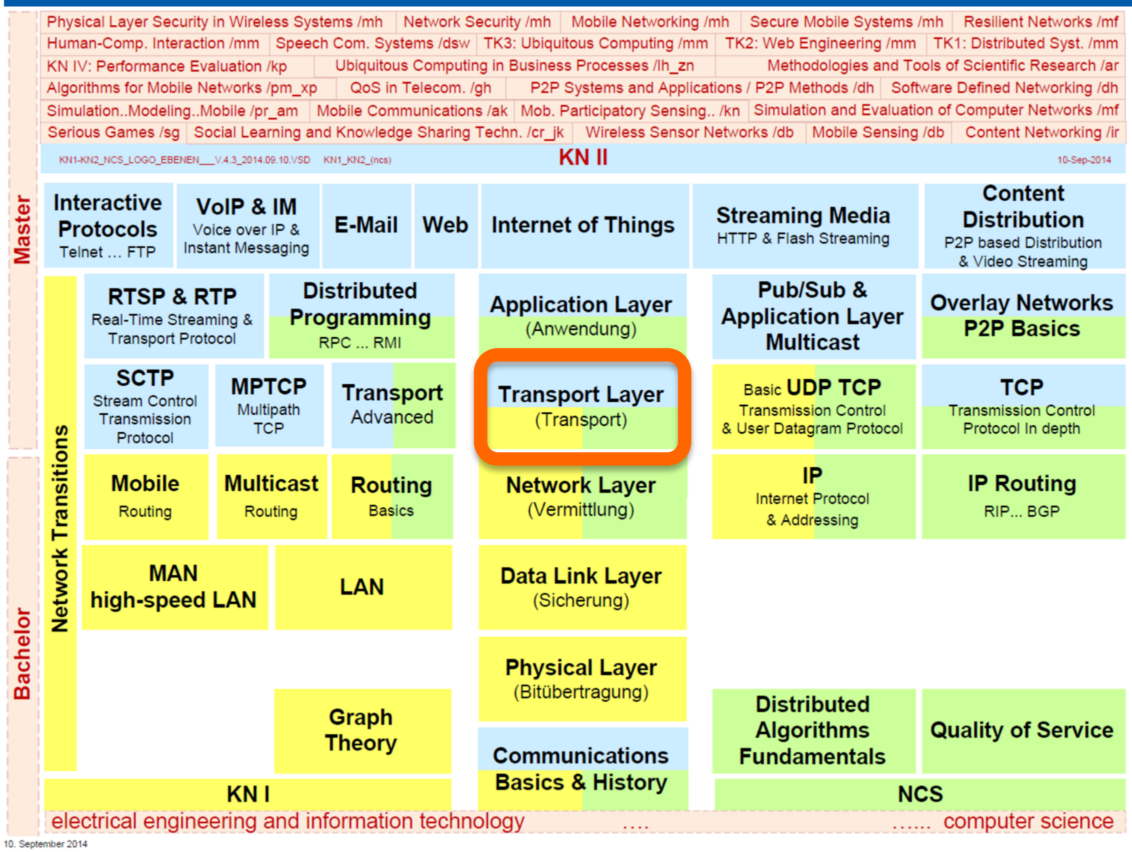
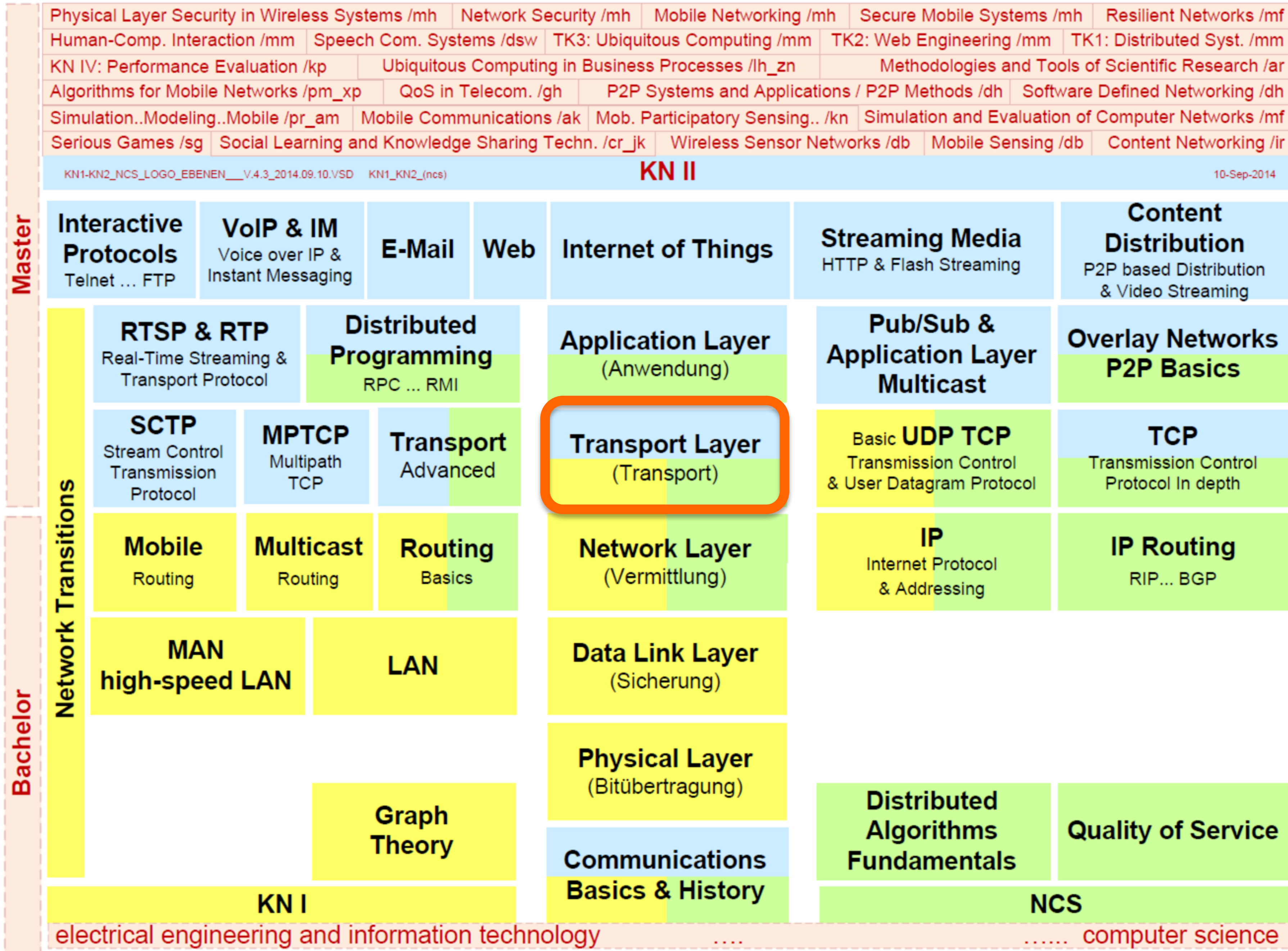
Communication Networks 2

