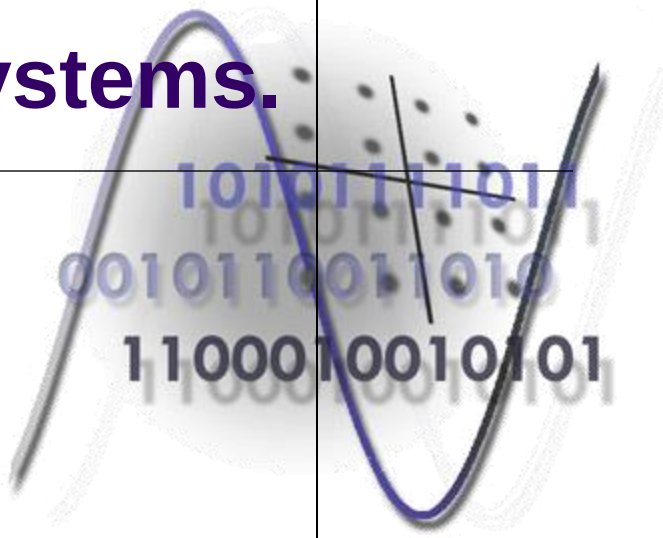
Course 4-5

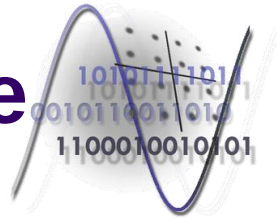
Signaling techniques used in classical telephone networks. The SS7 signaling systems.



Zsolt Polgar

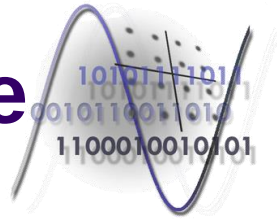
Communications Department
Faculty of Electronics and Telecommunications,
Technical University of Cluj-Napoca

Content of the course



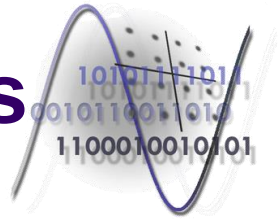
- Classification of the signaling techniques;
- Access signaling;
  - “loop start” and “ground start” signaling;
  - FX (FXS/FXO) signaling;
- Trunk signaling;
  - Basic signaling diagram;
  - E&M signaling;
  - MFC-R2 signaling;

Content of the course



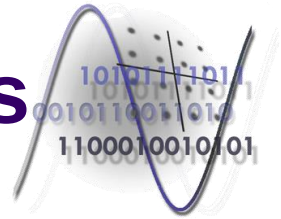
- The SS7 signaling system - general aspects;
- The SS7 architecture;
  - Node types;
  - Link types;
- Signaling operations for a telephone call;
- The SS7 protocol stack;
  - Basic characteristics;
- Transmission on the signaling links;
- MTP3 layer operations;
- Layer 4 protocols;
  - TUP and ISUP protocols;
  - Control of the signaling connection; SCCP operations;
- Higher layer protocols;
  - TCAP and MAP protocols;

Signaling. General aspects



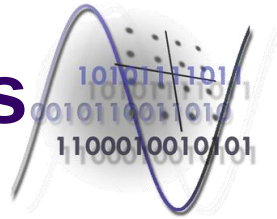
- The signaling in telephony refers to:
  - Call control signals;
  - Transmission techniques for control signals;
  - Call management algorithms;
- Purpose of the signaling:
  - Control of the set up, deployment and interruption of a telephone connection;
- There are several possible classifications:
  - According to the type of the controlled channel:
    - subscriber signaling;
      - used between the subscriber terminal and the local exchange.
    - trunk signaling;
      - used on the trunk lines between the exchanges of the public networks, between PBX and local exchanges and between PBX exchanges.

Signaling. General aspects



- According to the way the signaling is transmitted:
  - in-band signaling;
    - the signaling is transmitted in the same frequency band as the speech signal.
  - out-band signaling;
    - the signaling is transmitted outside the frequency band of the speech signal.
  - channel associated signaling;
    - each voice (data) channel has assigned a separate signaling channel.
  - common channel signaling;
    - the signaling assigned to all voice (data) channels or to a group of channels is realized on a common channel used specially for this operation.
- According to role performed:
  - network management signaling:
    - characteristic only to trunk signaling;
      - for example management of congestions in switches.

Signaling. General aspects



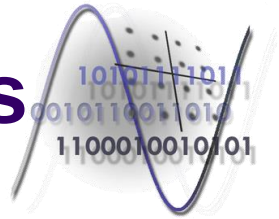
- alerting signaling;
  - refers usually to sending to the called terminal (telephone or trunk equipment) of a ringing signal;
  - this signal is applied to a line or a trunk.
- address signaling;
  - refers to the transmission of the information related to the called number on subscriber lines or on trunks;
  - performed by the terminal or by a switching equipment;
  - can be accomplished by sending impulses or DTMF tones or special data packets in digital networks (ISDN);
  - this information have to be sent in a public network across several links up to the final completion of the connection;
  - the address signaling on trunks is realized usually (in classical telephone networks) by using a MF (Multi-Frequency) type technique:
    - different to the DTMF technique used on the subscriber line (code 2 of 6);
    - this signaling has the format: KP + number +ST;
    - KP (Key Pulse) represents the beginning of the telephone number transmission;
    - ST (Start) represents the end of this transmission and the beginning of the call processing – see the following table.

Signaling. General aspects

- MF coding of the characters (digits) used in trunk address signaling:
  - the frequencies are expressed in Hz;

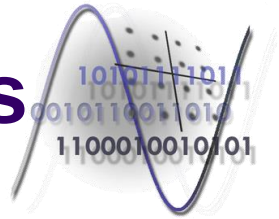
Digit/symbol	Frequency 1	Frequency 2
KP	1100	1700
KP2	1300	1700
1	700	900
2	700	1100
3	900	1100
4	700	1300
5	900	1300
6	1100	1300
7	700	1500
8	900	1500
9	1100	1500
0	1300	1500
ST	1500	1700

Signaling. General aspects



- call supervision (supervisory) signaling;
  - detects the state or changes the condition of a line or trunk;
    - there are two possible supervised conditions: ON-HOOK (idle state) and OFF-HOOK (active state);
    - when a line/trunk goes OFF-HOOK, it is interpreted as a seizure by the system and the operating state of the considered line goes from idle to active;
    - brief changes in the on-hook/off-hook status of a line or a trunk (transition called *wink* or *hook flash*) are also part of the supervision signaling.
  - out-band signaling is used usually;
    - an important part of supervisory signaling is represented by the (subscriber) access signaling and station loop signaling of the exchange.
      - the access signaling refers to detection of the off-hook state of the calling (subscriber) terminal or equipment (ex. PBX);
      - the station loop signaling refers to the answer of the local exchange (or PBX), signaling related the acceptance or non-acceptance of the access in the network;
        - access accepted/granted: the dial tone is transmitted;
        - unaccepted/rejected access: the busy ton is transmitted.

Signaling. General aspects



- another important component of the supervisory signaling is the answer and disconnect supervision;
  - it is important for billing.
- call progress indicator signals are tightly related to supervisory signaling;
  - these signals refer to audible tones that indicate to the calling side the progress of the telephone call;
  - these tones are characterized by frequency (or groups of frequencies) and timing (cadence);
  - these tones are the following:
    - dial tone – the CO/PBX is ready to accept the digits of the number from the subscriber;
    - busy tone – the called terminal is busy;
    - reorder tone – the same as the busy tone, but the call is rejected due to congestion of local/transit exchanges or to unavailability of trunk circuits;
    - special information tones – faulty line or non existent number, a.s.o.;
    - ring-back tone – indicates to the calling terminal the establishment of the connection and the alerting of the called terminal.

Access signaling

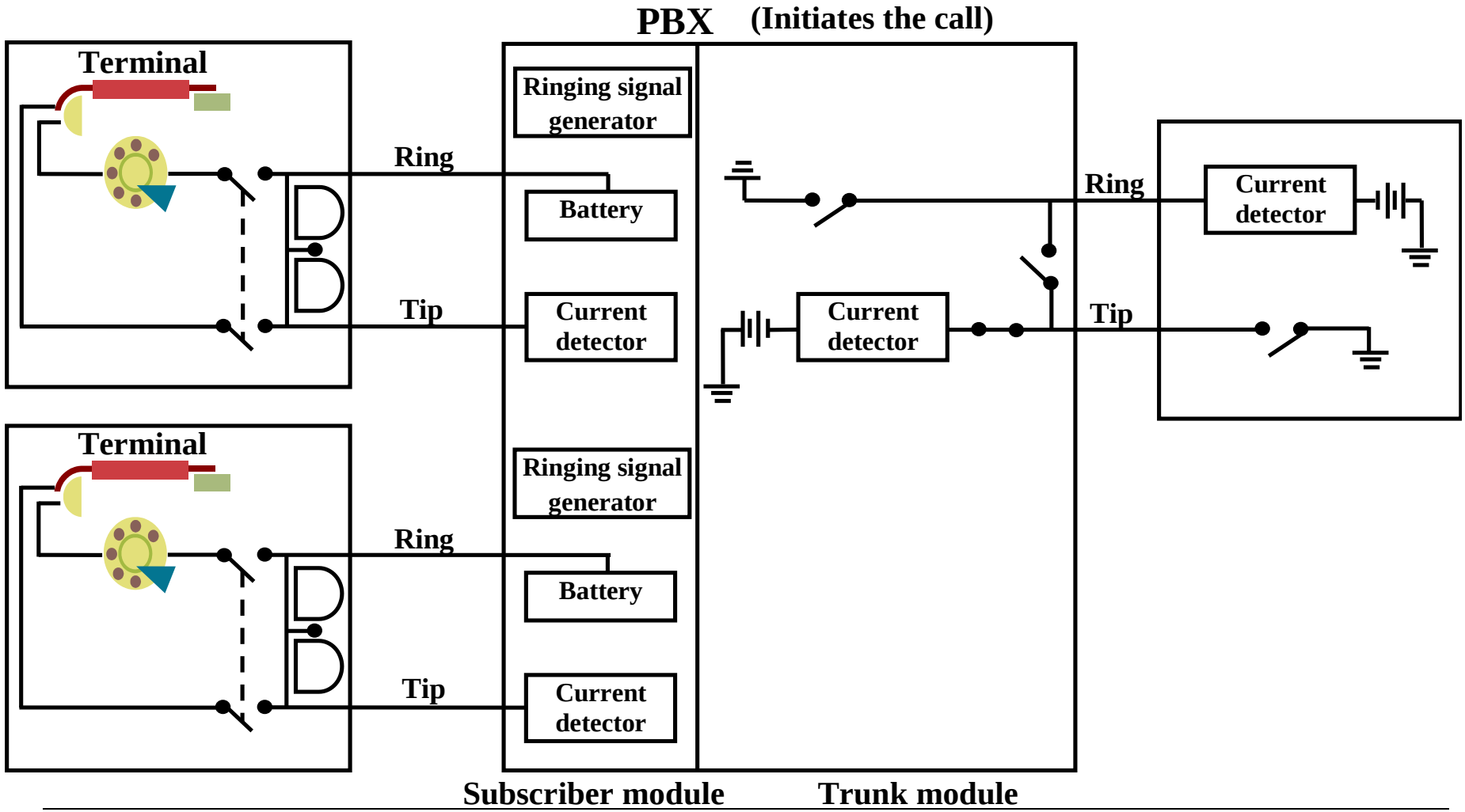
- The access signaling;
  - Determines (announces) when a line is off-hook or on-hook;
    - there are two basic variants of this signaling, namely:
      - „loop start” type signaling;
      - „ground start” type signaling.
    - „loop start” signaling is characteristic to PSTN networks (“Public Switched Telephone Network”);
      - when the phone is active a current loop is closed, loop composed of the phone, wires and the battery located in the exchange;
      - the current is detected by a current sensing circuit and the exchange responds with the dial tone;
      - the incoming call to the phone is signaled by a ringing signal repeated according to a given on/off pattern;
      - problems related to this type of signaling:
        - automatic answer machines could be blocked in off-hook state;
        - the exchange is not capable to interrupt the connection;
        - the line/trunk can be seized in the same time from both directions;
          - the dialing starts in the moment when a call is received;

Access signaling

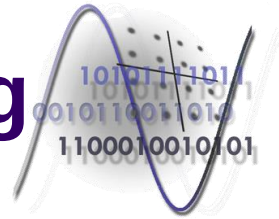
- the „ground start” type signaling is used especially on the analogue trunk connections (PBX - CO);
  - when an equipment tries to access the network (to initiate a call) it connects the RING lead to the ground;
  - the exchange (accessed) detects the current through this lead and if it can accept the call connects the TIP lead to the ground;
  - the call initiating equipment senses the current through the TIP lead and starts the call;
  - the interruption of the connection can be realized by both parts involved in communication;
  - a dial tone can be provided to the calling part, but it is optional.

