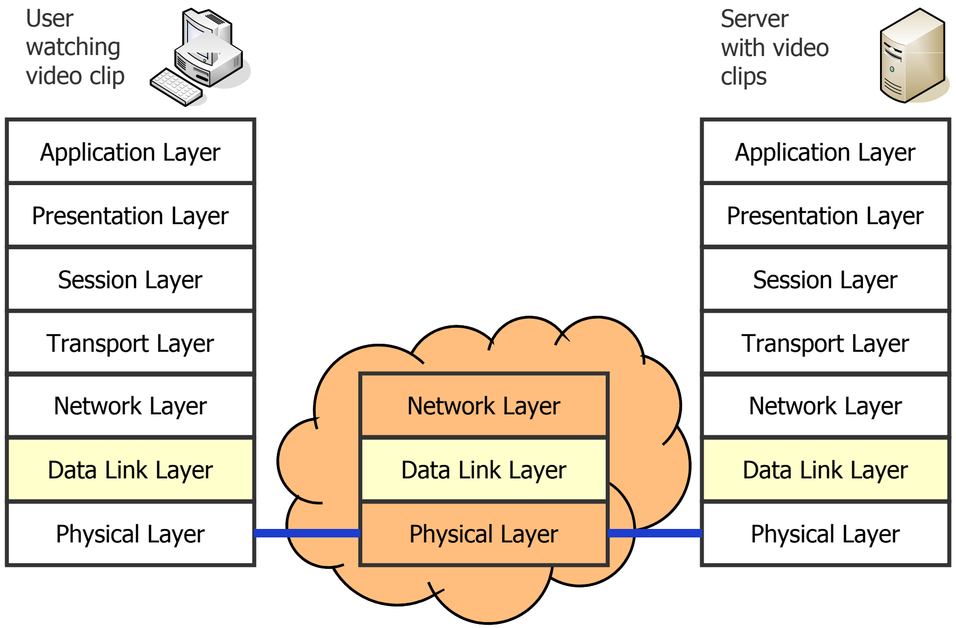
Telematics

Chapter 5: Medium Access Control Sublayer



Prof. Dr. Mesut Güneş

Computer Systems and Telematics (CST)

Distributed, embedded Systems

Institute of Computer Science

Freie Universität Berlin

http://cst.mi.fu-berlin.de

Contents

- Design Issues
- Network Topologies
- The Channel Allocation Problem
- Multiple Access Protocols
- Ethernet
- IEEE 802.2 – Logical Link Control
- Token Bus
- Token Ring
- Fiber Distributed Data Interface
- Structured Cabling
- Metropolitan Area Networks (MAN)
- Wide Area Networks (WAN)
- Frame Relay
- ATM
- SDH
- Network Infrastructure
- Virtual LANs

Design Issues

Design Issues

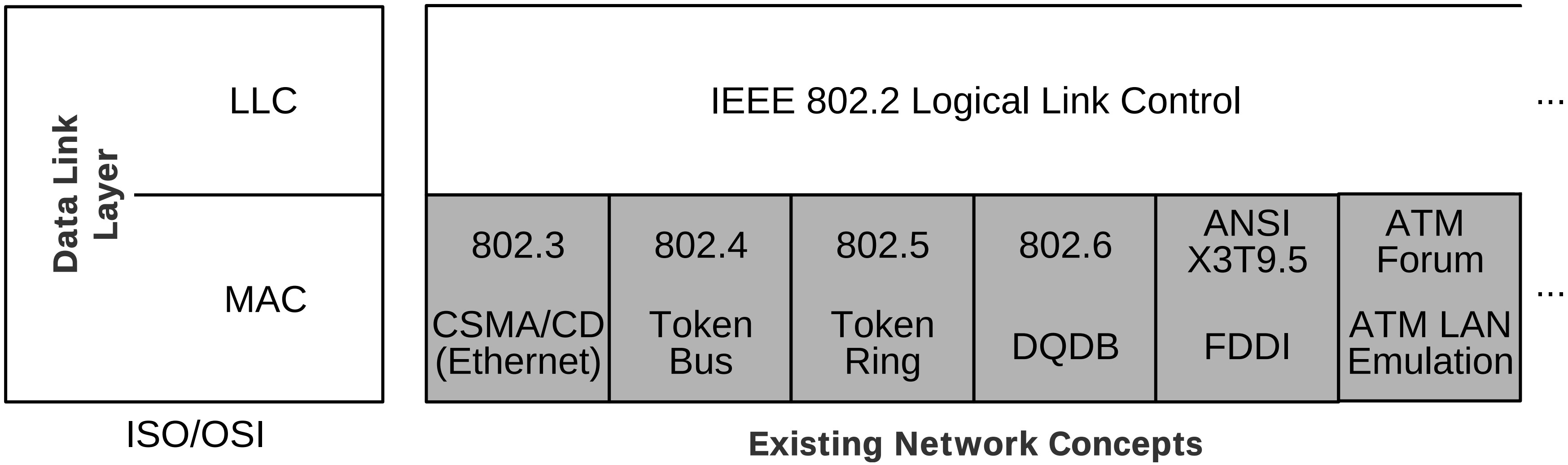
- Two kinds of connections in networks
  - Point-to-point connections
  - Broadcast (Multi-access channel, Random access channel)
- In a network with broadcast connections
  - Who gets the channel?
- Protocols used to determine who gets next access to the channel
  - Medium Access Control (MAC) sublayer

OSI Reference Model

OSI Reference Model
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Network Types for the Local Range

- **LLC layer**: uniform interface and same frame format to upper layers
- **MAC layer**: defines medium access



Both concepts are implemented together in existing networks (as a device driver):

1. **Packing of data into frames:** error detection during frame transmission and receipt
2. **Media Access Control:** this contains the frame transmission and the reaction to transmission errors

Standardization: IEEE

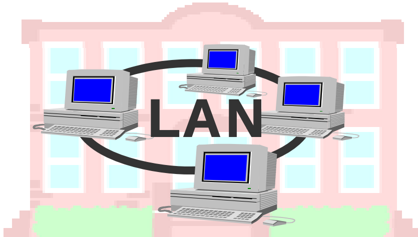
- **Institute of Electrical and Electronic Engineers (IEEE)**
  - Standardization of the IEEE 802.X-Standards for Local Area Networks (www.ieee802.org)

www.ieee.org

- 802.1 Overview and Architecture of LANs
- 802.2 Logical Link Control (LLC)
- 802.3 CSMA/CD (Ethernet)
- 802.4 Token Bus
- 802.5 Token Ring
- 802.6 DQDB (Distributed Queue Dual Bus)
- 802.7 Broadband Technical Advisory Group (BBTAG)
- 802.8 Fiber Optic Technical Advisory Group (FOTAG)
- 802.9 Integrated Services LAN (ISLAN) Interface
- 802.10 Standard for Interoperable LAN Security (SILS)
- 802.11 Wireless LAN (WLAN)
- 802.12 Demand Priority (HP's AnyLAN)
- 802.14 Cable modems
- 802.15 Personal Area Networks (PAN, Bluetooth)
- 802.16 Wireless MAN
- 802.17 Resilient Packet Ring
- 802.18 Radio Regulatory Technical Advisory Group (RRTAG)
- 802.19 Coexistence Technical Advisory Group
- 802.20 Mobile Broadband Wireless Access (MBWA)
- 802.21 Media Independent Handover

