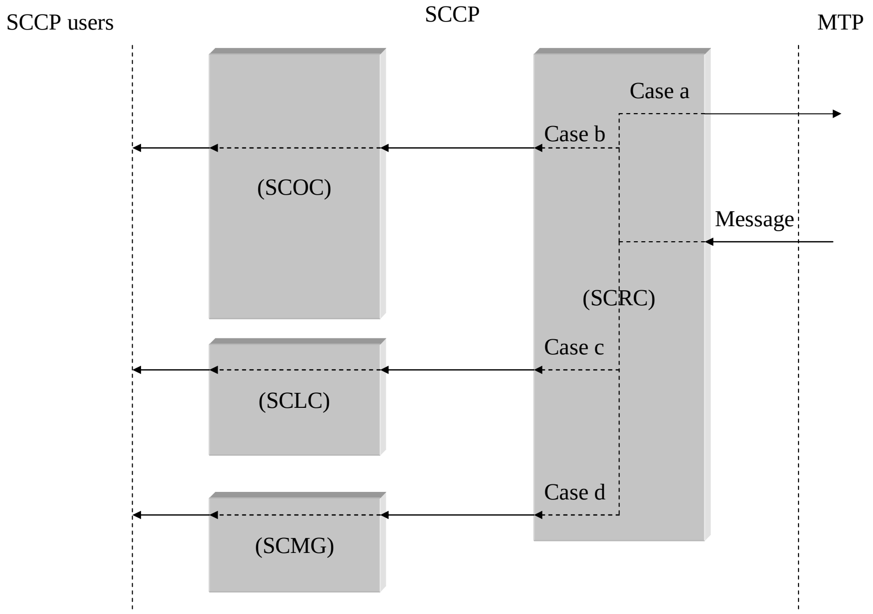


Performed by	Called SCCP Address	Translation Operation	New Called SCCP Address
STP	GT	GT → PC+SSN	SSN & PC used in routing label
STP	GT+SSN	GT → PC	SSN & PC used in routing label
STP	GT	GT → PC+GT	GT PC used in routing label
Endpoint	GT	GT → SSN	Nothing, message terminates

Routing

- SS7 routing is typically performed by MTP 3 without any assistance from SCCP
- If the DPC is complete and identifies a non-local signalling point no action by SCCP is required
- SCCP is invoked when the SU requires address translation

Processing Traffic Received from MTP 3

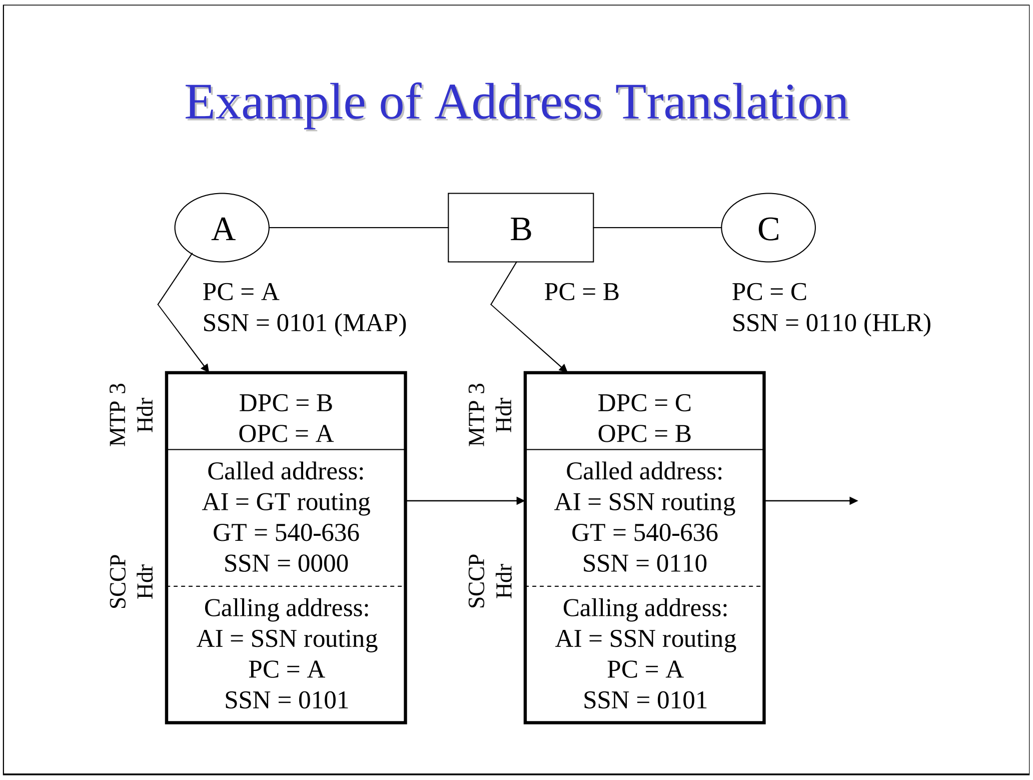


SCRC examines address indicator field in the SCCP header. If routing indicator bit indicates that the routing is to be performed on the global title, an address translation will be performed to determine both DPC and SSN. If the DPC is the node itself, and the SSN is correct, the message is passed either to SCOC or SCLC, which are labeled cases b and c, respectively, in the slide above.

If the DPC is not the node itself, the message is passed back to MPT 3 (case a). One exception to the previous statement should be explained. If the message is associated with an end-to-end connection (between three more more signalling points), it is passed to SCOC for some housekeeping operations, then back to SCRC, and to MPT 3.

If the message is non-user traffic, such as status messwages, diagnostics, etc., it is passed to SCMG for further processing (case d).

The processing of traffic received from the user and application parts of the signalling node are processed in the reverse fashion, mainly by case a routing.



Example of Address Translation

DPC = B
OPC = A

Called address:
AI = GT routing
GT = 540-636
SSN = 0000

Calling address:
AI = SSN routing
PC = A
SSN = 0101

DPC = C
OPC = B

Called address:
AI = SSN routing
GT = 540-636
SSN = 0110

Calling address:
AI = SSN routing
PC = A
SSN = 0101

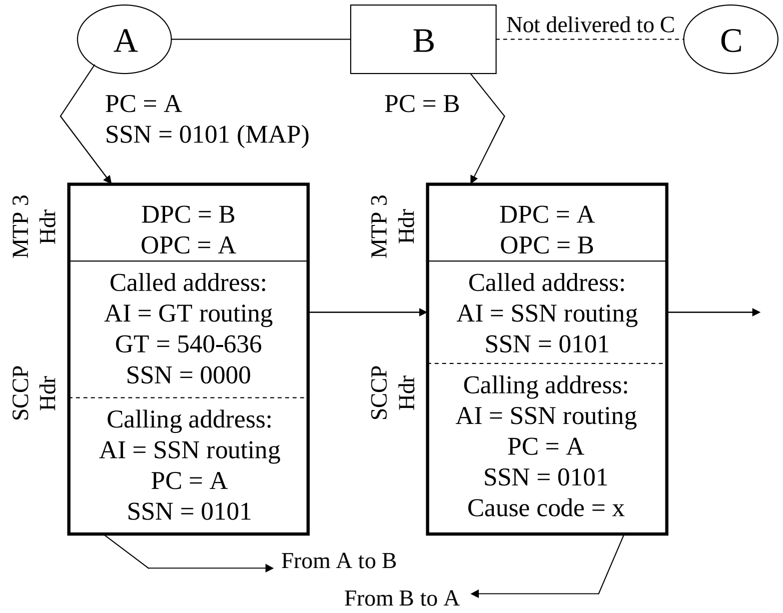
The slide shows an exampleof a successful operation, where the translations take place at signalling point B. Three nodes are involved, A, B, and C. A is sending traffic from its mobile application part (MAP) user application, which must be identified with the SSN = 0101.

A places its originating point code (OPC=A) and the destination point code (DPC = B) in the MTP 3 header. In the SCCP header, it codes the called address and calling address fields. For the called address, a bit in the address indicator (AI) field connotes that routing is to be performed on the global title (GT), which is 540-636. The subsystem number (SSN) is set to 0000, which is a reserved number stipulating that the SSN is not used (or not known).

For the calling address, the AI bit is set by A, but is not used (in this example). The PC is A (originating point code), and the SSN is set to 0101, which identifies the MAP. This message is routed to signalling point B. MTP 3 passes the message to SCCP, which examines the SCCP header. Based on the header, SCCP creates/modifies these fields, changes DPC and OPC values, and passes this information to its MTP 3 layer for sending on to node C.

SCCP has changed the DPC to C, and the OPC to B. In effect, SCCP translated the GT of 540-636 to PC = B; it also chnages SSN to 0110, the HLR application at node C. Notice that the AI bit is set to indicate SSN-based routing, which is used at C to determine what part of the SCCP address is used.

Routing or Translation Problem

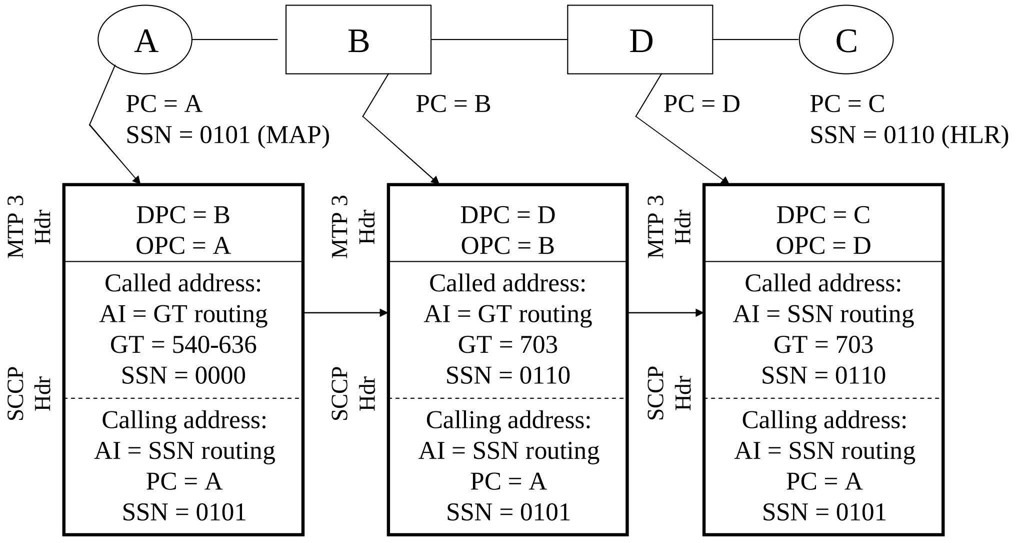


The slide shows an example of an unsuccessful routing/translation operation. The message sent from A to B is the same as in the previous slide. However, this time, node B cannot process the message, so nothing is delivered to C. Instead, B returns a message to A with a cause code that explains why the operation was not successful. The cause code may indicate that node B does not have a translation available for the SCCP called address party, or that some type of failure occurred that has nothing to do with translation. Whatever the case may be, the message from B has the SCCP called address coded as SSN routing, with A’s SSN of 0101 filled into the SSN value. This allows node A to give this response to the application that originated the message.

The SCCP called address is coded as GT routing, with GT set to the same value that was in A’s SCCP called address field. The presence of this value allows A to know GT 540-636 cannot be processed by B. Typically, this type of message will invoke troubleshooting procedures between A and B.

If the terminating node C experiences a problem, it returns a message to A, through B, but B will process the message only up to MTP 3 layer. SCCP will not participate in the operation at B, since it processed the request successfully. It is then up to nodes A and C to resolve the problem.

Operation with Two Translations



PC = A
SSN = 0101 (MAP)

PC = B

PC = D

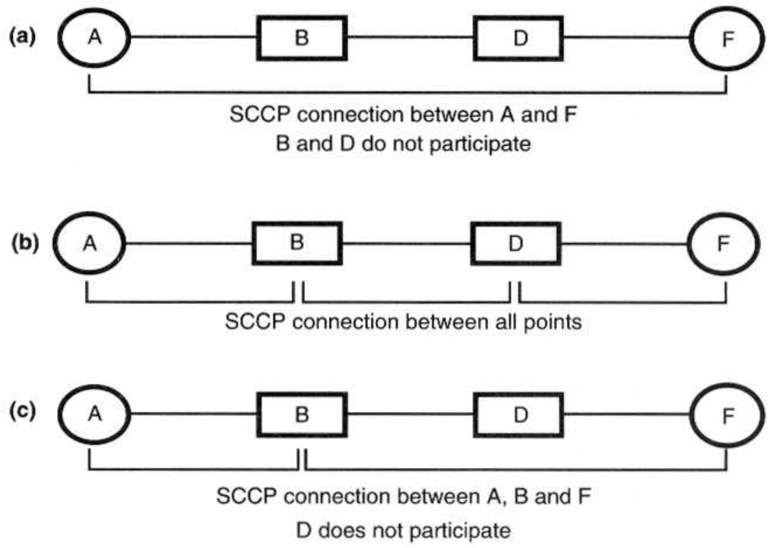
PC = C
SSN = 0110 (HLR)

DPC = B
OPC = A
Called address:
AI = GT routing
GT = 540-636
SSN = 0000
Calling address:
AI = SSN routing
PC = A
SSN = 0101

DPC = D
OPC = B
Called address:
AI = GT routing
GT = 703
SSN = 0110
Calling address:
AI = SSN routing
PC = A
SSN = 0101

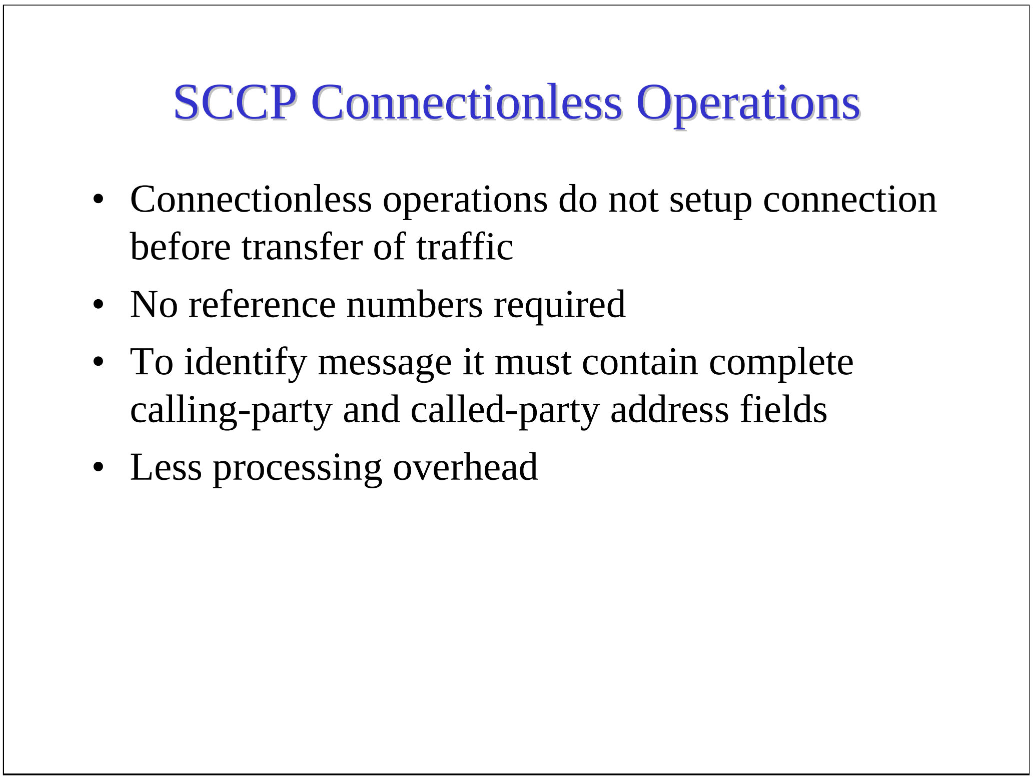
DPC = C
OPC = D
Called address:
AI = SSN routing
GT = 703
SSN = 0110
Calling address:
AI = SSN routing
PC = A
SSN = 0101

SCCP Connection-Oriented Operations


(a)
A
B
D
F
SCCP connection between A and F
B and D do not participate
(b)
A
B
D
F
SCCP connection between all points
(c)
A
B
D
F
SCCP connection between A, B and F
D does not participate

Connections between SCCP entities are not physical connections; rather the connection are logical, in that the SCCP creates entries in a database or memory that allow it to know about the ongoing interactions with another SCCP entity.