Access signaling

- „loop start” and „ground start” type access signaling;



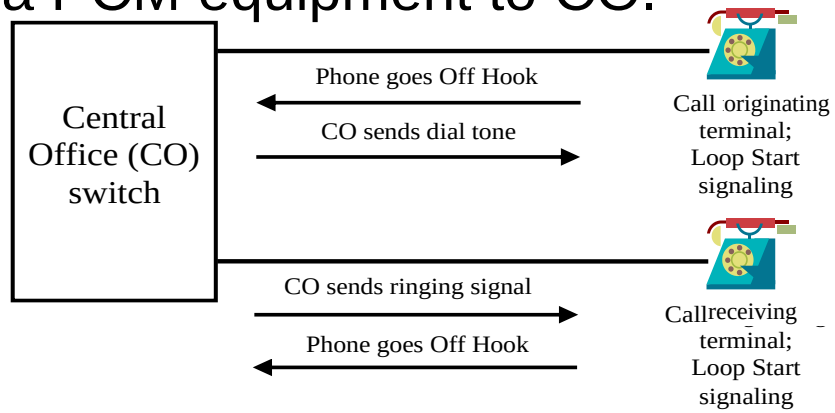
Access signaling

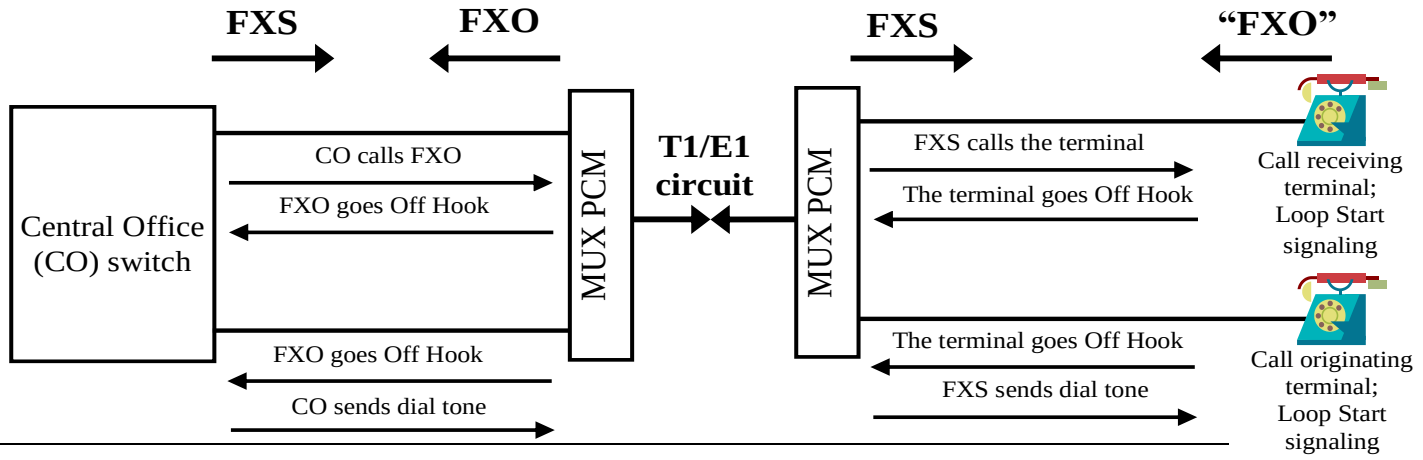


- **F**oreign e**X**change (FX) signaling;
  - called also FXS/FXO signaling – Foreign eXchange Station (FXS) / Foreign eXchange Office (FXO);
  - it was developed for connecting PBX exchanges to local exchanges (Central Office);
  - an FXS type interface is also used for connecting a multiplexer to the CO;
  - the interface between the phone device and the CO is similar with the FX interface;
  - the FXS interface located in the CO ensures:
    - the supply voltage;
    - ringing signal generation;
    - off-hook detection;
    - call progress indicator signals.
  - the FXO interface located in PBX (or phone) ensures:
    - detection of dial tone;
    - ringing signal detection;
    - call progress signal detection.

Access signaling

- The principle of FXS/FXO signaling;
  - Connecting a phone to CO;
  - Connecting a PCM equipment to CO.





Access signaling

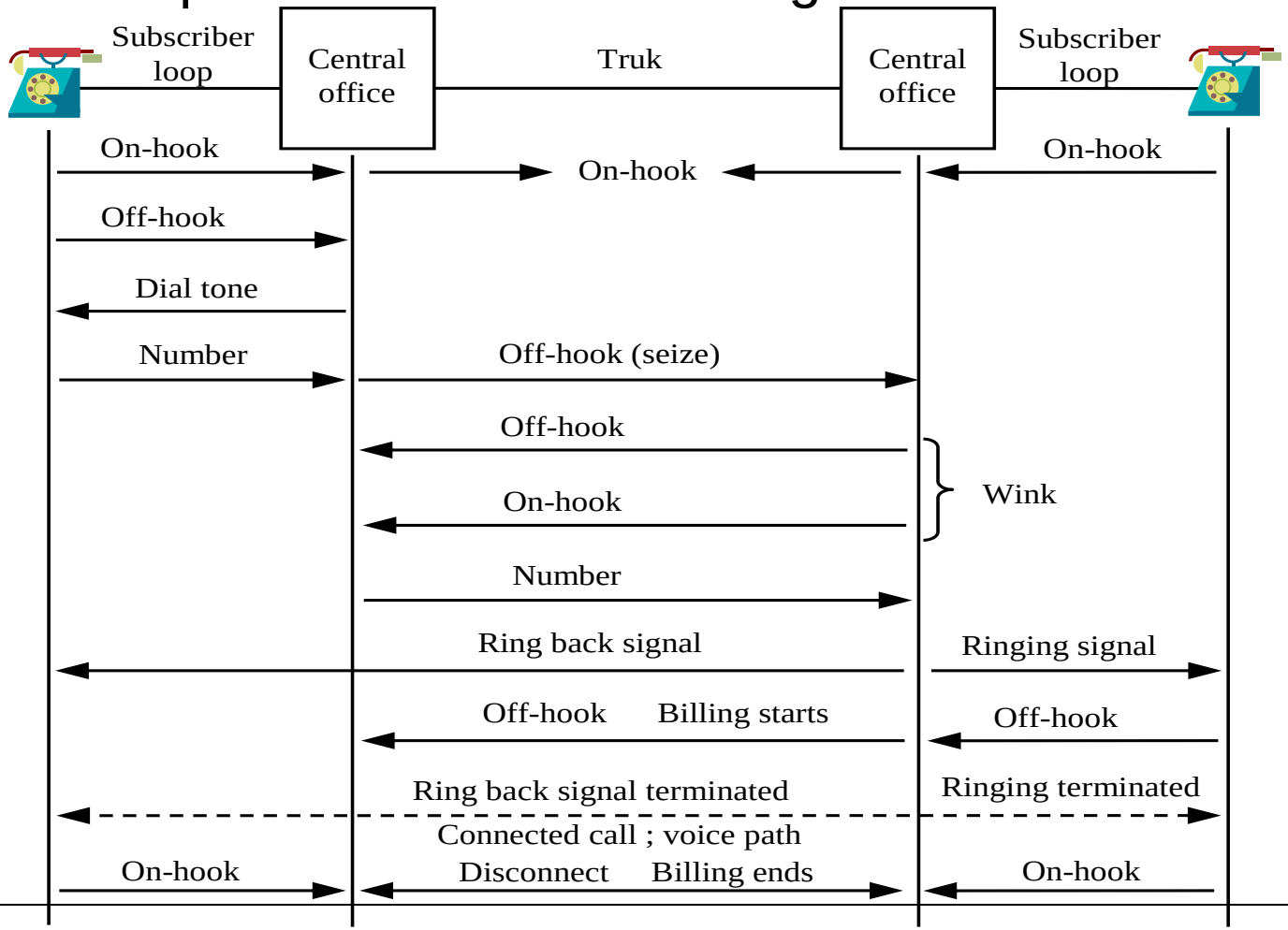
- Allocation of AB (see the E1 and T1 PCM frames) bits to signals associated to FXS/FXO signaling:

Signal / direction	Forward (to FXO)	Backward (to FXS)
IDLE / ON HOOK	AB = 0 1	AB = 0 1
OFF HOOK		AB = 1 1
RINGING	AB = 0 0	
RING GROUND		AB = 0 0 (only GS)
TIP CLOSED	AB = 0 1 (only GS)	
FORWARD DISCONNECT	AB = 1 1 (only GS)	

- GS: Ground Start;

Trunk signaling

- Signaling sequence associated to a telephone call in a classical telephone network involving a trunk connection;

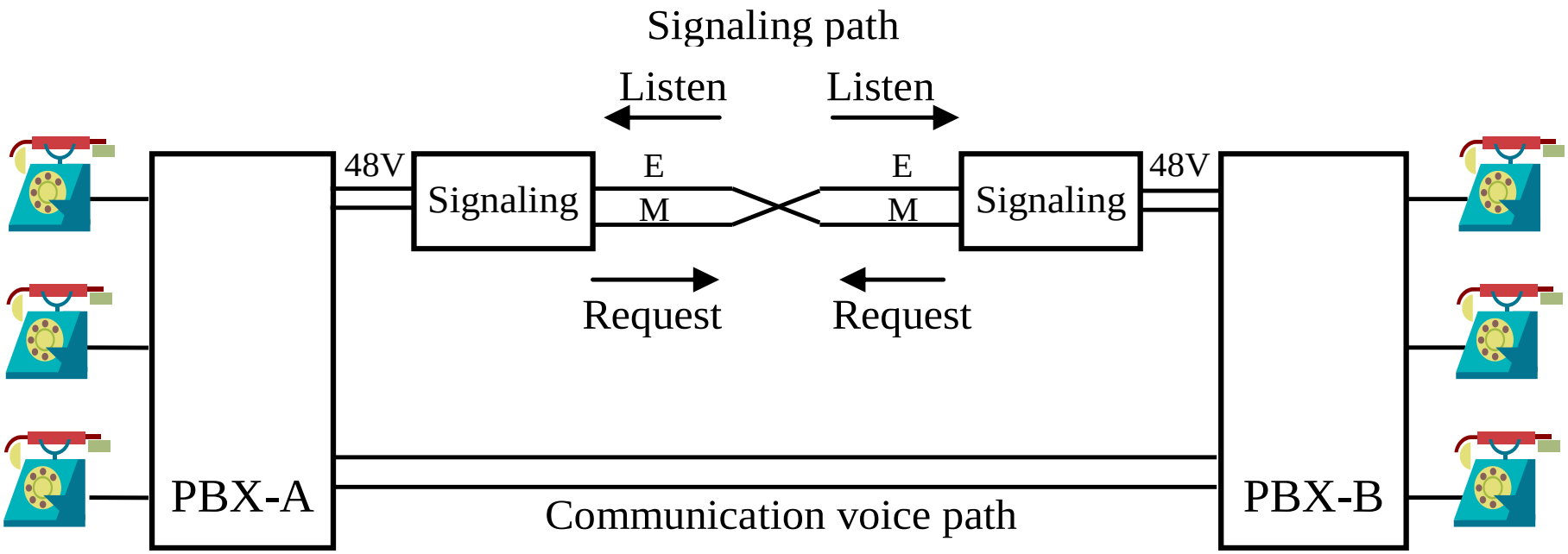


Trunk signaling

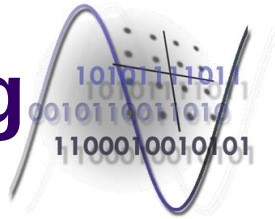
- E&M (“**E**ar and **M**outh” sau “rec**E**ive and trans**M**it”) signaling;
  - signaling technique developed for trunk signaling between PBX and PSTN exchanges;
  - there were developed different signaling variants (types I - V);
  - this signaling technique is based on two signals, called M and E;
    - the M signal is generated by the trunk call initiating exchange;
    - the E signal is a response sent by the exchange located at the opposite end of the trunk;
    - the E&M signaling channel is separated from the voice channel of the trunk;
    - the states of the equipment located at the two ends of the trunk connection using these two signals are coded :
      - equipment which can be in the IDLE / ON HOOK state or in the BUSY (SEIZED) / OFF HOOK state;
      - using some impulses (activation – deactivation : „wink”) other information can be transmitted on these lines as well.