Network Categories

- Local Area Networks (LAN): 10m - few km, simple connection structure
  - Ethernet/Fast Ethernet/Gigabit Ethernet/10Gigabit Ethernet
  - Token Bus, Token Ring
  - FDDI (up to 100 km, belongs to LANs nevertheless)
  - Wireless LAN (WLAN, up to a few 100 m)

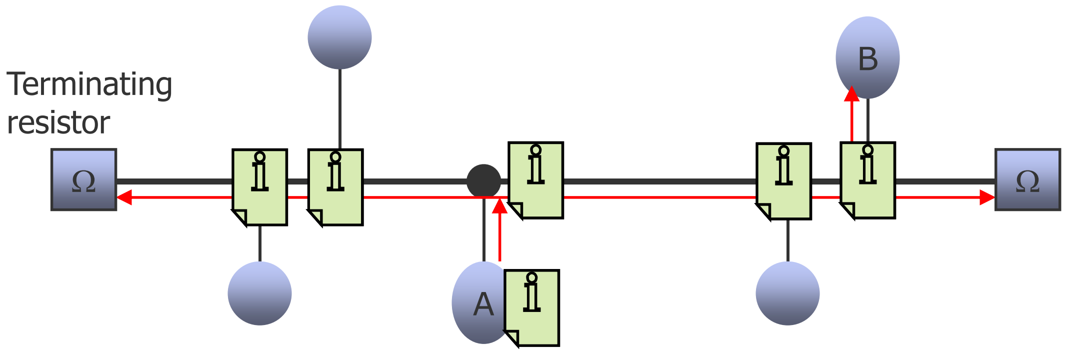


- Metropolitan Area Network (MAN): 10 - 100 km, city range
  - DQDB
  - FDDI II
  - Resilient Packet Ring
  - [also used: Gigabit Ethernet]

- Wide Area Networks (WAN): 100 – 10,000 km, interconnection of subnetworks
  - Frame Relay
  - ATM
  - SDH

Network Topologies

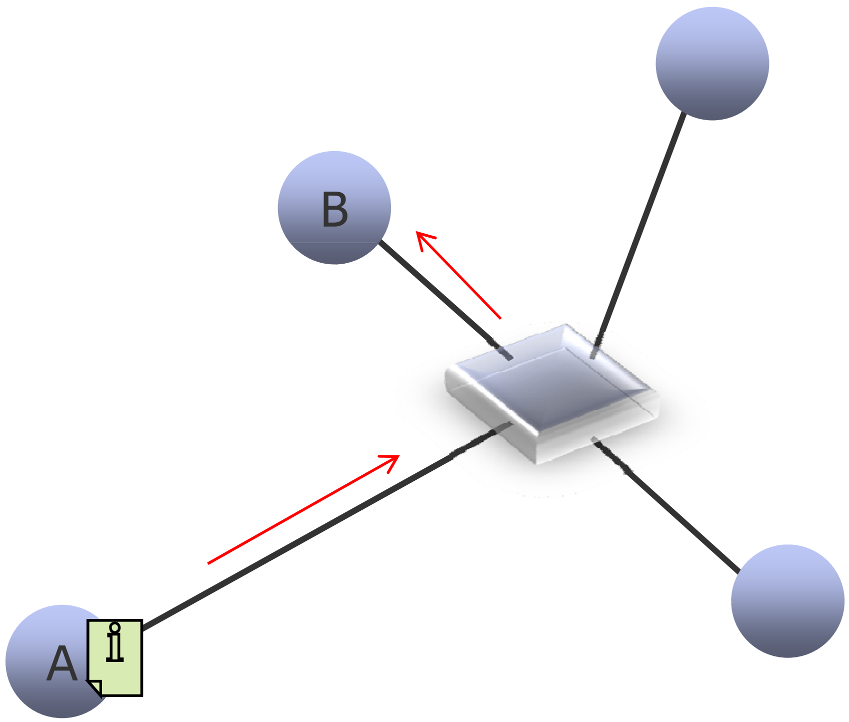
Bus



Example: **Ethernet**

- Bus
  - Broadcast Network: if station A intends to send data to station B, the message reaches all connected stations. Only station B processes the data, all other stations ignore it.
  - Passive coupling of stations
  - Restriction of the extension and number of stations to connected
  - Simple, cheap, easy to connect new stations
  - The breakdown of a station does not influence the rest of the network

Star

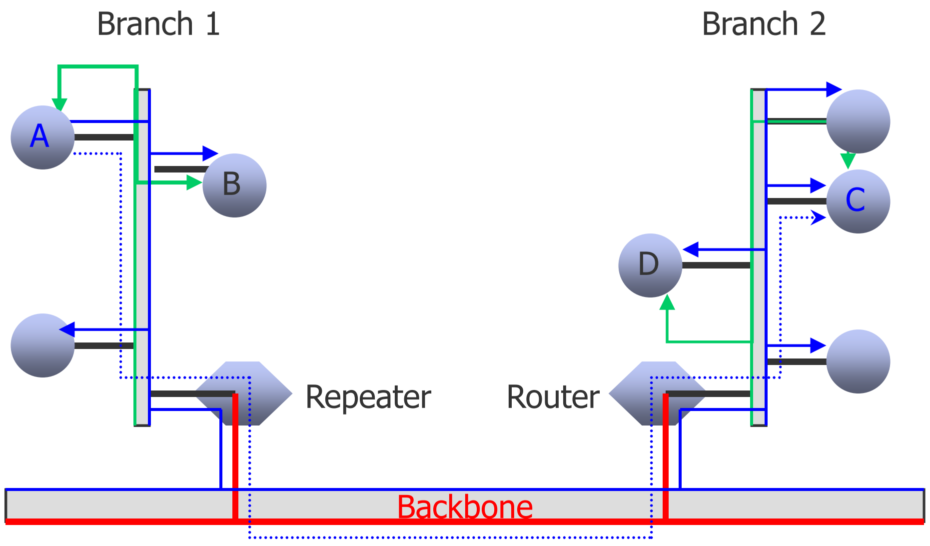


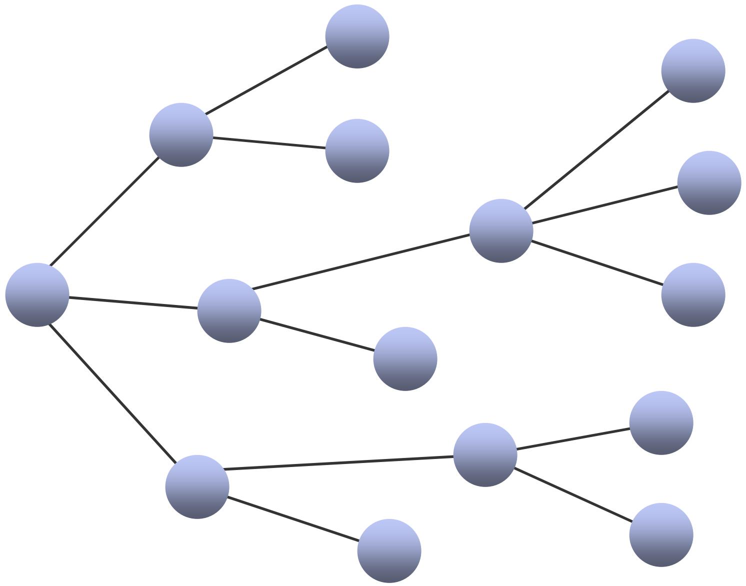
Example: **Fast Ethernet**

- Star
  - Designated computer as central station: a message of station A is forwarded to station B via the central station
  - Broadcast network (Hub) or point-to-point connections (Switch)
  - Expensive central station
  - Vulnerability through central station (Redundancy possible)
  - N connections for N stations
  - Easy connection of new stations