Furthermore, each SCCP in the signalling points between two communicating SCCPs do not have to particpate in the connection. The underlying MTP may be sufficient to route messages between the two end signalling points. Different scenarios are depicted in the slide above.



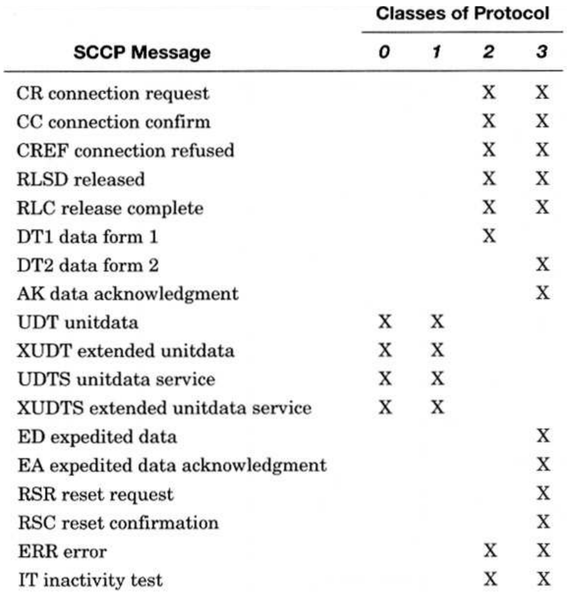
SCCP Connectionless Operations

- Connectionless operations do not setup connection before transfer of traffic
- No reference numbers required
- To identify message it must contain complete calling-party and called-party address fields
- Less processing overhead

SCCP Service Classes

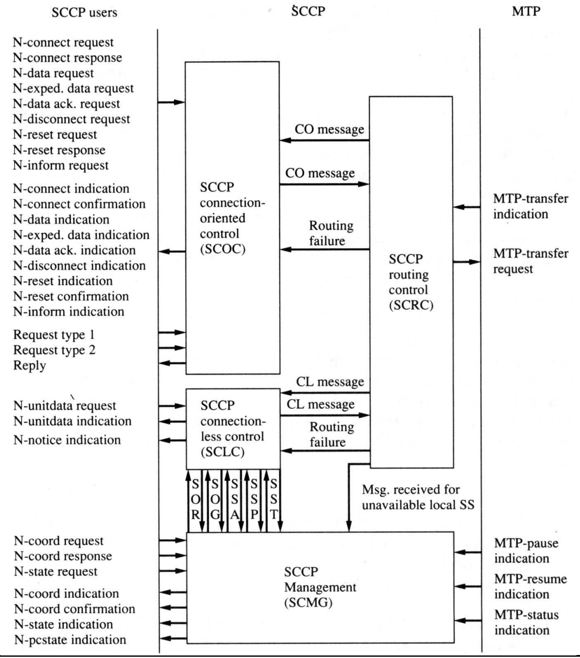
- SCCP supports four classes of service
  - Protocol class 0, Basic Connectionless Service
  - Protocol Class 1, Sequenced (MTP) Connectionless Sevice
  - Protocol Class 2, Basic Connection-Oriented Class
  - Protocol Class 3, Flow Control Connection-Oriented Class

SCCP Message Types and Protocol Classes



SCCP Message	Classes of Protocol			
	0	1	2	3
CR connection request			X	X
CC connection confirm			X	X
CREF connection refused			X	X
RLSD released			X	X
RLC release complete			X	X
DT1 data form 1			X	
DT2 data form 2				X
AK data acknowledgment				X
UDT unitdata	X	X		
XUDT extended unitdata	X	X		
UDTS unitdata service	X	X		
XUDTS extended unitdata service	X	X		
ED expedited data				X
EA expedited data acknowledgment				X
RSR reset request				X
RSC reset confirmation				X
ERR error			X	X
IT inactivity test			X	X

SCCP Service Definitions (Primitives)



N-UNITDATA, MTP-TRANSFER, N-DATA, N-EXPED.DATA: Service definitions transfer ongoing user traffic between the layers

N-NOTICE: Service definition is used for SCLC and the upper layers to notify each other about various activities

N-COORD: used to coordinate the withdrawal of some systems from active operations through SCMG

N-STATE: used to inform entities about various states of an entity within a layer, in particular to inform SCCP management about the status of the originating entity

N-TRAFFIC: used for the distribution of traffic-type information

MTP-PAUSE, MTP-RESUME: service definitions temporarily stop and resume the sending of traffic (messages)

MTP-STATUS: used to inform layer entities about the availability or non-availability of a destination address

N-CONNECT: service definition is used to set-up connections through SCOC

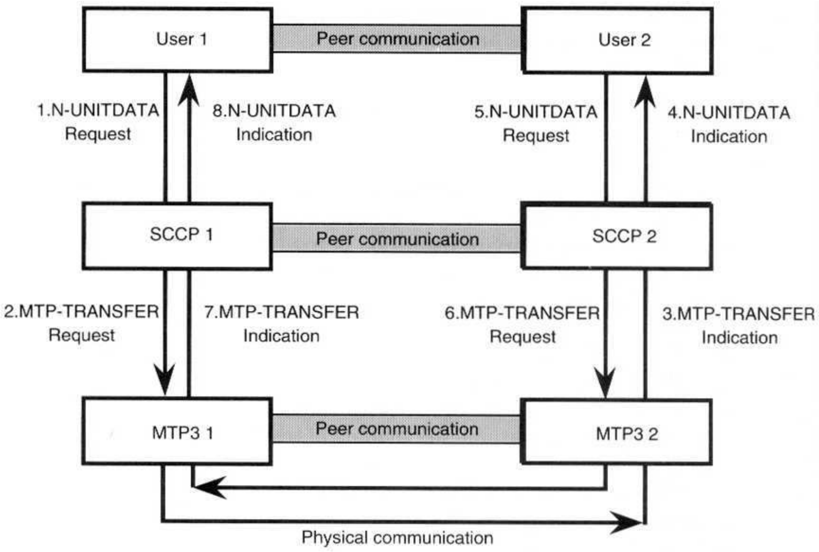
N-DATA-ACK: service definition is used to request and receive end-to-end acknowledgements of traffic (messages)

N-DISCONNECT: is used to tear down connections

N-RESET: used to reset connections

N-PCSTATE: service definition is used to inform a user about the status of a signalling point

Examples of Primitives to/from SCCP



User 1

Peer communication

User 2

1.N-UNITDATA Request

8.N-UNITDATA Indication

5.N-UNITDATA Request

4.N-UNITDATA Indication

SCCP 1

Peer communication

SCCP 2

2.MTP-TRANSFER Request

7.MTP-TRANSFER Indication

6.MTP-TRANSFER Request

3.MTP-TRANSFER Indication

MTP3 1

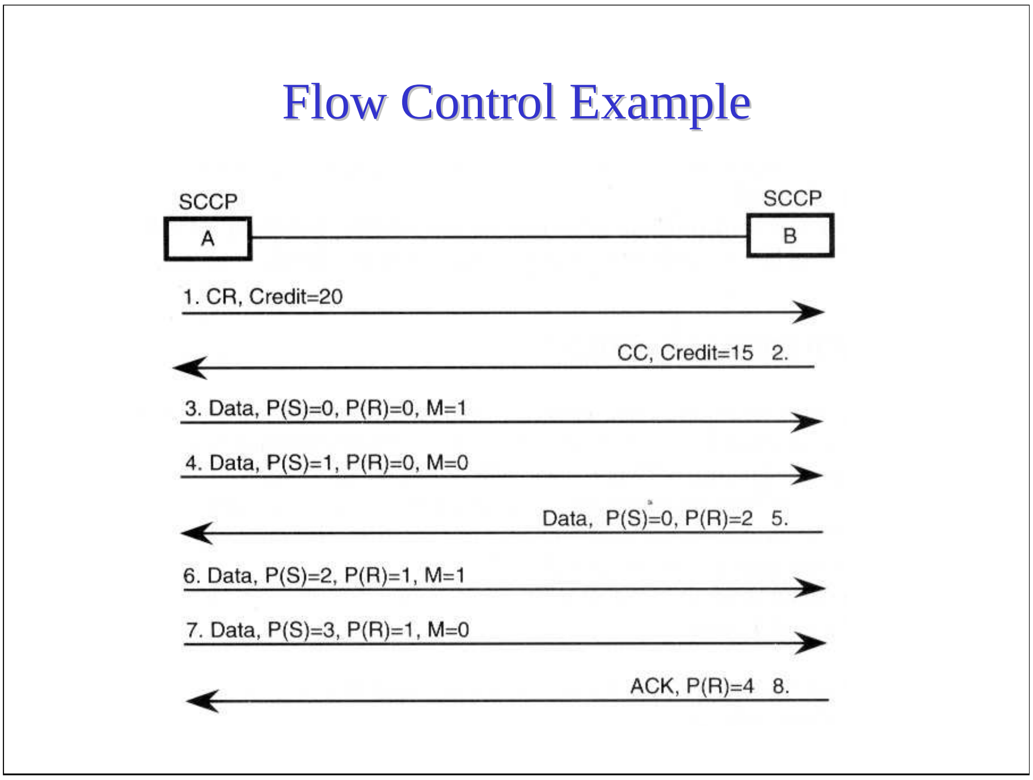
Peer communication

MTP3 2

Physical communication

Sequencing, Flow Control, and Segmentation/Reassembly

- SCCP protocol class 3 permits sequencing, flow control and segmentation/reassembly
- Sequencing may be needed in situations where more than one message needs to be exchanged between SCCPs (from TCAP for example)
- Segmentation/reassembly is required due to the limited SU size
- Flow control is required to protect adjacent SCCPs from buffer overflow



Flow Control Example

SCCP A

SCCP B

1. CR, Credit=20

CC, Credit=15 2.

3. Data, P(S)=0, P(R)=0, M=1

4. Data, P(S)=1, P(R)=0, M=0

Data, P(S)=0, P(R)=2 5.

6. Data, P(S)=2, P(R)=1, M=1

7. Data, P(S)=3, P(R)=1, M=0

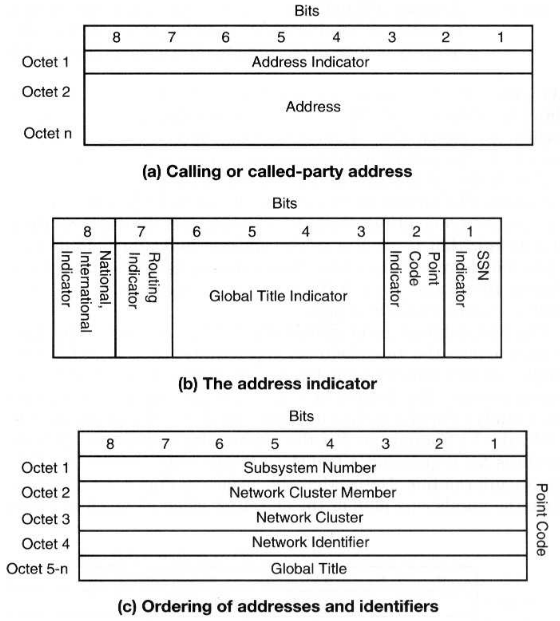
ACK, P(R)=4 8.

The flow control example in the slide above shows how flow control is implemented by using sequence numbers in the same way as at MTP 2. However, here sequence numbers are used for flow control only and it is not assumed that any errors occur as this is taken care of at the lower layers.

Event 1. In the slide shows the sending of a connection request (CR) message from SCCP A to B. The message has a number of parameters. This includes the called- nad calling-party address, the local reference number, the suggested protocol class, an optional data field, and a hop counter. This last parameter indicates the maximum number of intermediate signalling points the message is allowed to traverse before reaching its destination. Usually this parameter is set to 15, and if this limit is exceeded, an error is returned to the originator by the singalling point, which recognises the error (the sictenth hop). The hop counter is used to make sure that the message takes as short a route through the network as is feasible with regard to the traffic load.

The credit field, shown in the slide as "Credit=20", indicates the window length for flow control to the receiving station.

Examples of Key Information Elements



(a) Calling or called-party address

(b) The address indicator

(c) Ordering of addresses and identifiers

The slide above shows key fields within a SCCP message. Figure (a) shows the address field. The actual address field is preceeded by an 8 bit address indicator field. Figure (b) shows the structure of the address indicator field. The bits in the field are coded as follows:

Bit 1 value of 1 indicates address contains a SSN

Bit 2 value of 1 indicates address contains a PC

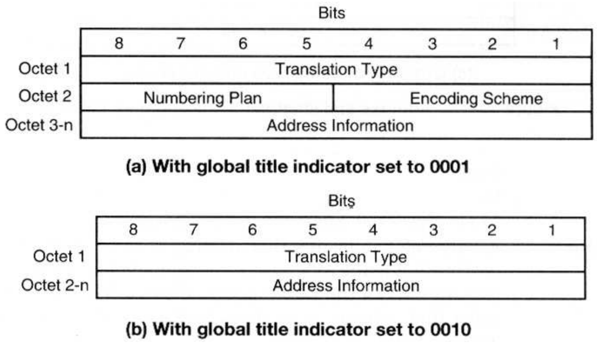
Bit 3-6 contain global title indicator, coding is

6543	Meaning
0000	no GT present
0001	GT includes translation type, numbering plan, and encoding scheme
0011	GT includes translation type
0100 to 1111	Reserved, spare, or not assigned

Bit 7 value of 1 indicates that routing is to be carried out with DPC in routing label and SSN in called party address; value of 0 indicates that routing is carried out with GT in address field

Bit 8 value of 1 indicates that the address is coded according to national specifications.; value of 0 indicates that addrss is coded according to international specifications (e.g. ITU-T E.164/E.163)

Examples of Key Information Elements



	Bits 8	7	6	5	4	3	2	1
Octet 1	Translation Type							
Octet 2	Numbering Plan				Encoding Scheme			
Octet 3-n	Address Information							

(a) With global title indicator set to 0001

	Bits 8	7	6	5	4	3	2	1
Octet 1	Translation Type							
Octet 2-n	Address Information							

(b) With global title indicator set to 0010

The translation type code is implementation specific.