L4 Transport Layer - Fundaments



Prof. Dr.-Ing. **Ralf Steinmetz**

KOM - Multimedia Communications Lab


Physical Layer Security in Wireless Systems /mh
Network Security /mh
Mobile Networking /mh
Secure Mobile Systems /mh
Resilient Networks /mf
Human-Comp. Interaction /mm
Speech Com. Systems /dsw
TK3: Ubiquitous Computing /mm
TK2: Web Engineering /mm
TK1: Distributed Syst. /mm
KN IV: Performance Evaluation /kp
Ubiquitous Computing in Business Processes /lh_zn
Methodologies and Tools of Scientific Research /ar
Algorithms for Mobile Networks /pm_xp
QoS in Telecom. /gh
P2P Systems and Applications / P2P Methods /dh
Software Defined Networking /dh
Simulation..Modeling..Mobile /pr_am
Mobile Communications /ak
Mob. Participatory Sensing.. /kn
Simulation and Evaluation of Computer Networks /mf
Serious Games /sg
Social Learning and Knowledge Sharing Techn. /cr_jk
Wireless Sensor Networks /db
Mobile Sensing /db
Content Networking /ir
KN1-KN2_NCS_LOGO_EBENEN__V.4.3_2014.09.10.VSD
KN1_KN2_(ncs)
KN II
10-Sep-2014
Master
Bachelor
Network Transitions
Interactive Protocols
Telnet … FTP
VoIP & IM
Voice over IP & Instant Messaging
E-Mail
Web
Internet of Things
Streaming Media
HTTP & Flash Streaming
Content Distribution
P2P based Distribution & Video Streaming
RTSP & RTP
Real-Time Streaming & Transport Protocol
Distributed Programming
RPC ... RMI
Application Layer
(Anwendung)
Pub/Sub & Application Layer Multicast
Overlay Networks
P2P Basics
SCTP
Stream Control Transmission Protocol
MPTCP
Multipath TCP
Transport Advanced
Transport Layer
(Transport)
Basic UDP TCP
Transmission Control & User Datagram Protocol
TCP
Transmission Control Protocol In depth
Mobile
Routing
Multicast
Routing
Routing
Basics
Network Layer
(Vermittlung)
IP
Internet Protocol & Addressing
IP Routing
RIP... BGP
MAN
high-speed LAN
LAN
Data Link Layer
(Sicherung)
Physical Layer
(Bitübertragung)
Graph Theory
Distributed Algorithms Fundamentals
Quality of Service
Communications Basics & History
KN I
NCS
electrical engineering and information technology
....
......
computer science

Physical Layer Security in Wireless Systems /mh	Network Security /mh	Mobile Networking /mh	Secure Mobile Systems /mh	Resilient Networks /mf
Human-Comp. Interaction /mm	Speech Com. Systems /dsw	TK3: Ubiquitous Computing /mm	TK2: Web Engineering /mm	TK1: Distributed Syst. /mm
KN IV: Performance Evaluation /kp	Ubiquitous Computing in Business Processes /lh_zn	Methodologies and Tools of Scientific Research /ar		
Algorithms for Mobile Networks /pm_xp	QoS in Telecom. /gh	P2P Systems and Applications / P2P Methods /dh	Software Defined Networking /dh	
Simulation..Modeling..Mobile /pr_am	Mobile Communications /ak	Mob. Participatory Sensing.. /kn	Simulation and Evaluation of Computer Networks /mf	
Serious Games /sg	Social Learning and Knowledge Sharing Techn. /cr_jk	Wireless Sensor Networks /db	Mobile Sensing /db	Content Networking /ir

Overview

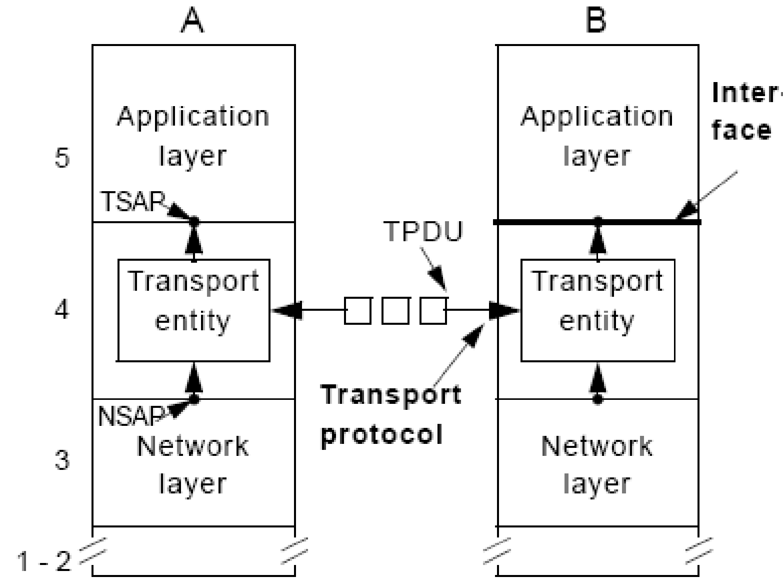
1 Transport Layer Function

To provide data transport

- reliably
- efficiently
- at low-cost

for

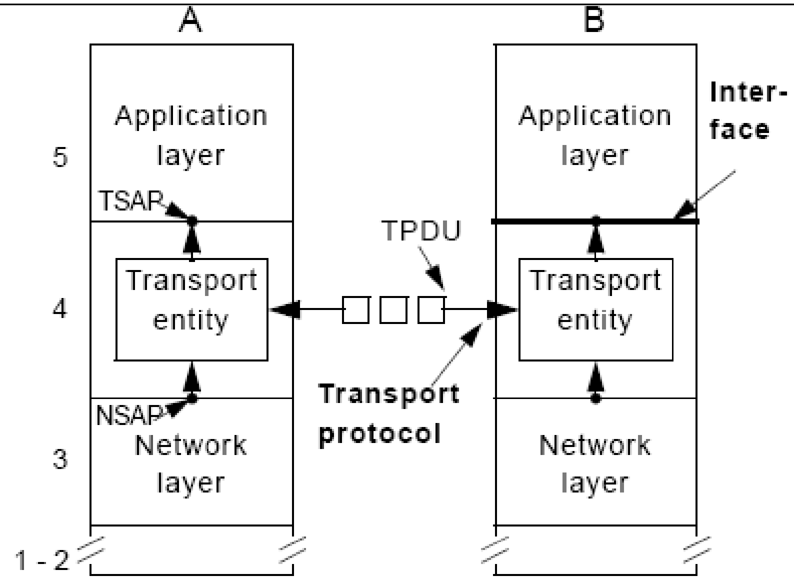
- process-to-process (applications)
- i.e. at end system-to-end system



(if possible) independent from

- particularities of the networks (lower layers) used

1.1 Transport Service



Connection oriented service

- 3 phases: connection set-up, data transfer, disconnect

Connectionless service

- transfer of isolated units

Implementation: transport entity

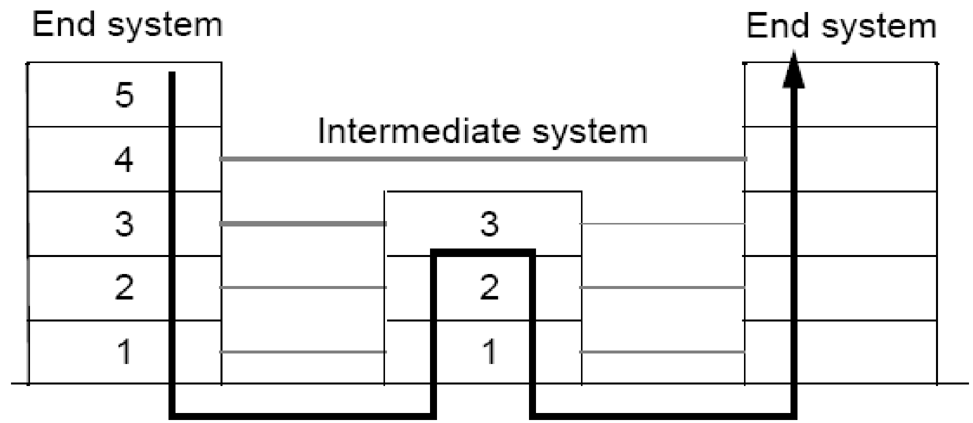
- software and/or hardware?
- software part usually contained within the kernel (process, library)

Transport Service

Similar services of

- network layer
  and transport layer:

  Why 2 Layers?