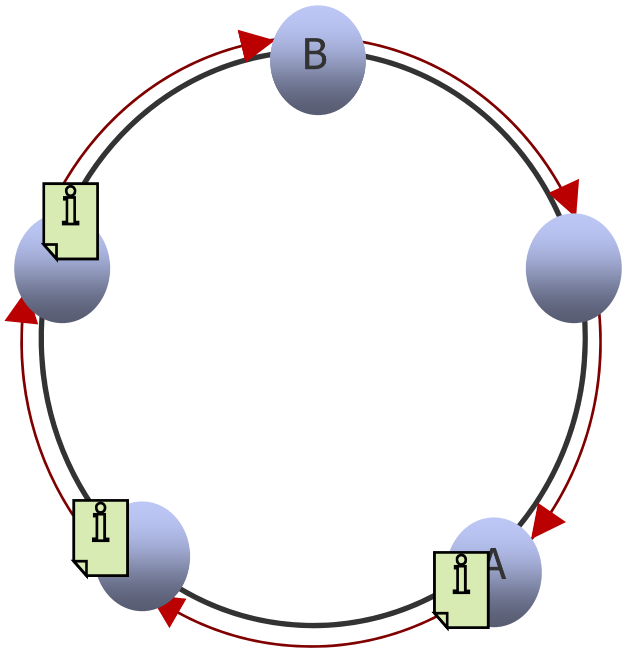
Tree

- Tree
  - Topology: Connection of several busses or stars
  - Branching elements can be active (Router) or passive (Repeater)
  - Bridging of large distances
  - Adaptation to given geographical structure
  - Minimization of the cable length possible





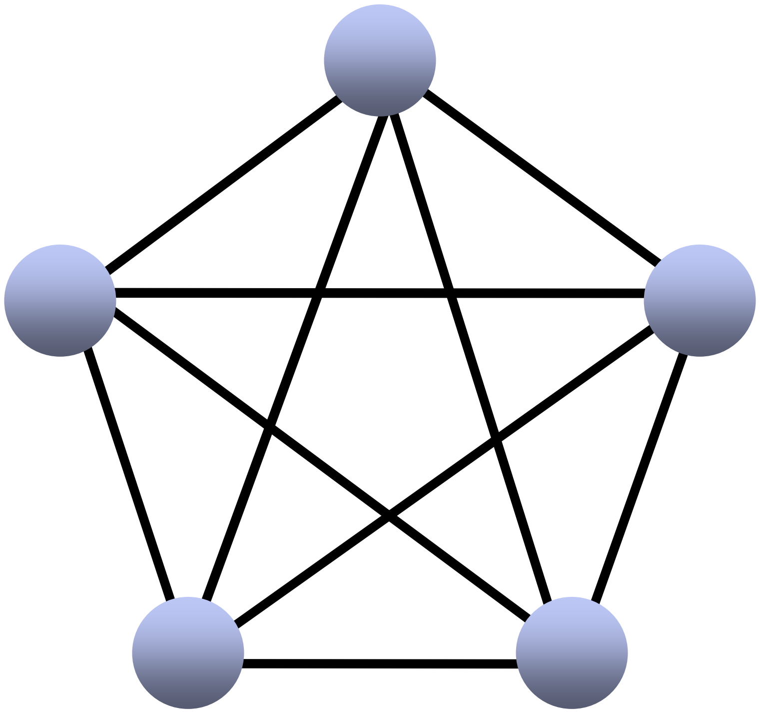
Ring



Example: **Token Ring, FDDI**

- Ring
  - Broadcast Network
  - Chain of point-to-point connections
  - Active stations: messages are regenerated by the stations (Repeater)
  - Breakdown of the whole network in case of failure of one single station or connection
  - Large extent possible
  - Easy connection of new stations
  - Only N connections for N stations
  - Variant: bidirectional ring
    - stations are connected by two opposed rings

Meshed Networks

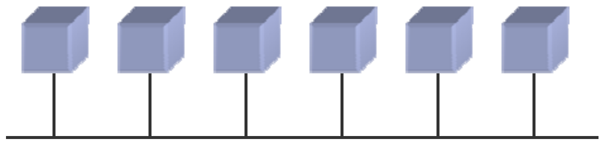


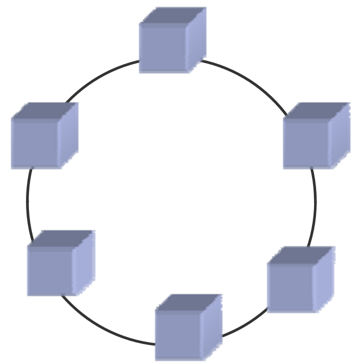
- Fully Meshed Network
  - Point-to-Point connections between all stations
  - For N stations $\frac{N(N-1)}{2}$ connections are needed
  - Connecting a new station is a costly process
  - Redundant paths
  - Maximal connection availability through routing integration

Partly meshed network: cheaper, but routing, flow control, and congestion control become necessary (Wide Area Networks)

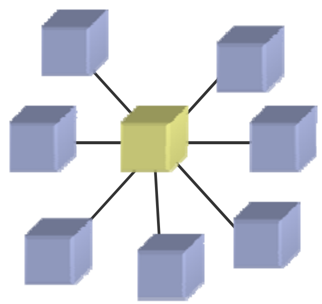
Examples

- Ethernet (IEEE 802.3, 10 Mbps)
  - originally the standard network
  - available in an “immense number” of variants





- Token Ring (IEEE 802.5, 4/16/100 Mbps)
  - for a long time the Ethernet competitor
  - extended to FDDI (Fiber Distributed Data Interface)
- Fast Ethernet (IEEE 802.3u, 100 Mbps)
  - at the moment the most widely spread network
  - extension of Ethernet for small distances

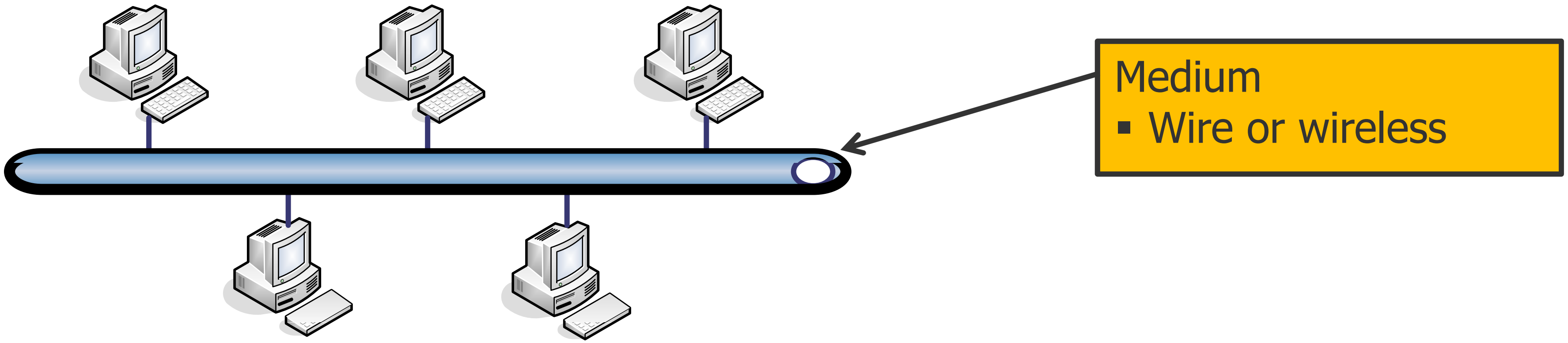


- Gigabit Ethernet (IEEE 802.3z, 1000 Mbps)
  - very popular at the moment; 10 Gbps are already in the planning phase at the moment

