Computer Networks - 2021

Mohammed El-Hajj

Jacobs University Bremen

Sept 3, 2021

JACOBS
UNIVERSITY

Course Content

1. Introduction
2. Fundamental Networking Concepts
3. Local Area Networks (IEEE 802)
4. Internet Network Layer (IPv4, IPv6)
5. Internet Routing (RIP, OSPF, BGP)
6. Internet Transport Layer (UDP, TCP)
7. Firewalls and Network Address Translators
8. Domain Name System (DNS)
9. Abstract Syntax Notation 1 (ASN.1)
10. External Data Representation (XDR)
11. Augmented Backus Naur Form (ABNF)
12. Electronic Mail (SMTP, IMAP)
13. Document Access and Transfer (HTTP, FTP)

Part 2: Fundamental Concepts

4 Classification and Terminology

5 Communication Channels and Transmission Media

6 Media Access Control

7 Transmission Error Detection

8 Sequence Numbers, Acknowledgements, Timer

9 Flow Control and Congestion Control

10 Layering and the OSI Reference Model

Section 4: Classification and Terminology

4 Classification and Terminology

5 Communication Channels and Transmission Media

6 Media Access Control

7 Transmission Error Detection

8 Sequence Numbers, Acknowledgements, Timer

9 Flow Control and Congestion Control

10 Layering and the OSI Reference Model

Network

- Distance
  - Local area network, wide area network, personal area network, . ..
- Topology
  - Star, ring, bus, line, tree, mesh, . . .
- Transmission media
  - Wireless network, optical network, . . .
- Purpose
  - Industrial control network, media distribution network, cloud network, access network, aggregation network, backbone network, vehicular network, . ..
- Ownership
  - Home networks, national research networks, enterprise networks, government networks, community networks, . . .

Communication Modes

- Unicast — Single sender and a single receiver (1:1)
- Multicast — Single sender and multiple receivers (1:n)
- Concast — Multiple senders and a single receiver (m:1)
- Multipeer — Multiple senders and multiple receivers (m:n)

- Anycast — Single sender and nearest receiver out of a group of receivers
- Broadcast — Single sender and all receivers attached to a network
- Geocast — Single sender and multiple receivers in a certain geographic region

Communication Protocol

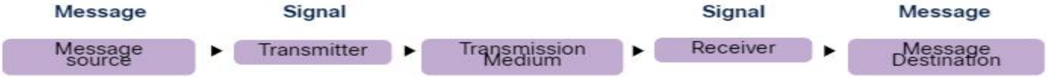
Definition (communication protocol)

A *communication protocol* is a set of rules and message formats that govern the communication between communicating peers. A protocol defines

- The set of valid messages (syntax of messages) and
- The meaning of each message (semantics of messages).

- A protocol is necessary for any function that requires cooperation between communicating peers
- A protocol implements ideally a well-defined service
- It is often desirable to layer new protocols on already existing protocols in order reuse existing services

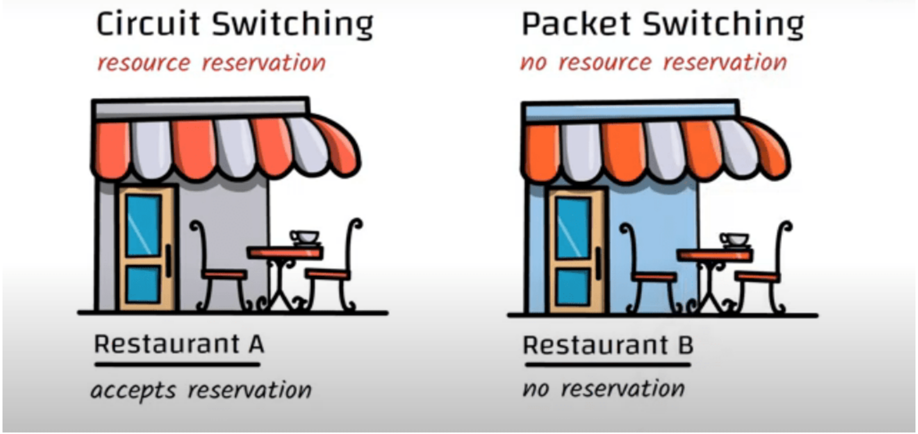
Communication Protocol



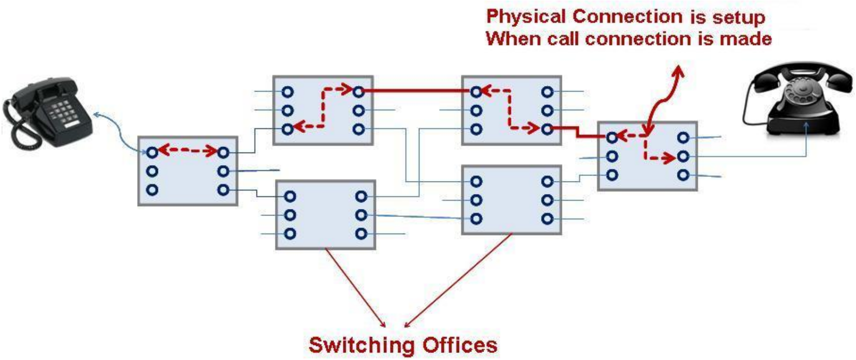
Message → Signal → Signal → Message

Message source ► Transmitter ► Transmission Medium ► Receiver ► Message Destination

Circuit vs. Packet Switching



Circuit vs. Packet Switching



Circuit vs. Packet Switching

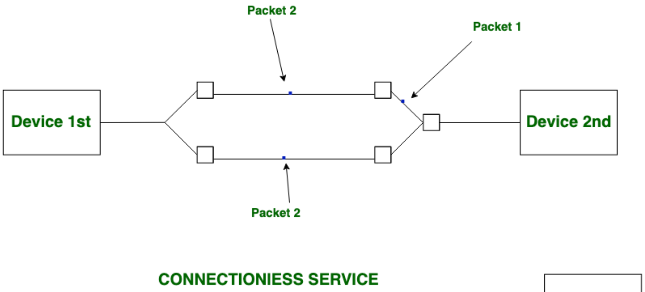
- Circuit switching:
  - Communication starts by creating a (virtual) circuit between sender and receiver
  - Data is forwarded along the (virtual) circuit
  - Communication ends by removing the (virtual) circuit
  - Example: Traditional telecommunication networks