Transport service:
to Improve the Network Service Quality

- users and layers want to get from the network layer, e.g.
  - reliable service
  - necessary time guarantees

Network service

- not to be self-governed or influenced by the user
- independent from application & user
  - enables compatibility between applications
- provides for example
  - “only” connection oriented communications
  - or “only” unreliable data transfer

Transport layer

- isolates upper layers from technology, design and imperfections of subnet

Traditionally distinction made between

- layers 1 - 4
  - transport service provider
- layers above 4
  - transport service user

Transport layer has key role

- major boundary between
  - provider and
  - user of reliable data transmission service

Transport Services Primitives

Primitives for a simple transport service:

Primitive	Packet sent	Meaning
LISTEN	(none)	Block until some process tries to connect
CONNECT	CONNECTION REQ	Actively attempt to establish a connection
SEND	DATA	Send Information
RECEIVE	(none)	Block until a DATA packet arrives
DISCONNECT	DISCONNECTION REQ	Request to release the connection

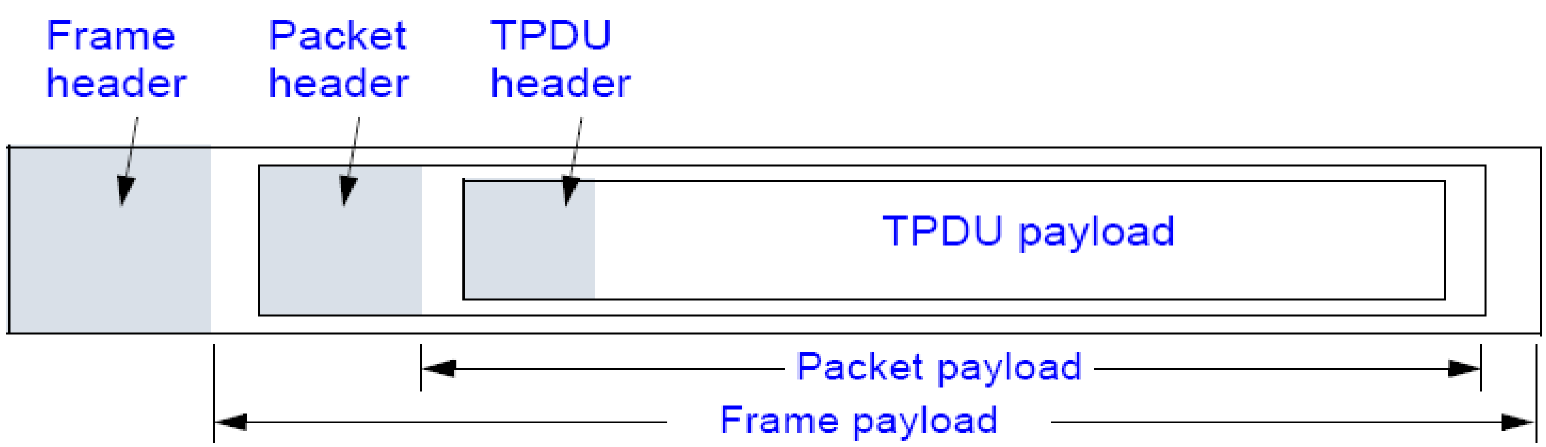
Transport Service: Terminology

Entities exchanged:

Layer	Data Unit
Transport	TPDU / Message
Network	Packet
Data Link	Frame
Physical	Bit/Byte (bit stream)

TPDU: Transport Protocol Data Unit

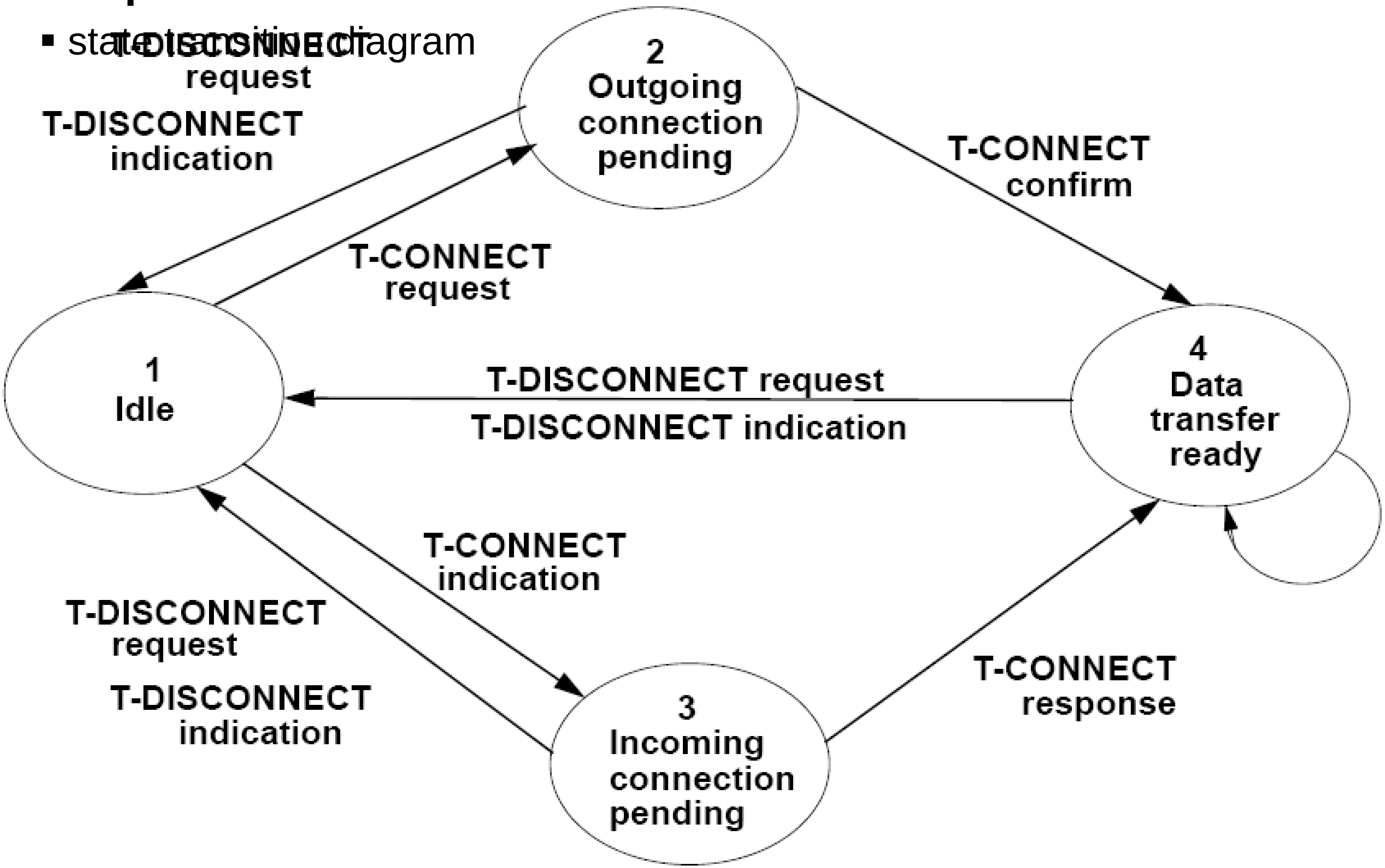
Nesting of TPDUs, packets, and frames:



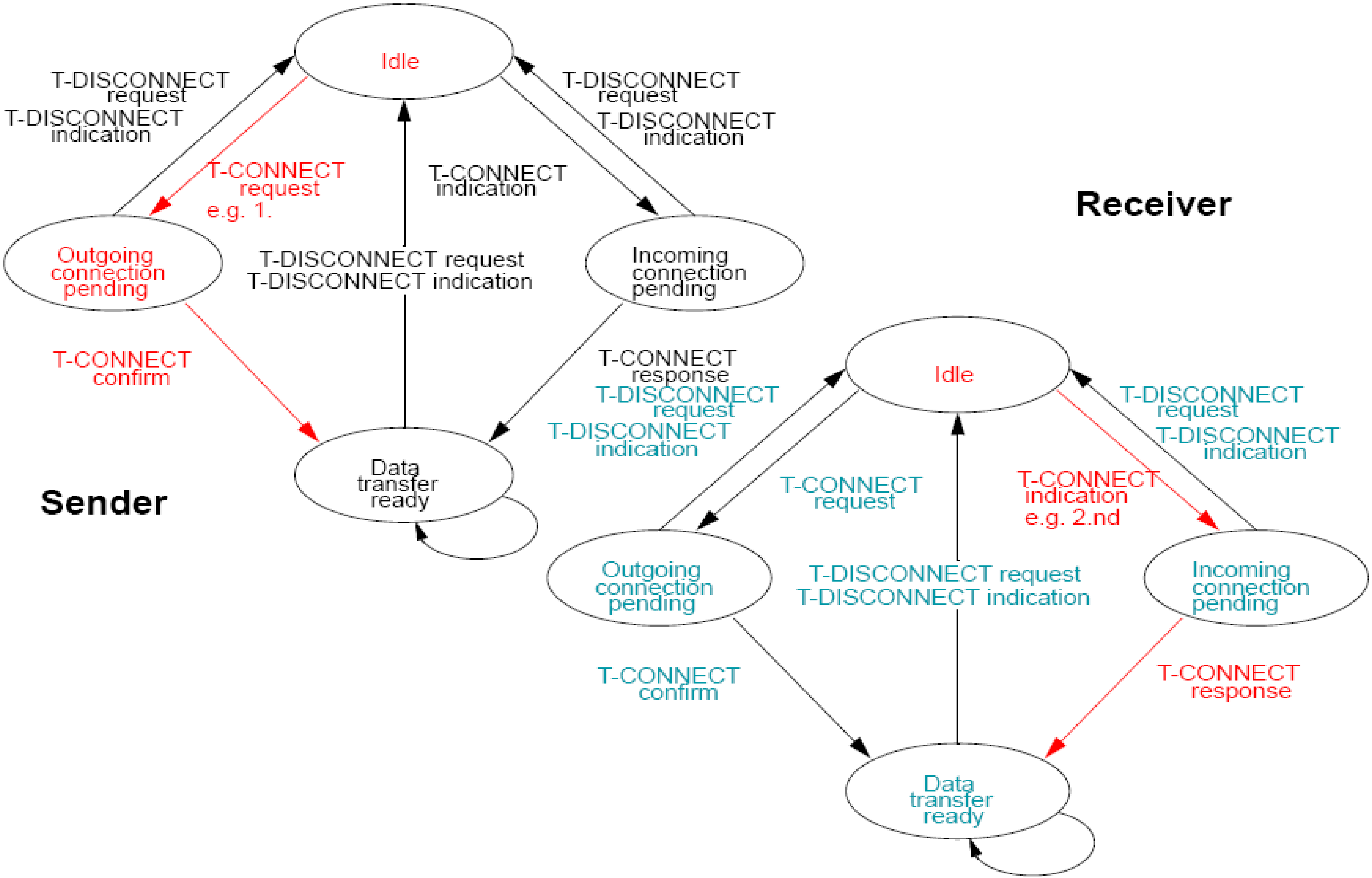
TECHNISCHE UNIVERSITÄT DARMSTADT

Example: ISO-OSI nomenclature

- state transition diagram



Connection Oriented Service: State Transition Diagram



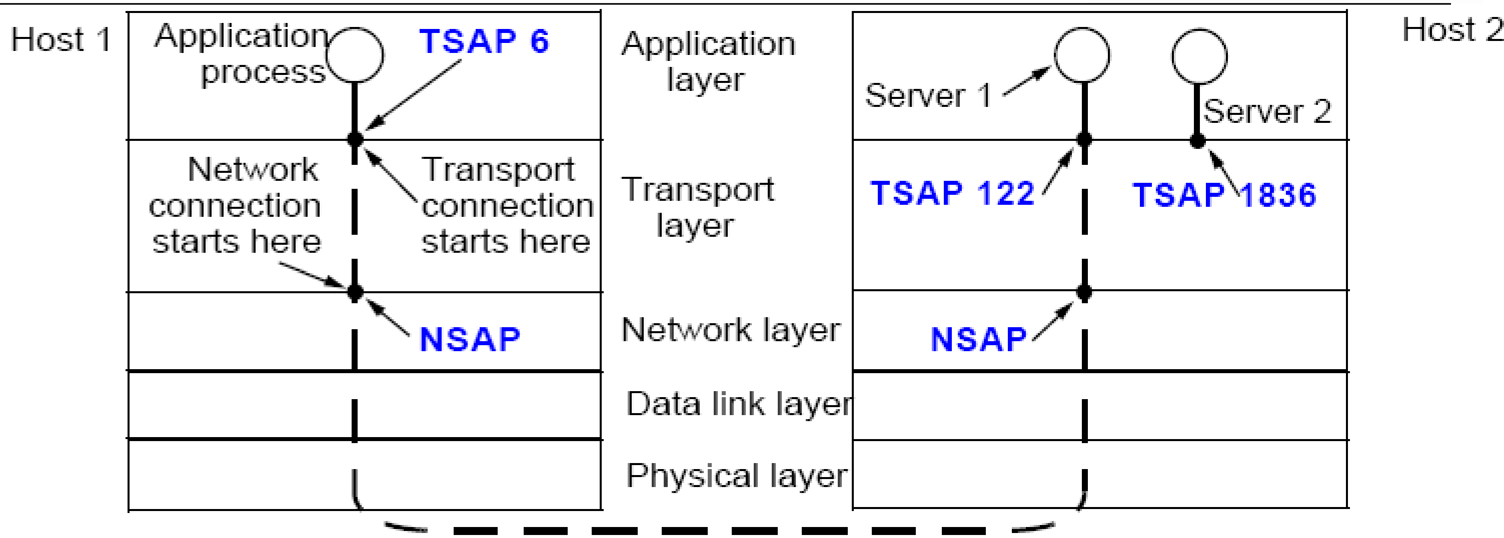
Example: Parameters for Disconnect

Example: ISO-OSI nomenclature, reason for a “T-Disconnect”

Reason	Notes
Normal disconnect initiated by session entity	1, 4
Remote congestion at transport entity during CC	1, 4
Failed connection negotiation	1, 3
Duplicated source reference for same NSAP pairs	1, 4
References are mismatched	1, 4
Protocol error	1, 4
Reference overflow	1, 4
Connection request refused	1, 4
Header or parameter length invalid	1, 4
No reason specified	2, 4
Congestion at TSAP	2, 4
TSAP and session entity not attached	2, 3
Unknown address	2, 3
(Note 1) Used for classes 1 to 4 …. Different “classes” were introduced …. To denote certain Quality of Service	
(Note 2) Used for all classes	
(Note 3) Reported to TS-user as persistent	
(Note 4) Reported to TS-user as transient	

2 Addressing (at Transport Layer)

Model:



Why identification?