The Channel Allocation Problem

The Channel Allocation Problem

- The channel allocation problem
  - Given N independent stations which want to communicate over a single channel
  - Organize the sending order of the stations

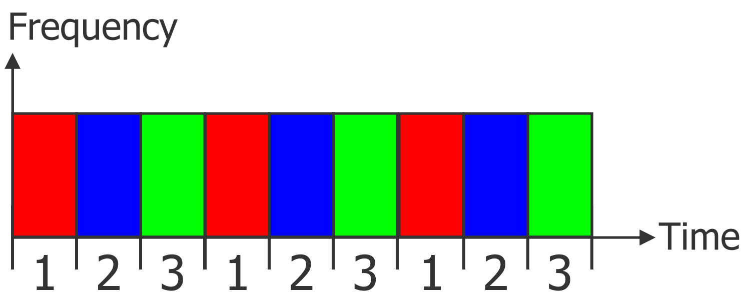


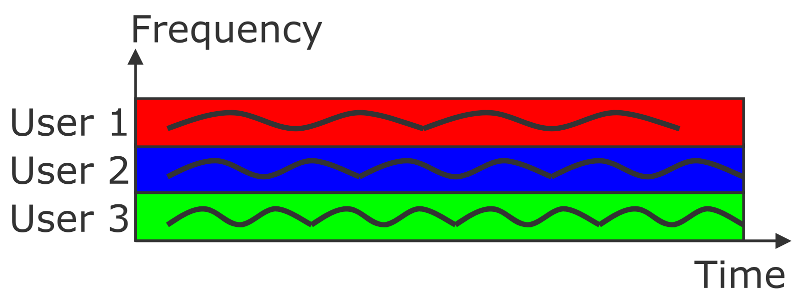
- Approaches
  - Static channel allocation
    - Simple procedures
  - Dynamic channel allocation
    - Complex procedure, that adapt to changes

Static Channel Allocation

- Time Division Multiple Access (**TDMA**)
  - Each user gets the **entire** transmission capacity for a fixed time interval
  - Baseband transmission

- Frequency Division Multiple Access (**FDMA**)
  - Each user gets a **portion** of the transmission capacity for the whole time
    - Frequency range
  - Broadband transmission





Static Channel Allocation

- Problems with static channel allocation
  - Works only for a fixed number of users
    - When number of users change, the allocation scheme does not work
  - Data traffic is very often bursty, i.e., long time no data and for a short time high data
  - Thus, users do not use their allocated channel capacity
  - ➡ Most of the channels will be idle most of the time

➡ **Dynamic Channel Allocation**

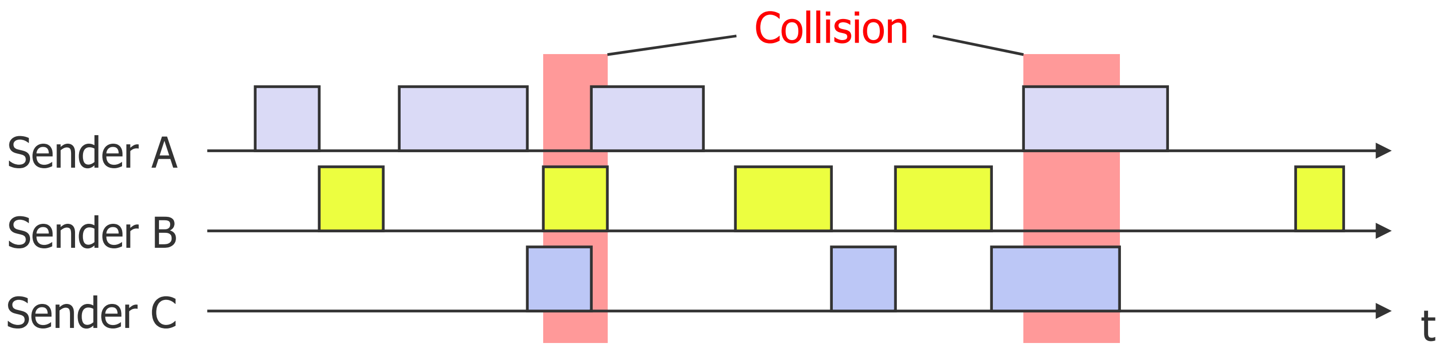
Dynamic Channel Allocation

- Assumptions on **dynamic** channel allocation
  - Station Model:
    - There are N independent stations (computers) that generate frames for transmission.
  - Single channel
    - A single channel is available for communication and all stations can transmit and receive on it.
  - Collisions
    - If two frames are transmitted simultaneously, they overlap and the signals are garbled.
  - Time
    - Continuous time: No master clock, transmission of frames can begin at anytime.
    - Slotted time: Time is divided into discrete intervals called slots. Frame transmissions begin always at the start of a slot.
  - Sensing of the medium
    - Carrier sense: Stations can sense channel and tell whether it is busy. If so, stations do not start with transmissions.
    - No carrier sense: Stations can not sense the channel.

Multiple Access Protocols

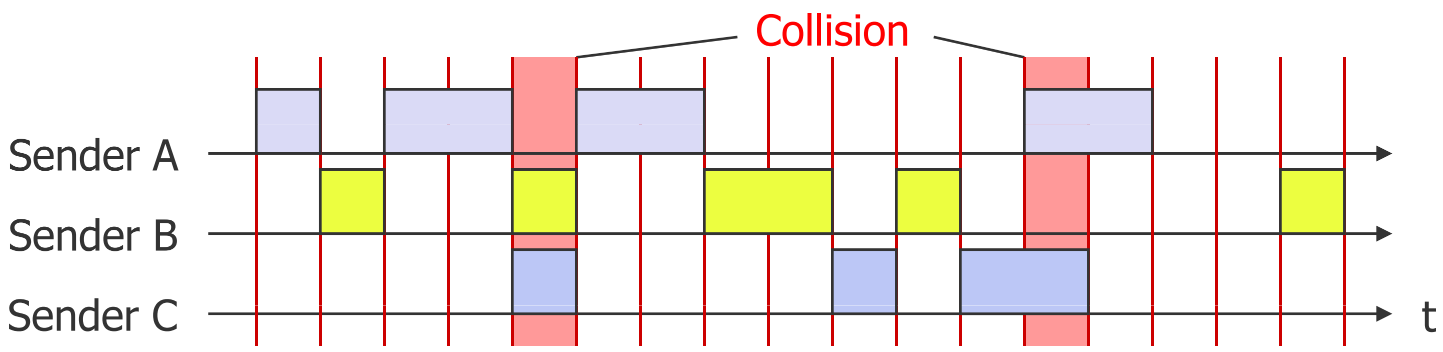
Multiple Access Protocols: ALOHA

- Best known protocol: ALOHA
  - Developed on the Hawaiian islands in 1970s: stations are connected by a satellite
  - Very simple principle, no coordination:
    - Stations are sending completely uncoordinated (random), all using the same frequency
    - When two (or more) stations are sending at the same time, a collision occurs: both messages are destroyed. Problem: collisions occur even with very small overlaps!
      - **Vulnerability period:** 2 times the length of a frame
    - When a collision occurs, frames are repeated after a random time
    - Problem: since traffic runs over a satellite a sender only hears after a very long time whether the transmission was successful or not.