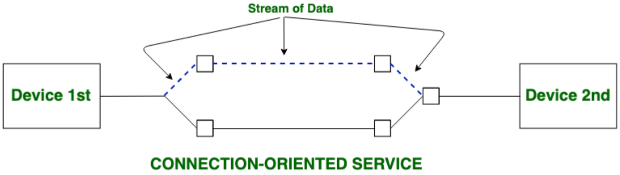
- Packet switching:
  - Data is carried in packets
  - Every packet carries information identifying the destination
  - Every packet is routed independently of other packets to its destination
  - Example: Internet

Connection-oriented vs. Connection-less

- Connection-oriented:
  - Usage of a service starts by creating a connection
  - Data is exchanged within the context of a connection
  - Service usage ends by terminating the connection
  - State may be associated with connections (stateful)
  - Example: Fetching a web page on the Internet
- Connection-less:
  - Service can be used immediately
  - Usually no state maintained (stateless)
  - Example: Internet name lookups

Connection-oriented vs. Connection-less

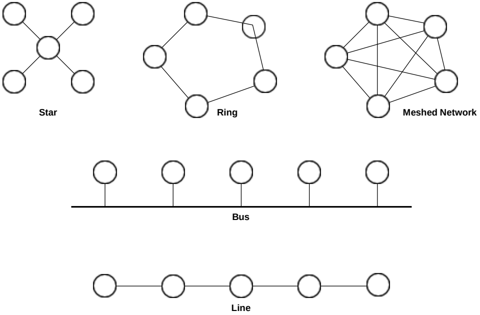




Data vs. Control vs. Management

- Data Plane:
  - Concerned with the forwarding of data
  - Acting in the resolution of milliseconds to microseconds
  - Often implemented in hardware to achieve high data rates
- Control Plane:
  - Concerned with telling the data plane how to forward data
  - Acting in the resolution of seconds or sub-seconds
  - Traditionally implemented as part of routers and switches
  - Recent move to separate the control plane from the data plane
- Management Plane:
  - Concerned with the configuration and monitoring of data and control planes
  - Acting in the resolution of minutes or even much slower
  - May involve humans in decision and control processes

Topologies



- The *topology* of a network describes the way in which nodes attached to the network are interconnected

Structured Cabling

- Networks in office buildings are typically hierarchically structured:
  - Every floor has a (potentially complex) network segment
  - The floor network segments are connected by a backbone network
  - Multiple buildings are interconnected by connecting the backbone networks of the buildings
- Cabling infrastructure in the buildings should be usable for multiple purposes (telephone network, data communication network)
- Typical lifetimes:
  - Network rooms and cable ways (20-40 years)
  - Fibre wires (about 15 years)
  - Copper wires (about 8 years)
  - Cabling should survive 3 generations of active network components

Section 5: Communication Channels and Transmission Media

4 Classification and Terminology

5 Communication Channels and Transmission Media

6 Media Access Control

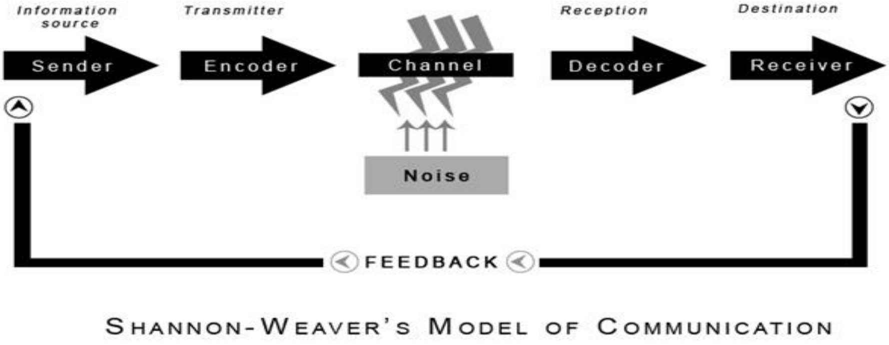
7 Transmission Error Detection

8 Sequence Numbers, Acknowledgements, Timer

9 Flow Control and Congestion Control

10 Layering and the OSI Reference Model

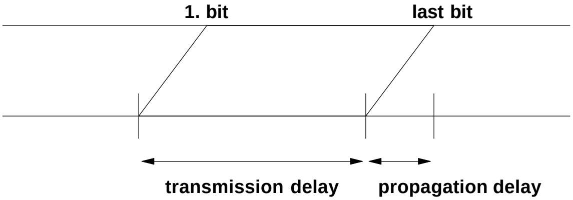
Communication Channel Model



- Signals are in general modified during transmission, leading to transmission errors.

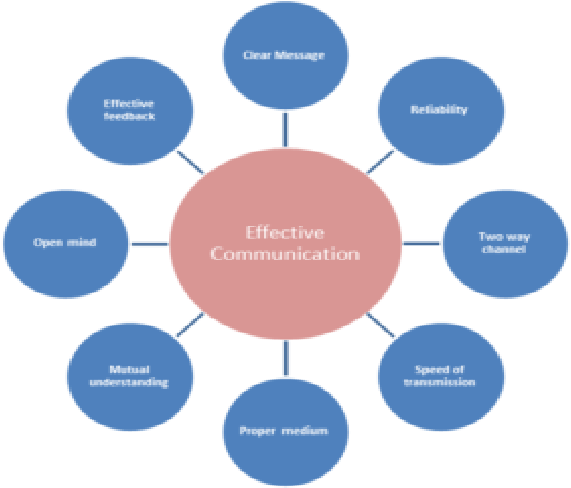
Channel Characteristics

- The *data rate* (bit rate) describes the data volume that can be transmitted per time interval (e.g., 100 Mbit/s)
- The *bit time* is the time needed to transmit a single bit (e.g., 1 microsecond for 1 Mbit/s)



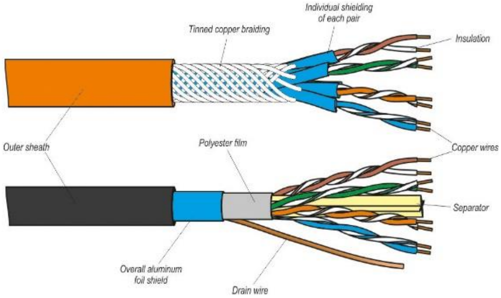
- The *delay* is the time needed to transmit a message from the source to the sink. It consists of the *propagation delay* and the *transmission delay*
- The *bit error rate* is the probability of a bit being changed during transmission