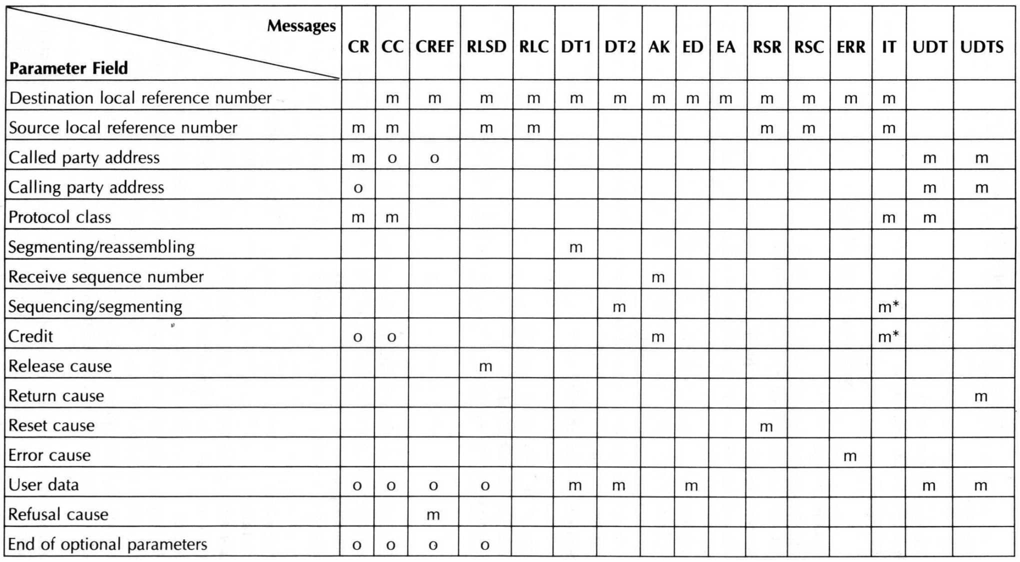
Coding of numbering plan, bits 5 to 8 in octet 2 of Figure (a) as below:

Bits 8765	*Meaning:*	*Pertinent ITU-T* Recommendation
0000	Unknown	
0001	ISDN/Telephone numbering plan	(E.164/E.163)
0010	Reserved	
0011	Data numbering plan	(X.121)
0100	Telex numbering plan	(F.69)
0101	Maritime mobile numbering plan	(E.210/E.211)
0110	Land mobile numbering plan	(E.212)
0111	ISDN/mobile numbering plan	(E.214)
1000 to 1110	Spare	
1111	Reserved	

The encoding scheme is the least significant nibble in octet 2 in Figure (a) above.

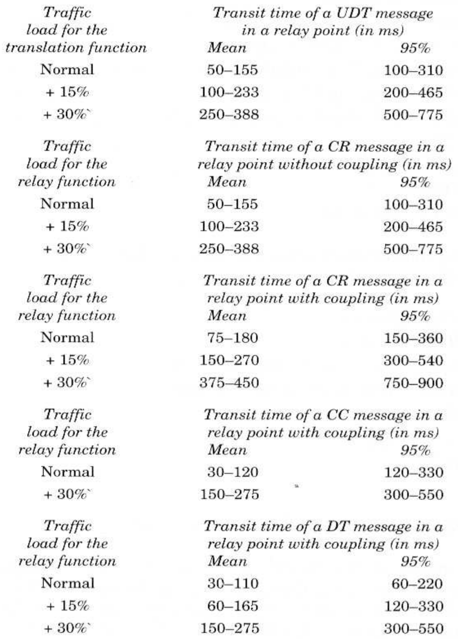
Bits 4321	*Meaning:*
0000	Unknown
0001	BCD, odd number of digits
0010	BCD, even number of digits
0011 to 1111	Spare

SCCP Messages and Information Elements



Messages Parameter Field	CR	CC	CREF	RLSD	RLC	DT1	DT2	AK	ED	EA	RSR	RSC	ERR	IT	UDT	UDTS
Destination local reference number		m	m	m	m	m	m	m	m	m	m	m	m	m		
Source local reference number	m	m		m	m						m	m		m		
Called party address	m	o	o												m	m
Calling party address	o														m	m
Protocol class	m	m												m	m	
Segmenting/reassembling						m										
Receive sequence number								m								
Sequencing/segmenting							m							m*		
Credit	o	o						m						m*		
Release cause				m												
Return cause																m
Reset cause											m					
Error cause													m			
User data	o	o	o	o		m	m		m						m	m
Refusal cause			m													
End of optional parameters	o	o	o	o												

Performance Requirement for SCCP



Traffic load for the translation function	*Transit time of a UDT message in a relay point (in ms)*	
	Mean	*95%*
Normal	50–155	100–310
+ 15%	100–233	200–465
+ 30%`	250–388	500–775

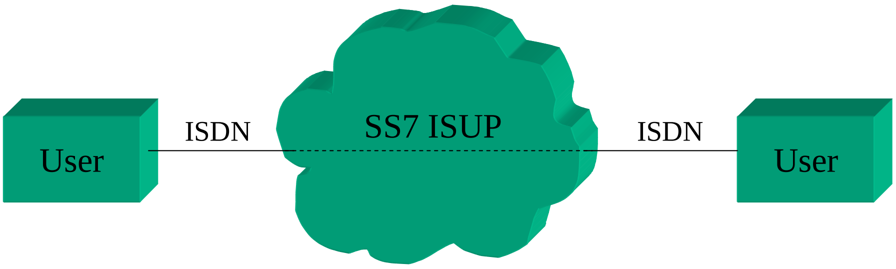
Traffic load for the relay function	*Transit time of a CR message in a relay point without coupling (in ms)*	
	Mean	*95%*
Normal	50–155	100–310
+ 15%	100–233	200–465
+ 30%`	250–388	500–775

Traffic load for the relay function	*Transit time of a CR message in a relay point with coupling (in ms)*	
	Mean	*95%*
Normal	75–180	150–360
+ 15%	150–270	300–540
+ 30%`	375–450	750–900

Traffic load for the relay function	*Transit time of a CC message in a relay point with coupling (in ms)*	
	Mean	*95%*
Normal	30–120	120–330
+ 30%`	150–275	300–550

Traffic load for the relay function	*Transit time of a DT message in a relay point with coupling (in ms)*	
	Mean	*95%*
Normal	30–110	60–220
+ 15%	60–165	120–330
+ 30%`	150–275	300–550

ISDN and SS7 ISUP



Abbreviations

MTP - Message Transfer Part

SCCP - Signalling Connection Control part

NSP - Network Service Part

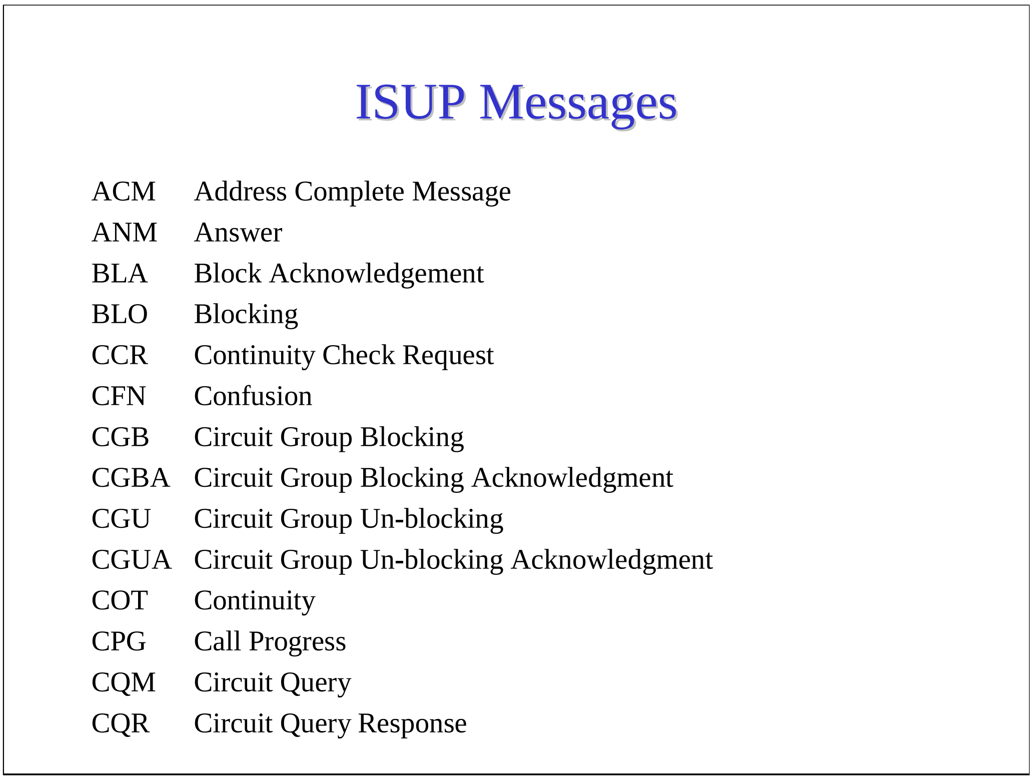
ISUP - ISDN User Part

TUP - Telephone User Part

TCAP - Transaction Capabilities Application Part

ASE - Application Service Entities

OMAP - Operations and Maintenance Application Part

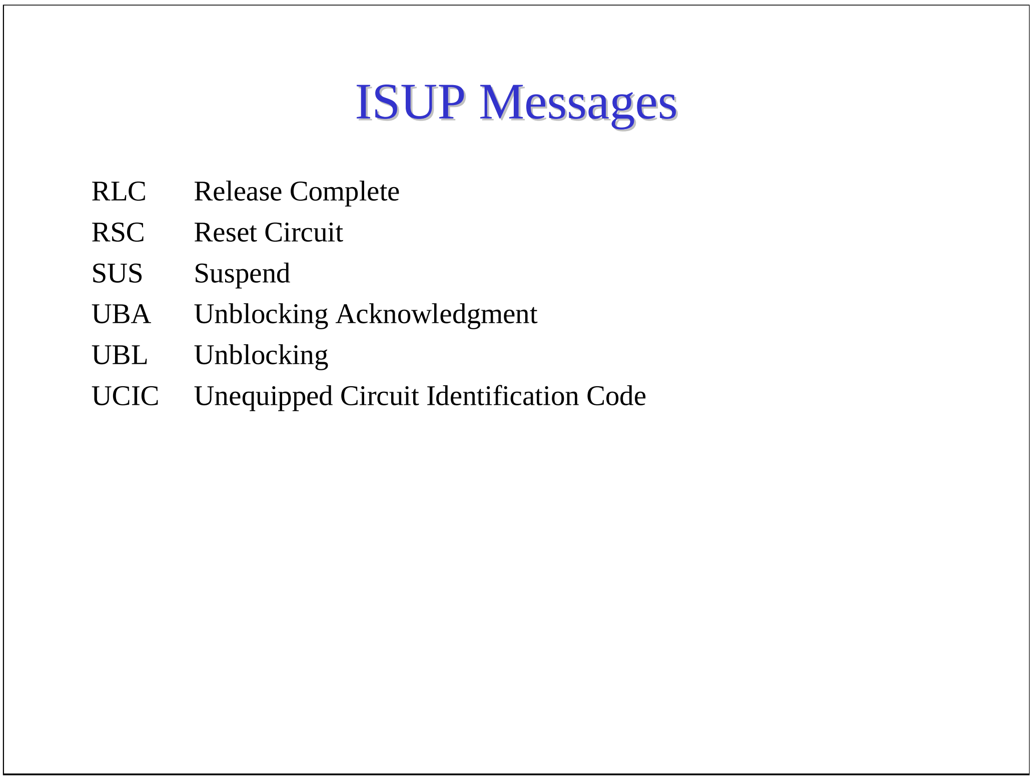


ISUP Messages

ACM	Address Complete Message
ANM	Answer
BLA	Block Acknowledgement
BLO	Blocking
CCR	Continuity Check Request
CFN	Confusion
CGB	Circuit Group Blocking
CGBA	Circuit Group Blocking Acknowledgment
CGU	Circuit Group Un-blocking
CGUA	Circuit Group Un-blocking Acknowledgment
COT	Continuity
CPG	Call Progress
CQM	Circuit Query
CQR	Circuit Query Response

ISUP Messages

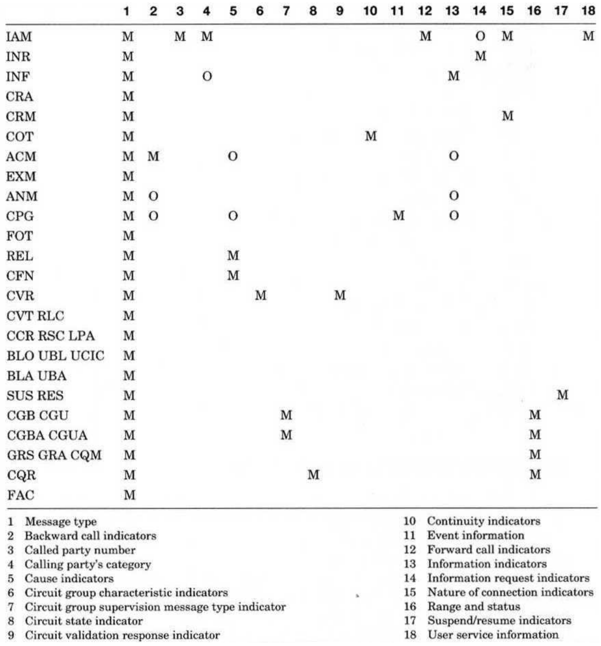
CRA	Circuit Reservation Acknowledgment
CRM	Circuit Reservation
CVR	Circuit Validation Response
EXM	Exit
FAC	Facility
FOT	Forward Transfer
GRA	Group Reset Acknowledgment
GRS	Group Reset
IAM	Initial Address Message
INF	Information
INR	Information Request
LPA	Loop-back Acknowledgment
REL	Release
RES	Resume



ISUP Messages

RLC	Release Complete
RSC	Reset Circuit
SUS	Suspend
UBA	Unblocking Acknowledgment
UBL	Unblocking
UCIC	Unequipped Circuit Identification Code