Trunk signaling

- E&M signaling basic schematics;
  - Sending of the called number on the trunk connection is achieved using a MF type (coding) transmission on the voice path;
    - it is ensured a larger speed of the address signaling;



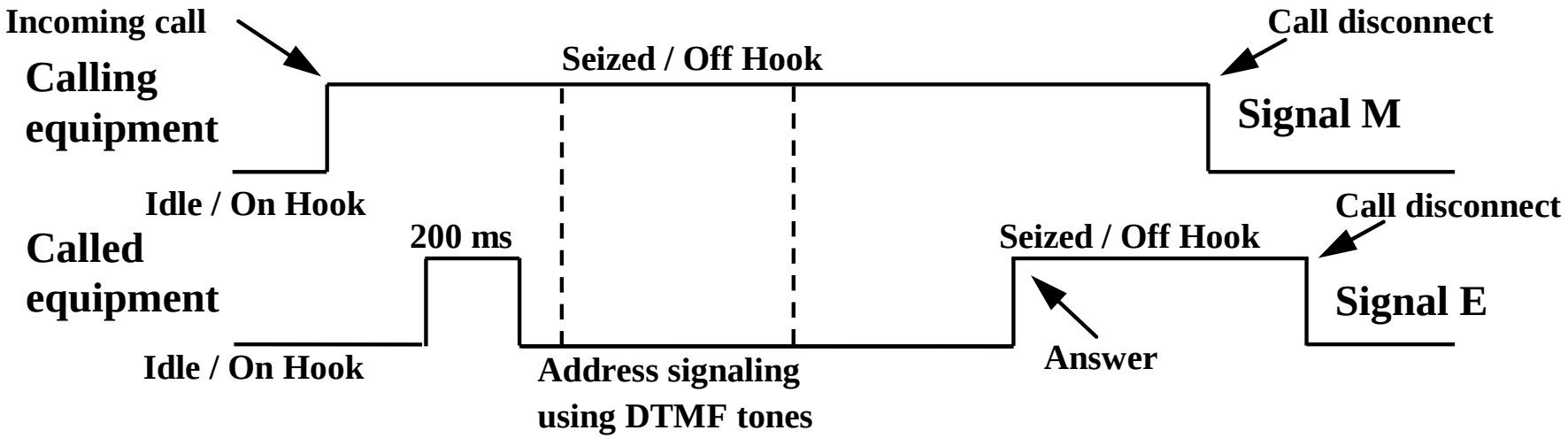
Trunk signaling



- Types of E&M signaling:
  - **E&M immediate:**
    - the trunk call initiating equipment goes OFF HOOK and transmits immediately the called number;
    - after the reception of the number the trunk equipment on the opposite end goes OFF-HOOK during the entire duration of the call;
    - both equipments can terminate the call by going in the ON-HOOK state;
    - there is the possibility that the called trunk equipment is not ready to receive the number;
  - **E&M wink:**
    - the terminal equipment responds to an OFF-HOOK state of the calling equipment with a short OFF-HOOK impulse („wink”) in the moment when is ready to receive the called number;
    - the opening of the voice path and the starting of the billing process is achieved after the E signal goes OFF-HOOK.

Trunk signaling

- Signaling sequence corresponding to E&M wink:



- **E&M wink-wink:**
  - the terminal equipment responds to an OFF-HOOK state of the calling equipment with a short impulse on signal E;
  - the call originating equipment sends the number in MF code on the voice path;
  - the receiving equipment sends another short impulse on signal E, signaling that it received all the digits.

Trunk signaling

- Allocation of AB(CD) bits to physical signals characteristic to E&M signaling:

Direction	State	A	B	C	D
Transmission	Idle/On-Hook	0	0	0	0
Transmission	Seized/Off-Hook	1	1	1	1
Reception	Idle/On-Hook	0	0	0	0
Reception	Seized/Off-Hook	1	1	1	1

General aspects

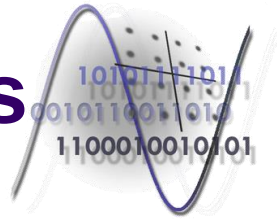
- Signaling System 7 (SS7) is an architecture for out-of-band signaling supporting the following operations:
  - call-establishment;
  - billing;
  - routing and information exchange functions for the Public Switched Telephone Network (PSTN).
- SS7 includes functions performed by a signaling network and a protocol which controls this network;
- SS7 is characterized by high-speed packet data and out-of-band signaling;
- Applications supported by SS7 are:
  - PSTN and ISDN;

General aspects

- Interaction with Network Databases and Service Control Points;
  - the databases are storing the information related to the telecommunication network;
  - it is ensured the control of the provided services;
- Mobile services;
- Administration and Maintenance operations of telecommunication networks;

- The SS7 network provides the following functionalities:
  - Basic call setup, management, billing, and call release;
  - Enhanced call features:
    - call waiting;
    - call forwarding;
    - calling party name/number display;
    - call restriction/rejection;
    - three-way call.

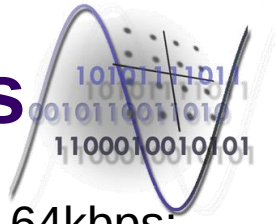
General aspects



- Handling congestion and priorities;
- Wireless services:
  - PCS (Personal Communication System);
  - wireless roaming;
  - mobile subscriber authentication.
- Local Number Portability (LNP);
- Toll-free and toll services;
- Exchange of database information between Network Elements (NEs);
- Network management.

- SS7 uses out-of-band signaling;
  - the signaling does not take place over the same path as the conversation;
  - a separate digital channel is used for exchange of signaling information between switching nodes;
    - this channel is called signaling link.

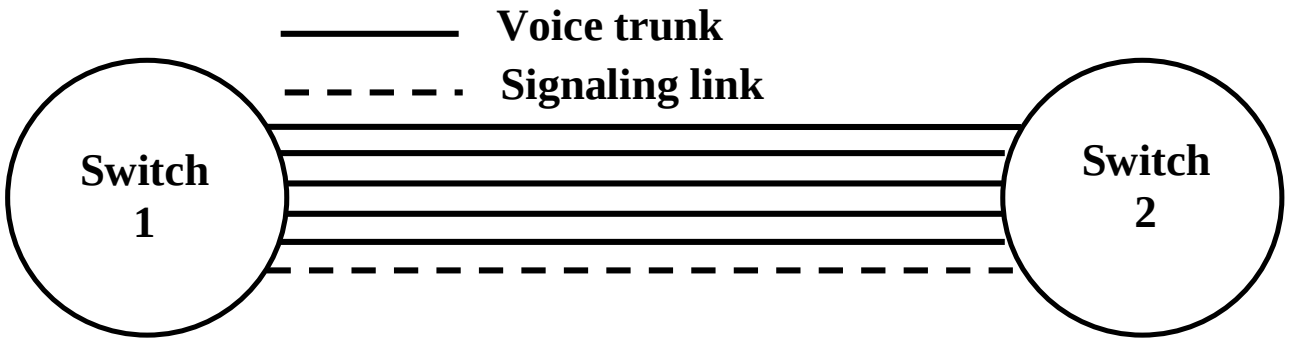
General aspects



- dedicated signaling links transmit information at rates of 56kbps or 64kbps;
  - the ISDN D channel extends the concept of out-of-band signaling to the interface between the subscriber and the CO.
- Advantages of out-of-band signaling;
  - it is ensured the transport of more data at higher speed;
    - faster call setup.
  - it allows signaling any time during the entire duration of the call;
  - it enables signaling with network elements having no direct trunk connections;
    - more efficient use of the voice circuit, especially in international or long distance calls.
  - it ensures improved control over fraudulent network usage;
  - it offers support for more services – see the previously presented aspects.

General aspects

- Methods for implementing the out-of-band signaling:
  - Associated signaling;
    - allocates a dedicated signaling link between a pair of interconnected switches;
      - it is about an associated signaling to a group of trunks;
      - it is a good solution as long as the signaling is performed between switches connected by direct trunk connections – simple and efficient solutions.

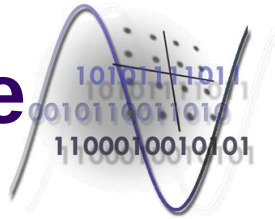


  - Quasi-associated signaling;
    - implements a signaling network that enables any node to exchange signaling information with any other node;
      - ensures an increased security in what concerns the fraudulent use of the network.

The SS7 architecture

- The SS7 network includes the following three basic components:
  - Service Switching Points (SSP);
    - SSPs are telephone switches (local offices or transit offices) equipped with SS7 capable software and terminating signaling links;
    - SSPs originate, terminate or switch the call;
      - SSP sends signaling messages to other SSPs to setup, manage and release voice circuits, operations required to complete a call;
      - SSP may also send a query to a database (SCP) to determine how to route a call (for example toll-free calls);
      - SSP nodes are service access points where the users access the network/service, using an access protocol.
  - Signaling Transfer Points (STP);
    - STPs are the packet switches of the SS7 network;
    - STPs receive and route incoming signaling messages toward the proper destination;
      - STP routes each incoming message to an outgoing signaling link based on the routing information included in the SS7 message;

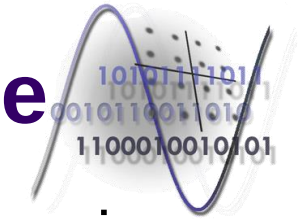
The SS7 architecture



- the intermediate nodes, STPs, act as SS7 routers and provide multiple paths to a destination in order to handle failures within the network;
- STPs also offer specialized routing functions for toll-free 800 numbers, calling card numbers or mobile subscriber identification;
- STPs may also be used to screen the messages exchanged with other networks;
- STPs are usually deployed in redundant not co-located pairs – they work redundantly to perform the same function.

- Signaling/Service Control Points (SCP);
  - SCPs are databases that provide information necessary for advanced call-processing capabilities;
  - SCPs are usually deployed in matted pair configurations in separate physical locations;
    - one of the SCP acts as backup system;
  - SCP executes network and data control functions:
    - billing;
    - toll free phone number translation.

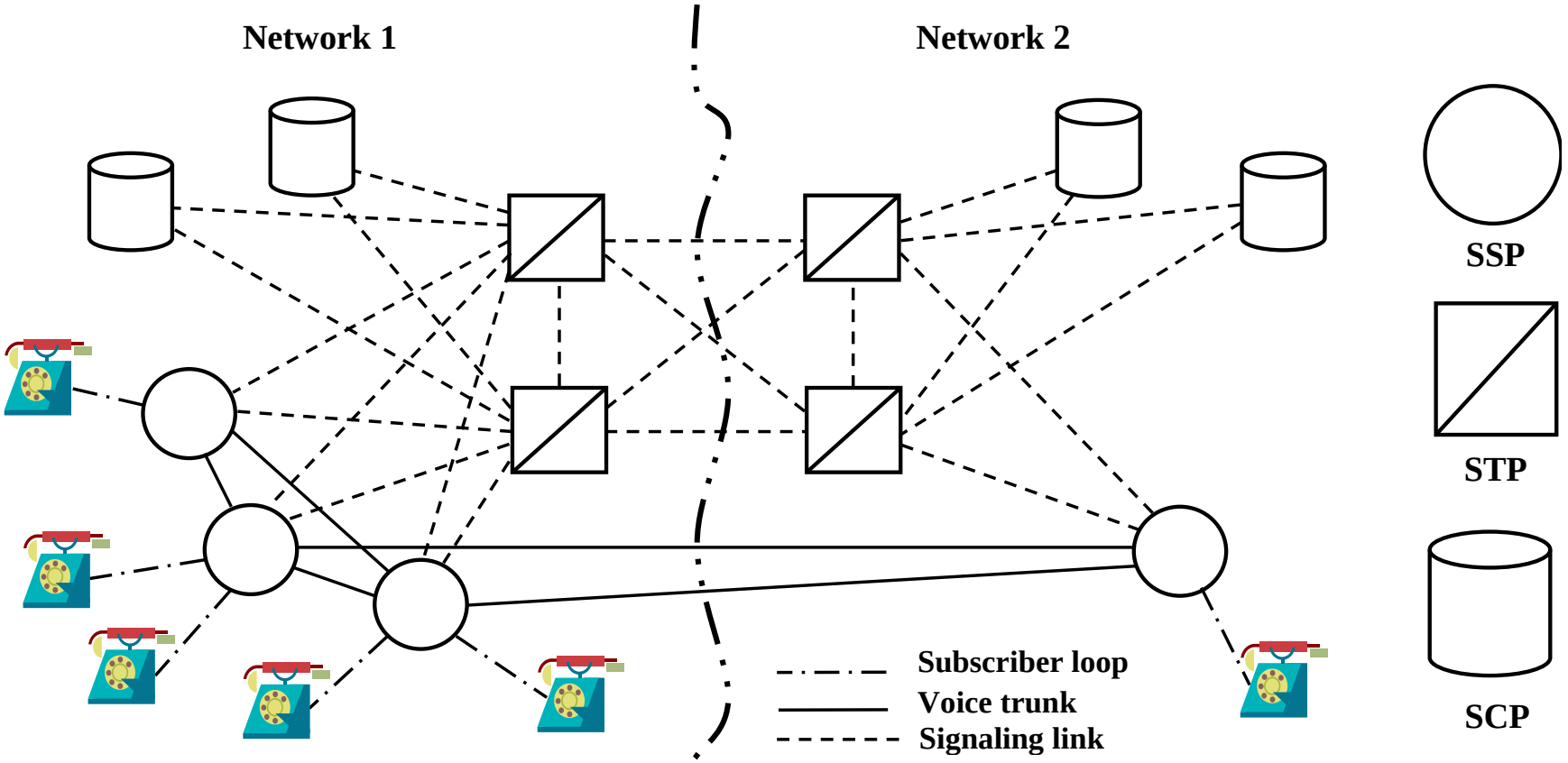
The SS7 architecture



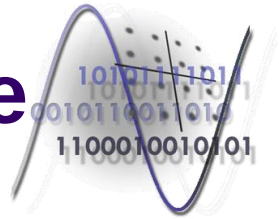
- The availability of SS7 networks is critical for call processing;
  - Without exchange of signaling information between SSPs it is not possible to complete any inter-switch call;
  - The SS7 network is built using a highly redundant architecture;
    - each individual element have to meet imposed requirements for availability;
    - protocols are defined between the interconnected elements, protocols which provide error correction and retransmission capabilities;
      - continuous services are allowed even in the event of signaling point or link failures.
- Each signaling point in the SS7 network is uniquely identified by a numeric point code (PC);
  - These PC codes are carried in the signaling messages exchanged between signaling points to identify:
    - the origination point (OPC),
    - the destination point (DPC) of each message.