- sender (process) wants to address receiver (process)
  - for connection setup or individual message
- receiver (process) can be approached by the sender (process)

Define transport addresses:

- generic term: (Transport) Service Access Point (TSAP)
- Internet: port

Reminder: analogous end points in network layer: NSAP

- e.g., IP addresses

2.1 Steps - In General

1. Server (service provider)

- connects itself to TSAP 122
- waits for service request (polling, signaling, ..)

2. Client (application)

- initiates connection via TSAP 6 as source and TSAP 122 as destination
  - i.e. CONNECT REQ

3. Transport system on host 1

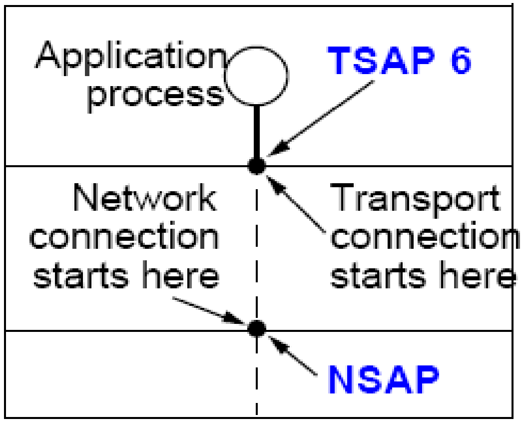
- identifies dedicated NSAP
- initiates communication at network layer
- communicates with transport entity on host2
- informs TSAP 122 about desired connection

4. Transport entity on host 2

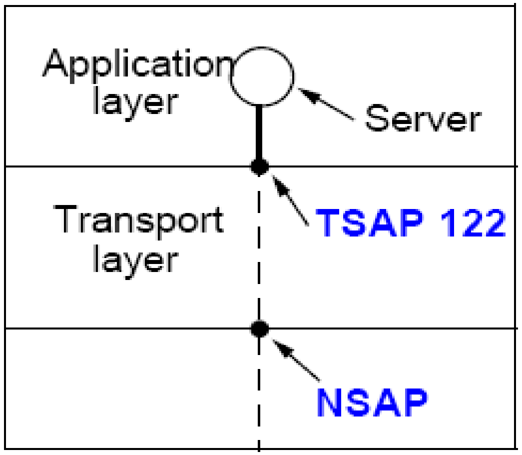
- addresses the server
- requests acceptance for the desired connection
  - i.e. CONNECT IND.

5. etc.

Host 1: Sender - Client

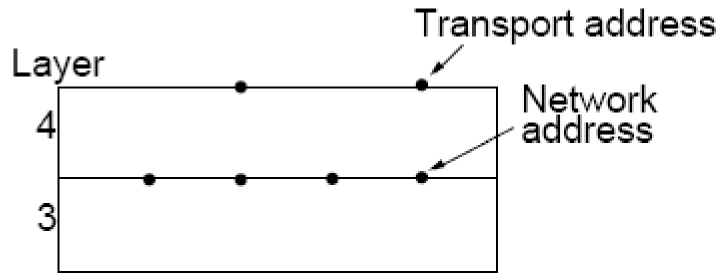


Host 2: Receiver - Server



2.2 Determination of Appropriate Service Provider TSAP

How does the specific address of a service becomes known?



1. Approach: TSAP known implicitly

- services that are well known and often used have pre-defined TSAPs
  - as "well-known ports" of a transport protocol
- e.g., stored in /etc/services file at UNIX systems

example: service ’time of day’

Characteristics:

- works well for small number of stable services
- not suitable for user specific processes
  - existing for short time, no known TSAP address
- waste of resources; seldom used servers active and listening

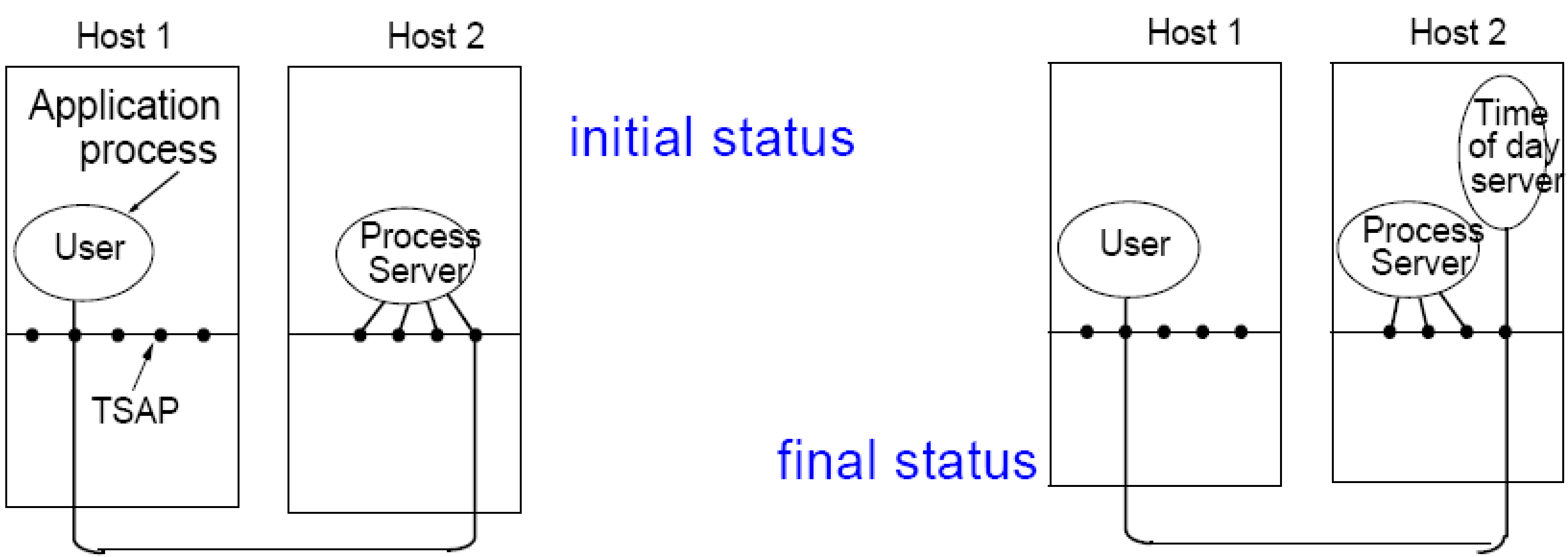
Determination of Appropriate Service Provider TSAP

2. Approach: “initial connection protocol”

- process server acting as proxy for less often used servers
- process server listens to a set of ports at same time
- waits for connection requests
- creates the appropriate service provider process
- transfers connection and desired service
- waits for further requests

Characteristics:

- works well for servers which can be created on demand
- not suitable if service exists independently of process server at another machine (e.g., file server)



Determination of Appropriate Service Provider TSAP

3. Approach: Name Server (directory server)

- context
  - server process already exists

- procedure
  - client addresses Name server (establishing connection)
  - client specifies the service as an ASCII data set
    - example “name of day”
  - name server supplies TSAP
  - client disconnects from name server
  - client addresses TSAP provided by name server
  - .....

- comments
  - new services
    - have to register at the name server
  - name server
    - adds corresponding information at the database

TECHNISCHE UNIVERSITÄT DARMSTADT

How to localize the respective endsystem NSAP (layer 3!!) ?

- i.e. how to determine the appropriate NSAP?