Information Elements in ISUP Messages

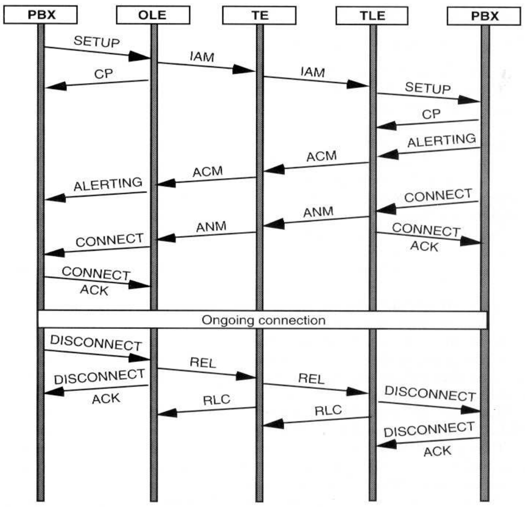


	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
IAM	M		M	M								M		O	M			M
INR	M													M				
INF	M			O									M					
CRA	M																	
CRM	M														M			
COT	M									M								
ACM	M	M			O								O					
EXM	M																	
ANM	M	O											O					
CPG	M	O			O						M		O					
FOT	M																	
REL	M				M													
CFN	M				M													
CVR	M					M			M									
CVT RLC	M																	
CCR RSC LPA	M																	
BLO UBL UCIC	M																	
BLA UBA	M																	
SUS RES	M																M	
CGB CGU	M						M									M		
CGBA CGUA	M						M									M		
GRS GRA CQM	M															M		
CQR	M							M								M		
FAC	M																	

1 Message type
2 Backward call indicators
3 Called party number
4 Calling party's category
5 Cause indicators
6 Circuit group characteristic indicators
7 Circuit group supervision message type indicator
8 Circuit state indicator
9 Circuit validation response indicator

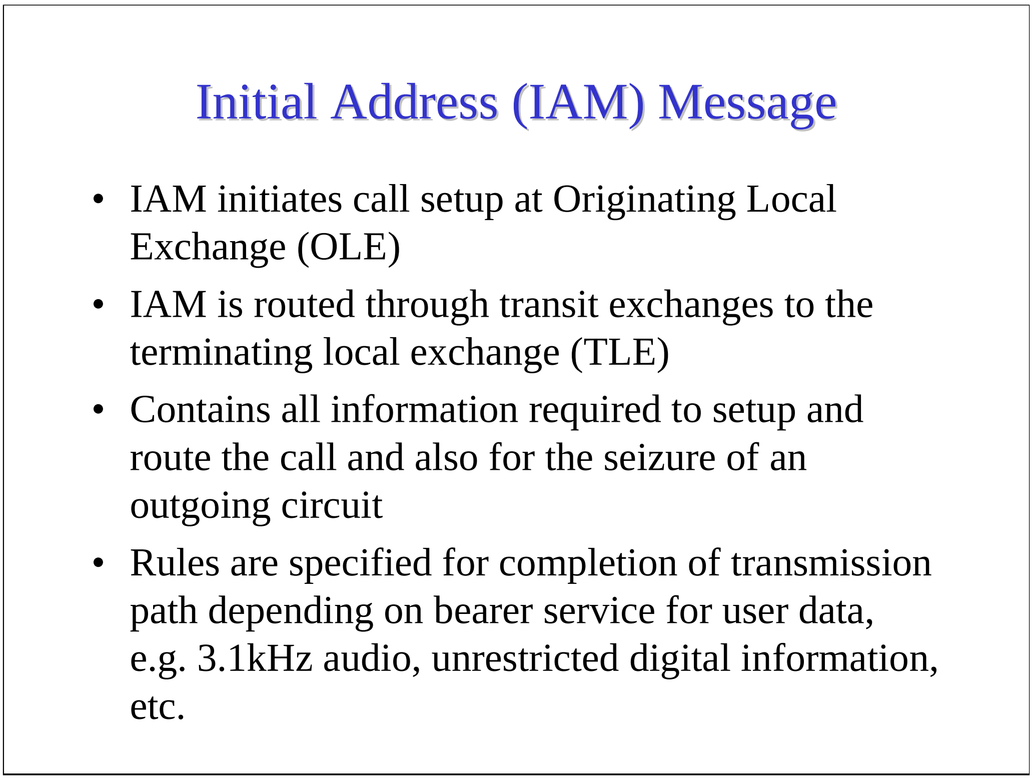
10 Continuity indicators
11 Event information
12 Forward call indicators
13 Information indicators
14 Information request indicators
15 Nature of connection indicators
16 Range and status
17 Suspend/resume indicators
18 User service information

Example of ISDN/SS7 Call



where:

ACM	Address complete message
ANM	Answer message
CP	Call proceeding
IAM	Initial address message
OLE	Originating local exchange
PBX	Private branch exchange
RLC	Release complete
TE	Transit exchange
TLE	Terminating (destination)local exchange



Initial Address (IAM) Message

- IAM initiates call setup at Originating Local Exchange (OLE)
- IAM is routed through transit exchanges to the terminating local exchange (TLE)
- Contains all information required to setup and route the call and also for the seizure of an outgoing circuit
- Rules are specified for completion of transmission path depending on bearer service for user data, e.g. 3.1kHz audio, unrestricted digital information, etc.

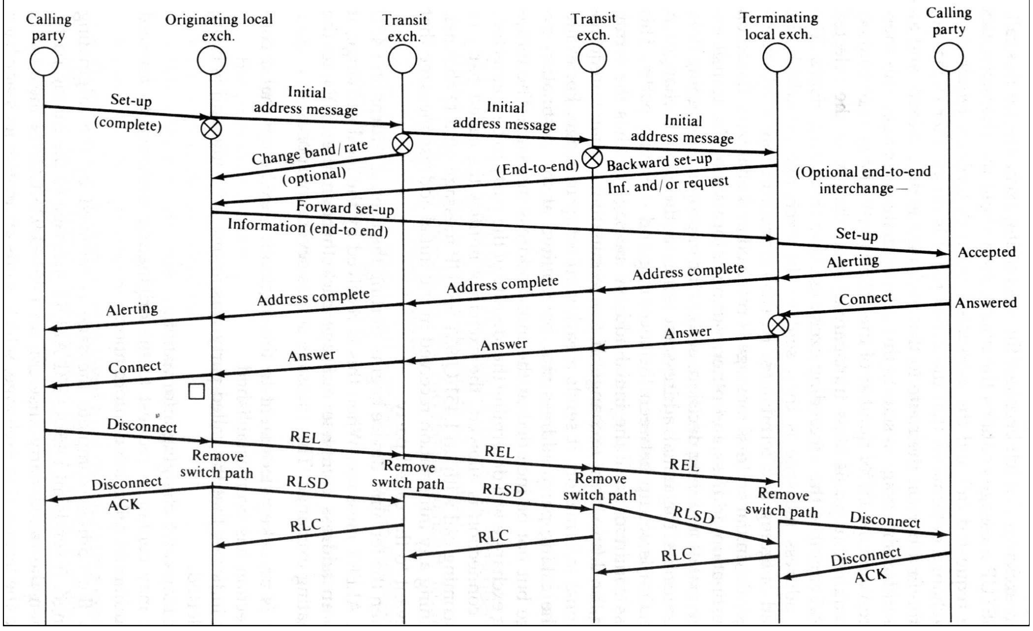
Address Complete (ACM) Message

- Created when called party responds with an ISDN ALERTING message
- TLE sets field indicating “subscriber is free” in ACM
- If response is delayed, TLE indicates “excessive delay” in ACM
- TLE must connect ringing tone through to OLE
- At OLE, an ISDN ALERTING message is sent to the user

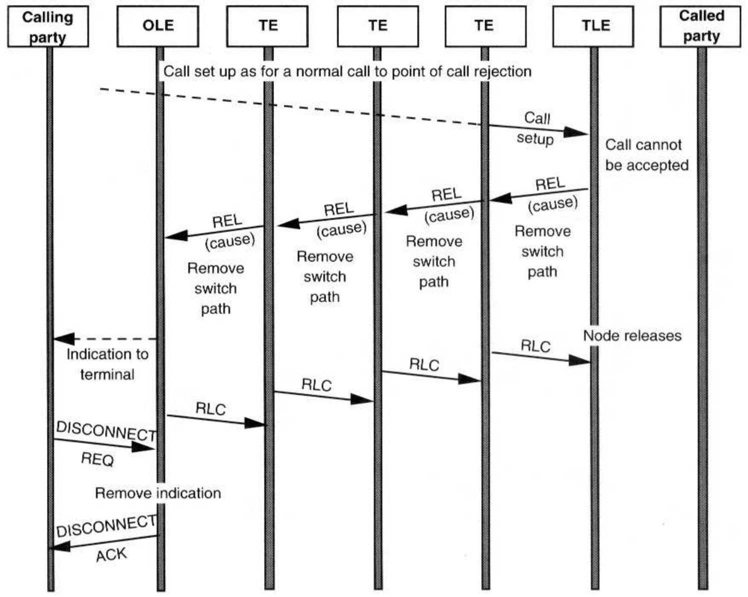
Answer (ANM) Message

- When terminating end answers the call, an ISDN CONNECT is sent, which TLE maps onto SS7 ANM message
- At the OLE this is mapped onto an ISDN CONNECT message
- When called party answers, TLE removes ringing tone and connects the user voice/data path through
- TLE replies with an ISDN CONNECT ACK message

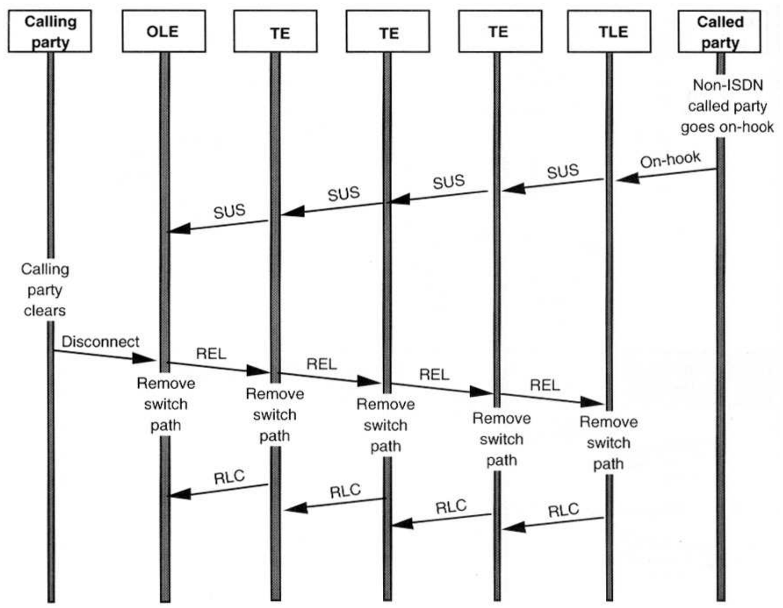
Call Setup Example

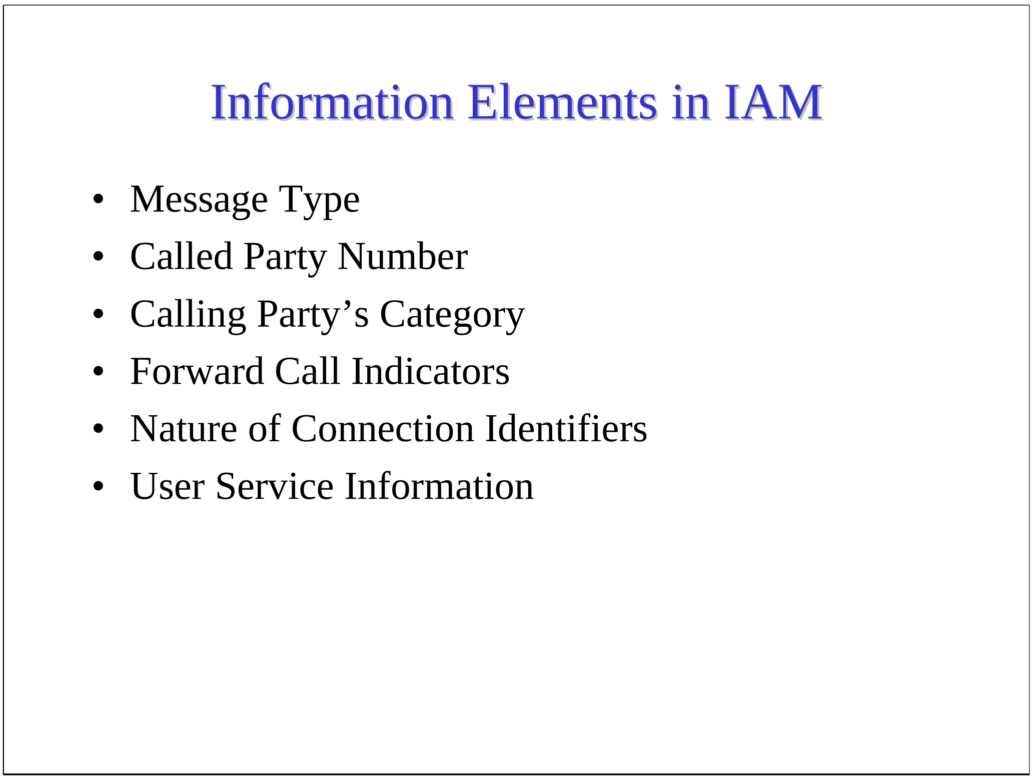


Called Part cannot be Reached



Called Part goes On-hook during Call





Information Elements in IAM

- Message Type
- Called Party Number
- Calling Party’s Category
- Forward Call Indicators
- Nature of Connection Identifiers
- User Service Information

Although a wide variety of information elements can be sent in an Initial Address Message, the six IE shown above are manadatory.

The *message type* IE is a one octet code that identifies the message. For the IAM message the IE is coded as 00000001.

The *called party number* IE (from 2 to 11 octets) contains the the telephone umber of the called party. It also identifies the addressing plan, e.g. E.164, and a field to indicate the nature of the address, I.e. subscriber number, test line number, internation number, etc. Each digit of the number is coded as 4-bit BCD codes.

The *calling party’s category* IE is a one octet IE that contains information about, (a) the language used by the originating operator, (b) the type of call (test, data, regular voice, pay phone, emergency, etc.

The *forward call indicators* IE is a two octet IE that contains many parameters that are used to inform the receiving exchange about the services that are used to be associated with the call. Information is coded to indicate if (a) call is of international origin, (b) signalling method is pass-alone or SCCP, (c) any intervening network is not SS7 based, (d) the IAM is segmented into more than one message, (e) ISUP is used end-to-end, (f) ISUP is required end-to-end, (g) originating access is ISDN, and (h) SCCP is employed.