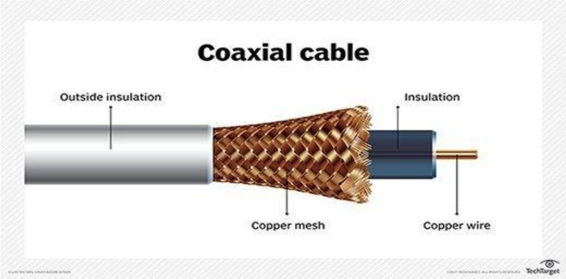
Channel Characteristics(2)



Transmission Media Overview

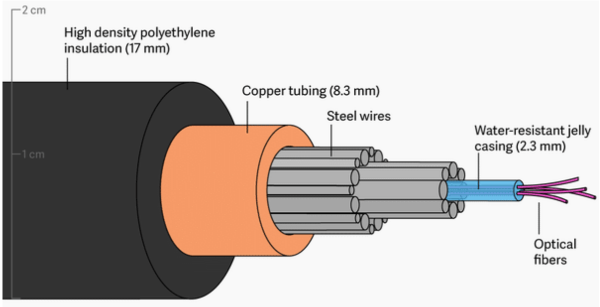
- Copper wires:
  - Simple wires
  - Twisted pair
  - Coaxial cables





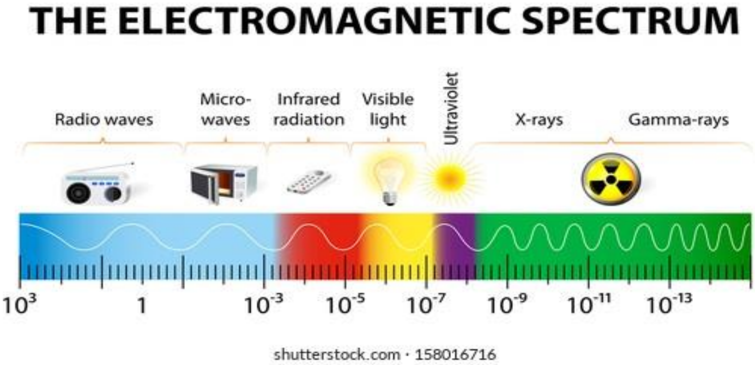
Transmission Media Overview

- Optical wires:
  - Fibre (multimode and single-mode)
- Air:
  - Radio waves
  - Micro waves
  - Infrared waves
  - Light waves


2 cm
1 cm
High density polyethylene insulation (17 mm)
Copper tubing (8.3 mm)
Steel wires
Water-resistant jelly casing (2.3 mm)
Optical fibers

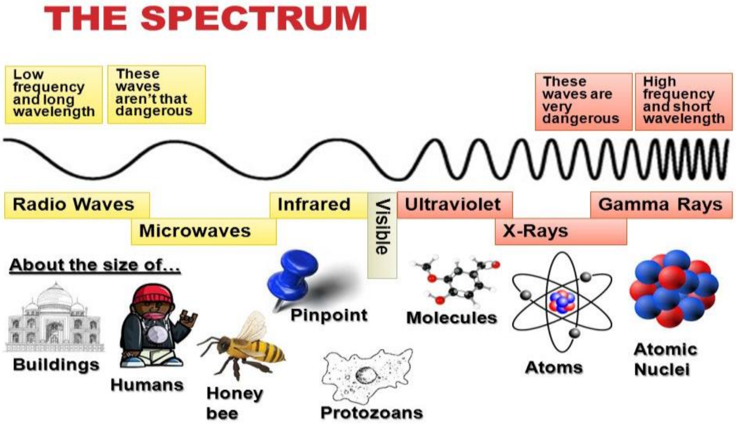
Transmission Media Overview

- Air:
  - Radio waves
  - Micro waves
  - Infrared waves
  - Light waves



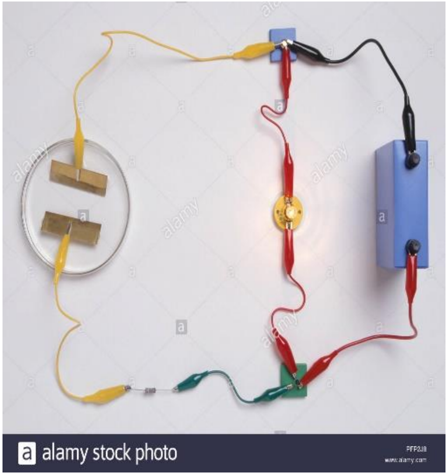
Transmission Media Overview

- Air:
  - Radio waves
  - Micro waves
  - Infrared waves
  - Light waves



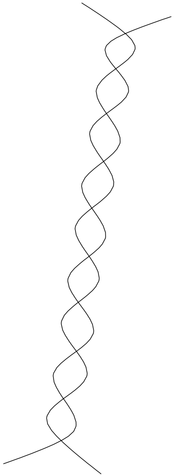
Simple Electrical Wires

- Simple two-wire open lines are the simplest transmission medium
- Adequate for connecting equipment up to 50 m apart using moderate bit rates
- The signal is typically a voltage or current level relative to some ground level
- Simple wires can easily experience crosstalk caused by capacitive coupling
- The open structure makes wires suspectible to pick-up noise signals from other electrical signal sources

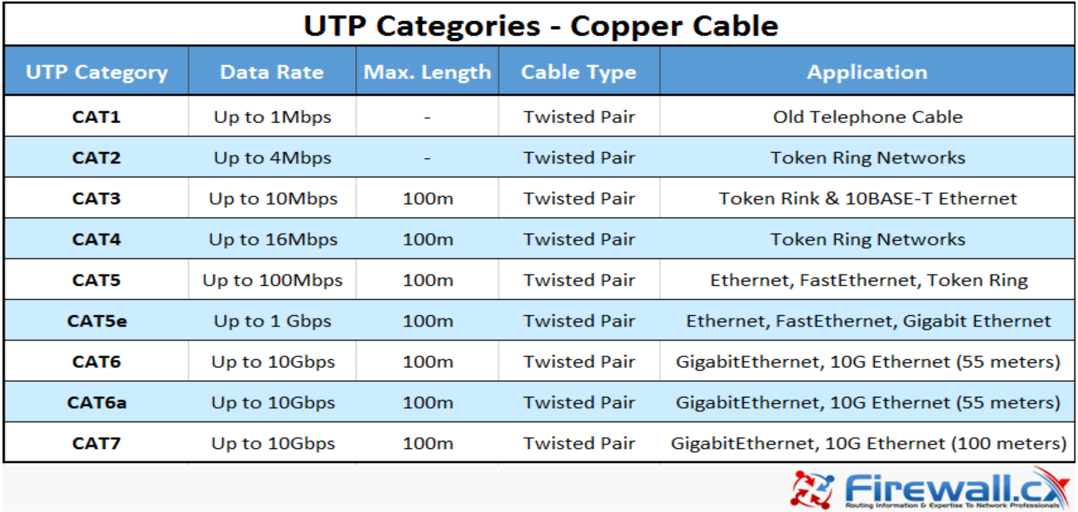


Twisted Pairs

- A twisted pair consists of two insulated copper wires
- Twisting the wires in a helical form cancels out waves
- Unshielded twisted pair (UTP) of category 3 was the standard cabling up to 1988
- UTP category 5 and above are now widely used for wiring (less crosstalk, better signals over longer distances)
- Shielded twisted pair (STP) cables have an additional shield further reducing noise