The SS7 architecture

- Each signaling point uses a routing table to select the appropriate signaling path for each message;
- The general architecture of a digital telephone network with SS7 signaling:



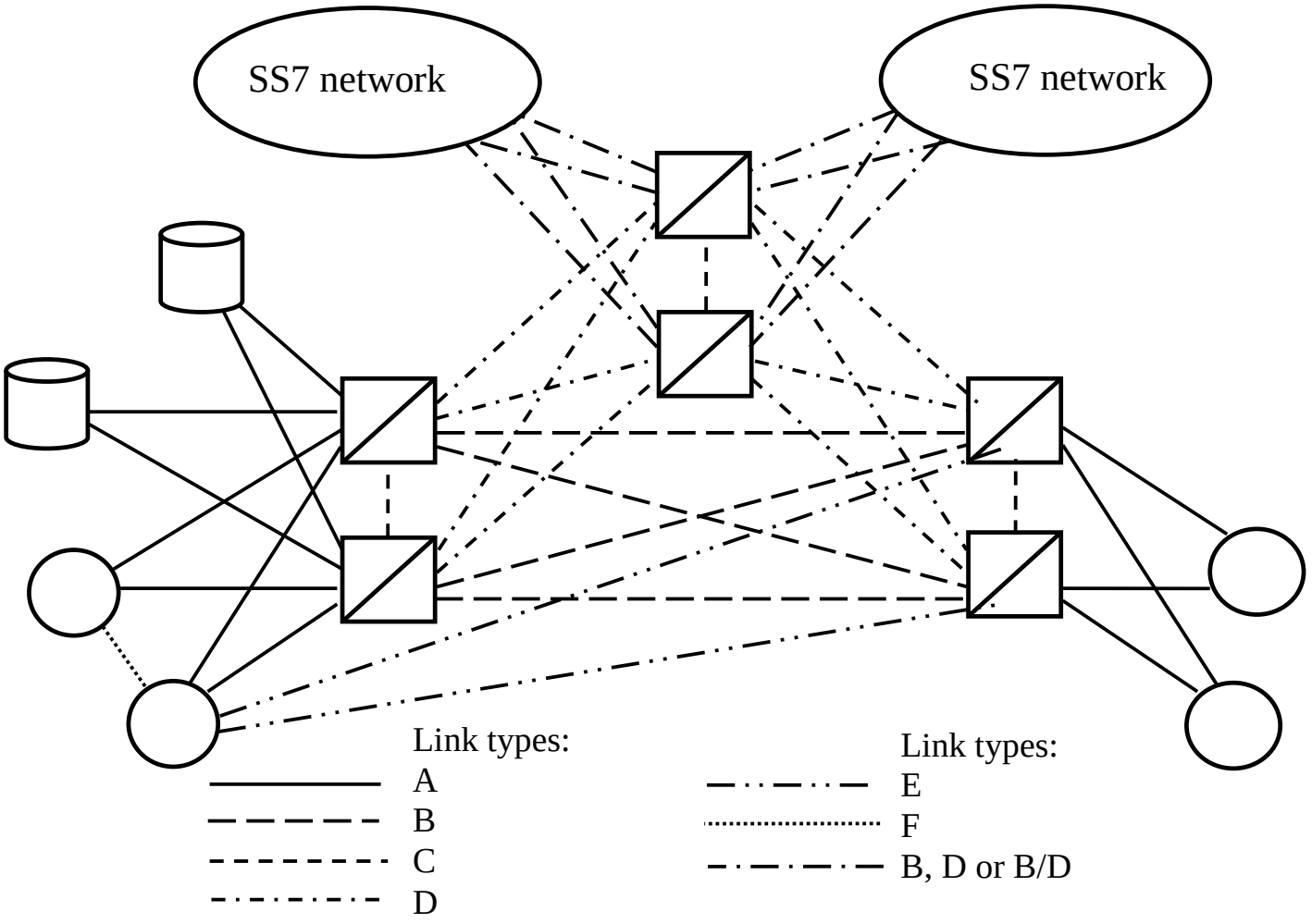
The SS7 architecture



- STPs are deployed in pairs performing identical functions;
  - they are redundant and together they are referred to as mated pairs of STPs;
  - the STPs of a mated pair are joined by a link (or set of links);
  - two mated pairs of STPs are interconnected by four links (or set of links);
    - these links are referred to as a quad.
- each SSP has two links (or set of links);
  - one link to each STP of a mated pair;
  - the messages sent over either link (to either STP) are treated equivalently.
- SCPs are usually (not always) deployed in redundant pairs;
  - they are not directly joined by links.
- the SS7 signaling architectures provide indirect signaling paths between the network elements;
  - it is a network offering quasi-associated signaling.

The SS7 architecture

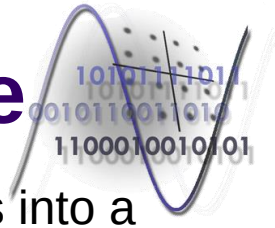
- SS7 signaling link types;



The SS7 architecture

- The SS7 architecture allows different types of SP connections;
  - the links are logically organized by types (A to F), according to their use in the network;
  - all links are identical (56 or 64 kbps bidirectional data links) and support the same lower layers of the protocols;
  - one time slot of the T1 or E1 frames can be used for transmission of the SS7 messages;
- SS7 signaling link types:
  - **A link** – access link – connects a signaling end point or source point (SSP or SCPs) to an STP;
    - only messages originating from or terminating in the signaling end points are transmitted on an A link.
  - **B link** – bridge link – connects STPs;
    - typically, quads of B links interconnect primary STPs of one network to the primary STPs of another network;
    - these links carry signaling messages beyond their initial point of entry in the signaling network toward their destination;
    - the interconnected pairs of STPs are on the same hierarchy level.

The SS7 architecture

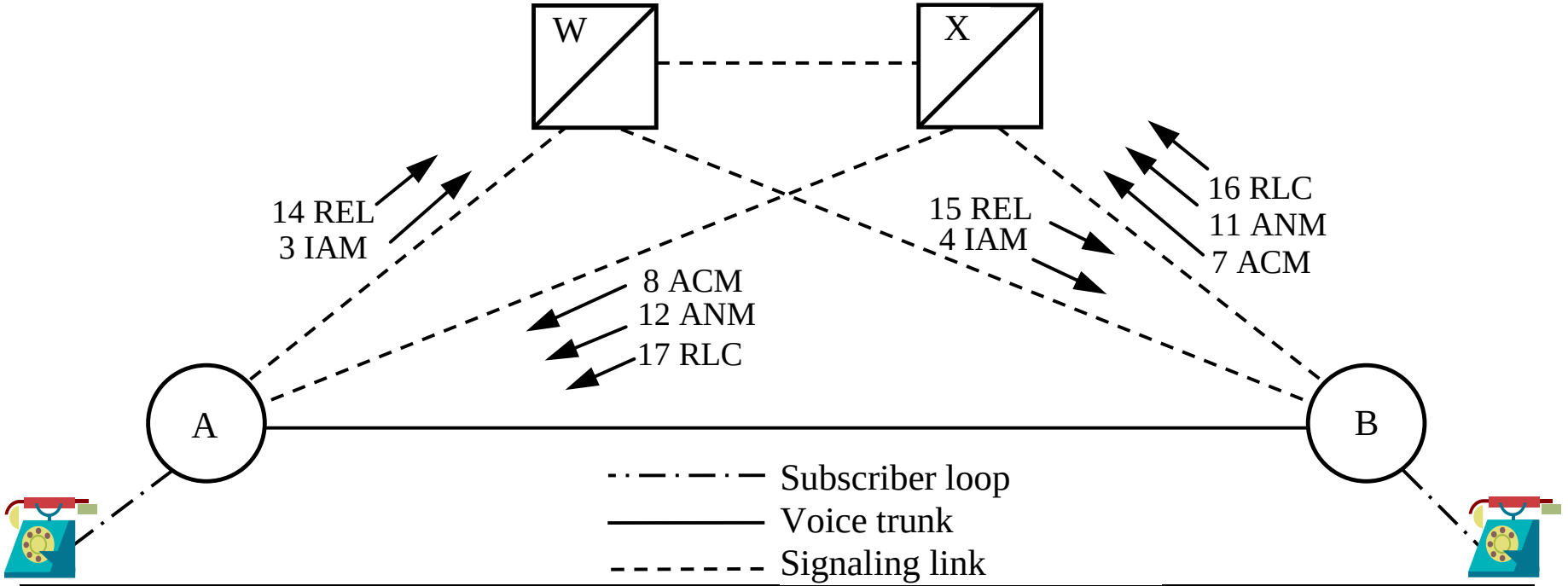


- **C link –** cross link – connects STPs performing identical functions into a mated pair;
  - these links are used to increase the reliability of the signaling network;
  - a C link is used only when an STP has no other route available to a destination signaling point due to link failures;
  - C links are not used between mated SCPs.
- **D link –** diagonal link – connects pairs of STPs at different hierarchical levels (secondary /local or regional STP pair to a primary/inter-network STP pair);
  - it is used a quad-link configuration;
  - there is no clear hierarchy associated with a connection between networks;
    - interconnecting links are referred to as either B, D or B/D links.
- **E link –** extended link – connects an SSP to an alternate STP to provide an alternate signaling path;
  - E links are not provisioned usually, unless the benefit of a higher degree of reliability justifies the additional expenses;
  - these links provide backup connectivity to the SS7 network in the event that the STPs cannot be reached via the A links;

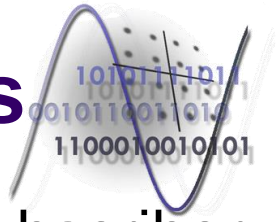
SS7 signaling operations

- **F link** – fully associated link – directly connects two signaling end points (SSPs or SCPs);
  - these links allows associated signaling only;
  - these links are not usually deployed in networks with STPs;
    - they bypass the security features provided by the STPs.

- Basic call setup based on SS7 signaling;

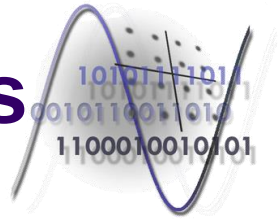


SS7 signaling operations



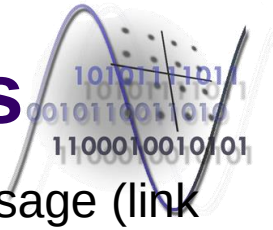
- Scenario: a subscriber of switch A places a call to a subscriber of switch B;
  - The steps of call establishment, maintenance and release are the following:
    1. switch A analyzes the dialed digits and finds out that the call is intended to switch B;
    2. switch A selects an idle trunk between switches A and B and generates an Initial Address Message (IAM) – the basic message necessary to initiate a call;
       - the IAM message is addressed to switch B;
    3. Switch A accesses one of its access links (for ex. A-W) and transmits the message over the link for routing to switch B;
    4. STP W receives the message, inspects its routing label, and determines that it is to be routed to switch B; it transmits the message on link B-W;
    5. Switch B receives the message, analyzes it and determines that it serves the called number and that this number is idle;

SS7 signaling operations



6. switch B generates an Address Complete Message (ACM);
   - this indicates that the IAM message has reached the proper destination;
   - the message identifies the recipient switch (A), the sending switch (B), and the selected trunk;
7. switch B accesses one of its A links (B-X) and transmits the ACM over the link for routing to switch A and at the same time, it completes the call path in the backward direction, sends the ring back signal over the seized trunk toward switch A and rings the line of the called subscriber;
8. STP X receives the message, inspects its routing label and determines that it has to be routed to switch A; it transmit the message on link A-X;
9. on reception of the ACM message, switch A connects the calling subscriber line to the selected trunk in the backward direction;
   - the caller can hear the ring back signal sent by switch B;
10. when the called subscriber picks up the phone, switch B generates an Answer Message (ANM);
    - the message identifies the intended recipient switch (A), the sending switch (B), and the selected trunk;