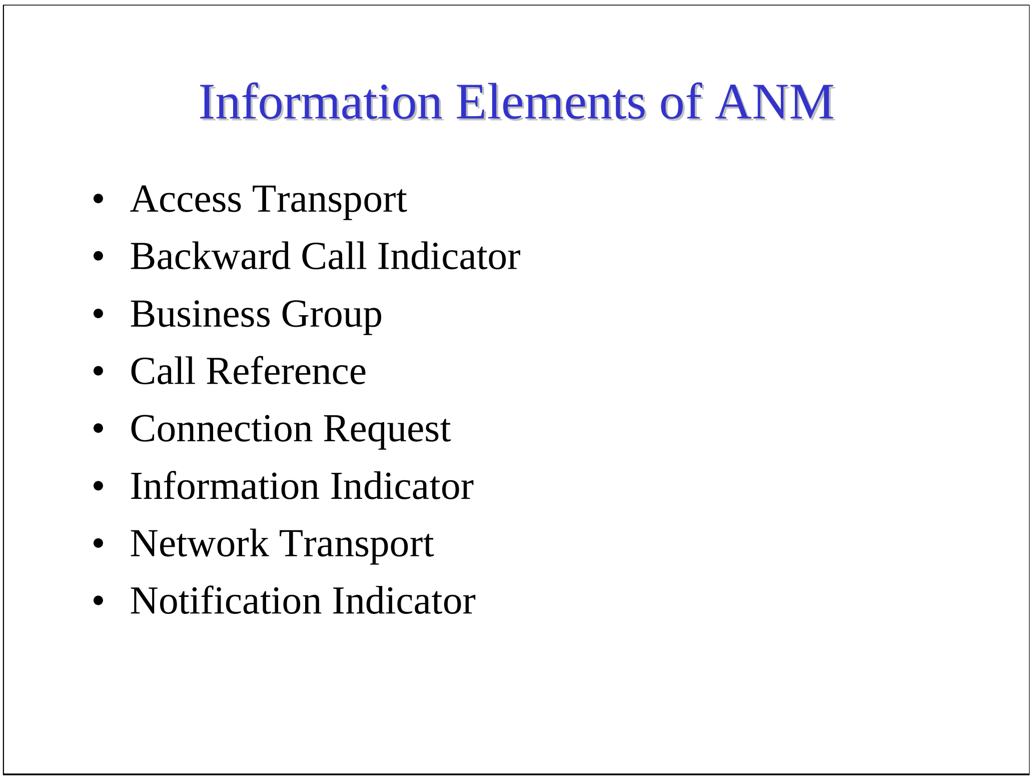
The *nature of connection* IE is a one octet IE that contains information about the circuit being setup, e.g. satellite links, echo cancellation, etc.

The *user service information* IE is variable length. Purpose is to provide information regarding a data call.

Information Elements of ACM

- Backward Call Indicator
- Fields within Backward Call Indicator
  - Charge Indicator
  - Called Party Status Indicator
  - Called Party Category Indicator
  - Echo Control Device Indicator
  - IAM Segmentation Indicator
  - End-to-end method Indicator
  - Interworking Indicator
  - Holding Indicator
  - ISDN User Part Indicator
  - ISDN Access Indicator
  - SCCP Method Indicator

The Address Complete message contains only one mandatory information element, the *backward call indicator*. This IE is two octets in length and contains the fields (a) charge indicator, (b) called party status indicator, e.g. called party available, busy, (c) called party’s category indicator, e.g. pay phone or ordinary subscriber, (d) echo control device indicator, (e) IAM segmentation indicator, (f) end-to-end method indicator, e.g. pass-along or SCCP, (g) interworking indicator, (h) holding indicator, (I) ISDN user part indicator, (j) ISDN access indicator, e.g. terminating device uses ISDN, (k) SCCP method indicator.



Information Elements of ANM

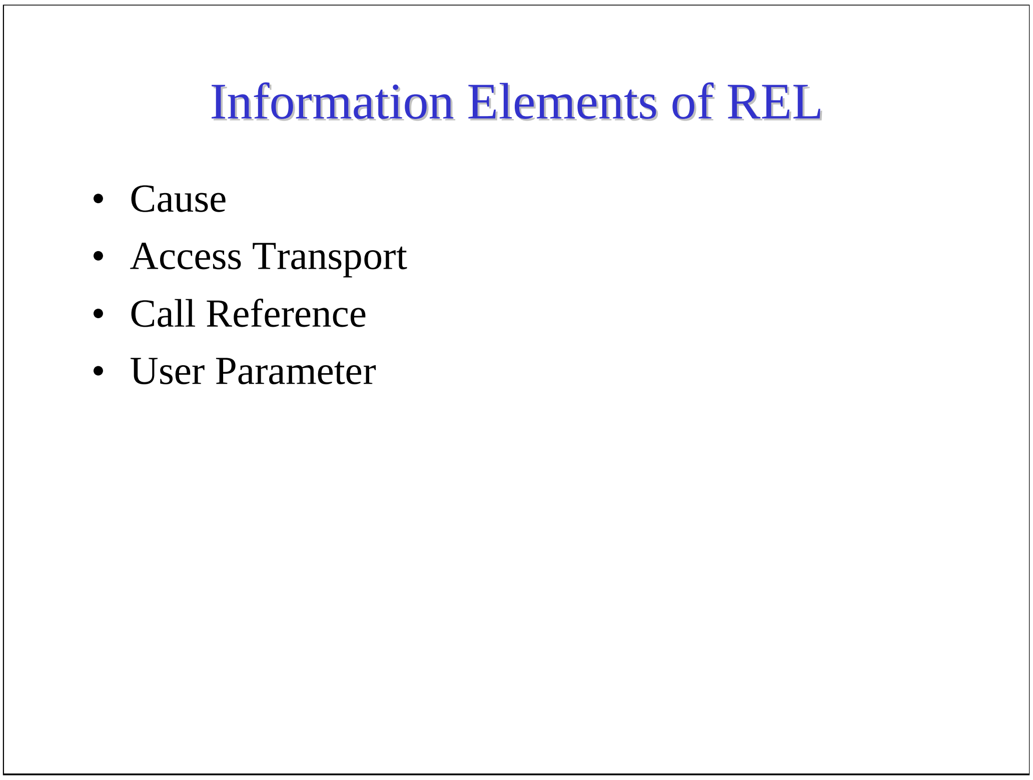
- Access Transport
- Backward Call Indicator
- Business Group
- Call Reference
- Connection Request
- Information Indicator
- Network Transport
- Notification Indicator

All information elements in the Answer Message (ANM) are optional except for the CI and routing label. In the following some of the optional IE are explained.

The *backward call indicator* IE is sent to provide information regarding the call. The *business group* IE is used to code the characteristics and identifiers of business group. Examples of fields are (a) identifier of the business group, (b) originating and terminating line privileges,(c) party selector, and (d) multilocation bsiness group identifier.

The *connection request* IE provides information on the terminal that originated the connection request, e.g. local reference number, point code, and window size.

The *information indicator* IE provides a wide variety of information, e.g. calling party address not available, calling party address is held, charge information on multilocation business group, etc.



Information Elements of REL

- Cause
- Access Transport
- Call Reference
- User Parameter

The Release message is used to disconnect the parties and free network resources that were reserved for the call. It can be sent in either direction, when a party goes on-hook. The only mandatory IE is the *cause* IE, which is usually coded to indicate a normal clearing. However, abnormal call termination can also be conveyed.

TCAP

- Transaction Capabilities Application Part (TCAP) provides standardised method for network providers to communicate with each other
- TCAP provides non-circuit-related communications facilities
- TCAP is a connectionless remote procedure call (RPC) in a similar fashion to those used in the Internet application layer
- TCAP operates on top of SCCP and supports database access for SS7 switches

Prior to the standardisation and implementation of TCAP, no standardised way existed for network operators to communicate with each other about matters pertaining to non-circuit-related information exchange. This problem became evident as the 1800 number service was introduced. Todate, TCAP facilitates monst aspects of what is termed the intelligent network.

To solve the 1800 number problem, TCAP is used by telephone companies to access centralised 1800 number databases in a standardised manner. The term standardised is important, because TCAP defines the format and fields that allow a service switching point (SSP) or a service control point (SCP) to formulate a TCAP access request to another node and a database, regardless of the node’s architecture and the database structure (see next slide).

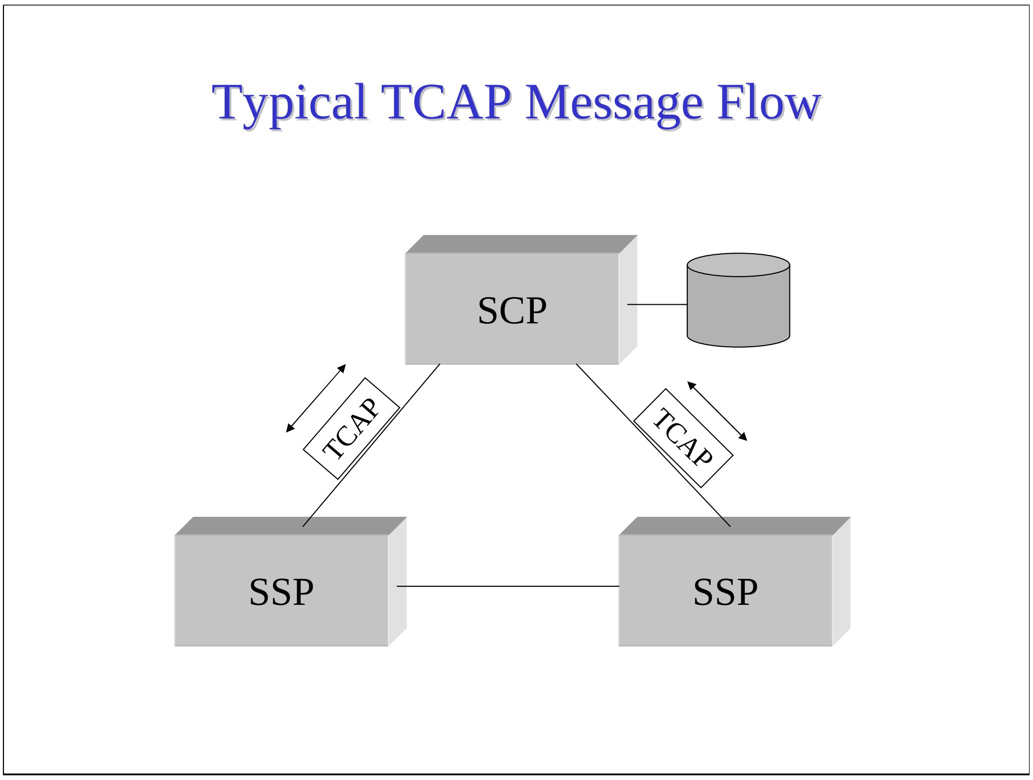
TCAP operates at the application layer of the OSI model but may also include other lower-layer protocols needed to support it. TCAP provides other services to applications that implement intelligent network features such as

• *CLASS services*: Use TCAP to edit customer-programmable lists such as distinctive ringing/call waiting (DRCW)

• *ISDN queries*: Use TCAP to query remote ISDN switches about a customer’s ability/desire to forward calls

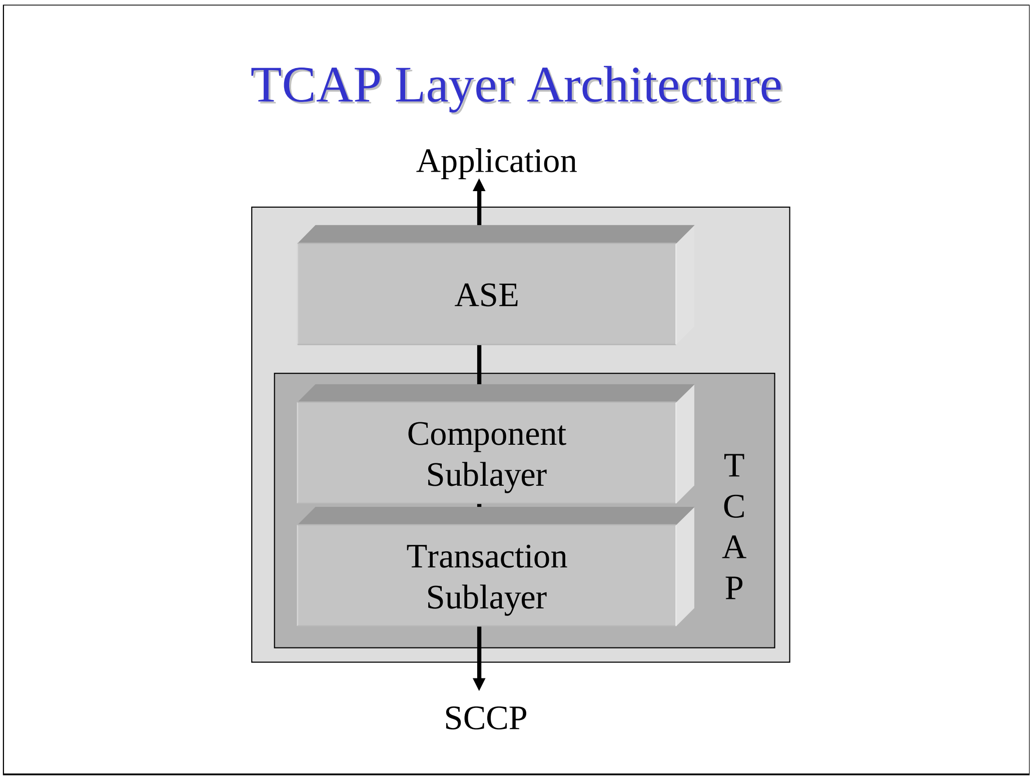
• *Local exchange queries*: Use TCAP to query a remote local exchange to check the status of a telephone line without the need to establish a connection

• *Subscriber profiles*: Use TCAP to access databases that contain information about subscriber’s profiles (call forward, do not disturb, billing data, etc.)



Typical TCAP Message Flow

The slide above depicts a typical TCAP message flow in order to identify the real network address of an 1800 number. The SSP queries the database at the SCP by remotely invoking a procedure that retrieves the number. The SCP returns the information in a TCAP message.