Multiple Access Protocols: ALOHA

- Problem with ALOHA: even small overlaps result in transmission conflicts. Therefore, often collisions arise causing many repetitions:
  - No guaranteed response times
  - Low throughput
- Improvement: Slotted ALOHA
  - The time axis is divided into **time slots** (similar to TDMA, but time slots are not firmly assigned to stations)
  - The transmission of a block has to start at the beginning of a time slot
    - Fewer collisions, **vulnerability period of one frame length**
  - But: the stations must be synchronized!



Multiple Access Protocols: ALOHA

- Performance of ALOHA
  - Assumptions
    - Infinite number of interactive users generating data
      - In fact data is generated according to a Poisson distribution X with mean G frames/s
    - Collided frames are also retransmitted
    - Probability of k transmission trials per frame time is according to a Poisson distribution with mean G

$$P(X = k) = \frac{G^k}{k!} e^{-G} \quad \text{with} \quad G = \lambda t$$

  - Throughput (S) is given by the load (G) and the probability of a successful transmission (P_0)

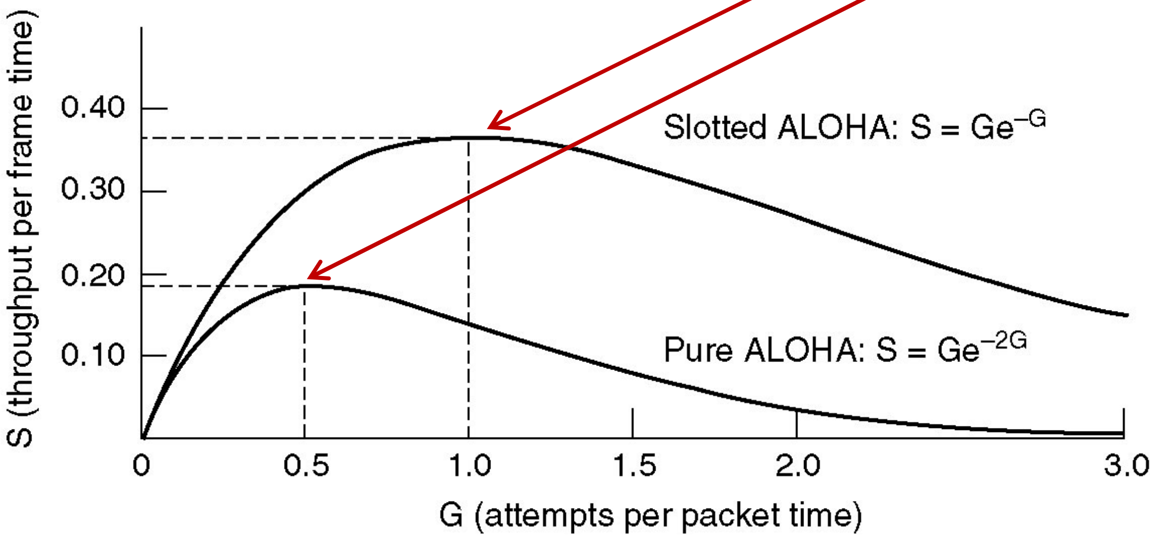
$$S = G\, P_0$$

  - What is a successful transmission?
    - A frame is transmitted successful if no other frames are sent within one frame time of its start

Multiple Access Protocols: ALOHA

- Probability of zero frames is: $P(X=0)=\frac{G^0}{0!}e^{-G}=e^{-G}$
- Collision time
  - ALOHA: $2t$
  - Slotted ALOHA: t
- Throughput
  - ALOHA: $S = G\ P_0 = \mathrm{G\ e}^{-2G}$
  - Slotted ALOHA: $S = G\ P_0 = \mathrm{G\ e}^{-G}$

Maximum
- Slotted ALOHA ~36%
- ALOHA ~18%



Multiple Access Protocols: CSMA

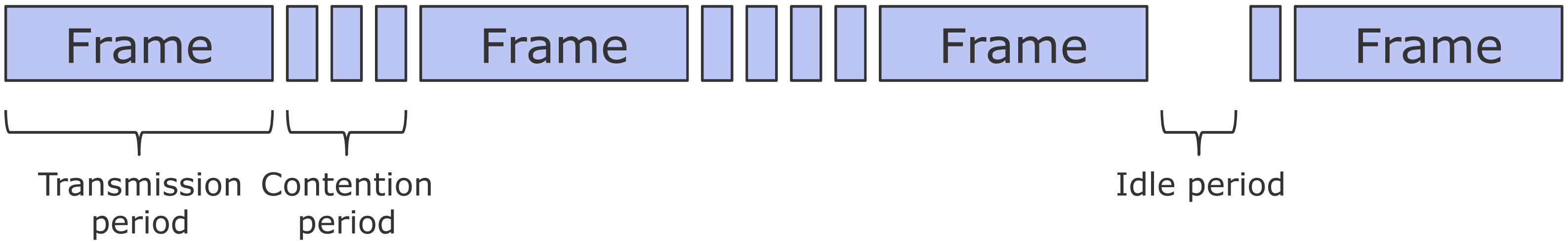
- Variant of ALOHA for networks with small distances exists
  - Similar to ALOHA: no coordination of the stations
  - But: each station which wants to send first examines whether already another station is sending
  - If nobody sends, the station begins to send (**Carrier Sense Multiple Access, CSMA**)
  - Notice: this principle only works with networks having a short transmission delay
    - Application of this principle for satellite systems is not possible, because there would be no chance to know whether a conflict occurred before the end of the transmission
  - Advantages: simple, because no master station and no tokens are needed; nevertheless good utilization of the network capacity
  - Disadvantage: no guaranteed medium access, a large delay up to beginning a transmission is possible

Multiple Access Protocols: CSMA

- Persistent and Nonpersistent CSMA
  - 1-persistent CSMA
    - When a station has data to send, it first listens to the channel.
    - If channel busy, the station waits until it becomes idle.
    - When channel is idle, station transmits a frame.
    - When a collision occurs, the station waits a random amount of time and starts all over again.
    - 1-persistent = station transmits with probability of one if channel idle
  - Nonpersistent CSMA
    - When channel is busy, it waits a random time, and repeats
  - p-persistent CSMA
    - Applied in slotted channels (slotted ALOHA)
    - If channel idle, station transmits with probability p in current slot and with probability $(1-p)$ it defers until next slot
    - If next slot is idle, the station again transmits with probability p and defers with $(1-p)$

Multiple Access Protocols: CSMA

- CSMA with Collision Detection: CSMA/CD
  - Basis of Ethernet
  - A station who detects a collision stops immediately transmitting
  - Afterwards it waits a random time and tries again