Twisted Pairs

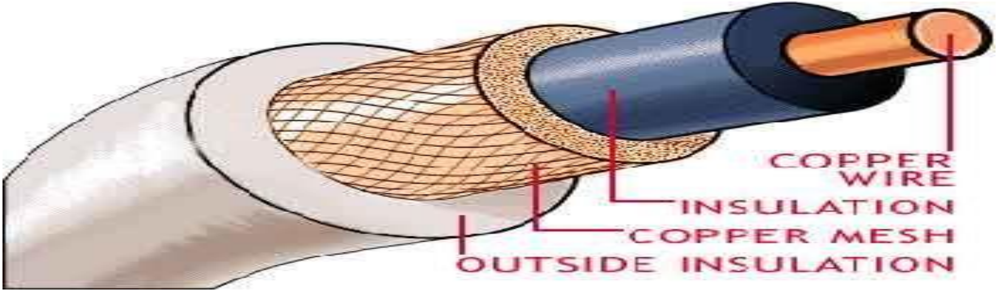


UTP Categories - Copper Cable

UTP Category	Data Rate	Max. Length	Cable Type	Application
CAT1	Up to 1Mbps	-	Twisted Pair	Old Telephone Cable
CAT2	Up to 4Mbps	-	Twisted Pair	Token Ring Networks
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Rink & 10BASE-T Ethernet
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1 Gbps	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT7	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)

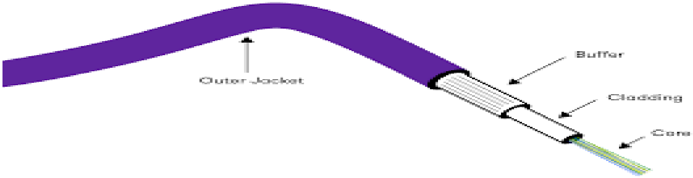
Firewall.cx
Routing Information & Expertise To Network Professionals

Coaxial Cable



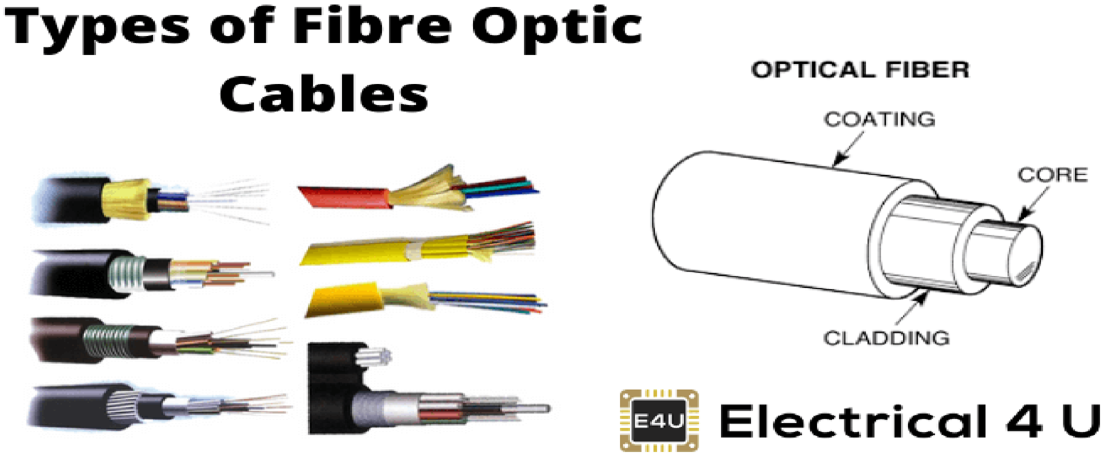
- Coax cables are shielded (less noise) and suffer less from attenuation
- Data rates of 500 mbps over several kilometers with a error probability of 10^{-7} achievable
- Widely used for cable television broadcast networks (which in some countries are heavily used for data communication today)

Fibre

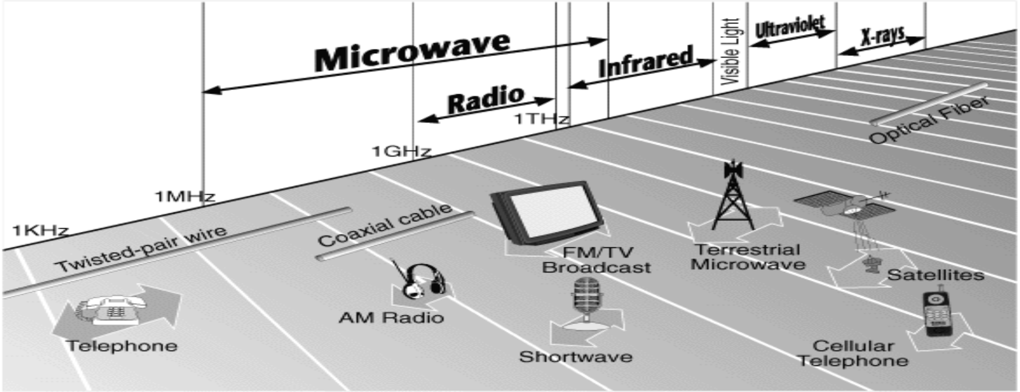


- The glass core is surrounded by a glass cladding with a lower index of refraction to keep the light in the core
- Multimode fiber have a thick core (20-50 micrometer) and propagate light using continued refraction
- Single-mode fiber have a thin core (2-10 micrometer) which guides the light through the fiber
- High data rates, low error probability, thin, lightweight, immune to electromagnetic interference

Fibre


Types of Fibre Optic Cables
OPTICAL FIBER
COATING
CORE
CLADDING
E4U
Electrical 4 U