SS7 signaling operations

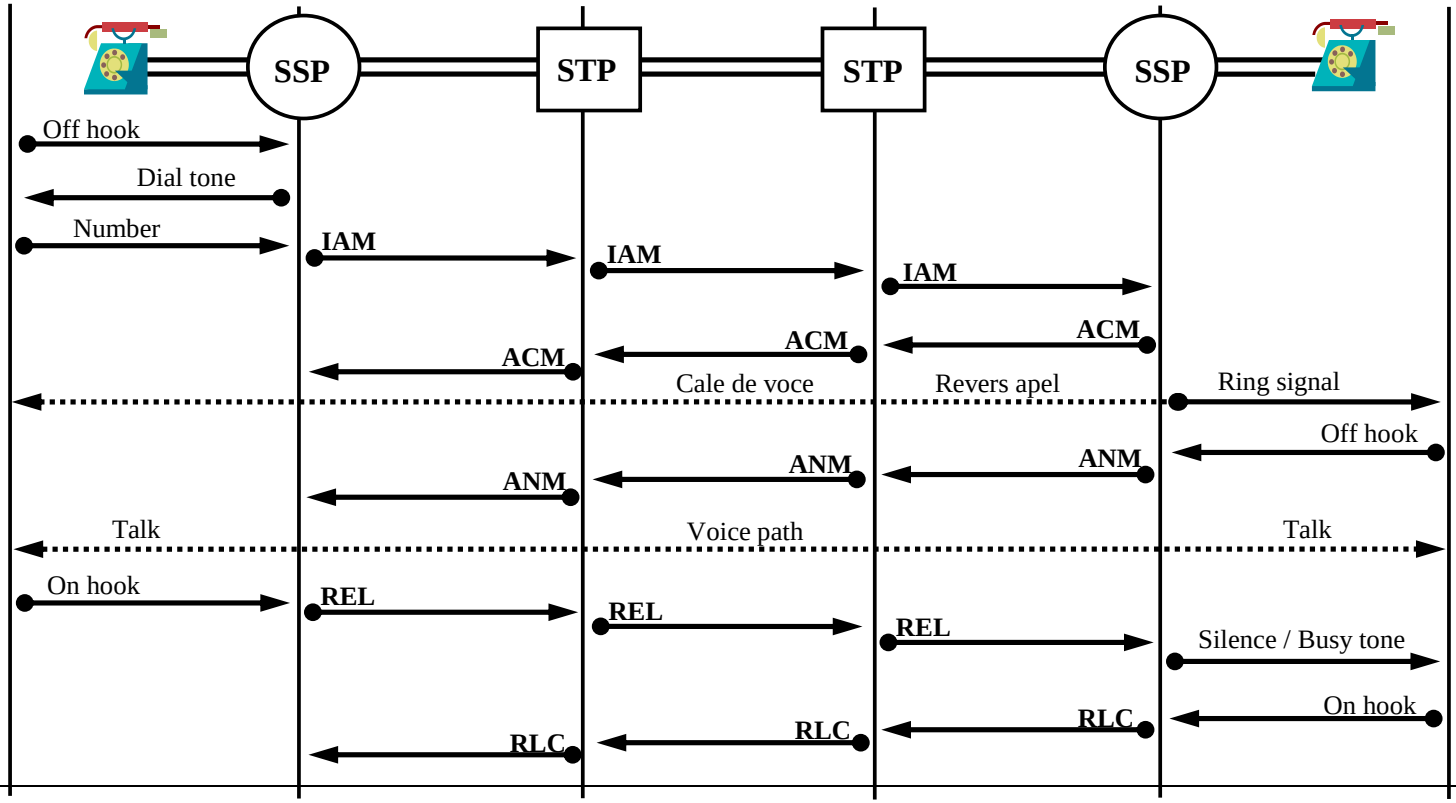


11. switch B selects the same A link it used to transmit the ACM message (link B-X) and sends the ANM message;
    - in this moment the trunk must be connected to the called line in both directions;
12. STP X understands that the ANM message is addressed to switch A and forwards it over link A-X;
13. switch A ensures that the calling subscriber is connected to the outgoing trunk (in both directions);
    - conversation can take place;
14. if the calling subscriber hangs up first (following the conversation), switch A will generate a Release message (REL) addressed to switch B;
    - the message identifies the trunk associated with the call;
15. STP W receives the REL message, determines that it is addressed to switch B, and forwards it using link W-B;
16. switch B receives the REL message, disconnects the trunk from the subscriber line, returns the trunk to idle state, generates a Release Complete message (RLC) addressed to switch A, and transmits it on link B-X;
    - the RLC identifies the trunk used to carry the call;

SS7 signaling operations

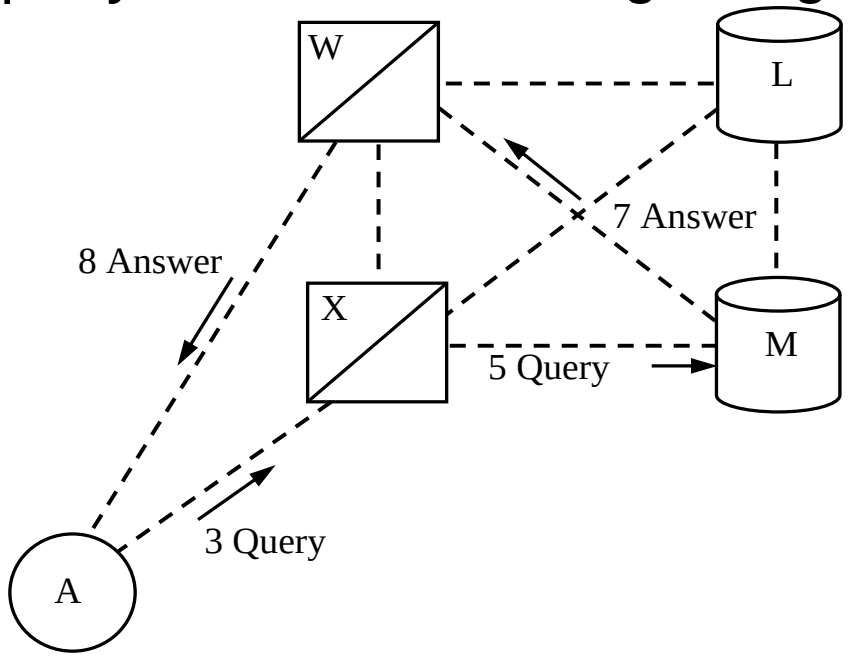
17. STP X receives the RLC message, determines that it is addressed to switch A, and forwards it over link A-X;
18. on reception of the RLC message, switch A places the identified trunk in idle state.

- Basic call setup based on SS7 signaling – alternative representation



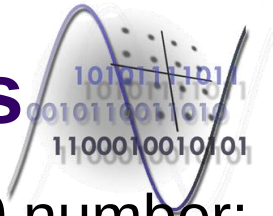
SS7 signaling operations

- Basic database query based on SS7 signaling;



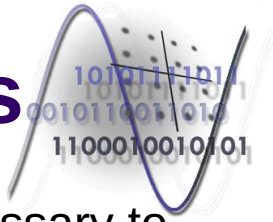
  - a possible example is related to calls addressed to toll-free 800 or 888 number;
    - these numbers are virtual telephone numbers, not assigned to a subscriber line;
  - when a subscriber dials an 800 number the switch must seek further instructions from a database;
    - the database provides either a real phone number to which the call should be directed, or it will identify another network to which the call should be routed.

SS7 signaling operations



- Scenario:a subscriber connected to switch A dials an 800 number;
  - The steps of call establishment, maintenance and release are the following:
    1. the subscriber dials an 800 number;
    2. when the subscriber has finished dialing, switch A finds out that this is an 800 call and that it requires assistance to handle it;
    3. switch A formulates an 800 query message;
       - the message includes the calling and called number;
       - the query is forwarded to one of STPs connected to the SSP (for example STP X) over its access link (for ex. link A-X);
    4. STP X determines that the received query is an 800 query and selects a database suitable handle the query (for ex. database or SCP M);
    5. STP X forwards the query to SCP M over the appropriate access link (M-X);
       - SCP M receives the query, extracts the information from the received data packets and based on its stored records selects either a real phone number or a network or both to which the call should be routed;

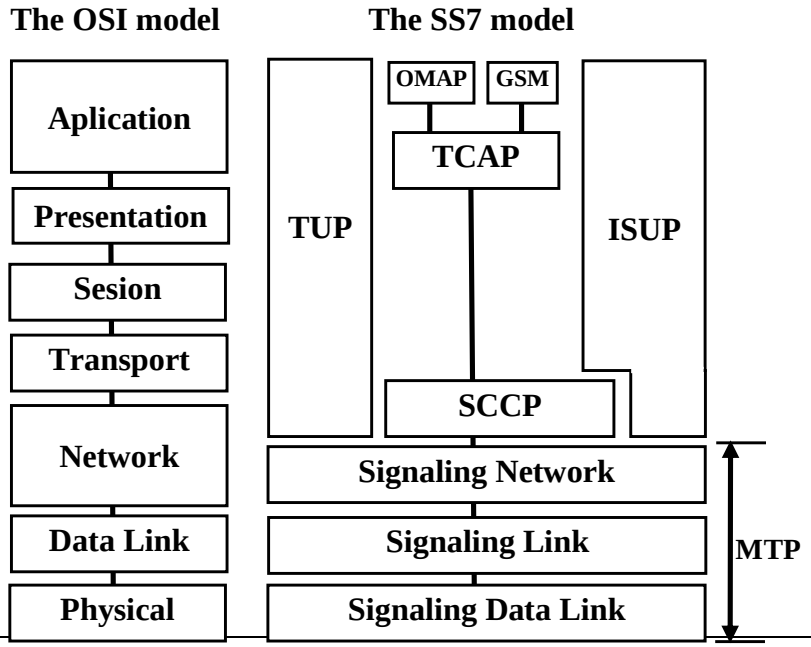
SS7 signaling operations



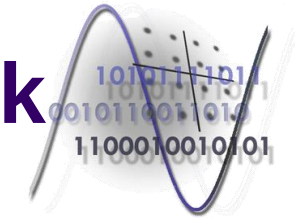
6. SCP M generates a response message with the information necessary to properly process the call;
   - it addresses the message to switch A, access an STP and an access link (for example M-W) and routes the response message;
7. STP W receives the response message, recognizes that it is addressed to switch A, and routes it to A over the A-W link;
8. switch A receives the response and uses the information to determine where the call should be routed;
   - it seizes a trunk to that destination;
   - generates an IAM message;
   - proceeds to set up the call – see the previous example.

The SS7 protocol stack

- The SS7 protocol is designed to facilitate the exchange of signaling messages and to ensure the network maintenance;
- The SS7 protocol is divided into several functional layers;
  - It was designed initially for circuit-related telephony;
  - It evolved as new requirements have emerged and now it allows also the transfer of non-circuit related information.

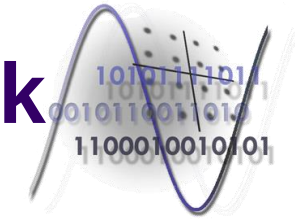


The SS7 protocol stack



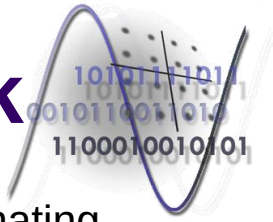
- Message Transfer Part – MTP:
  - Signaling Data Link:
    - defines the physical, electrical, and functional characteristics of the digital signaling link;
    - the defined physical interfaces include:
      - DS1 (one slot of the T1 frame having a bit rate of 1.544Mbps);
      - E1 (one time slot of the E1 frame having a bit rate of 2.048Mbps, usually time slot 16);
      - V.35 (synchronous serial interface at 64kbps or 56kbps);
      - DS0 (64kbps), DS0A (56kbps) – these are the more common implementation.
  - Signaling Link:
    - defines the functions and procedures necessary to ensure that messages are reliably transmitted across a signaling link;
    - the mentioned functions implement flow control, message sequence validation, and error checking;
      - when an error occurs on a signaling link, the messages are retransmitted.

The SS7 protocol stack



- Signaling Network:
  - defines those transport functions and procedures that are common to and independent of individual signaling links;
  - provides node addressing and message routing between signaling points in the SS7 network;
  - re-routes traffic away from failed links and signaling points, and controls the traffic when congestion occurs;
  - ensures that the messages can be delivered between signaling points across the SS7 network regardless of whether they are or are not connected directly.
- Signaling Connection Control Part – SCCP:
  - provides additional functions to the MTP, to support connectionless and connection-oriented network services and Global Title Translation (GTT);
    - it is used as an end to end transport layer;
    - SCCP provides subsystem numbers;
      - it allows messages to be addressed to specific applications or subsystems at specified signaling points;

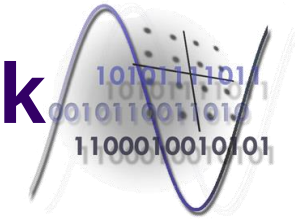
The SS7 protocol stack



- GTT adds the ability to perform incremental routing and frees the originating signaling point of having to know every possible destination address;
  - a global title is an address (an 800 number, calling card number, or mobile subscriber identification number) which is translated by the SCCP into a destination point code and subsystem number;
  - a subsystem number uniquely identifies an application at the destination signaling point.
- SCCP is used as transport layer for TCAP based services.

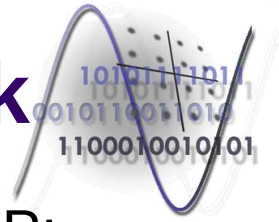
- Telephone User Part – TUP:
  - defines the international call control functions for basic call setup and release;
    - represents an earlier implementation of SS7 and does not allow data applications.
- ISDN User Part – ISUP:
  - defines the protocols used to setup, manage, and release trunk circuits that carry voice and data between SSPs;
  - is used both for ISDN and non-ISDN calls;
    - calls that originate and terminate at the same switch do not use ISUP signaling.

The SS7 protocol stack



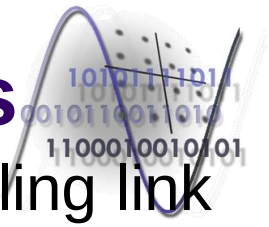
- Transaction Capabilities – TC:
  - provides the means to establish non-circuit related transmissions between two signaling points (SPs);
- Transaction Capabilities Application Part – TCAP:
  - supports the exchange of non-circuit related data between applications across the SS7 network;
  - it uses the SCCP connectionless service as a transport layer;
  - it defines the messages and protocols used to communicate between applications running on SS7 network nodes;
  - queries and responses sent between SSPs and SCPs are carried in TCAP messages;
  - in mobile networks TCAP carries the Mobile Application Part (MAP);
    - messages are sent between mobile switches and databases to support user authentication, equipment identification and roaming;

The SS7 protocol stack



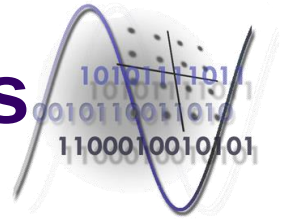
- Operation, Maintenance and Administration Part – OMAP;
  - defines the messages and protocols used in the administration of the SS7 networks ;
  - the services provided by OMAP are used to verify network routing databases and diagnose link problems;
  - OMAP includes messages that use both MTP and SCCP for routing.