TCAP Layer Architecture

Application

ASE

Component Sublayer

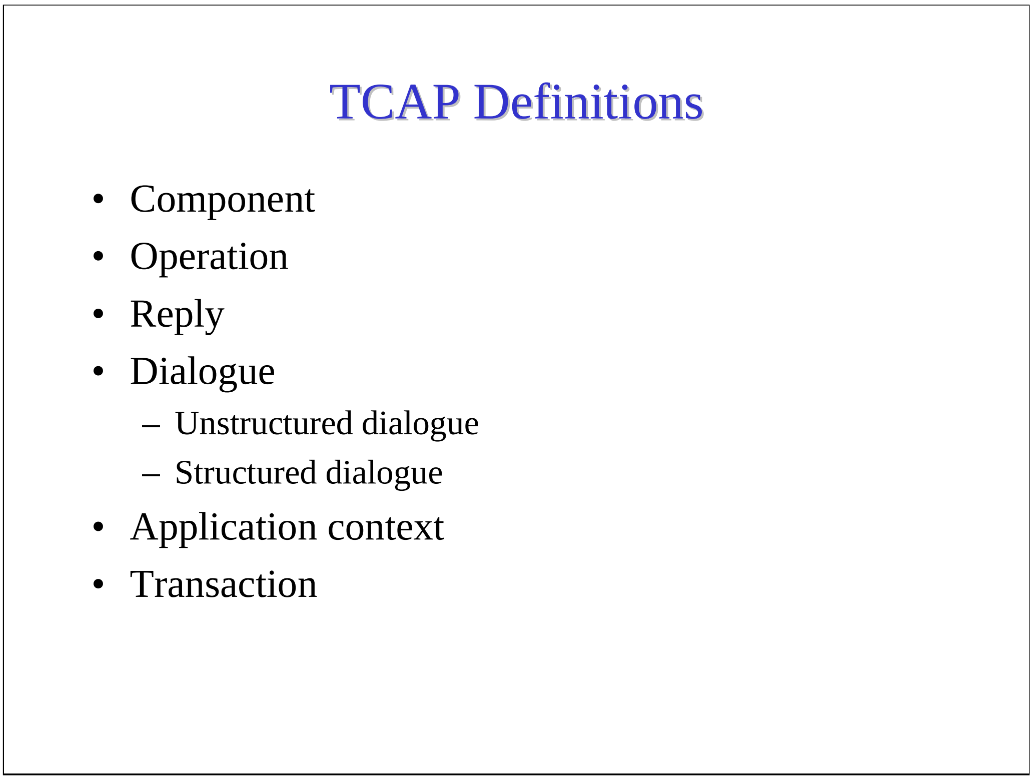
Transaction Sublayer

TCAP

SCCP

The slide above shows that TCAP is divided into two sublayers. The transaction sublayer has services that are somewhat similar to the OSI commitment-concurreny-recovery (CCR) protocol and the component sublayer, which is modelled closely on the remote operation service element (ROSE). The transaction sublayer is organised around two types of dialogues that take place between peer entities in two machines operating in the transaction sublayer. The first dialogue is called the *unstructured dialogue* and is so named because no association is estalished between the users of this service. Additionally, no responses are provided from the receiver of this type of traffic. The second type of dialogue is the *structured dialogue* and requires the retention of information about the ongoing communications between the two transaction sublayers. A dialogue identifer is associated with each message pertaining to a specific dialogue.

The component sublayer uses an entity to issue invoke operations. It then returns results about what happened at the machine in which the invoke operation occurred. Some of the TCAP operations are based on the OSI X.409 and X.410 application layer standards. Four services are described in X.410. An application entity (AE) begins operations by transferring operation protocol data units (OPDUs).



TCAP Definitions

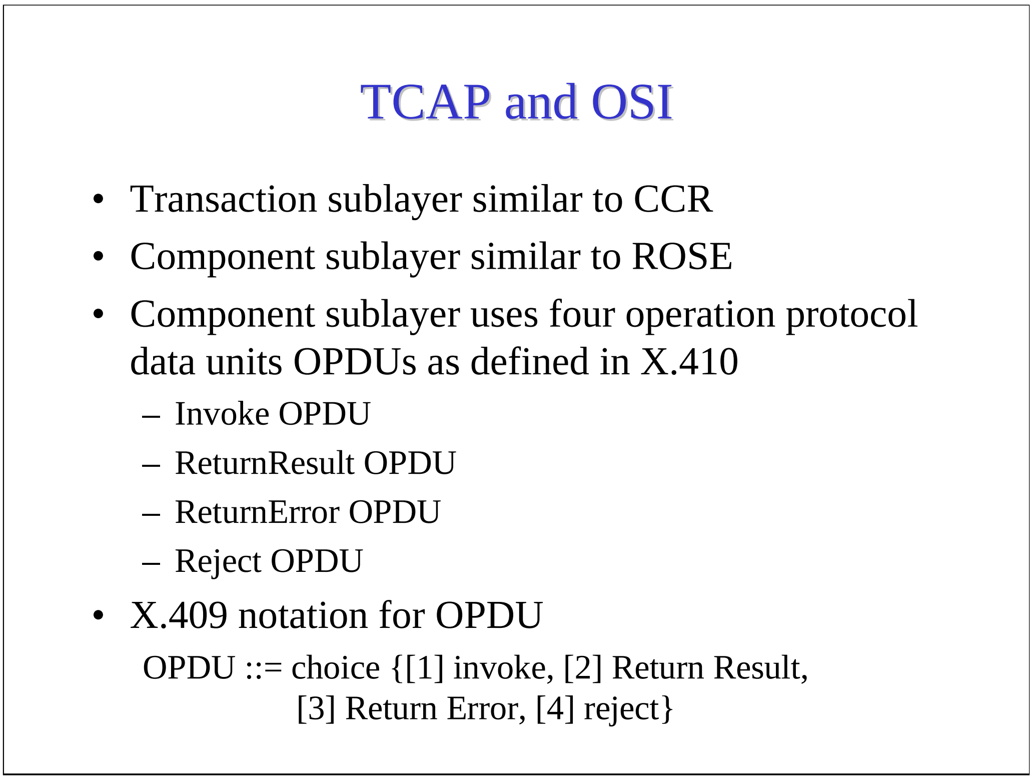
- Component
- Operation
- Reply
- Dialogue
  - Unstructured dialogue
  - Structured dialogue
- Application context
- Transaction

A component is the means by which TCAP conveys a request top perform an operation or a reply. An operation is an action to be performed by the remote end. An invocation of an operation is identified by an ivoke ID. A reply is a respose to an operation. Only one reply may be sent to an operation. However, serveral components may be passed to the component sublayer before they are transmitted, i.e. included in a single TCAP message.

A dialogue is a series of successive components exchanged between two TCAP users to perform an application. An unstructured dialogue consists of components that do not expect replies. A structured dialogue has a beginning and an end and is identified by a dialogue ID. Multiple structured dialogues can run concurrently between TCAP users.

An application context is an explicitely identified set of application service elements (ASE), related options and other necessary information for the interworking between cooperating application entities. The application context information is referred to as the dialogue control portion within the dialogue.

A transaction is a one-to-one mapping of a dialogue onto the services of the transaction sublayer when the users are the component sublayer. The mapping is explicit in a structured dialogue(the transaction ID identifies the transaction) and implicit in an unstructured dialogue.



TCAP and OSI

- Transaction sublayer similar to CCR
- Component sublayer similar to ROSE
- Component sublayer uses four operation protocol data units OPDUs as defined in X.410
  - Invoke OPDU
  - ReturnResult OPDU
  - ReturnError OPDU
  - Reject OPDU
- X.409 notation for OPDU

```
OPDU ::= choice {[1] invoke, [2] Return Result,
                [3] Return Error, [4] reject}
```

The Invoke OPDU is used when an AE wishes to communicate with another AE. The OPDU contains an identifier that is used to ensure atomic actions of the OPDUs. The protocol data unit also specifies the operation to be performed. However, since the operation is application specific, X.410 does not define this aspect of the AE-AE process. The notation for the Invoke OPDU is

```
Invoke ::= SEQUENCE {invokeID INTEGER, OPERATION,
                argument ANY}
```

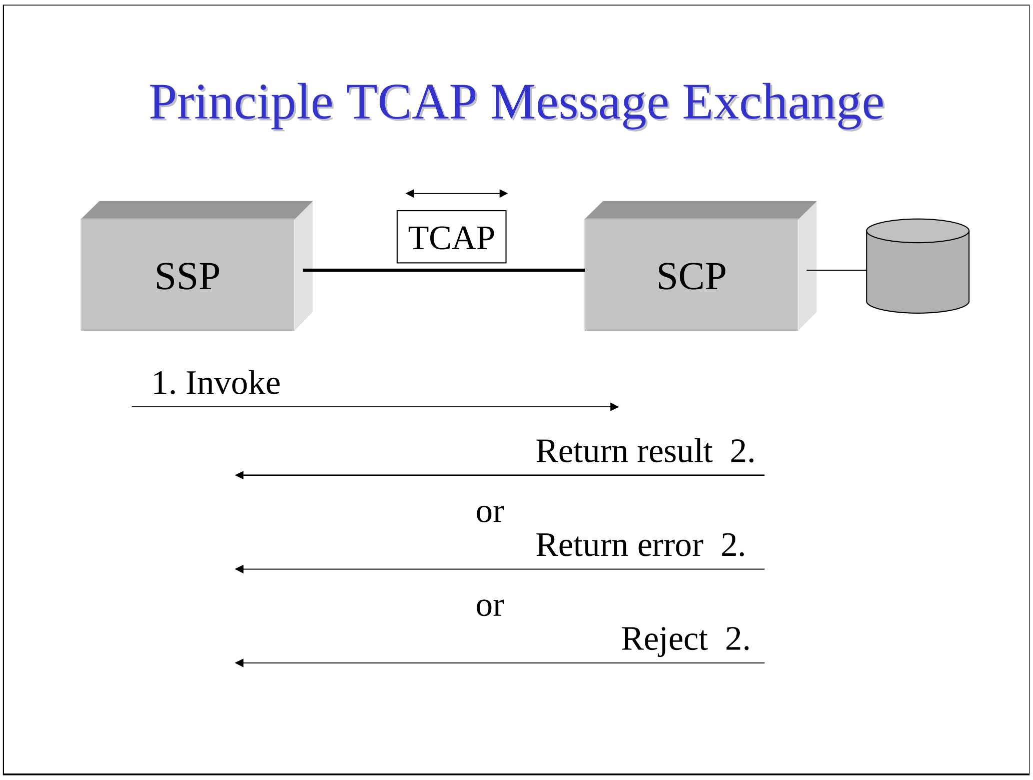
The ReturnResult OPDU reports the result of the AE-AE operation. It is sent if the result is successful. The ReturnError OPDU is sent if the operation is unsuccessful. The Reject OPDU is returned if the OPDU is rejected due to a content or formatting error. These OPDUs are coded in accordance with X.409:

```
ReturnResult ::= SEQUENCE {invokeID INTEGER, result ANY}

ReturnError ::= SEQUENCE {invokeID INTEGER, ERROR,
                                parameter ANY}
```

The Reject OPDU is returned if the Invoke is not accepted. It is coded as

```
Reject ::= SEQUENCE {invokeID INTEGER, Problem, parameter ANY}
```



Principle TCAP Message Exchange

TCAP

SSP

SCP

1. Invoke

Return result 2.

or

Return error 2.

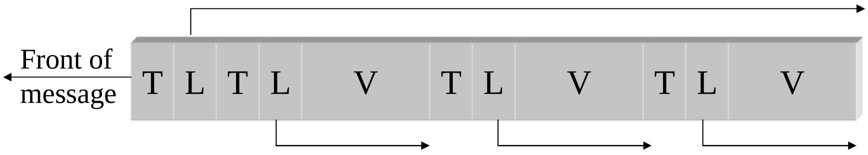
or

Reject 2.

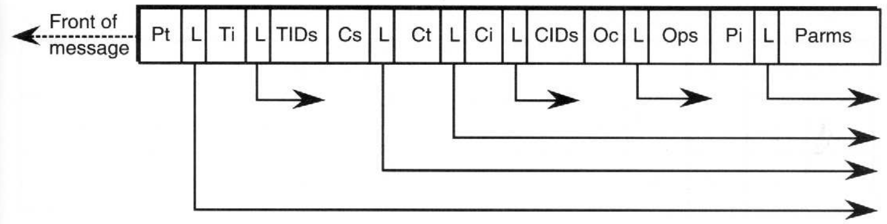
Operation (message)	Contents
Invoke	Invoke ID, Correlation ID, Operation,
Argument	
Return result	Correlation ID, Result
Return error	Correlation ID, Error, Parameter
Reject	Correlation ID, Problem, Parameter

Coding Conventions and Transfer Syntax

- Basic encoding rules (BER) provide conventions for transfer syntax for TCAP messages
- TCAP message described by representation, the data element
- Data element consists of three components (TLV convention)
  - Identifier (Type) T
  - Length of Value L
  - Contents (Value) V



TLV Structure of TCAP Message



where:

Pt	Package type identifier	Ci	Component ID identifier
L	Length	CIDs	Component IDs
Ti	Transaction ID identifier	Oc	Operation code identifier
TIDs	Transaction IDs	Ops	Operation codes
Cs	Component sequence identifier	Pi	Parameter set/sequence identifier
Ct	Component type identifier	Parms	Parameters

An example of the TLV format of TCAP messages is shown in the slide above. All identifiers use the two MSBs to indicate the identifier classes. The identifier distinguishes one type from another (for example, a SEQUENCE of fields, a field that is coded as INTEGER, or a field that is a BIT STRING) and specifies how the remainder of the lement is interpreted. The identifier distiguishes four classes of type (information): universal, application-wide, context-specific, and private-use. They are defined as

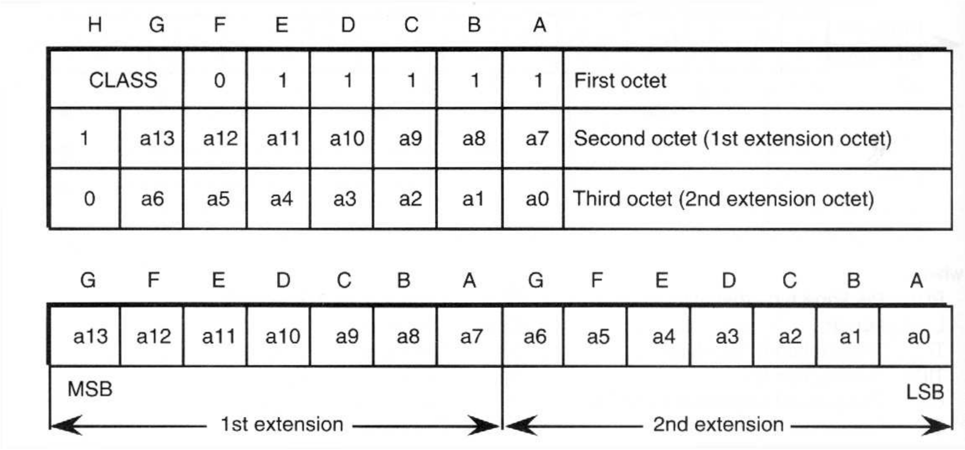
Universal: these types are standardised identifiers (ITU-T), and application-independent types

Application-wide: these types are specific to an application. For TCAP, an application-wide type identifier is used to refer to the TCAP international standards.

Context-specific: these types are specific to an application but also are limited to a set within the application

Private-use: these types are reserved for private use. TCAP uses this identifier for national and private applications.

