Distributed Systems

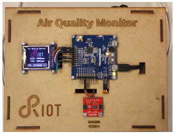
Network Services

Prof. Dr. Oliver Hahm

Frankfurt University of Applied Sciences
Faculty 2: Computer Science and Engineering
oliver.hahm@fb2.fra-uas.de
https://teaching.dahahm.de

27.04.2023

Reminder: Beware of the RIOT!



RIOT is the friendly OS for the IoT!

You would like to...

- ...learn how to develop exciting IoT applications?
- ...contribute to a huge open source project in a globally distributed team?
- ...realize your own ideas in software or hardware?

No previous knowledge required.

Contact

The next meeting takes place next week on Thursday in room 1-237 at 16:00 (open end).

Check `https://teaching.dahahm.de/allriot/` or subscribe to the https://lists.stillroot.org/postorius/lists/frankfurt.lists.riot-os.org/.

Recap

- Which types of transparency do you remember?

Recap

- Which types of transparency do you remember?
- Can you define it?

Typical Properties of a Communication Service

- End-to-end communication between processes

Typical Properties of a Communication Service

- End-to-end communication between processes
- Quality-of-Service (QoS) parameter
  - QoS characteristics, e.g.,
    - Performance characteristics (response time, throughput)
    - Real-time properties
    - Failure characteristics

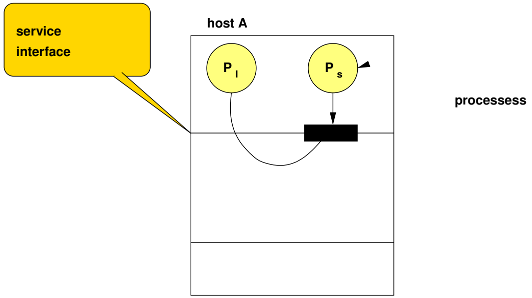
Typical Properties of a Communication Service

- End-to-end communication between processes
- Quality-of-Service (QoS) parameter
  - QoS characteristics, e.g.,
    - Performance characteristics (response time, throughput)
    - Real-time properties
    - Failure characteristics
- Transparency wrt network topology and transmission method

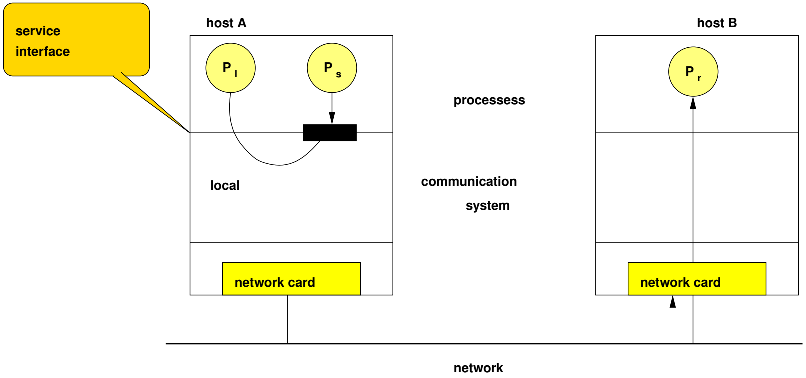
Typical Properties of a Communication Service

- End-to-end communication between processes
- Quality-of-Service (QoS) parameter
  - QoS characteristics, e.g.,
    - Performance characteristics (response time, throughput)
    - Real-time properties
    - Failure characteristics
- Transparency wrt network topology and transmission method
- Important internal aspects:
  - Error control
  - Flow control
  - Routing

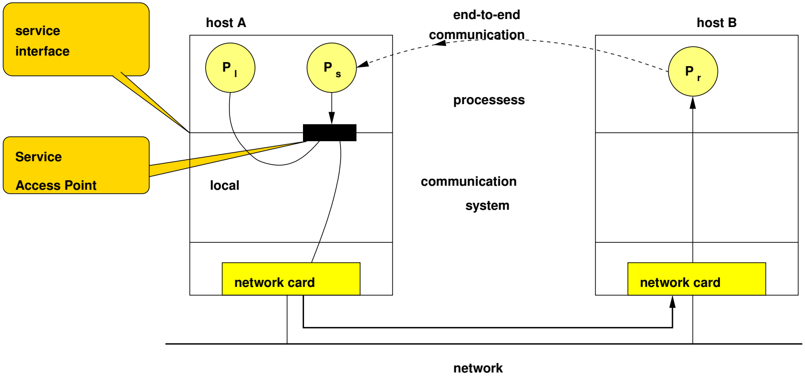
Generic Model for System wide Inter Process Communication (IPC)