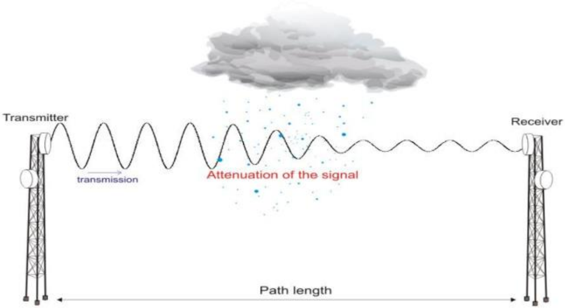
Electromagnetic Spectrum



- Usage of most frequencies is controlled by regulation
- The Industrial/Scientific/Medical (ISM) band (2400-2484 MHz) can be used without special licenses

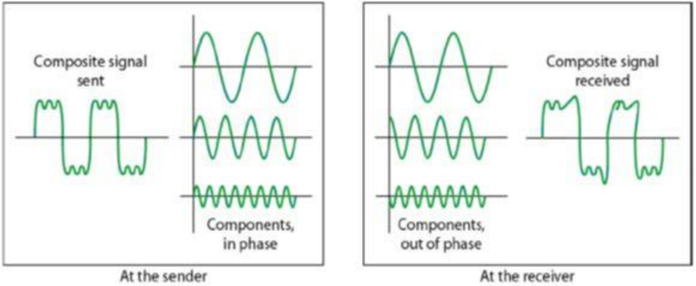
Transmission Impairments (1/3)

- *Attenuation*:
  - The strength of a signal falls off with distance over any transmission medium
  - For guided media, attenuation is generally an exponential function of the distance
  - For unguided media, attenuation is a more complex function of distance and the makeup of the atmosphere



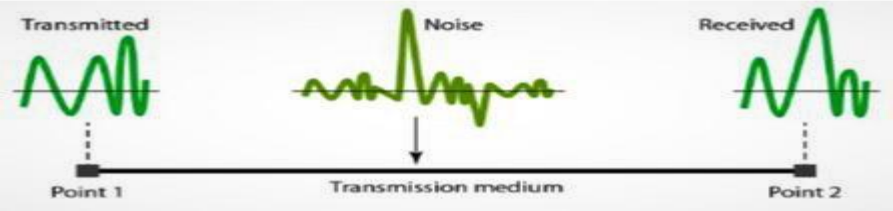
Transmission Impairments (2/3)

- *Delay distortion*:
  - Delay distortion occurs because the velocity of propagation of a signal through a guided medium varies with frequency
  - Various frequency components of a signal will arrive at the receiver at different times



Transmission Impairments (3/3)

- Noise
  - Thermal noise (white noise) is due to thermal agitation of electrons and is a function of temperature
  - Intermodulation noise can occur if signals at different frequencies share the same transmission medium
  - Crosstalk is an unwanted coupling between signal paths
  - Impulse noise consists of irregular pulses or noise spikes of short duration and of relatively high amplitude



Section 6: Media Access Control

4 Classification and Terminology

5 Communication Channels and Transmission Media

6 Media Access Control

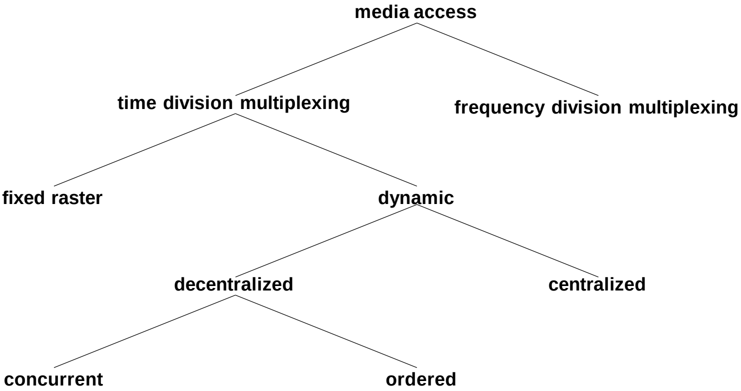
7 Transmission Error Detection

8 Sequence Numbers, Acknowledgements, Timer

9 Flow Control and Congestion Control

10 Layering and the OSI Reference Model

Media Access Control Overview



media access

time division multiplexing

frequency division multiplexing

fixed raster

dynamic

decentralized

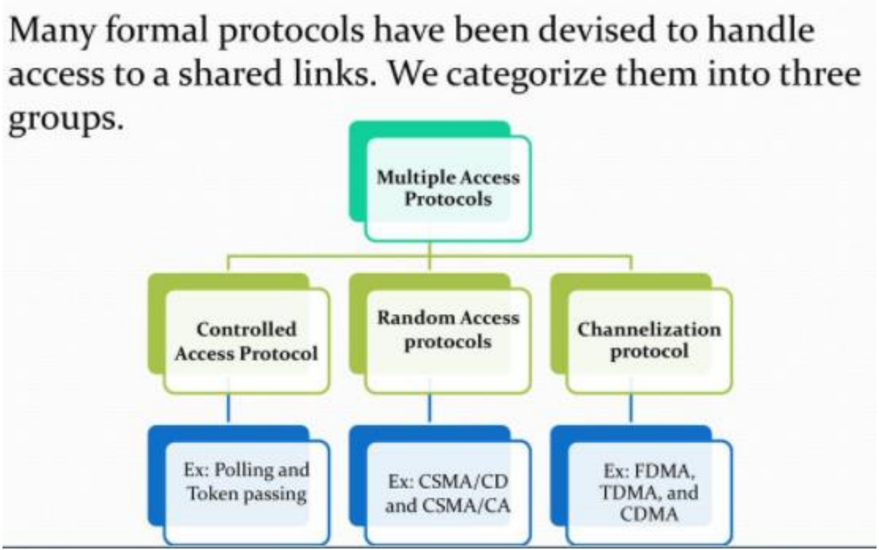
centralized

concurrent

ordered

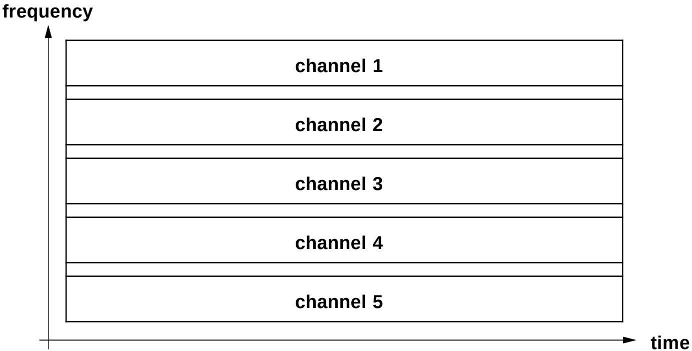
- Shared transmission media require coordinated access to the medium (media access control)

Media Access Control Overview



Many formal protocols have been devised to handle access to a shared links. We categorize them into three groups.