Multiple Access Protocols

Collision-Free Protocols

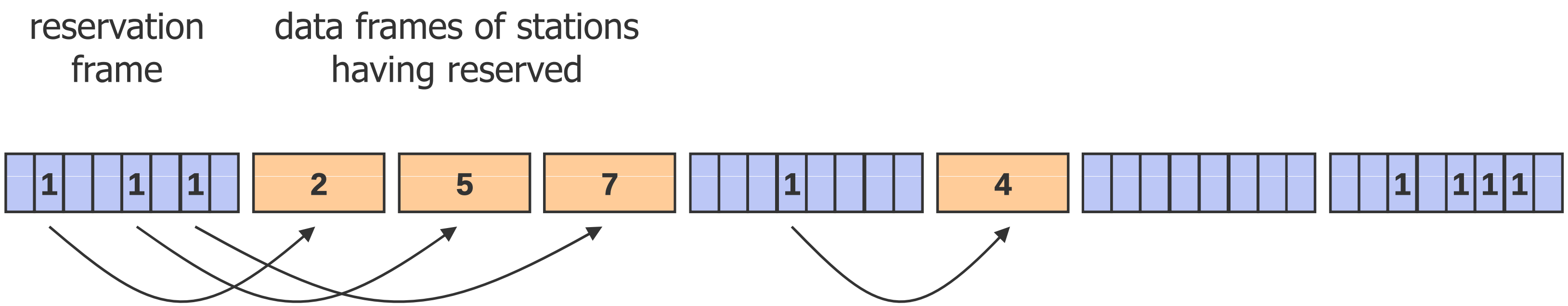
Collision-Free Protocols: Reservation Protocols

- Communication follows in a two-phase scheme (alternating phases)
  - Phase 1: Reservation
    - In the reservation phase the sender makes a reservation by indicating the wish to send data (or even the length of the data to be sent)
  - Phase 2: Transmission
    - In the transmission phase the data communication takes place (after successful reservation)
  - Advantage: very efficient use of the capacity
  - Disadvantage:
    - Delay by two-phase procedure
    - Often a master station is needed, which cyclically queries all other stations whether they have to send data. The master station assigns sending rights.

- Techniques for “easy” reservation without master station:
  - Explicit reservation
  - Implicit reservation

Collision-Free Protocols: Bit-Map Protocol

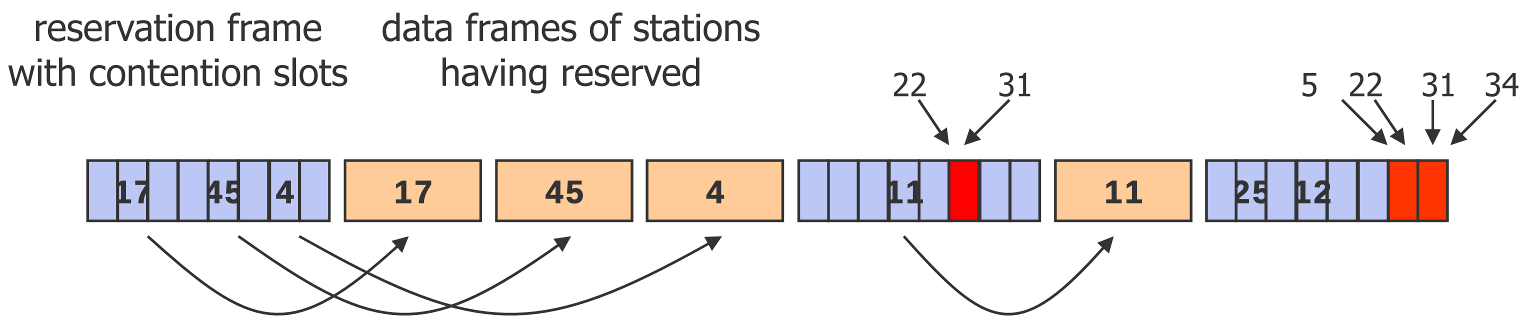
- Uses two frame types:
  - reservation frame (very small) in the first phase
  - data frame (constant length) in the second phase
- **Variant 1: Without contention**
  - Only suitable for small number of users
  - Each user i is assigned the i-th slot in the reservation frame. If it wants to send data, it sets the i-th bit in the reservation frame to 1.
  - After the reservation phase, all stations having set their reservation bit can send their data in the order of their bits in the reservation frame.



This procedure is called **Bit-Map Protocol**

Collision-Free Protocols: Bit-Map Protocol

- **Variant 2: With contention**
  - For higher number of users
  - The reservation frame consists of a limited number of contention slots (smaller than the number of participating stations)
  - Users try to get a contention slot (and by that make a reservation for a data slot) by random choice, writing their station number into a slot
  - If there is no collision in the reservation phase, a station may send.



Collision-Free Protocols: Implicit Reservation

- Implicit reservation scheme
  - No reservation slots, only data slots of certain length.
  - A window consists of N data slots, window is cyclically repeated
  - The duration of the window must be longer than the round-trip time
- Procedure:
  - A station which wants to send observes N slots without doing anything and marks the slots as follows:
    - 0, if the slot is empty or collided
    - 1, if the slot is used by somebody else
  - In the following window the station randomly chooses one of the slots marked with 0 (Simplification: choose the first slot marked with "0")
  - Two cases:
    - conflict: try again
    - successful transmission: slot reserved for the station as long as it sends data. If the station is not using its slot in one window, the reservation is dismissed.

Collision-Free Protocols: Implicit Reservation

Example: 8 data slots, Stations A - F

Reservation	Slots:	1	2	3	4	5	6	7	8
	Window 1								
	Window 2	A	C	D	A	B	A	**B/D**	F
ACDABA-F	Window 3	A	C		A	B	A		
AC-ABA--	Window 4	A		**B/F**		B	A	F	
A---BAF-	Window 5	A				B	A	F	D
A---BAFD	Window 6	A	C	E	E	B	A	F	D

t

Stations observing 8 slots

Collision within slot 7; the other slots are reserved

Collision-Free Protocols: Binary Countdown

- Binary Countdown
  - For large number of stations
  - Binary station addresses, all addresses to be the same length
  - A station wanting to use the channel broadcasts its address as a binary string starting with the high-order bit
  - The bits from different stations are ORed
  - As soon as a station sees that a high-order bit position that is 0 in its address has been overwritten to a 1, gives up
  - Example: four stations with addresses 0010, 0100, 1001, 1010

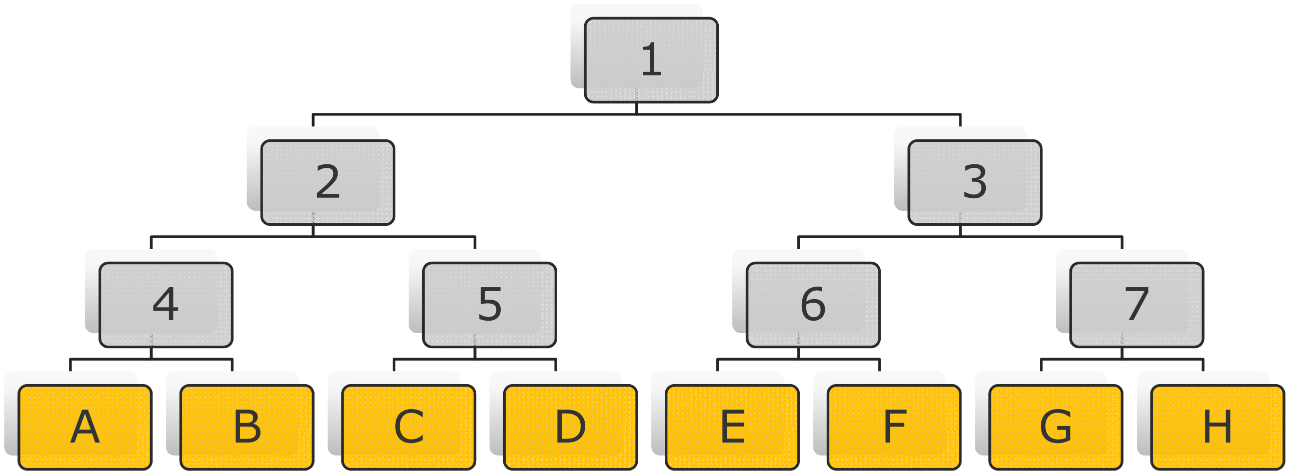
	Bit time			
Stations	0	1	2	3
0010	0			
0100	0			
1001	1	0	0	
1010	1	0	1	0
Result	**1**	**0**	**1**	**0**