Generic Model for System wide Inter Process Communication (IPC)



Generic Model for System wide Inter Process Communication (IPC)



Agenda

- Internet Protocols
- Network Performance

Agenda

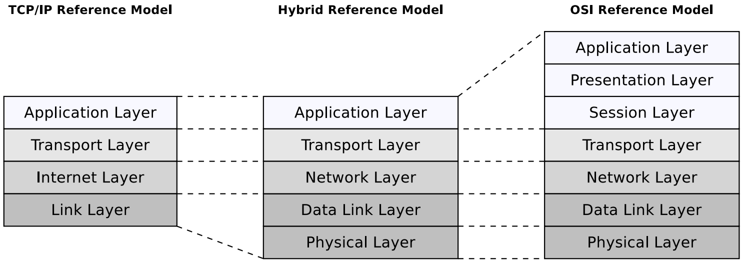
- Which functions needs to be implemented by a computer network?

- Which functions needs to be implemented by a computer network?
- How can we handle all these functionalities?

OSI Reference Model

Central concepts of the OSI model are:

Services	Define what the layer does, i.e., its semantics
Interfaces	Define how to access it
Protocols	Describe how the layer is implemented



What are the tasks, devices, and protocols for each layer?

Tasks of Layer 1

- Layer 1: Physical Layer (PHY)
  - Definition of mechanical/electrical/optical specifications and procedures required for the Bit transmission on the carrier.
  - The Physical Layer can be subdivided into
    1. *PMD Sublayer*: Physical Media Dependent (mechanical/electrical/optical) specifications
    2. *PHY Sublayer*: Physical (Signals $\leftrightarrow$ bits: en/de-coding)
  - Transmits the ones and zeros

Tasks of Layer 2

- Layer 2: Data Link Layer (DL):
  - Provides mechanisms how two nodes on the same physical network guarantee a safe communication.
  - For this purpose, the information (= bits) are grouped together in *frames* and are complemented by checksum as final part of the frame. The checksum allows an error detection (and potentially correction).
  - The Data Link Layer can be subdivided two sublayers as well:
    1. *MAC Sublayer*: Media Access Control defines the access to the physical carrier and how nodes are addressed
    2. *LLC Sublayer* Logical Link Control provides an additional safety and control functionality

Tasks of Layers 3 and 4

- Layer 3: Network Layer
  - The task of this layer is to transmit the data in *packets* between the (network) nodes.
  - Forwards *packets* between logical networks (over physical networks)
  - Thus, layer 3 can be understood as packet exchange layer.
- Layer 4: Transport Layer
  - The transport layer provides a (potentially *reliable*) virtual *end-to-end connection* for the data transport between the end nodes
  - Acts as a *multiplexer* between the various processes on the hosts via ports
  - Transport protocols can implement connection-oriented or connectionless communication

Tasks of Layers 5 and 6

- Layer 5: *Session Layer*
  - This is the lowest application-specific layer and is responsible to raise, maintain, and gracefully terminate communication relationships between the end nodes: a *Session*.
  - It's particular scope is to provide dialog-functionalities among the communication partners, in particular to allow a synchronization between the involved communication processes.
- Layer 6: *Presentation Layer*
  - The conversion and translation of different data representations (e.g. character set families like ASCII and EBCDIC) to a common format prior of sending, is main task of the Presentation Layer.
  - This layer may include functionalities which allow compression of data, conversion, and encryption.
  - Known presentation schemes here were ASN.1 (*Abstract Syntax Notation No. 1*) and XDR (*eXternal Data Representation*); however XML (*eXtensible Markup Language*) is now mostly used instead.