1. approach: hierarchical addressing

- TSAP contains this information

example: <country>.<network>.<port>

2. approach: “flat” addressing

- dedicated “name server”
  - entry

TSAP address: address of the endsystem + port

- request via broadcast
  - e.g. as correlation of Ethernet address and internet address
  - i.e. possible in geographically and topologically limited spaces

Initial Situation:

- network has
  - varying transit times for packets
  - certain loss rate
  - storage capabilities
- packets can be
  - manipulated
  - duplicated
  - resent by the original system after timeout

In the following, uniform term: "Duplicate"

- a duplicate originates due to one of the above mentioned reasons and
- is at a later (undesired) point in time passed to the receiver

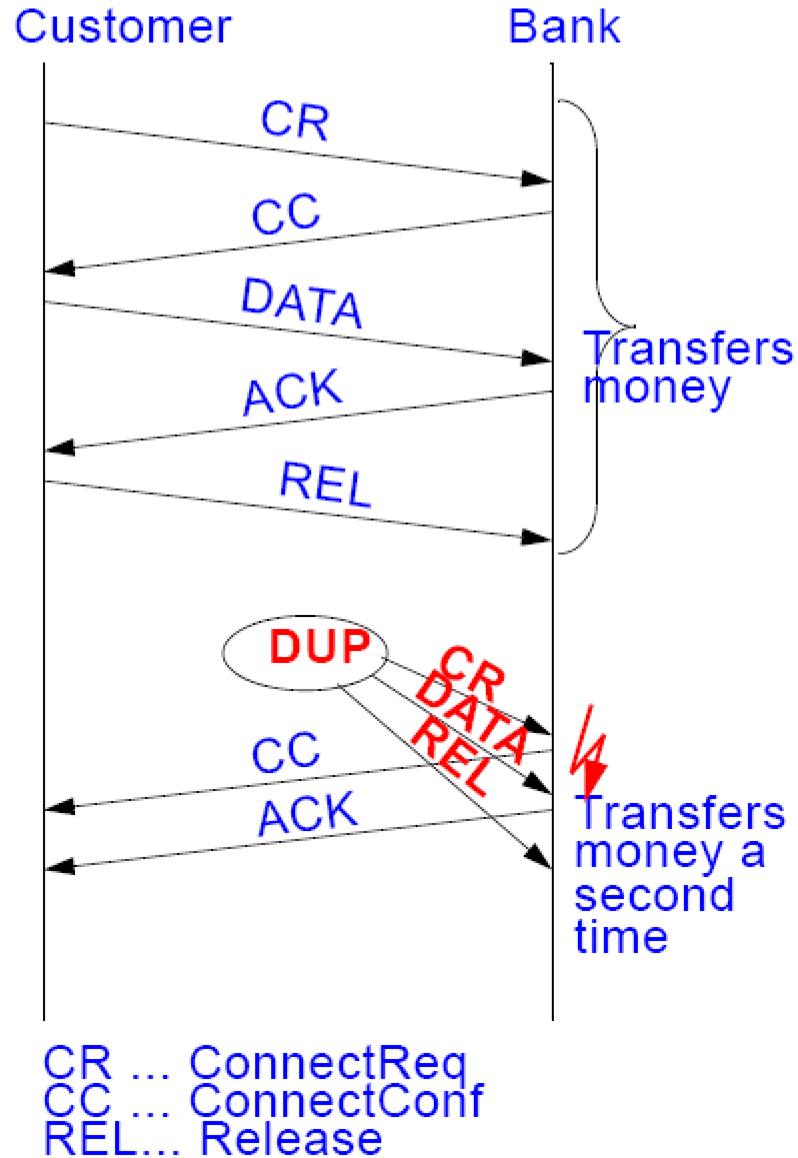
3.1 Basic Challenges - Example

E.g. description of possible error causes and their possible consequences (5 steps)

- due to network capabilities
  - duplication of sender's packets
  - subsequent to the first 5 packets duplicates are transferred in correct order to the receiver
  - also conceivable is that an old delayed DATA packet (with faulty contents) from a previous session may appear; this packet might be processed instead of or even in addition to the correct packet

Result:

- without additional means the receiver cannot differentiate between correct data and duplicated data
- would re-execute the transaction



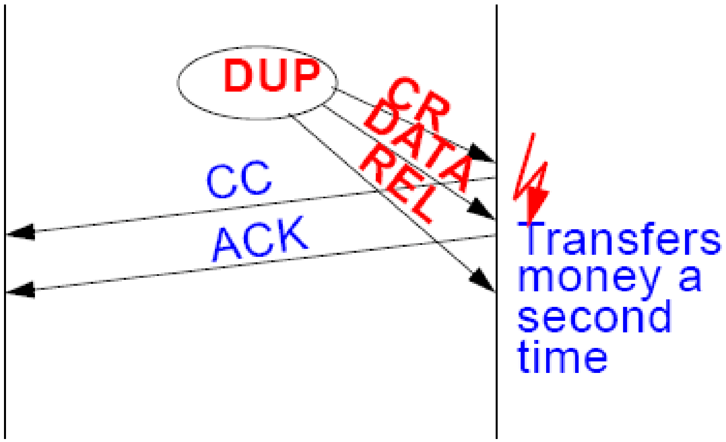
Duplicates – Description of Problematic Issues

3 somehow disjoint problems

1. how to handle duplicates WITHIN a connection?

2. what characteristics have to be taken into account regarding
   - consecutive connections or
   - connections which are being re-established after a crash?

3. what can be done to ensure that a connection that has been established …
   - has actually been initiated by and with the knowledge of both communicating parties?
   - see also the lower part of the previous illustration



3.2 Basic Methods of Resolution

1. to use temporarily valid TSAPs

- method:
  - TSAP valid for one connection only
  - generate always new TSAPs
- evaluation
  - in general not always applicable:
  - process server addressing method not possible, because
    - server is reached via a designated/known TSAP
    - some TSAPs always exist as “well-known”

2. to identify connections individually

- method
  - each individual connection is assigned a new SeqNo and
  - endsystems remember already assigned SeqNo
- evaluation
  - endsystems must be capable of storing this information
  - prerequisite:
    - connection oriented system (what if connection-less?)
  - endsystems, however, will be switched off and it is necessary that the information is reliably available whenever needed

Duplicates – Methods of Resolution

3. to identify PDUs individually:

individual sequential numbers for each PDU

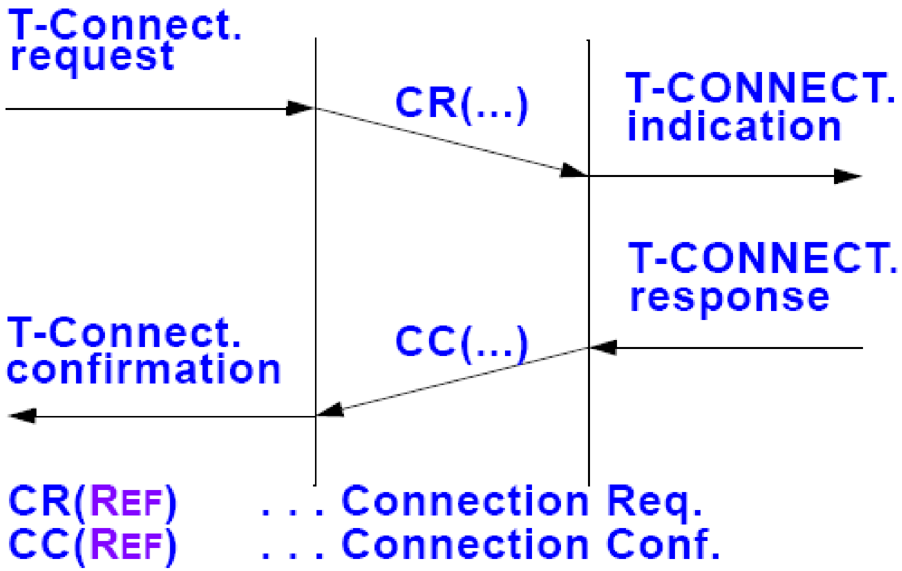
- method
  - SeqNo basically never gets reset
  - e.g. 48 bit at 1000 msg/sec: reiteration after 8000 years