Transmission of signaling packets



- The signaling information is transmitted over the signaling link in messages, which are called signal units (SUs);
  - There are three types of signal units defined in the SS7 protocol:
    - Fill-In Signal Units – FISUs;
    - Link Status Signal Units – LSSUs;
    - Message Signal Units – MSUs.
  - The SUs are transmitted continuously in both directions on any link that is in service;
    - a signaling point that does not have messages or status signals to transmit will send FISUs over the link;
      - the FISUs facilitate link transmission monitoring and acknowledgement of other SUs;
      - the FISUs are transmitted continuously on a signaling link in both directions to keep the link alive and aligned;
      - these units carry CRC and in this way the link quality is continuously checked by the SPs at each end of the link.

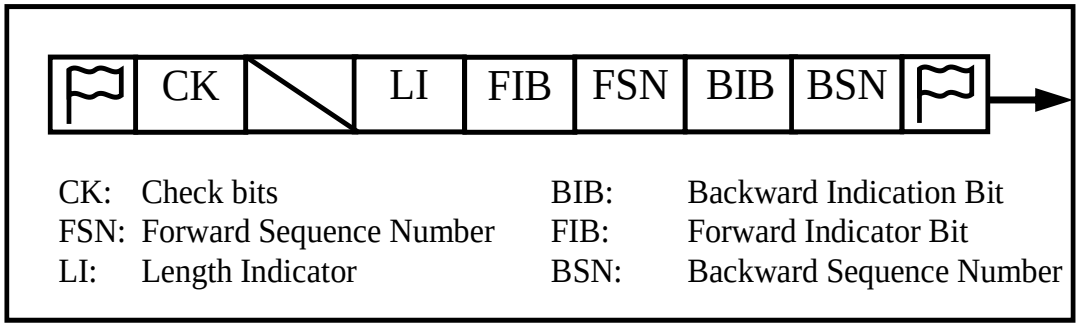
Transmission of signaling packets



- Link Status Signal Units (LSSU) are used to exchange link status information between the SPs at each end of the link;
  - LSSUs are used also to control link alignment;
  - before an SS7 link is able to convey information from the higher layers, the layer 2 entities at each end of the link follow a handshaking procedure known as the proving period, lasting for 0.5 to 8.2 seconds (depending on the availability of routes served by the link in question);
    - during this time LSSUs are exchanged between the layer 2 entities of the protocol, the number of the errors received during this time being monitored;
      - if the detected number of errors is less than a threshold, the link enters the in service state, and may carry MSU packets containing information from the upper layers;
  - the layer 2 entities also monitor the state of the link and communicate this link state information to their peers in LSSU messages;
    - these messages are transmitted, for example, when links become congested or are placed out of service.

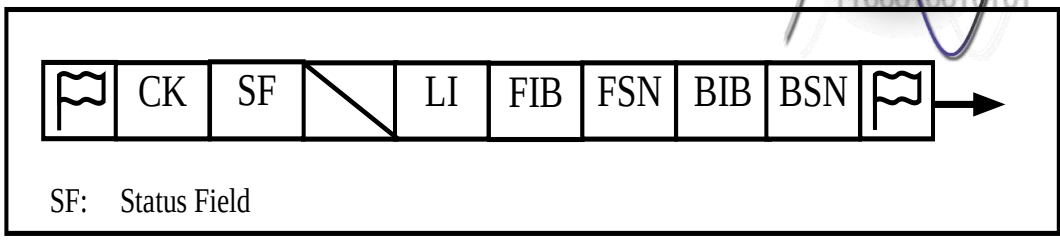
Transmission of signaling packets

- The Message Signal Units are the containers that carry TUP, ISUP, and SCCP protocol messages within the information field;
  - the MSU packets carry:
    - all call control signals;
    - database queries and responses;
    - network management and network maintenance data;
    - additional specialized functions for mobile cellular applications.
  - these units have a routing label;
    - that allows an originating signaling point to send information to a destination signaling point across the SS7 network.
- The structure of the FISU messages:

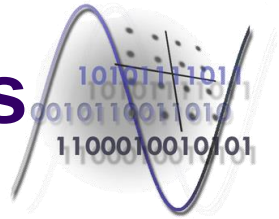


Transmission of signaling packets

- The structure of the LSSU messages;
  - Flag: 0 1 1 1 1 1 1 0;
    - indicates the beginning of a new signal unit and the end of the previous unit;
      - two flags could be placed between SUs, one to mark the end of the current message and one to mark the start of the next message;
        - in practice just one flag is used;
      - bit manipulation techniques are used to ensure that this pattern does not occur within the message transmitted on the link;
        - the SU is reconstructed once it has been taken off the link and any bit manipulation is reversed;
        - a possible bit manipulation consists in insertion of a zero after any sequence of five ones;
  - Backward Sequence Number – BSN;
    - acknowledges the receipt of signal units by the remote signaling point;
    - contains the sequence number of the signal unit being acknowledged;
    - every single message needs to be acknowledged by means of BSN.

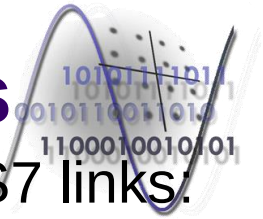


Transmission of signaling packets



- Backward Indicator Bit – BIB;
  - is used for error recovery and indicates a negative acknowledgement by the remote signaling point when inverted.
- Forward Sequence Number – FSN;
  - contains the sequence number of the signal unit.
- Forward Indicator Bit – FIB;
  - is used in error recovery;
  - when a negative acknowledgement is received all previous forward messages are retransmitted beginning with the corrupted one - in these messages FIB is inverted;
- BSN+BIB and FSN+FIB are used to confirm the receipt of SUs and to ensure that they are received in the correct order;
  - these fields are used also to provide flow control;
  - the sequence numbers of the transmitted messages are stored until these messages are acknowledged by the receiving signaling point;
    - seven bits are allocated to the forward sequence number and in this way is possible to store 128 separate values
    - a signaling point is restricted to sending 128 unacknowledged SUs before it must await for an acknowledged SU which frees the SUs sequence numbers at the transmitting point.

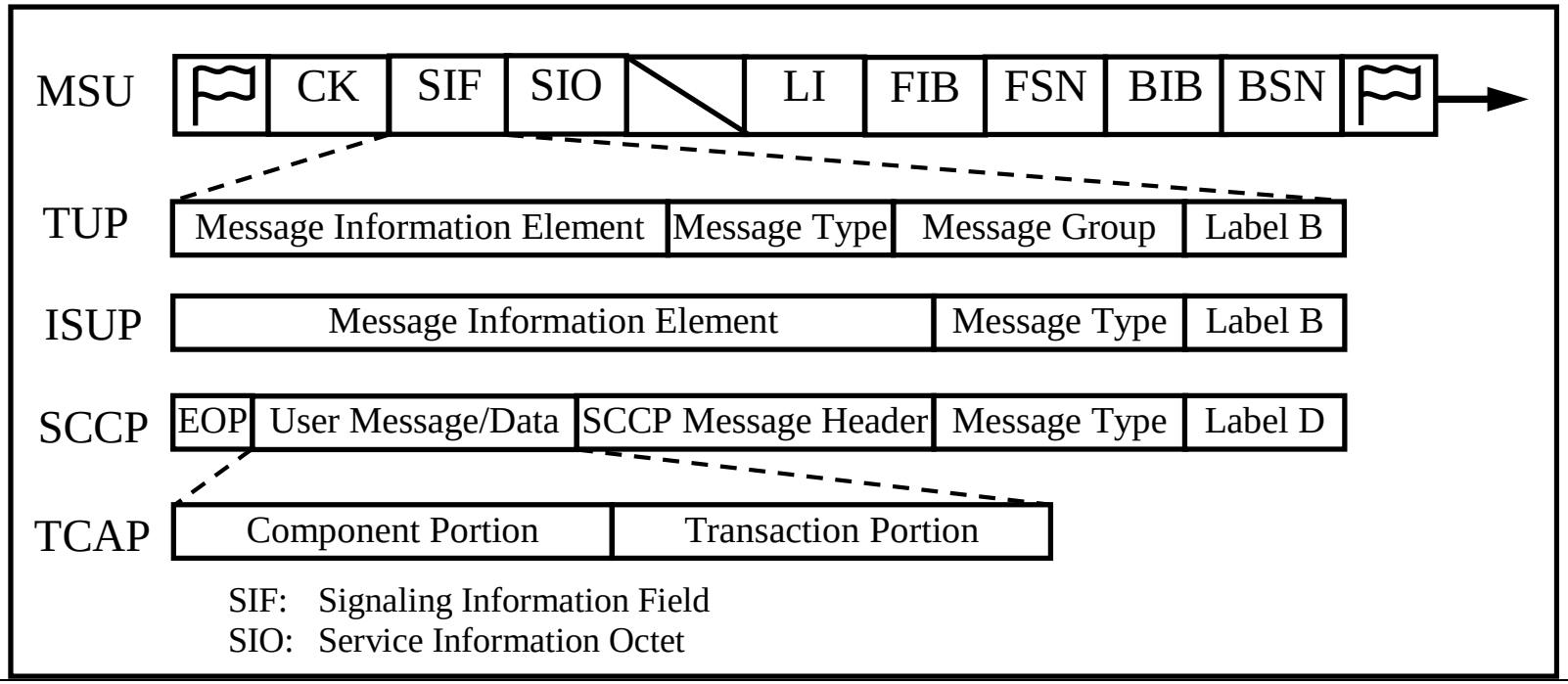
Transmission of signaling packets



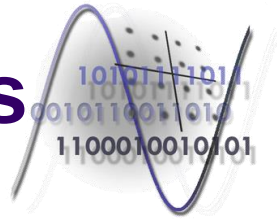
- Remark: There are two error control methods used on SS7 links:
  - the basic method:
    - a message is retransmitted on the receipt of a negative acknowledgement;
    - the method uses the BSN+BIB, FSN+FIB and CK fields;
  - the Preventative Cyclic Retransmission (PCR):
    - a message is repeatedly sent when the upper layers have no information to be sent in the network;
    - the PCR method is used only over transmission paths where the transmission delay is large, such as satellite links.
- Length Indicator – LI;
  - indicates the number of octets between itself and the checksum (CRC);
  - it serves both as a check on the integrity of the SU and as a mean of discriminating between different types of SUs;
    - FISUs have a length indicator of 0;
    - LSSUs have a length indicator of 1 or 2 (in general LSSUs have a LI=1);
    - MSUs have a length indicator greater than 2;
    - only 6 of the 8 bits of the LI field are used to store the mentioned length: max. LI=63;
    - MSUs with more than 63 octets after the LI field use a value of 63.

Transmission of signaling packets

- Check bits – CK;
  - is a CRC value used to detect transmission errors.
- Status Field – SF;
  - link status indicator; indicates the number of the detected CRC errors.
- The structure of the MSU messages;

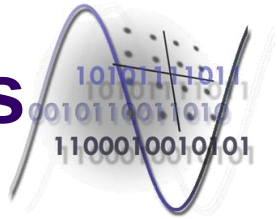


Transmission of signaling packets



- Service Information Octet – SIO;
  - contains the subservice field and service indicator – see the presentation of the MTP3 level (layer).
- Signaling Information Field – SIF;
  - contains the routing label and signaling information, i.e. SCCP, TCAP and ISUP message data – see the presentation of level 4;
  - LSSUs and FISUs have no routing label and SIO;
    - they are sent between two directly connected signaling points;

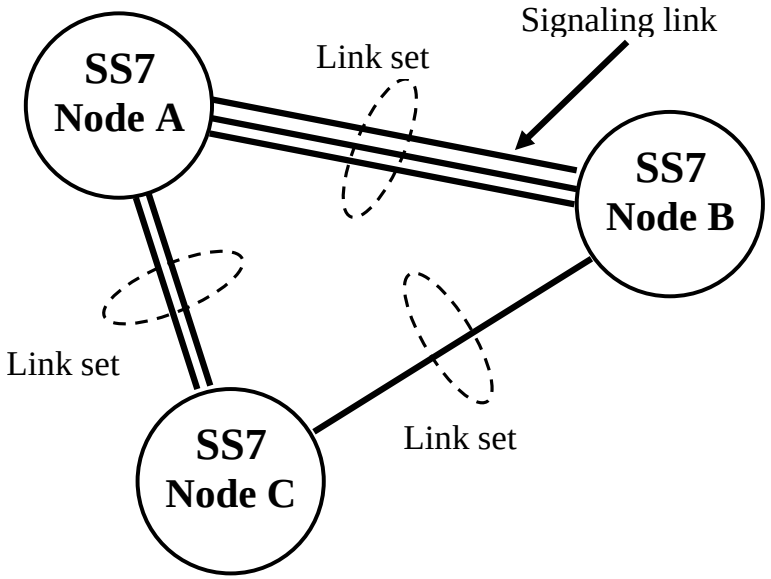
MTP3 operations



- Layer 3 provides message routing and failure handling capabilities for the message transport.
  - Each SS7 node, which could be a classic switch or a node containing 800 number translation records, is uniquely identified within a network using an SS7 address called a *Point Code*;
    - the European networks use 14 bit point codes and the North American networks use 24 bit point codes.
      - individual signaling points belongs to a cluster of signaling points and within that cluster, each signaling point has a member number; similarly, a cluster is part of a network
      - the routing addresses have three levels defined by the network, cluster and member number;
      - each of these numbers is an 8 bit number (the American system);
      - the whole address number is known as the point code of the signaling point, code which uniquely identifies a signaling point.