Multiple Access Protocols

Limited Contention Protocols

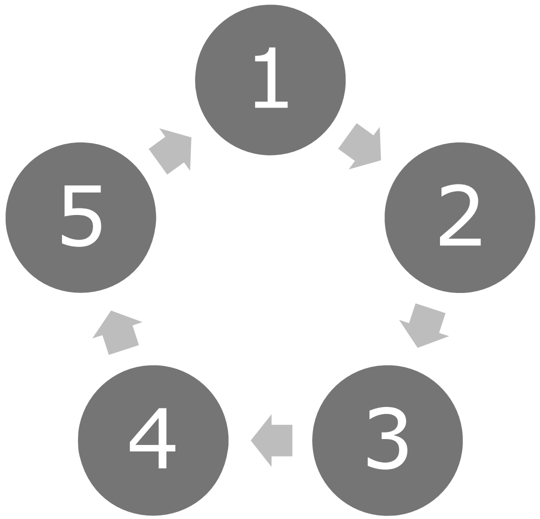
Limited Contention Protocols: Adaptive Tree Walk

- Adaptive Tree Walk Protocol
  - Stations are the leaves of a binary tree
  - In the first contention slot following a successful frame, slot 0, all stations (A-H) are permitted to try to acquire the channel
  - If collision, during slot 1 only stations under node 2 (A-D) may compete
    - If one gets the channel, next slot is reserved for stations under node 3 (E-H)
    - If collision, during slot 2, only stations under node 4 (A, B)



Coordination by using a Token

- Introduction of a token (determined bit sequence)
  - Only the owner of the token is allowed to send
  - Token is cyclically passed on between all stations
    - particularly suitable for ring topologies
    - Token Ring (4/16/100 Mbps)



Passing on of the token

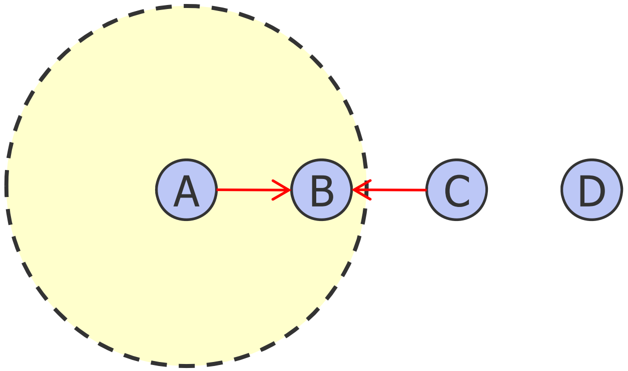
- Characteristics
  - Guaranteed accesses, no collisions
  - Very good utilization of the network capacity, high efficiency
  - Fair, guaranteed response times
  - Possible: multiple tokens
  - But: complex and expensive

Multiple Access Protocols

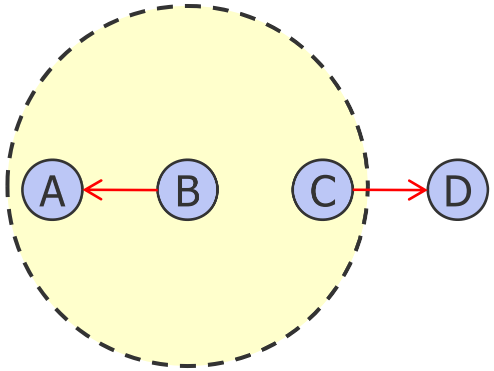
MAC for Wireless Networks

MAC for Wireless LANs

- MAC for Wireless LANs
  - Carrier Sense Multiple Access (CSMA) does not work
  - Problem: interference at the receiver



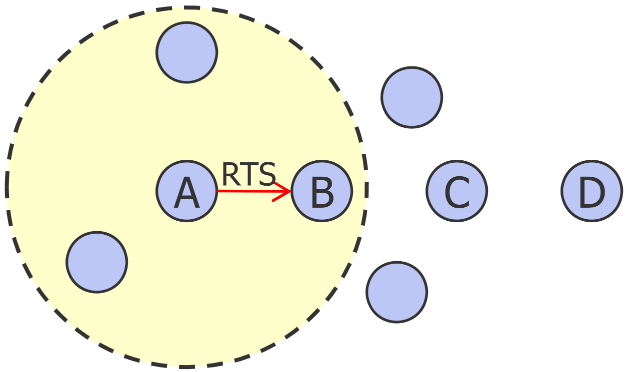
Hidden Station Problem

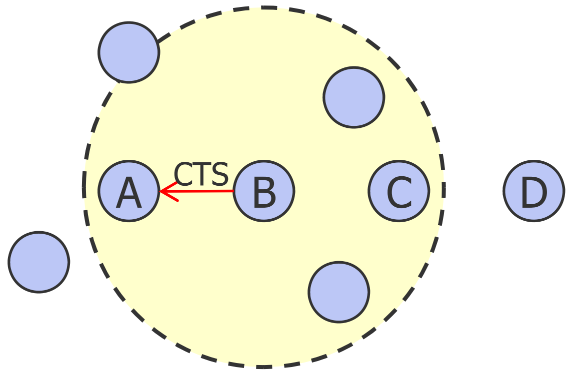


Exposed Station Problem

MAC for Wireless LANs

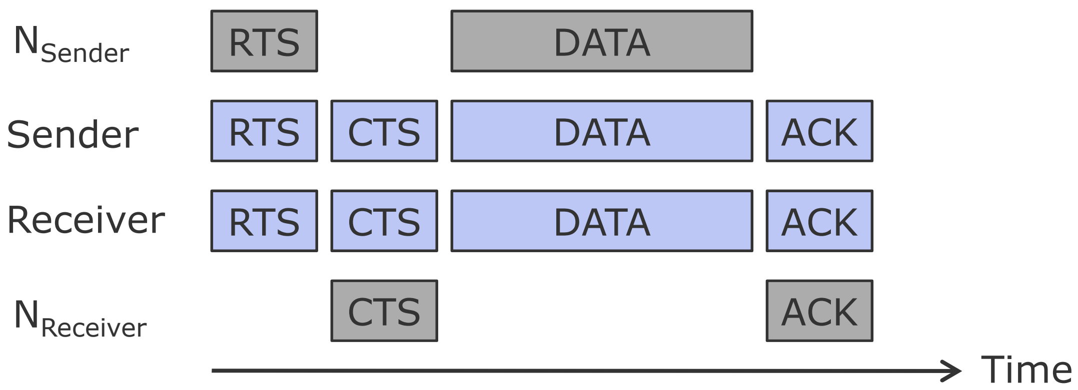
- Multiple Access with Collision Avoidance (MACA)
  - Idea: Inform stations in the neighborhood about the transmission
  - Ready To Send (RTS)
    - Informs the neighbors of the sender
  - Clear To Send (CTS)
    - Informs the neighbors of the receiver
  - Collision can occur, e.g., A and C could send RTS to B