Identifier Field and Extensions



H	G	F	E	D	C	B	A	
CLASS		0	1	1	1	1	1	First octet
1	a13	a12	a11	a10	a9	a8	a7	Second octet (1st extension octet)
0	a6	a5	a4	a3	a2	a1	a0	Third octet (2nd extension octet)

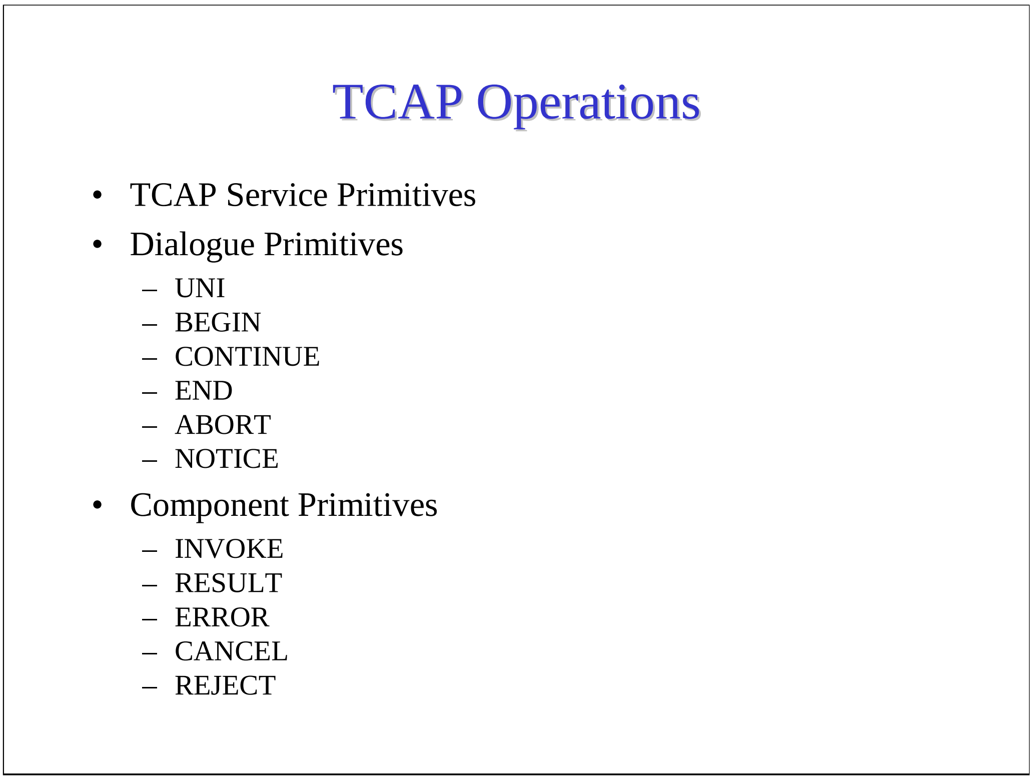
G	F	E	D	C	B	A	G	F	E	D	C	B	A
a13	a12	a11	a10	a9	a8	a7	a6	a5	a4	a3	a2	a1	a0

The identifier is coded in the first octet of the message as depicted in the slide above. In ANSI TCAP for example, bits HG identify the four type classes by the following bit assignments

Universal	00
Application-wide	01 International TCAP
Context-specific:	10
Private-use:	11 National TCAP/Private TCAP

Bit F identifies the forms of the data element. Two forms are possible. A primitive element (F = 0) has no further internal structure of data elements. That is, it has one value. A constructor element (F = 1) is recursively define in that it contains a series of elements. The remaining five bits (E, D, C, B, and A) distinguish one data type from another of the same class. For example, the field may distinguish BOOLEAN from INTEGER. Codes ranging between 00000 to 11110 are permitted. If more bits are required, the five bits are coded 11111 and bit H of the subsequent octet is 1 to indicate more octets follow. A 0 in H indicates the last octet of the extension. The bottom of the figure in the slide depicts this concept.

The length (L) specifies the length of the contents. It may take three forms: short, long, and indefinite. The short form is one octet long and is used when L is less than 128 octets. The long form is used when L is between 128 and 2^{1008} octets. The content is interpreted based on the identifier (type) field.

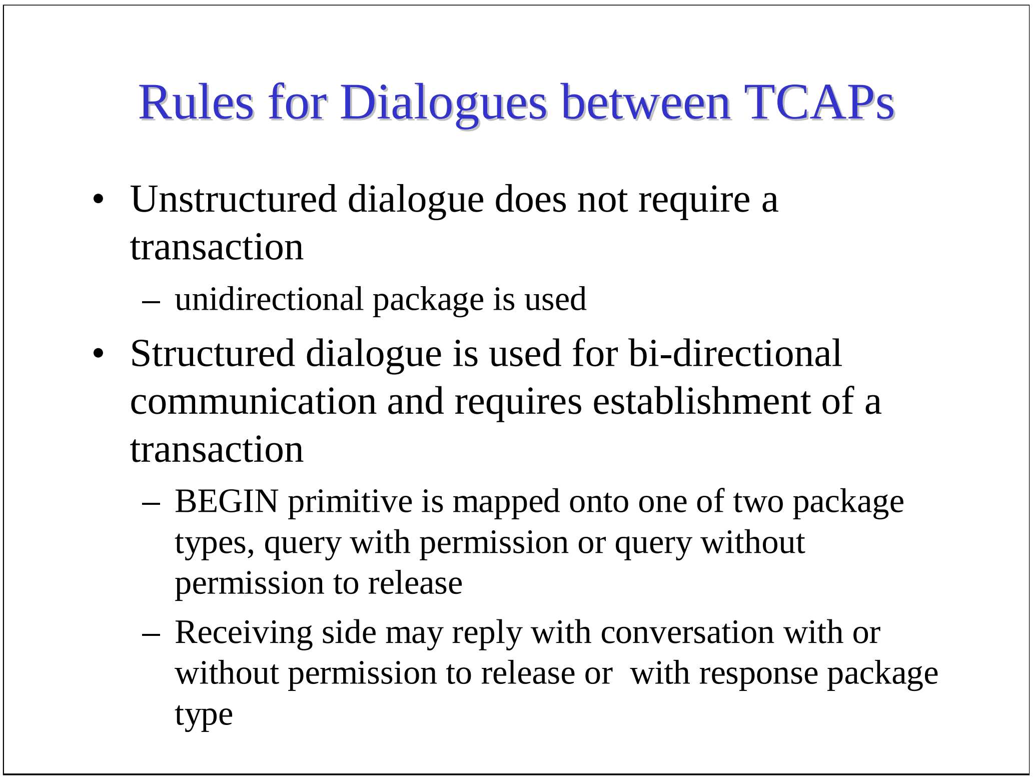


TCAP Operations

- TCAP Service Primitives
- Dialogue Primitives
  - UNI
  - BEGIN
  - CONTINUE
  - END
  - ABORT
  - NOTICE
- Component Primitives
  - INVOKE
  - RESULT
  - ERROR
  - CANCEL
  - REJECT

TCAP operations revolve around the use of transactions that operate between two application processes and two TCAPs. The application process passes a primitve to a TCAP, which contains the application traffic. The traffic is coded into parameters and placed in a TCAP transaction. A transaction may consist of more than one TCAP message running between the two application processes. Additonal application processes can become involved in the processing of these messages through an action called *handover*. Transactions can be exchanged in one direction only or in both directions. The application process decides which mode to use. The application is also permitted to change the mode during the transaction. When the application initiates a transaction, a transaction ID is assigned and is used for all messages pertaining to that transaction. Termination of a transaction can occur from either side by sending a primitive to its TCAP.

More than one operation may take plce within one transaction and within each operation one or more components may be involved. The components are *invoke*, *return result*, *return error*, and *reject*. The invoke component is correlated with the other components through a correlation ID that must be the same as the invoke ID.



Rules for Dialogues between TCAPs

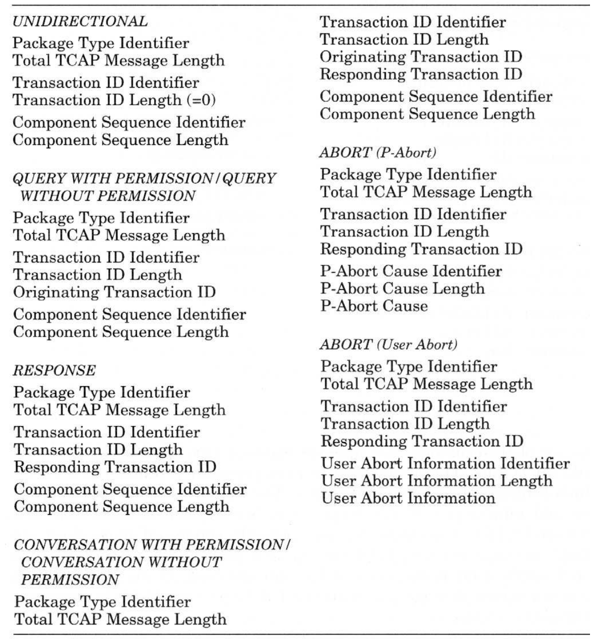
- Unstructured dialogue does not require a transaction
  - unidirectional package is used
- Structured dialogue is used for bi-directional communication and requires establishment of a transaction
  - BEGIN primitive is mapped onto one of two package types, query with permission or query without permission to release
  - Receiving side may reply with conversation with or without permission to release or with response package type

TCAP user can enter or not enter into TCAP transaction. A TCAP transaction is required for structured dialogue, unstructured dialogue does not require a transaction. The unstructured dialogue uses a message called the unidirectional package. This package type means that a component correlation is not needed nor is a transaction ID established. This package type is used when a UNI primitive is received.

For bidirectional caese, a transaction is established and a transaction IS must be reserved. This ID identifies the applications transaction process from the perspective of the local node. A structured dialogue is initiated by the ASE through a BEGIN primitive. This result in the creatin of tone of two package types, called query with permission to release and query without permission to release. A transaction ID is then selected that is used between both users. The query without permission to release is issued if more components will be sent within this transaction, the query with permission to release is used if the recipient does not need to expect more components.

When the receiving end receives a query package, is must initiate an application process transaction an respond to the sending party. It may respond with a conversation package type with or without permission to release. If the package type is with permission to release, the receiving user must decide whether to establish its own transaction ID or to use the initiators transaction ID. The END primitive is used to end a dialogue and results in a response package type. Intermediate packages are intiated with a CONTINUE primitive.

Transaction Portion of Package Type



UNIDIRECTIONAL

Package Type Identifier
Total TCAP Message Length

Transaction ID Identifier
Transaction ID Length (=0)

Component Sequence Identifier
Component Sequence Length

QUERY WITH PERMISSION/QUERY WITHOUT PERMISSION

Package Type Identifier
Total TCAP Message Length

Transaction ID Identifier
Transaction ID Length
Originating Transaction ID

Component Sequence Identifier
Component Sequence Length

RESPONSE

Package Type Identifier
Total TCAP Message Length

Transaction ID Identifier
Transaction ID Length
Responding Transaction ID

Component Sequence Identifier
Component Sequence Length

CONVERSATION WITH PERMISSION/ CONVERSATION WITHOUT PERMISSION

Package Type Identifier
Total TCAP Message Length

Transaction ID Identifier
Transaction ID Length
Originating Transaction ID
Responding Transaction ID

Component Sequence Identifier
Component Sequence Length

ABORT (P-Abort)

Package Type Identifier
Total TCAP Message Length

Transaction ID Identifier
Transaction ID Length
Responding Transaction ID

P-Abort Cause Identifier
P-Abort Cause Length
P-Abort Cause

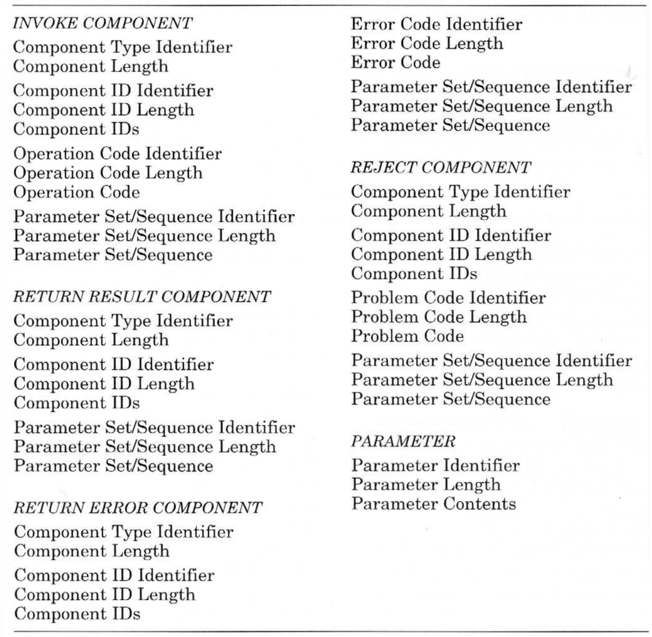
ABORT (User Abort)

Package Type Identifier
Total TCAP Message Length

Transaction ID Identifier
Transaction ID Length
Responding Transaction ID

User Abort Information Identifier
User Abort Information Length
User Abort Information

Component Portion of Package Type



INVOKE COMPONENT

Component Type Identifier
Component Length

Component ID Identifier
Component ID Length
Component IDs

Operation Code Identifier
Operation Code Length
Operation Code

Parameter Set/Sequence Identifier
Parameter Set/Sequence Length
Parameter Set/Sequence

RETURN RESULT COMPONENT

Component Type Identifier
Component Length

Component ID Identifier
Component ID Length
Component IDs

Parameter Set/Sequence Identifier
Parameter Set/Sequence Length
Parameter Set/Sequence

RETURN ERROR COMPONENT

Component Type Identifier
Component Length

Component ID Identifier
Component ID Length
Component IDs

Error Code Identifier
Error Code Length
Error Code

Parameter Set/Sequence Identifier
Parameter Set/Sequence Length
Parameter Set/Sequence

REJECT COMPONENT

Component Type Identifier
Component Length

Component ID Identifier
Component ID Length
Component IDs

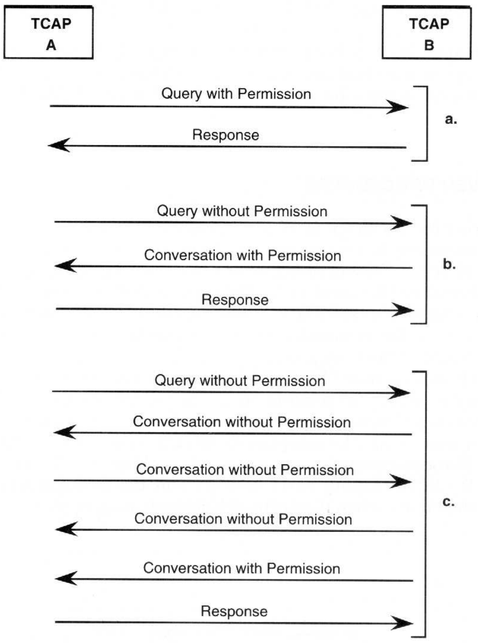
Problem Code Identifier
Problem Code Length
Problem Code

Parameter Set/Sequence Identifier
Parameter Set/Sequence Length
Parameter Set/Sequence

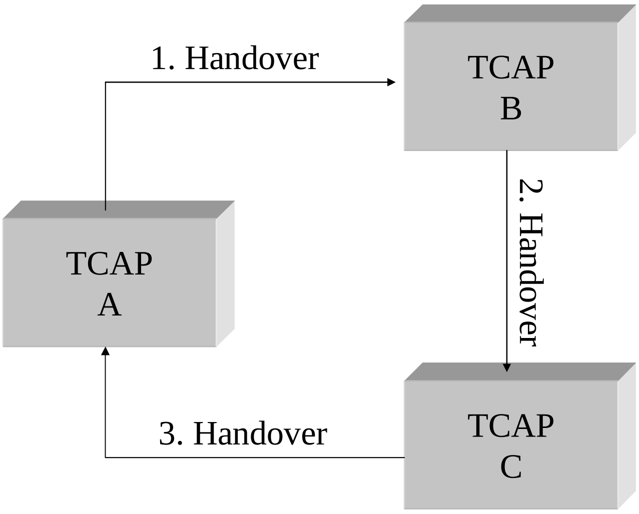
PARAMETER

Parameter Identifier
Parameter Length
Parameter Contents

TCAP Message Exchange


TCAP
A
TCAP
B
Query with Permission
Response
a.
Query without Permission
Conversation with Permission
Response
b.
Query without Permission
Conversation without Permission
Conversation without Permission
Conversation without Permission
Conversation with Permission
Response
c.