- evaluation
  - higher usage of bandwidth and memory
  - sensible choice of the sequential number range depends on
    - the packet rate
    - a packet's probable “lifetime” within the network

Connection

- see also
  Connection Oriented Service:
  State Transition Diagram

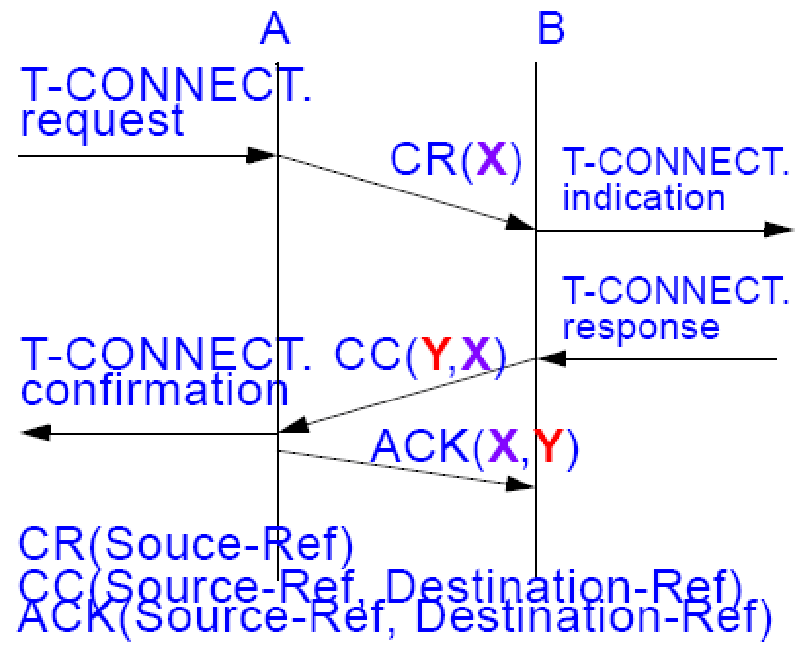
- by simple protocol
  - approach using 2 messages
    (2 phases)
    - problems may occur due to delayed duplicates
    - compare with previous example (bank transaction)



Connect: Three-way Handshake Protocol

TECHNISCHE UNIVERSITÄT DARMSTADT

Principle



1. CR: Connect Request

- initiator (A) sends request with
  - SequenceNo (**X**) selected by sender

2. CC: Connect Confirmation

- receiver (B) responds with
  - sequence number transmitted by the initiator (**X**) and
  - (randomly) selected sequence number (**Y**) by receiver
    - while observing the previously discussed criteria for selection, in order to avoid a collision with delayed duplicates

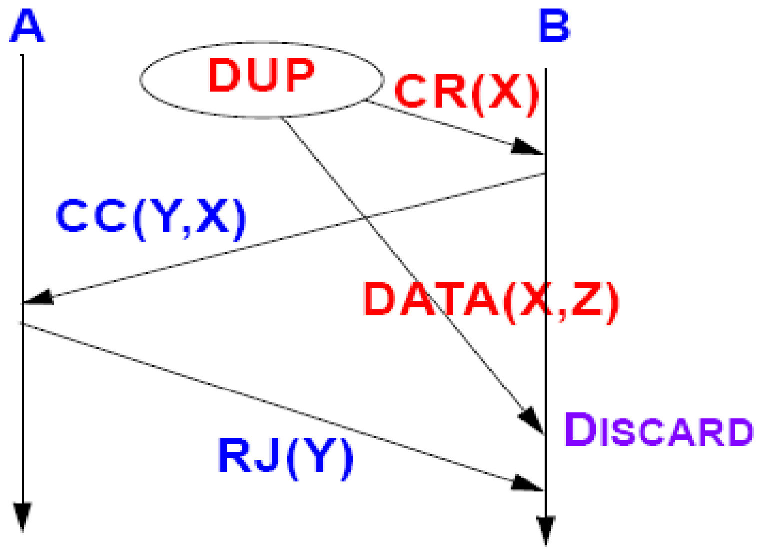
3. Acknowledgment

- initiator (A) acknowledges
  - sequence numbers **X**, **Y** (as received before)
- after receiving a valid ACK, receiver (B) accepts data

Note:

- some protocols (including TCP) acknowledge the next byte expected
  - (ACK X+1,Y+1), not the last byte received

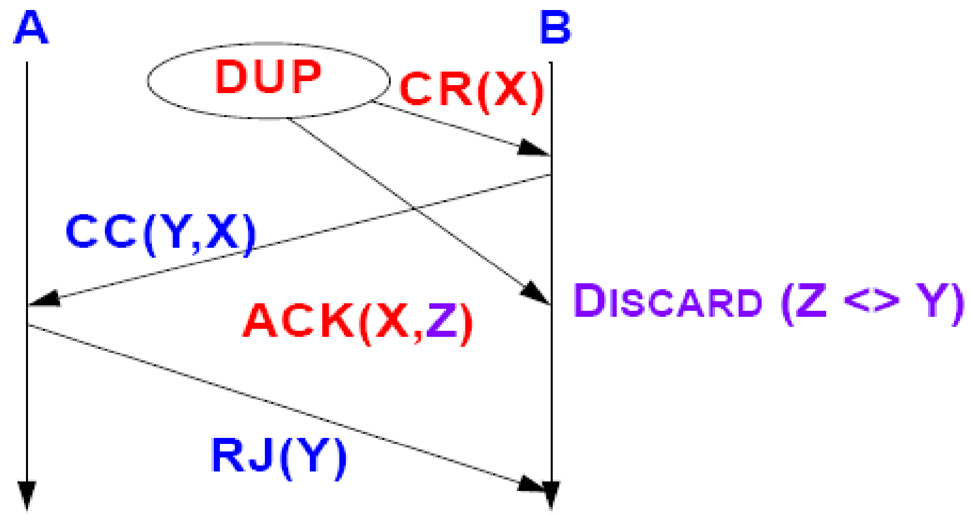
Three Way Handshake Protocol: Results



CR and data duplicate

- duplicated data is discarded
  - for success
    - should have occurred an ACK (X,Z) before

Three Way Handshake Protocol: Results



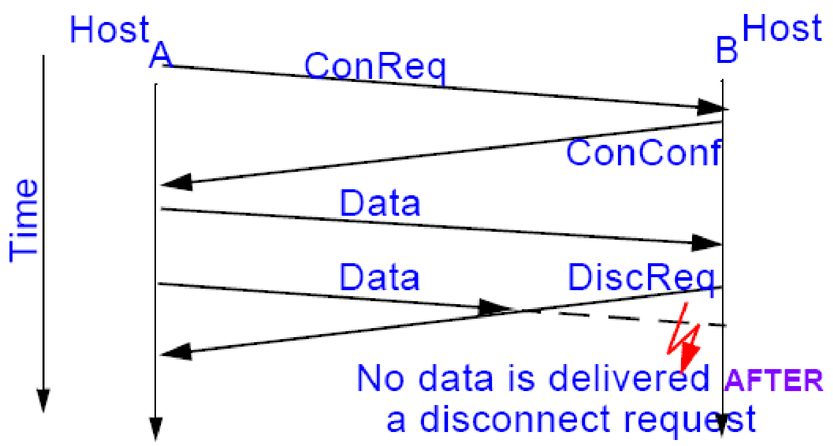
Connect Request CR Duplicate and Acknowledgment ACK Duplicates