Frequency Division Multiplexing

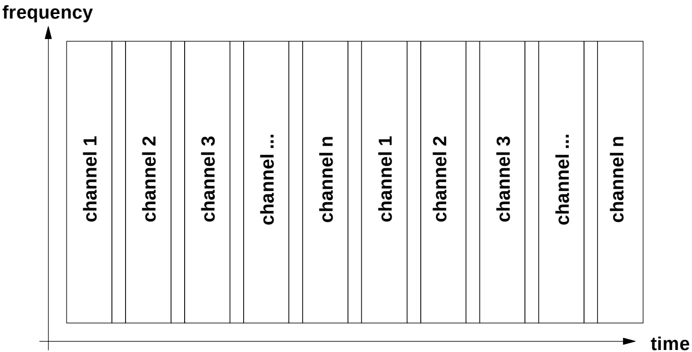


- Signals are carried simultaneously on the same medium by allocating to each signal a different frequency band

Wavelength Division Multiplexing

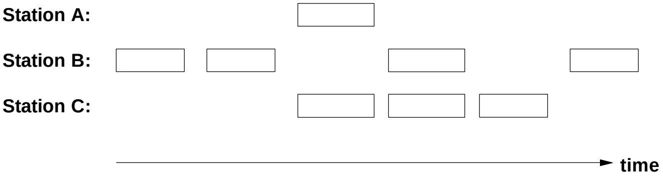
- Optical fibers carry multiple wavelength at the same time
- WDM can achieve very high data rates over a single optical fiber
- Dense WDM (DWDM) is a variation where the wavelengths are spaced close together, which results in an even larger number of channels.
- Theoretically, there is room for 1250 channels, each running at 10 Gbps, on a single fiber (= 12.5 Tbps).
- A single cable often bundles a number of fibers and for deployment or reasons, fibres are sometimes even bundled with power cables.

Time Division Multiplexing



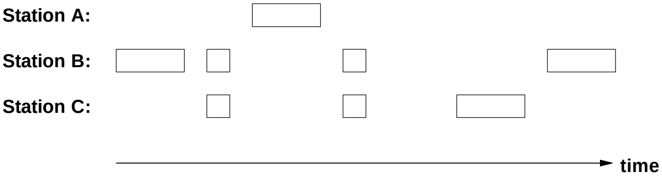
- Signals from a given sources are assigned to specific time slots
- Time slot assignment might be fixed (synchronous TDM) or dynamic (statistical TDM)

Carrier Sense Multiple Access



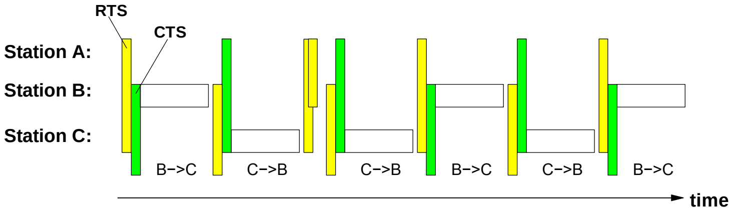
- Sense the media whether it is unused before starting a transmission
- Collisions are still possible (but less likely)
- 1-persistent CSMA: sender sends with probability 1
- p-persistent CSMA: sender sends with probability p
- non-persistent CSMA: sender waits for a random time period before it retries if the media is busy

CSMA with Collision Detection (CSMA-CD)



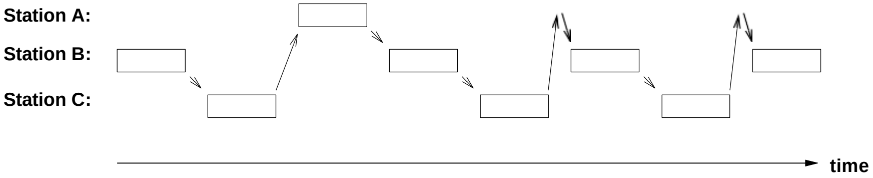
- Terminate the transmission as soon as a collision has been detected (and retry after some random delay)
- Let τ be the propagation delay between two stations with maximum distance
- Senders can be sure that they successfully acquired the medium after 2τ time units
- Used by the classic Ethernet developed at Xerox Parc

Multiple Access with Collision Avoidance



- A station which is ready to send first sends a short RTS (ready to send) message to the receiver
- The receiver responds with a short CTS (clear to send) message
- Stations who receive RTS or CTS must stay quiet
- Solves the *hidden station* and *exposed station* problem

Token Passing



- A token is a special bit pattern circulating between stations - only the station holding the token is allowed to send data
- Token mechanisms naturally match physical ring topologies - logical rings may be created on other physical topologies
- Care must be taken to handle lost or duplicate token

Section 7: Transmission Error Detection

4 Classification and Terminology

5 Communication Channels and Transmission Media

6 Media Access Control

7 Transmission Error Detection

8 Sequence Numbers, Acknowledgements, Timer

9 Flow Control and Congestion Control

10 Layering and the OSI Reference Model

Transmission Error

- Data transmission often leads to transmission errors that affect one or more bits
- Simple parity bits can be added to code words to detect bit errors
- Parity bit schemes are not very strong in detecting errors which affect multiple bits
- Computation of error check codes must be efficient (in hardware and/or software)

Cyclic Redundancy Check

- A bit sequence (bit block) $b_n b_{n-1} \dots b_1 b_0$ is represented as a polynomial $B(x) = b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0$
- Arithmetic operations:

$$0 + 0 = 1 + 1 = 0 \qquad 1 + 0 = 0 + 1 = 1$$

$$1 \cdot 1 = 1 \quad 0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$$

- A generator polynomial $G(x) = g_r x^r + \dots g_1 x + g_0$ with $g_r = 1$ and $g_0 = 1$ is agreed upon between the sender and the receiver
- The sender transmits $U(x) = x^r \cdot B(x) + t(x)$ with

$$t(x) = (x^r \cdot B(x)) \bmod G(x)$$

Cyclic Redundancy Check

- The receiver tests whether the polynomial corresponding to the received bit sequence can be divided by $G(x)$ without a remainder
- Efficient hardware implementation possible using XOR gates and shift registers
- Only errors divisible by $G(x)$ will go undetected
- Example:
  - Generator polynomial $G(x) = x^3 + x^2 + 1$ (corresponds to the bit sequence 1101)
  - Message M = 1001 1010 (corresponds to the polynomial $B(x) = x^7 + x^4 + x^3 + x$)