MTP3 operations

- Example of SS7 network and signaling link sets;



- A single SS7 link is able to carry traffic for thousands of circuits;
  - depending on traffic a single SS7 link is normally engineered to control 1000 to 2000 circuits;
  - failure of this single link would disable all the circuits that are controlled by that link;
  - for resilience and also to increase traffic capacity, more than one signaling link is provisioned usually between any two SS7 nodes;
    - the collection of *signaling links* between two adjacent nodes is known as a *link set*, each link set can include up to 16 signaling links;

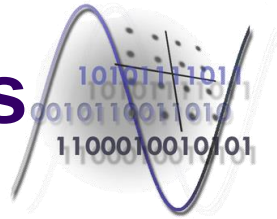
MTP3 operations

- MTP3 adds information into the Signaling Information Field (SIF) of the MSU packets.
  - This information includes:
    - the Destination Point Code (DPC) identifying the destination of a message;
    - the Originating Point Code (OPC) identifying the originator of a message;
    - a Signaling Link Selection (SLS) code;
      - ensures the load sharing between links in a link set.
- Structure of the MTP3 header;

Layer 4	SLS	OPC	DPC

  - The MTP3 protocols automatically shares the traffic between the links within a link set and re-routes traffic from failed links to a working link within the same link set on detection of failure.
    - MTP3 layer also attempts to automatically restore failed links and return traffic to a recovered link;
      - these two procedures are called as *Changeover* and *Changeback*.

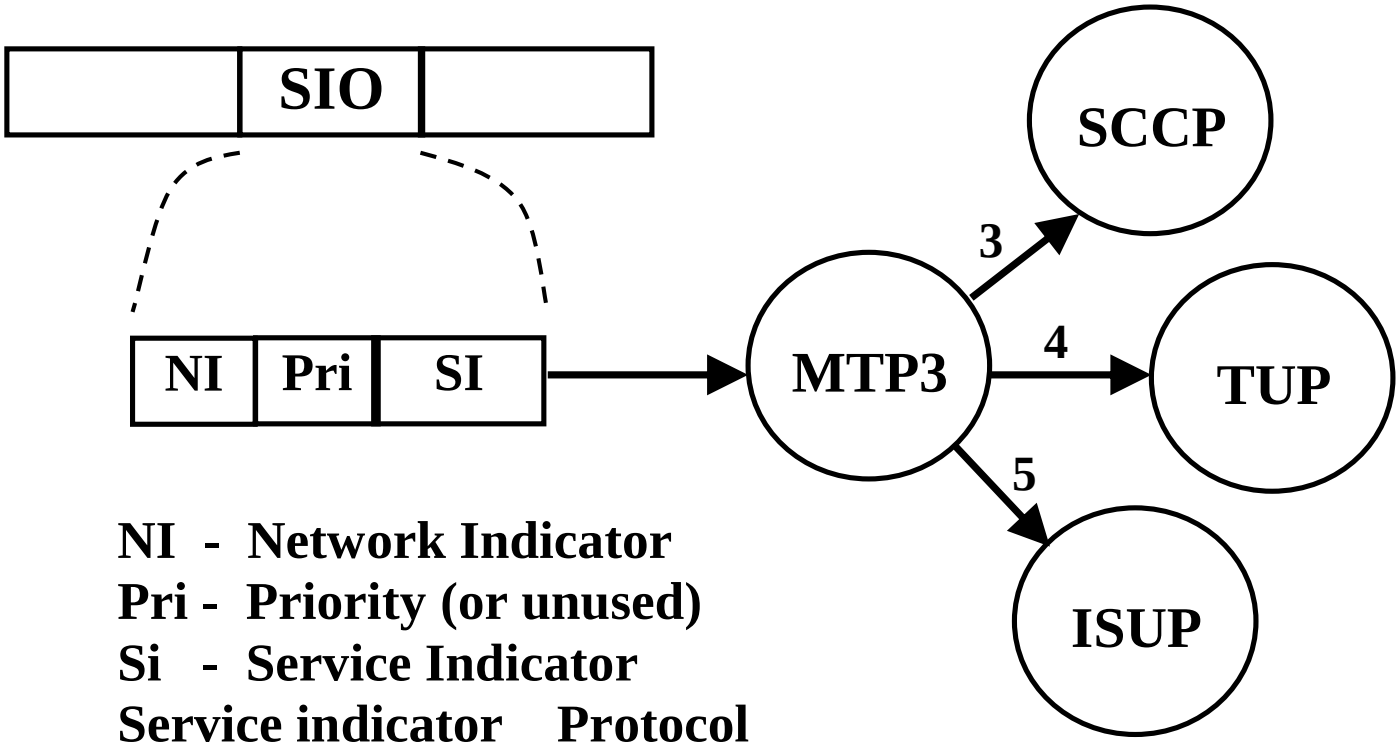
MTP3 operations



- MTP3 is also able to share traffic between two link sets that serve the same destination, by the use of intermediate nodes;
  - the link sets in discussion are contained by a *route set*.
- The routing of messages to a destination by MTP3 could be:
  - quasi-associated:
    - the message passes through an intermediary node before reaching the destination;
  - completely associated:
    - it exists a direct signaling link between the source and the destination.
- MTP3 provides a reliable message transport service to the higher layer protocols, which use MTP as a message transport service;
  - the protocols located at higher layer are generically called *User Parts;*
  - in order to deliver a received message to the correct user part, MTP3 examines the *Service Indicator* (SI) which is a part of the *Service Information Octet* (SIO);

MTP3 operations

- The structure of the SIO octet and classification of MTP3 messages:

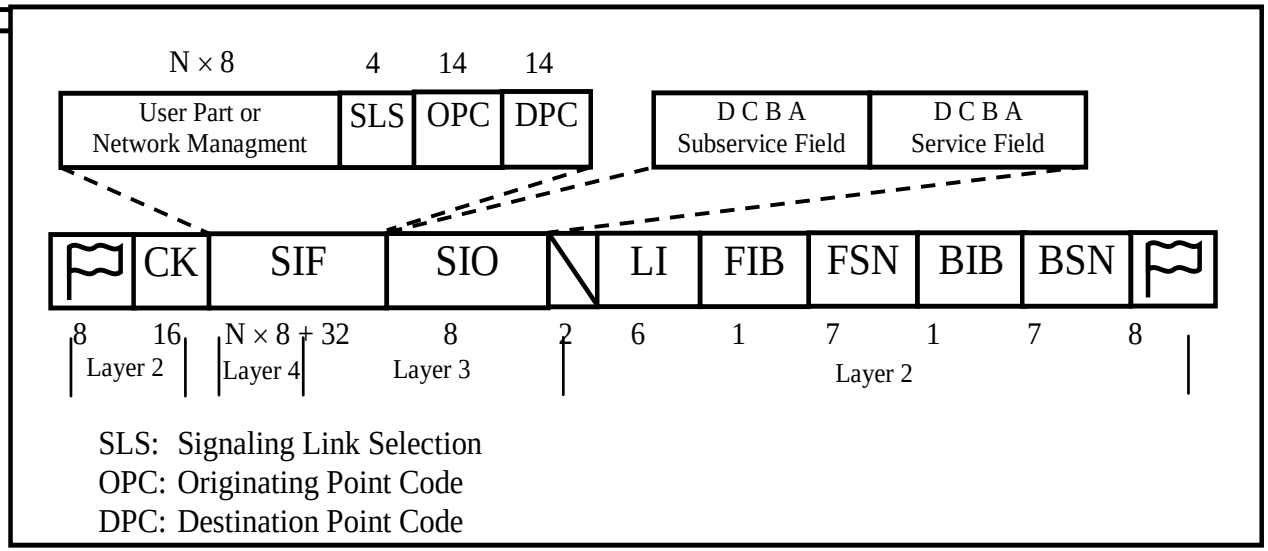


NI - Network Indicator
Pri - Priority (or unused)
Si - Service Indicator

Service indicator	Protocol
0	MTP3
1	MTP3
3	SCCP
4	TUP
5	ISUP

MTP3 operations

- SIO – Service Information Octet;
  - includes the Subservice Field and the Service Indicator;
  - the Subservice Field contains the network indicator (national or international) and the message priority;
    - low priority messages may be discarded during periods of congestion;
    - signaling link test messages have a higher priority than call setup messages;
  - the Service Indicator;
    - specifies the MTP user, which could be TUP, ISUP, SCCP or other;
- Structure of the SIF and SIO fields;



Layer 4 protocols

- The layer 4 protocols define the contents of the messages and sequences of messages sent to MTP3 in order to control network resources, such as circuits and databases;
- Telephony User Part – TUP;
  - It is a layer 4 protocol which provides conventional PSTN telephony services through the SS7 network;
    - TUP was the first of the standardized layer 4 protocol;
    - it does not provide ISDN services;
  - The message (signal) sequence used for set up – control – release of a normal telephone call is similar with the message sequence characteristic to the ISUP protocol.
    - see slides 16 – 20, presenting the message sequence controlling the set up of a classical telephone connection.
- ISDN User Part – ISUP;
  - It is a layer 4 protocol;

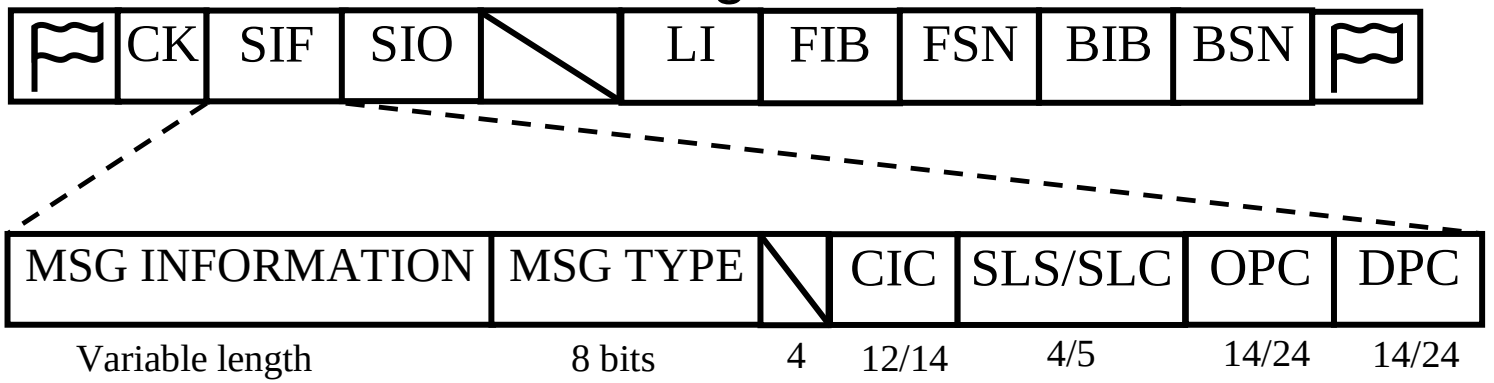
Layer 4 protocols

- Defines the procedures used to set up, manage, and release trunk circuits that carry voice and data calls over the public switched telephone network;
- It is used for both ISDN and non-ISDN calls;
  - the calls that originate and terminate at the same switch do not use ISUP signaling.
  - ISUP offers a greater variety of messages and parameters in order to implement ISDN type services within the network;
- Both ISUP and TUP provide additional messaging and management for circuit state control;
  - It is possible to reset a circuit or a group of circuits;
    - Circuits are normally reset on system initialization or after a failure;
    - Similar procedures exist for blocking circuits, making a circuit temporarily unavailable for calls.
      - any call received for a blocked circuit is automatically rejected.

Layer 4 protocols

- blocking may wait for any active calls to terminate before taking effect;
  - this is know as either maintenance blocking or blocking without release and is used prior to maintenance action.
- hardware blocking or blocking with release is used on detection of failure of physical equipment or trunks that disrupt a voice circuit, and cause instant release of associated circuits and calls.

- Structure of the ISUP messages:



CIC: Circuit Identification Code SLS: Signaling Link Selection SLC: Signaling Link Code

- The SIF field contains the routing labels: DPC and OPC;
- The CIC code identifies the trunk circuit reserved by the originating switch to carry the call;

Layer 4 protocols

- A trunk is uniquely identified by the CIC code and point codes of the interconnected SSPs.
- The MSGTYPE field specifies the type of the message, that are:
  - IAM, ACM, ANM, REL and RLC;
    - see slide 16 – 20;
  - this field defines the content of the message field – MSG INFORMATION.

- Signalling Connection Control Part – SCCP;
  - SCCP enhances the routing and addressing capabilities of MTP3;
    - it enables the addressing of individual processing components or *sub-systems* at each signaling point;
  - SCCP routes the messages through the network using a sub-system number and point code to identify a destination;
    - each sub-system could be a phone number translation database;
    - an SS7 point code can potentially have many sub-systems attached.