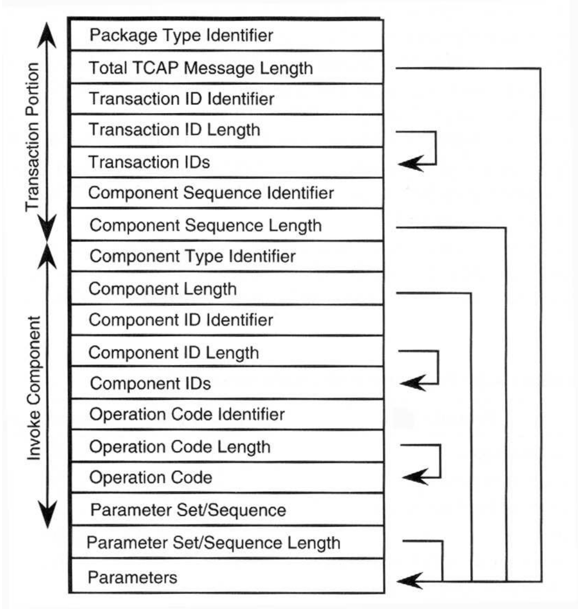
Handover Procedures



During the exchange of TCAP messages between two nodes, it may become necessary to request services from another node. From the perspective of TCAP, this operation means that one or more components will be transferred to this third node. This transfer of component processing is called handover (see slide above). A handover may be permanent, which lasts for the remainder of the transaction, or temporary, which lasts for a part of the transaction.

The initiatng user (TCAP B) decides when a handover is required. It begins the process by sending an invoke TCAP message (to TCAP C) that specifies a temporary handover operation is taking place. Next, the initiating user sends the components that it wishes this third node to process. These parameters must contain the transaction ID of party B, as well as B’s SCCP calling party address and the packages type that party C should use when it returns the message to party A.

Layout of TCAP Message



Transaction Portion

Invoke Component

Package Type Identifier

Total TCAP Message Length

Transaction ID Identifier

Transaction ID Length

Transaction IDs

Component Sequence Identifier

Component Sequence Length

Component Type Identifier

Component Length

Component ID Identifier

Component ID Length

Component IDs

Operation Code Identifier

Operation Code Length

Operation Code

Parameter Set/Sequence

Parameter Set/Sequence Length

Parameters

• *Package type identifier*. This field is an identifier field coded as natioanl (11) in bits HG and a constructor (1) in bit F. It is coded in one of seven forms to identify the specific package type.

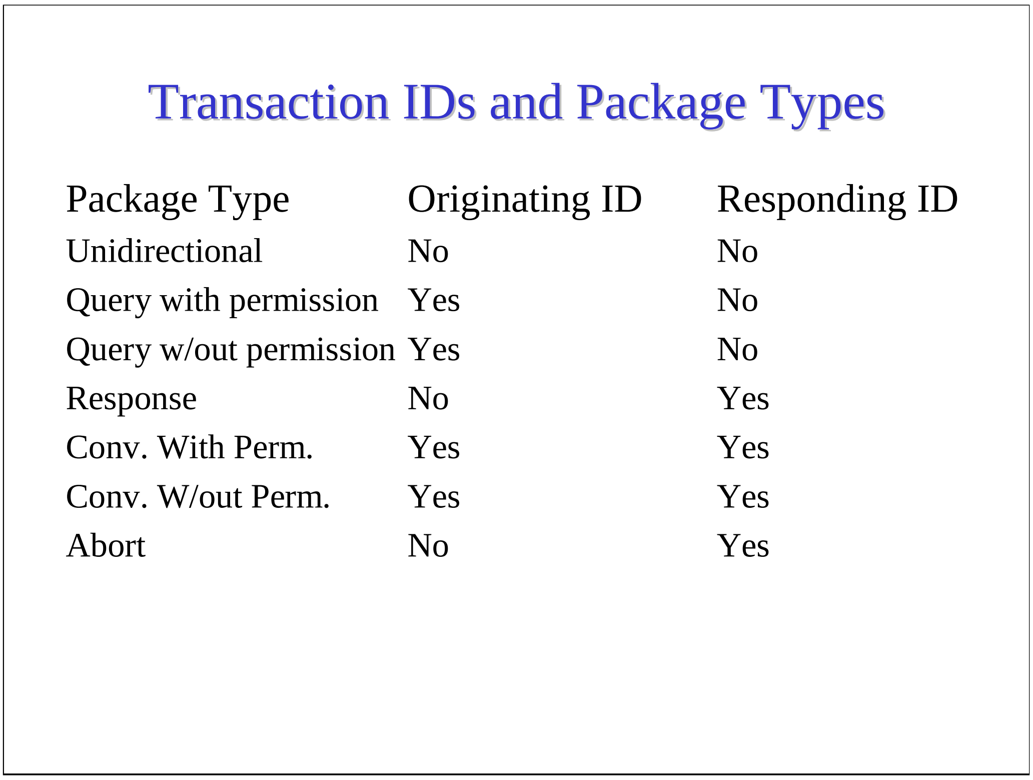
• *Transaction ID identifier*. Transaction IDs are placed in each TCAP message to correlate the messages associated with a transaction. It is coded as national and primitive with bits A-E set to 7.

• *Transaction IDs*. This field contains one or more transaction IDs unless the package type is unidirectional. The rules for use of transaction Ids in the seven package types are listed in the next slide. The originating transaction ID is assigned by the originator of the message. It must always be the first transaction ID if more than one is present. The responding transaction ID is assigned by the recipient of the message and it must be the same value as the originating transaction ID.

• *Component sequence identifier*. Identifies a component sequence and is coded as national constrcutor with bits A-E set to 8.

• *Component type identifier*. Coded in one of six values (a) Invoke (last), (b) Return Result (last),(c) Return Error, (d) Reject, (e) Invoke (not last), (f) Return Result (not last)

• *Component ID identifier*. One octet in length and is sued to indicate theat components follow in the message. A-E set to 15

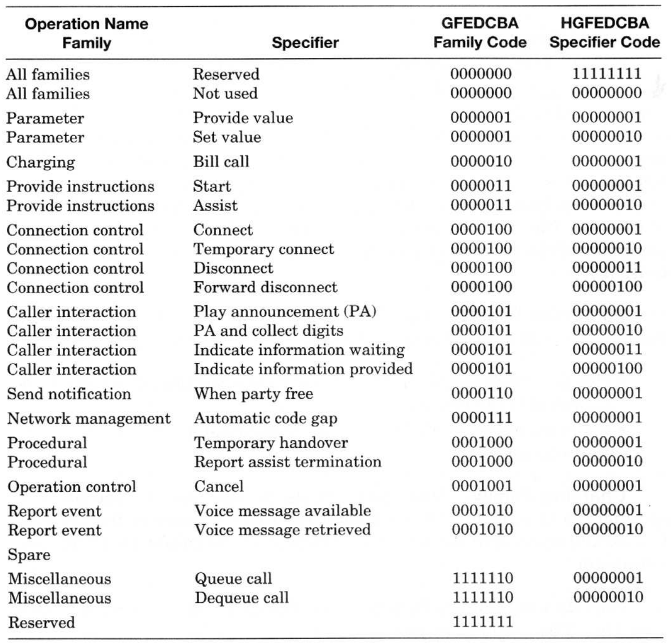


Transaction IDs and Package Types

Package Type	Originating ID	Responding ID
Unidirectional	No	No
Query with permission	Yes	No
Query w/out permission	Yes	No
Response	No	Yes
Conv. With Perm.	Yes	Yes
Conv. W/out Perm.	Yes	Yes
Abort	No	Yes

- *Component IDs*. Identifies each component
- *Operation code identifier*. Identifies either national or private TCAP
- *Operation code*. Application specific and not exmined by TCAP
- *Parameter set/sequence identifier*. Identifies either type sequence or type set depending on how following parameters are organised. Both identifiers are coded as national constructors with bits A-E set to 18 for Set or 16 for Sequence
- *Parameters*. The reason the TCAP message is exchanged between fields is to convey the values in the parameterfield. Currently the TCAP spcification by ANSI defines 25 national parameters.

TCAP National Operations

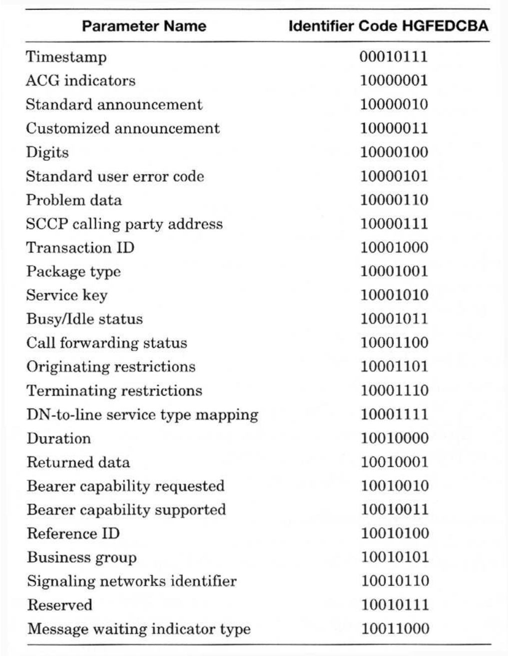


Operation Name Family	Specifier	GFEDCBA Family Code	HGFEDCBA Specifier Code
All families	Reserved	0000000	11111111
All families	Not used	0000000	00000000
Parameter	Provide value	0000001	00000001
Parameter	Set value	0000001	00000010
Charging	Bill call	0000010	00000001
Provide instructions	Start	0000011	00000001
Provide instructions	Assist	0000011	00000010
Connection control	Connect	0000100	00000001
Connection control	Temporary connect	0000100	00000010
Connection control	Disconnect	0000100	00000011
Connection control	Forward disconnect	0000100	00000100
Caller interaction	Play announcement (PA)	0000101	00000001
Caller interaction	PA and collect digits	0000101	00000010
Caller interaction	Indicate information waiting	0000101	00000011
Caller interaction	Indicate information provided	0000101	00000100
Send notification	When party free	0000110	00000001
Network management	Automatic code gap	0000111	00000001
Procedural	Temporary handover	0001000	00000001
Procedural	Report assist termination	0001000	00000010
Operation control	Cancel	0001001	00000001
Report event	Voice message available	0001010	00000001
Report event	Voice message retrieved	0001010	00000010
Spare			
Miscellaneous	Queue call	1111110	00000001
Miscellaneous	Dequeue call	1111110	00000010
Reserved		1111111	

TCAP Operations

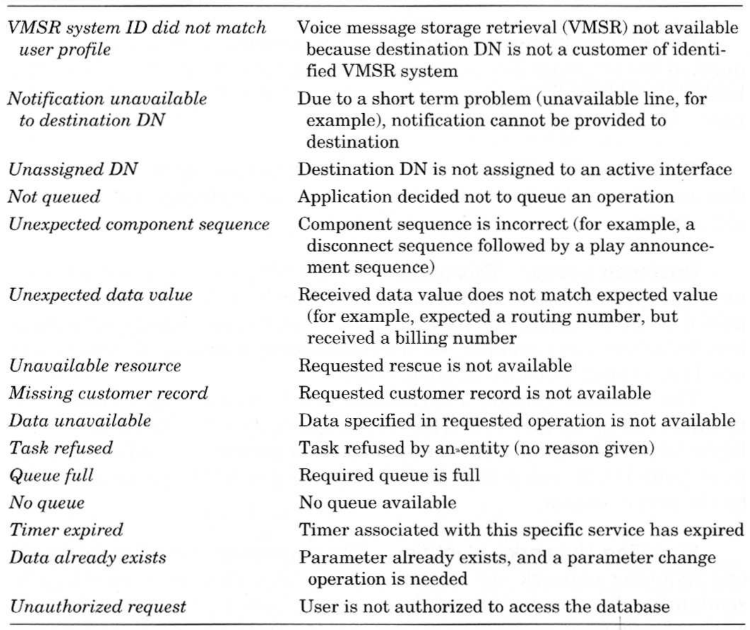
- TCAP operations are divided into operation family and operation specifier
- Operation Family
  - Parameter family
  - Charging family
  - Provide instructions family
  - Connection control family
  - Call interaction family
  - Send notification family
  - Network management family
  - Procedural family
  - Operation control family
  - Report event family
  - Miscellaneous family

TCAP Parameters



Parameter Name	Identifier Code HGFEDCBA
Timestamp	00010111
ACG indicators	10000001
Standard announcement	10000010
Customized announcement	10000011
Digits	10000100
Standard user error code	10000101
Problem data	10000110
SCCP calling party address	10000111
Transaction ID	10001000
Package type	10001001
Service key	10001010
Busy/Idle status	10001011
Call forwarding status	10001100
Originating restrictions	10001101
Terminating restrictions	10001110
DN-to-line service type mapping	10001111
Duration	10010000
Returned data	10010001
Bearer capability requested	10010010
Bearer capability supported	10010011
Reference ID	10010100
Business group	10010101
Signaling networks identifier	10010110
Reserved	10010111
Message waiting indicator type	10011000

TCAP Error Codes



VMSR system ID did not match user profile	Voice message storage retrieval (VMSR) not available because destination DN is not a customer of identified VMSR system
Notification unavailable to destination DN	Due to a short term problem (unavailable line, for example), notification cannot be provided to destination
Unassigned DN	Destination DN is not assigned to an active interface
Not queued	Application decided not to queue an operation
Unexpected component sequence	Component sequence is incorrect (for example, a disconnect sequence followed by a play announcement sequence)
Unexpected data value	Received data value does not match expected value (for example, expected a routing number, but received a billing number
Unavailable resource	Requested rescue is not available
Missing customer record	Requested customer record is not available
Data unavailable	Data specified in requested operation is not available
Task refused	Task refused by an entity (no reason given)
Queue full	Required queue is full
No queue	No queue available
Timer expired	Timer associated with this specific service has expired
Data already exists	Parameter already exists, and a parameter change operation is needed
Unauthorized request	User is not authorized to access the database