Tasks of layers 7

- Layer 7: Application Layer
  - Contains all protocols, that interact with the application programs (e.g., browser or email program)
  - Here is the actual payload (e.g., HTML pages or emails), formatted according to the used application protocol
  - Comprises the biggest variety of protocols

Main Characteristics of the TCP/IP Architecture

- **Connectionless best-effort** protocol (IP) on the network layer
- Packet switching via network nodes
- Static and dynamic **routing**
- Transport protocol with reliable **end-to-end transmissions** (TCP)

What does packet switching mean?

Circuit versus Packet switching

- Circuit switching
  - A sustained (virtual) connection is present between both communication partners (end nodes) as long as the data transmission lasts

  → End nodes must be attached to a specific exchange node
  - **Drawback:** The communication breaks down, in case the connection fails

Circuit versus Packet switching

- Circuit switching
  - A sustained (virtual) connection is present between both communication partners (end nodes) as long as the data transmission lasts

  → End nodes must be attached to a specific exchange node
  - **Drawback:** The communication breaks down, in case the connection fails
- Packet switching
  - The data to be exchanged will be encapsulated in packets as complete information units
  - These packets are dropped on the network and exchanged between the communication partners
    - Packets do include an address-information about the sender and the recipient node
    - Packets can be buffered on the transmission path
  - **Drawback:** Some per-packet overhead for long-lasting connections

Essential Properties of IP

- Connectionless protocol
- best-effort transport of individual messages (Datagram, =Packet)
- Addressing of hosts via 32 bit (IPv4) or 128 bit (IPv6) IP addresses
- *Fragmentation* if necessary (optional in IPv6)
- IPv4 contains a checksum for the header, but not the payload; IPv6 does not contain any checksum
- IPv4 packets may contain optional header fields, IPv6 uses extension headers
- The lifetime (*TTL*) of a packet in the network is limited

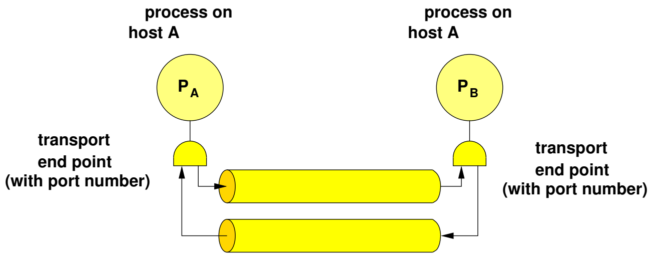
Transport Layer Protocols

- Tasks of the Transmission Control Protocols (TCP):
  - Reliable bidirectional point-to-point transport of a bytestream between two hosts on the endpoints
- Tasks of the User Datagram Protocols (UDP):
  - Best-effort datagram service of IP layer is accessible for the processes on the endpoints
- Classification:

Application Layer (OSI Layer 5-7)	HTTP FTP SSH SMTP IMAP ...	NTP DNS TFTP ...	
Layer 4	TCP	UDP	$\Longleftarrow$
Layer 3	IP		

TCP Communication Model

- connection oriented
- virtual, bidirectional, full-duplex capable connection between endpoints (used by their processes)
- Addressing of transport layer endpoints via 16 bit port numbers (in addition to the node's IP addresses)
- Bytestream oriented, not blockwise
- A single packet containing a chunk of the bytestream is called segment


process on host A
process on host A
P_A
P_B
transport end point (with port number)
transport end point (with port number)

Main Characteristics of TCP

- Reliable transmission due to . . .
  - Sequence numbers
  - Checksum calculation (same algorithm as IPv4)
  - Reception receipts (acknowledgements) and timeouts
  - Retry after timeout
- Preserved order
- *Sliding window* principle for flow control
- *AIMD* principle for congestion control

Main Characteristics of TCP

- Reliable transmission due to . . .
  - Sequence numbers
  - Checksum calculation (same algorithm as IPv4)
  - Reception receipts (acknowledgements) and timeouts
  - Retry after timeout
- Preserved order
- *Sliding window* principle for flow control
- *AIMD* principle for congestion control
  - **AIMD** := Additive Increase/Multiplicative Decrease