Layer 4 protocols

- SCCP offers four classes of services, numbered 0 to 3:

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

- The most commonly used classes of SCCP are 0 and 1;
  - are used by TCAP and higher layers in the control of mobile/wireless and intelligent networks;
  - classes 2 and 3 can be used by mobile networks in the communication between radio base-stations and the base-station controllers.

Layer 4 protocols

- SCCP maintains a state of every sub-system that it is aware of;
  - Sub-systems may be:
    - on-line (*Allowed*) – can be accessed;
    - off-line (*Prohibited*) – can not be accessed;
      - a message can be delivered only to an allowed destination subsystem;
      - a communication session can be opened only to an allowed subsystem.
- The basic message of connectionless SCCP is the SCCP UNITDATA (also called UDT);
  - The UDT messages intended to prohibited sub-systems can be either discarded or returned to the originator as a UNITDATA SERVICE message (UDTS);
    - a return option parameter has to be set in the quality of service field of the message
  - In order to track and report the status of sub-systems, SCCP transmits management messages, encapsulated in UDT messages;
    - sent between the entities of each SCCP.

Layer 4 protocols

- Sub-system state verification messages are generated and sent periodically (approximately every 30 seconds) to all prohibited sub-systems in order to find out when routing to those destinations becomes available;
  - SCCP also provides an option to make subsystems *concerned* about the state of other subsystems;
    - any changes in the routing process are reported immediately.
- SCCP also provides an advanced addressing capability;
  - A sub-system is represented as a sequence of digits known as a *Global Title*;
  - A Global Title is a method of hiding the SS7 point code and sub-system number from the originator of a message;
    - for example inter-working between different networks where no common allocations of SS7 point codes are provided;
    - such a method is used in GSM mobile roaming between countries.

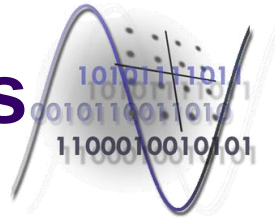
Layer 4 protocols

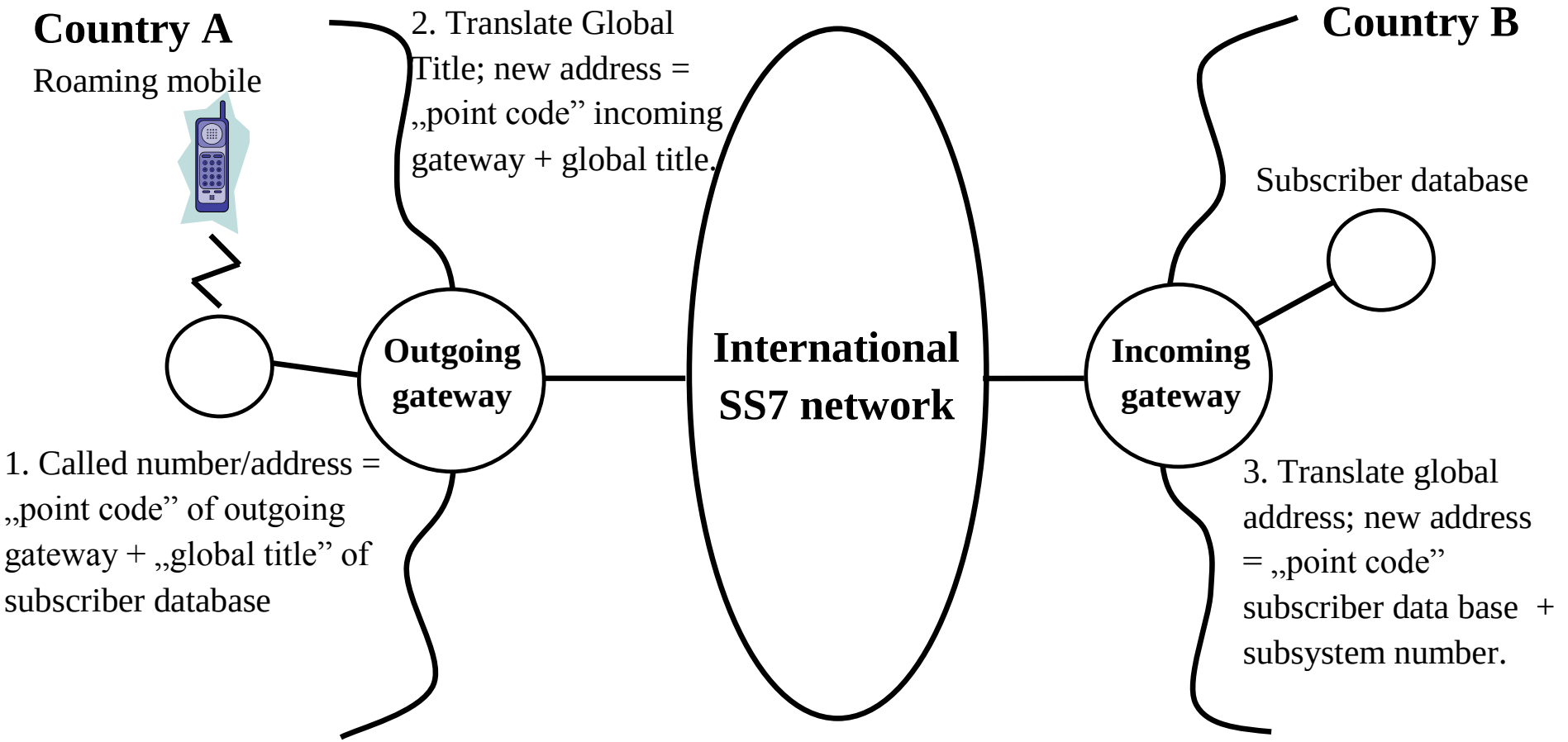
- Depending on network topology, Global Titles are translated either at a STP or at a gateway exchange;
  - the gateway is a network node having interworking functions with an adjacent network;
- The address information delivered to SCCP for message routing may contain a destination point code, a sub-system number and optionally a global title;
  - for successful transmission of the message, the minimum requirement is for a destination point code in order for the message to leave the SCCP node;
  - if no point code can be identified, the called address information is submitted for Global Title Translation.
    - the operation produces a destination point code and optionally a sub-system number or new global title;
    - the address information in a received message contains a routing indicator to instruct SCCP to route on either point code and sub-system number or Global Title;
    - if the routing is based on Global Title, the destination address is submitted to translation in order to produce a new destination address;
      - this may be an information processing node or a different SCCP node in the network.

Layer 4 protocols

- Use of global title translation (GTT) in mobile roaming;
  - Global Titles are used in GSM mobile operations to locate subscriber account information;
  - The subscribers account information is held in a database in the home network;
    - the *Home Location Register* subsystem (HLR);
    - HLR has to be interrogated in order that the subscriber to obtain service from the visited network;
    - the database query is sent through SCCP, with Global Title address constructed from information within the subscriber's handset;
      - either the Equipment Identity or Mobile Subscriber Number;
      - these codes are giving sufficient information to route the message to the correct outgoing gateway using Global Title translation.
      - subsequent translation within the home network routes the query to the correct database.

Layer 4 protocols





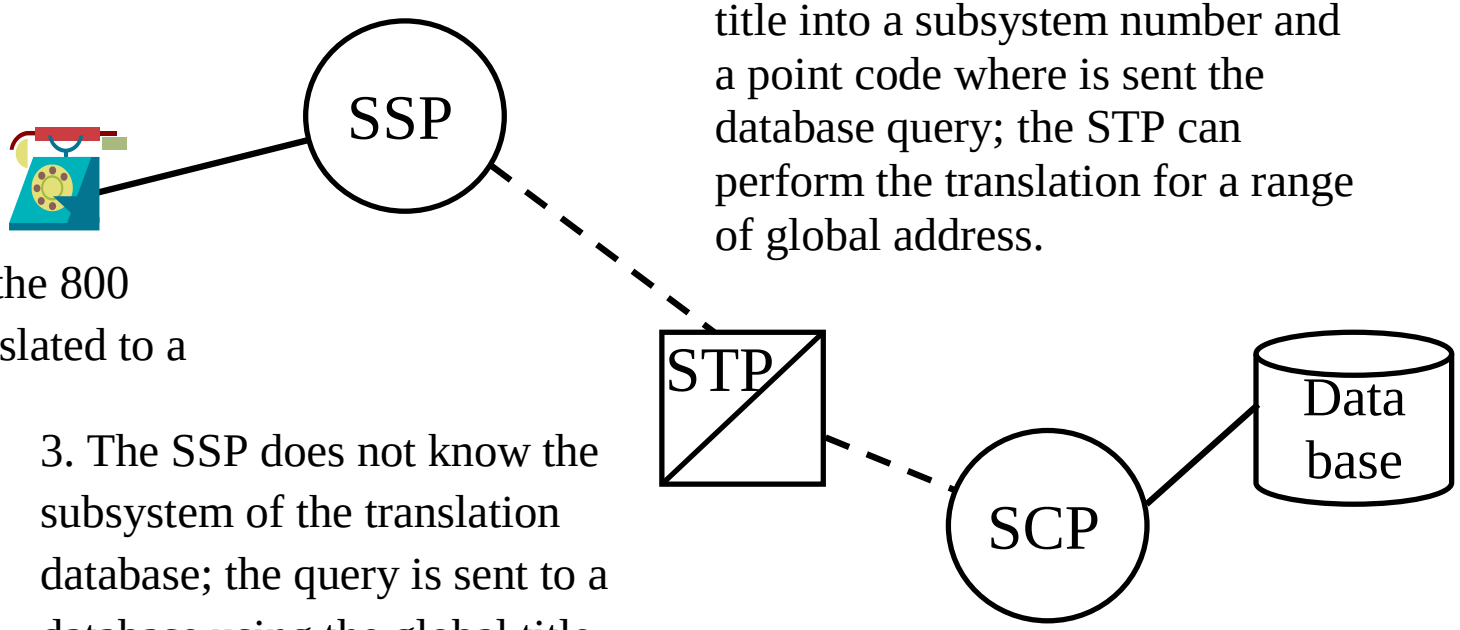
Layer 4 protocols

- Global title translation can be used also to find out the location of a toll free-phone number translation database;
  - It is located in a SCP;
  - The data base is accessed by using an 800 number as a Global Title;
    - the translation takes place at an STP;
      - it gives the database containing the entries for a range of 800 numbers;
      - for example, 800-1xxxxx could match to database A and 800-2xxxxx could match to database B;

Layer 4 protocols

- Use of global title translation (GTT) to locate an 800 number translation data base;

1. The subscriber dials 800-xxxxxxx



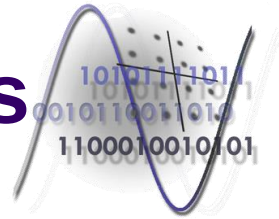
2. To route the call, the 800 number must be translated to a real number.

3. The SSP does not know the subsystem of the translation database; the query is sent to a database using the global title set to the dialed 800 number.

4. The STP translates the global title into a subsystem number and a point code where is sent the database query; the STP can perform the translation for a range of global address.

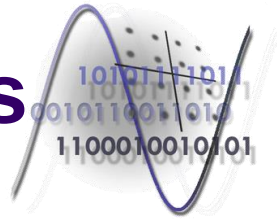
5. The query reaches the database and it is returned a real number/address.

Higher layer protocols



- Transaction Capabilities – TCAP;
  - The Transaction Capabilities Application Part provides a structured method to request an operation at a remote node, defining the information flow necessary to control the operation and the reporting of its result;
  - Operations and their results are carried out within a session:
- TCAP typical applications:
  - Mobile services:
    - ex. registration of roamers;
  - Intelligent Network services:
    - ex. free-phone and calling card services;

Higher layer protocols

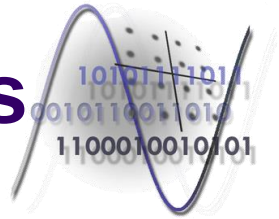


- Mobile Application Part – MAP;
  - Is used within mobile/wireless networks:
    - to access roaming information;
    - to control terminal handover
    - to provide short message services (SMS);
    - it uses typically TCAP over SCCP and MTP as transport mechanism.
- Mobile networks are database intensive:
  - The point of subscription of a subscriber is a database known as a *Home Location Register* (HLR);
  - When a subscriber roams to a cell and registers within the network, information regarding the subscriber is temporarily stored at the visited equipment in a second database, known as Visitor Location Register (VLR);

Higher layer protocols

- MAP specifies a set of services and the information flows that enable information transfer between databases, in order to:
  - register and locate subscribers;
  - deliver calls to a roaming subscriber;
    - the roaming term refers also to the change of the MSC (Mobile Switching Center) and not only to international calls.

Higher layer protocols



- A mobile terminal call initiated by a fixed terminal;
  - Call routing between the fixed and the mobile network;
    - step 1: The calling subscriber dials the mobile subscriber number;
    - step 2: The mobile network area code cause the call to be routed to the mobile network gateway MSC – GMSC;
    - step 3: The gateway MSC uses information in the called address to locate the mobile subscriber's HLR;
    - step 4: The HLR has already been informed of the location (VLR address) for the mobile subscriber and requests a temporary routing number to allow the call to be routed to the correct MSC;
    - step 5: The MSC/VLR responds with a temporary routing number that will be valid only for the duration of this call;
    - step 6: The routing number is returned to the GMSC;
    - step 7: The call is performed using standard ISUP (or similar) signaling between the GMSC and the visited MSC;

Higher layer protocols

- Steps of a mobile terminated call;