CRC Computation

```
1001 1010 000 : 1101
1101
----
 1001
 1101
 -----
  1000
  1101
  -----
   1011
   1101
   -----
     1100
     1101
     ----
        1000
        1101
        -----
          101    =>    transmitted bit sequence 1001 1010 101
```

CRC Verification

```
1001 1010 101 : 1101
1101
----
 1001
 1101
 -----
  1000
  1101
  -----
   1011
   1101
   -----
     1100
     1101
     ----
        1101
        1101
       -----
            0     =>    remainder 0, assume no transmission error
```

Internet Checksum

```
uint16_t
checksum(uint16_t *buf, int count)
{
    uint32_t sum = 0;
    while (count--) {
        sum += *buf++;
        if (sum & 0xffff0000) {  sum
            &= 0xffff;  sum++;
        }
    }
    return ~(sum & 0xffff);
}
```

Internet Checksum Computation

data[] = dead cafe face (hexadecimal)

```
     0000
+    dead (data[0])

     dead
+    cafe (data[1])

    1a9a
+   b  ’--
    >1
     a9ac
+    face (data[2])

    1a47
+   a  ’--
    >1
    -----          complement
     a47b     -------------> 5b84 (checksum)
```

verification:

```
      0000
+’    dead (data[0])
    ____________________
      dead
+’    cafe (data[1])
    ____________________
      a9ac
+’    face (data[2])

    ____________________
      a47b
+’    5b84 (checksum)
    ____________________
      ffff (test passed)
```

Internet Checksum Properties

- Summation is commutative and associative
- Computation independent of the byte order
- Computation can be parallelized on processors with word sizes larger than 16 bit
- Individual data fields can be modified without having to recompute the whole checksum
- Can be integrated into copy loop
- Often implemented in assembler or special hardware
- For details, see RFC 1071, RFC 1141, and RFC 1624

Section 8: Sequence Numbers, Acknowledgements, Timer

4 Classification and Terminology

5 Communication Channels and Transmission Media

6 Media Access Control

7 Transmission Error Detection

8 Sequence Numbers, Acknowledgements, Timer

9 Flow Control and Congestion Control

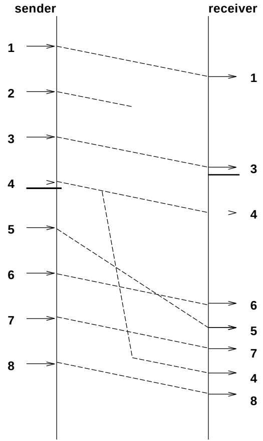
10 Layering and the OSI Reference Model

Errors Affecting Complete Data Frames

- Despite bit errors, the following transmission errors can occur
  - Loss of complete data frames
  - Duplication of complete data frames
  - Receipt of data frames that were never sent
  - Reordering of data frames during transmission
- In addition, the sender must adapt its speed to the speed of the receiver (*end-to-end flow control*)
- Finally, the sender must react to congestion situations in the network (*congestion control*)

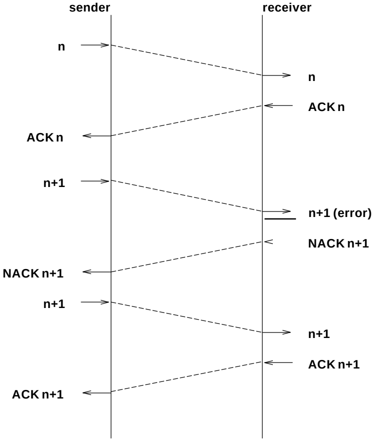
Sequence Numbers

- The sender assigns growing sequence numbers to all data frames
- A receiver can detect reordered or duplicated frames
- Loss of a frame can be determined if a missing frame cannot travel in the network anymore
- Sequence numbers can grow quickly on fast networks



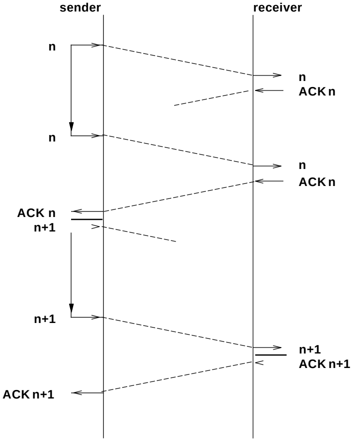
Acknowledgements

- Retransmit to handle errors
- A positive acknowledgement (ACK) is sent to inform the sender that the transmission of a frame was successful
- A negative acknowledgement (NACK) is sent to inform the sender that the transmission of a frame was unsuccessful
- Stop-and-wait protocol: a frame is only transmitted if the previous frame was been acknowledged



Timers

- Timer can be used to detect the loss of frames or acknowledgments
- A sender can use a timer to retransmit a frame if no acknowledgment has been received intime
- A receiver can use a timer to retransmit acknowledgments
- Problem: Timers must adapt to the current delay in the network



Section 9: Flow Control and Congestion Control

4 Classification and Terminology

5 Communication Channels and Transmission Media

6 Media Access Control

7 Transmission Error Detection

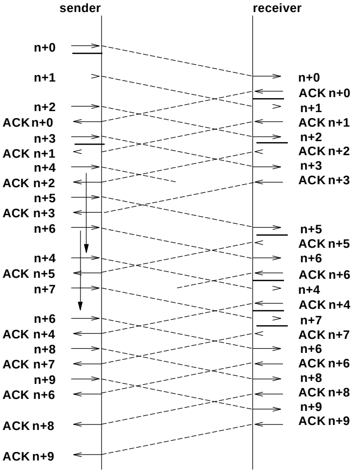
8 Sequence Numbers, Acknowledgements, Timer

9 Flow Control and Congestion Control

10 Layering and the OSI Reference Model

Flow Control

- Allow the sender to send multiple frames before waiting for acknowledgments
- Improves efficiency and overall delay
- Sender must not overflow the receiver
- The stream of frames should be smooth and not bursty
- Speed of the receiver can vary over time