- AK (X,Z) discarded because
  - AK (X,Y) expected
  - AK (X,Z) received, Z <> Y
    - B will be ensured by a premise of a maximum packet lifetime by selecting the initial sequence number according to the described algorithms

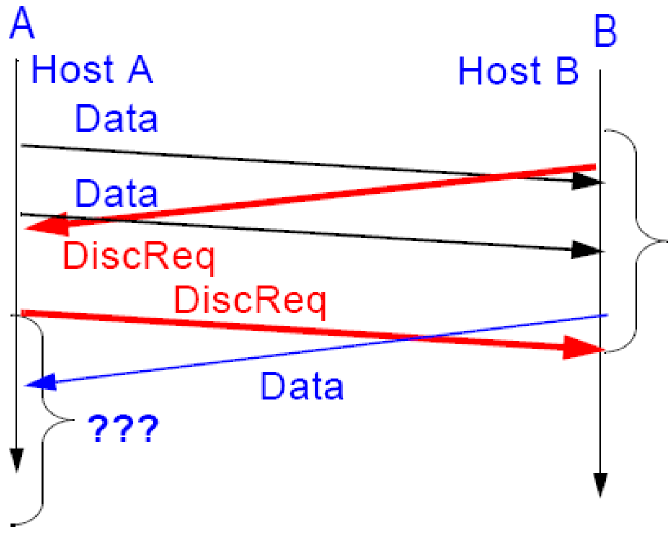
5 Disconnect

Two alternatives

asymmetric disconnect



symmetric disconnect



Joint characteristics (flow control on data link layer)

- fast sender shall not flood slow receiver
- sender shall not have to store all not acknowledged packets

Differences (flow control on data link layer)

- L2-DLL: router serves few connections to other routers
- L4-TL: endsystem contains a multitude of
  - connections
  - data transfer sequences
- L4-TL: receiver may (but does not always have to) store packets

Strategies

- E.g.
- credit mechanism / dynamic buffer allocation

Credit Mechanism

Flow control

- credit mechanism

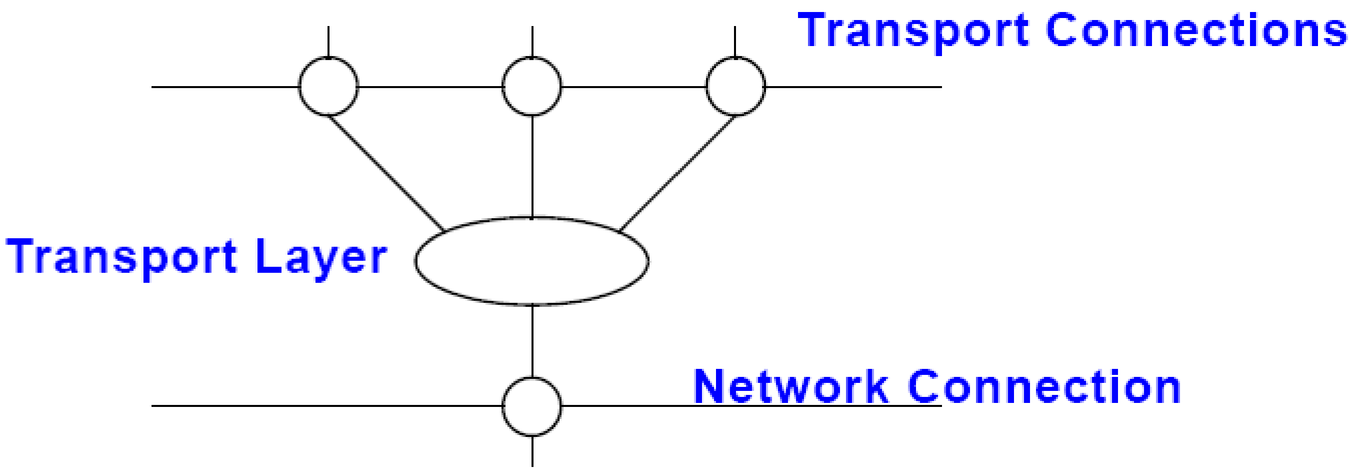
Buffer reservation

- receiver allocates buffers dynamically for the connections
- allocation depends on the current situation

Principle

- sender requests required buffer amount
- receiver reserves as many buffers as the current situation permits
- receiver returns ACKs and buffer-credits separately
  - ACK: confirmation only (does not imply buffer release)
  - CREDIT: buffer allocation
- sender will be blocked, when all credits have been used up

TECHNISCHE UNIVERSITÄT DARMSTADT



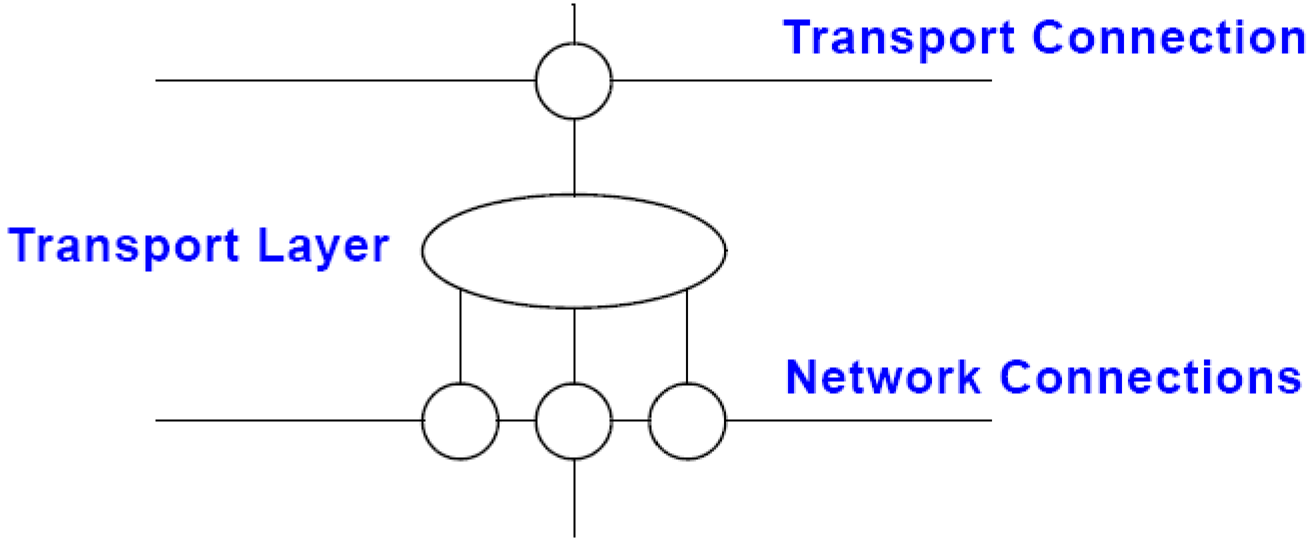
Application

- minimizing costs when num. of connections/ connection time represents the main cost factor

Multiplexing function

- grouping of T connections by destination address
- each group is mapped to the minimum number of network connections
  - too many L4-T connections per L3-N connection
    - ➔ possibly poor throughput
  - too few T connections per N connection
    - ➔ possibly transfer costs too high

Splitting / Recombination



Application:

- implementation of T connections with high bandwidth

Splitting function

- distributing the TPDUs onto the various network connections
- usual algorithm: Round Robin

Comment

- also known as “upward” multiplexing