Essential Properties of UDP

- Connectionless protocol
- Addressing of the user via 16 bit port numbers
- *best-effort* transmission of datagrams (individual messages), IP services from the network layer are made accessible for application processes $\rightarrow 1:1$ mapping
- Multicast/Broadcast capable (1:n communication), direct application of multicast capable networks like, for instance, Ethernet
- Integrity check via an optional checksum
- No further guarantees:
    - No receipts or other guarantees, i.e., datagrams can get lost, arrive in a different order, or getting duplicated
    - No flow control, i.e, on the receiver site datagrams may get discarded in case of full or missing buffers
- Well suited for the implementation of simple request/response protocols

For which type of application would you use TCP and for which UDP?

Agenda

- Internet Protocols
- Network Performance

- How can we measure the network performance?

- How can we measure the network performance?
- What does affect the network performance?

Effecting the Network Performance

- Data and messages, which are transmitted over networks may be **lost** and/or **corrupted**:
  - Insufficient quality of the transmission carrier
  - External distortion impacts (e.g., because of electromagnetic fields)
- The communication protocol has to deal with these cases and has to provide:
  - Error/Fault Control:
    Identification and compensation for transmission errors/failures
  - Flow Control:
    Adaptive means to adjust the amount of data to be send w.r.t. the recipient's (announced) capacity
  - Congestion Control:
    Additional means, to reduce the potential lost of data (packets) on the network

Failure Causes

Signal Transmission Errors

During the transmission of bit sequences on the physical layer errors may occur

They are typically caused by. . .

- Signal deformation
  - Attenuation of the transmission medium
- Noise
  - Thermal or electronic noise
- Crosstalk
  - Interference by neighboring channels
  - Capacitive coupling increases with increasing frequency
- Short-time disturbances
  - Cosmic radiation
  - Defective or insufficient insulation

Error Types

Burst errors are more common than single bit errors

Typical BER values

POTS	$2 * 10^{-4}$
Radio link	$10^{-3} - 10^{-4}$
Ethernet	$10^{-9} - 10^{-10}$
Fiber	$10^{-10} - 10^{-12}$

The LLC sublayer tries to detect and handle bit errors that occur during signal

Checksum

Checksum

The checksum is calculated by a pre-defined algorithm for a block of data. They are typically used for the verification of the data integrity.

- For error detection, the sender attaches a checksum at each frame
- The receiver can now detect erroneous frames and discard them
- Possible checksums:
  - Parity-check codes
  - The polynomial code – Cyclic Redundancy Checks (CRCs)

Error Control

- In order to detect transmission errors on the upper layers positive A^+ and negative acknowledgments A^- are feasible.
  - However, acknowledgments can be corrupted or get lost as well
  - The sender has to consider a *deferment period* until the acknowledgment has been finally received
  - In addition, the data blocks (or even the transmitted byte) can be *enumerated* (bookkeeping).
- The sender has to keep the transmitted data in his *sending buffer* until he finally has received the acknowledgment.

Flow control

- Flow control enables the adaption of the transmission rate of the sender with respect to
  - the recipient or
  - any network component which is responsible for the data transfer
- Typical flow control methods:
  - Messages hold and continue (`XON/XOFF`) issued by the recipient also know as Ready-for-Reception/Clear-to-Send (RFR/RTS+CTS),
  - By issuing credits
  - Window mechanism where the communication partners mutually tell their reception buffer to each other and adjust the data to transmit according to the provided value

Congestion control

- Any physical network as only a certain capacity to transmit only a certain amount of data during a certain time period.
- Congestion occurs when. . .
  - the recipient buffer in any network component is exaggerated ($\Rightarrow$ incoming data packets need to be dropped)
  - the sender is required to build up additional send buffers (*queues*) without being able to transmit the data packets on the network
- congestion avoidance is task of congestion control, since any congestion will impact
  - the data throughput and
  - the transfer latency (delay)

  negatively

Important takeaway messages of this chapter

- The Internet's TCP/IP architecture provides a flexible and generic communication system for many types of higher layer services
- While IP provides a packet switching best-effort service, transport layer protocols can offer additional services
- The network has to manage transmission errors and control the data flow