Sliding Window Flow Control

- Sender and receiver agree on a window of the sequence number space
- The sender may only transmit frames whose sequence number falls into the sender's window
- Upon receipt of an acknowledgement, the sender's window is moved
- The receiver only accepts frames whose sequence numbers fall into the receiver's window
- Frames with increasing sequence number are delivered and the receiver window is moved.
- The size of the window controls the speed of the sender and must match the buffer capacity of the receiver

Sliding Window

- Implementation on the sender side:
  - SWS (send windowsize)
  - LAR (last ackreceived)
  - LFS (last framesend)
  - Invariant: LFS - LAR+ 1 ≤ SWS
- Implementation on the receiver side:
  - RWS (receiver windowsize)
  - LFA (last frameacceptable)
  - NFE (next frameexpected)
  - Invariant: LFA - NFE+ 1 ≤ RWS

Congestion

- Flow control is used to adapt the speed of the sender to the speed of the receiver
- Congestion control is used to adapt the speed of the sender to the speed of the network
- Principles:
  - Sender and receiver reserve bandwidth and puffer capacity in the network
  - Intermediate systems drop frames under congestion and signal the event to the senders involved
  - Intermediate systems send control messages (choke packets) when congestion builds up to slow down senders

Section 10: Layering and the OSI Reference Model

4 Classification and Terminology

5 Communication Channels and Transmission Media

6 Media Access Control

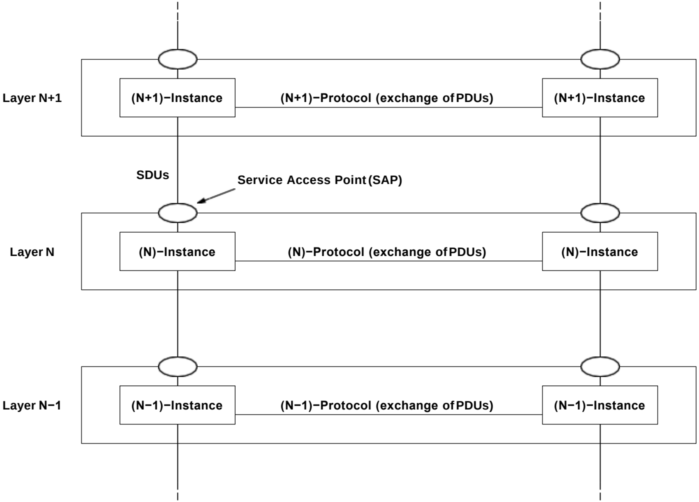
7 Transmission Error Detection

8 Sequence Numbers, Acknowledgements, Timer

9 Flow Control and Congestion Control

10 Layering and the OSI Reference Model

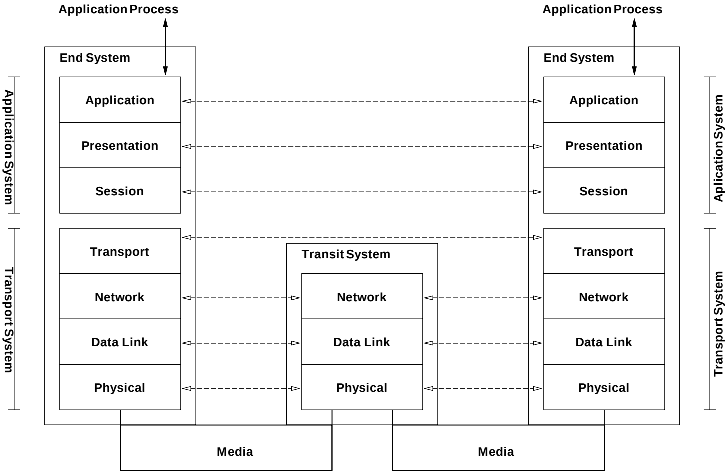
Layering


Layer N+1
(N+1)−Instance
(N+1)−Protocol (exchange of PDUs)
(N+1)−Instance
SDUs
Service Access Point (SAP)
Layer N
(N)−Instance
(N)−Protocol (exchange of PDUs)
(N)−Instance
Layer N−1
(N−1)−Instance
(N−1)−Protocol (exchange of PDUs)
(N−1)−Instance

Layering

- Principles:
  - A layer provides a well defined service
  - A layer (service) is accessed via a service access point (SAP)
  - Multiple different protocols may implement the same service
  - Protocol data units (PDUs) are exchanged between peer entities
  - Service data units (SDUs) are exchanged between layers (services)
  - Every service access point (SAP) needs an addressing mechanism
- Advantages:
  - Information hiding and reuse
  - Independent evolution of layers
- Disadvantages:
  - Layering hinders certain performance optimizations
  - Tension between information-hiding (abstraction) and performance

OSI Reference Model



Physical and Data Link

- Physical Layer:
  - Transmission of an unstructured bit stream
  - Standards for cables, connectors and sockets
  - Encoding of binary values (voltages, frequencies)
  - Synchronization between sender and receiver
- Data Link Layer:
  - Transmission of bit sequences in so called frames
  - Data transfer between directly connected systems
  - Detection and correction of transmission errors
  - Flow control between senders and receivers
  - Realization usually in hardware

Network and Transport

- Network Layer:
  - Determination of paths through a complex network
  - Multiplexing of end-to-end connections over intermediate systems
  - Error detection / correction between network nodes
  - Flow and congestion control between end systems
  - Transmission of datagrams or packets in packet switched networks
- Transport Layer:
  - Reliable/unreliable and ordered/unordered end-to-end communication channels
  - Connection-oriented and connection-less services
  - End-to-end error detection and correction
  - End-to-end flow and congestion control

Session, Presentation and Application

- Session Layer:
  - Synchronization and coordination of communicating processes
  - Interaction control (check points and restarts)
  - Today often used to provide security services
- Presentation Layer:
  - Harmonization of different data representations
  - Serialization of complex data structures
  - Data compression, data integrity services
- Application Layer:
  - Service primitives supporting classes of applications
  - Terminal emulationen, name and directory services, database access, network management, electronic messaging systems, process and machine control, *. . .*

Referenc

J. F. Kurose and K. W. Ross.
Computer Networking: A Top-Down Approach Featuring the Internet.
Addison-Wesley, 3 edition, 2004.

A. S. Tanenbaum.
Computer Networks.
Prentice Hall, 4 edition, 2002.

J. Stone and C. Partridge.
When The CRC and TCP Checksum Disagree.
In *Proc. SIGCOMM 2000*, pages 309–319, Stockholm, August 2000. ACM.