MAC for Wireless LANs

- Multiple Access with Collision Avoidance for Wireless (MACAW)
  - With MACA retransmission of lost frames have to be triggered from the transport layer ➡ Bad performance
  - Extension of MACA by an acknowledgement



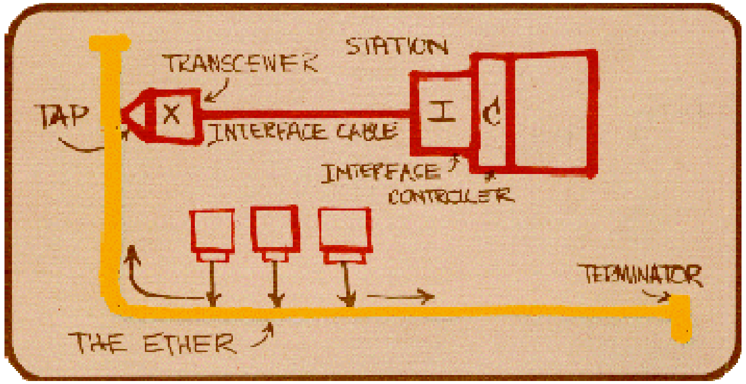
Ethernet

Ethernet

- Evolution of Ethernet
  - 1970s on Hawaii ALOHANET (Abramson)
    - Connecting computers on islands over radio
    - Two channels
      - Uplink shared by the clients (collision may occur)
      - Downlink exclusively used by main computer
    - Packets are acked by main computer
    - Good performance under low traffic, but bad under heavy load
  - 1970's: experimental network on the basis of coaxial cables, data rate of 3 Mbps. Developed by the Xerox Corporation as a protocol for LANs with sporadic but bursty traffic.
  - 1976 Ethernet by Robert Metcalf at Xerox Parc
    - Ether: luminiferous ether through which electromagnetic radiation was thought to propagate
  - Improvements to ALOHANET
    - Listen to the medium before transmitting

Ethernet

- 1978: Development of 10 Mbps-variant by Digital Equipment Corporation (DEC), Intel Corporation, and Xerox (**DIX-standard**)
- 1983: DIX-standard became the IEEE 802.3 standard
- Metcalf founded 3Com
  - Sold many, many million Ethernet adapters

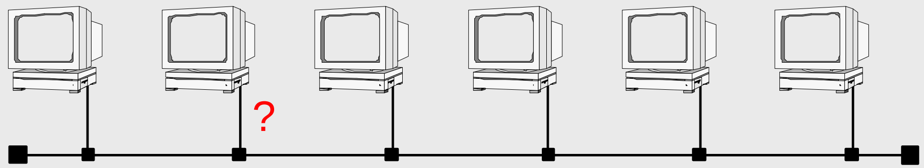


- Original Ethernet structure:
  - **Bus topology** with a maximum segment length of 500 meters, connection of a maximum of 100 passive stations.
  - **Repeaters** are used to connect several segments.
- Most common medium: Copper cable.
  - In addition, optical fibers are used (the segment length increases).
- Early 90's: the bus topology is displaced more and more by a **star topology**, in which a **central hub** or **switch** (based on Twisted Pair or Optical Fiber) realizes connections to all stations.
  - The switch offers the advantage that several connections can run in parallel.

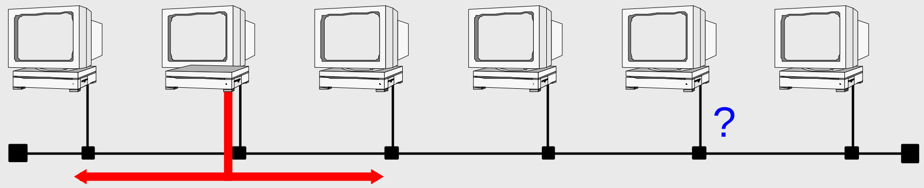
Ethernet

- Based on the standard IEEE 802.3 “**CSMA/CD**”
  (Carrier Sense Multiple Access/Collision Detection)
- Several (passive) stations - one shared medium (random access)
- Originally, bus topology:

1. Is the medium available?
   (Carrier Sense)

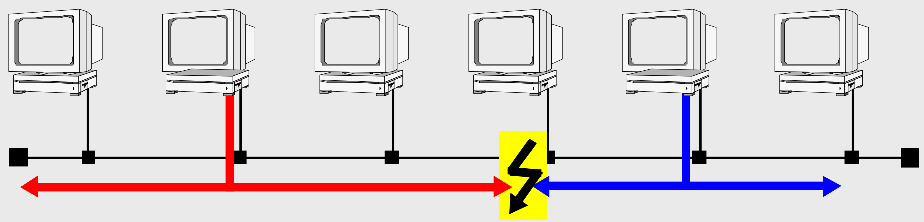


2. Data transmission



3. Check for collisions (Collision Detection)

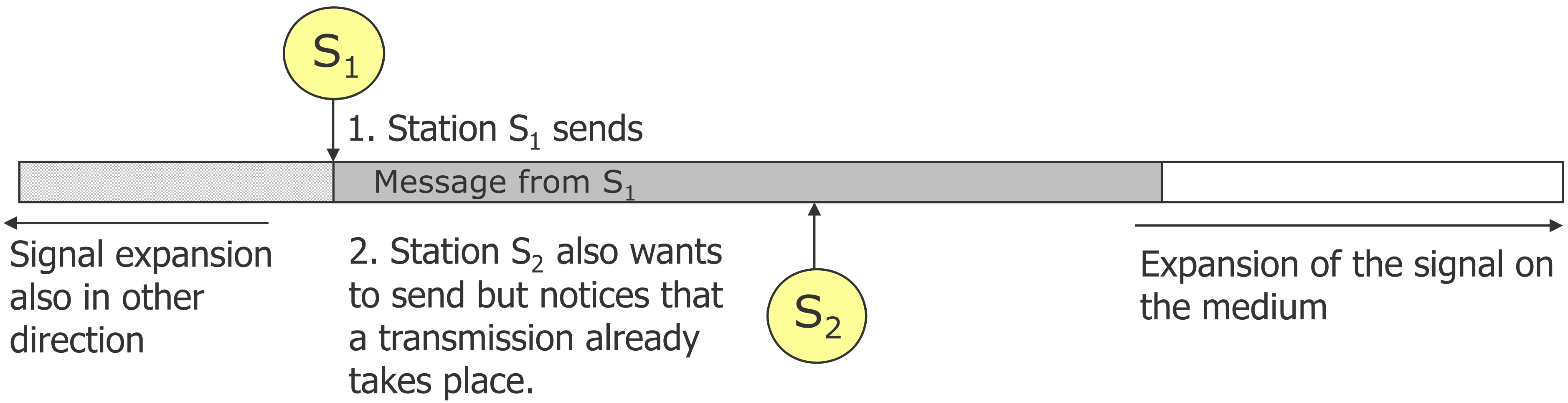
   If so: send jamming signal and stop transmission. Go on with binary exponential backoff algorithm



Carrier Sense Multiple Access

Principle:

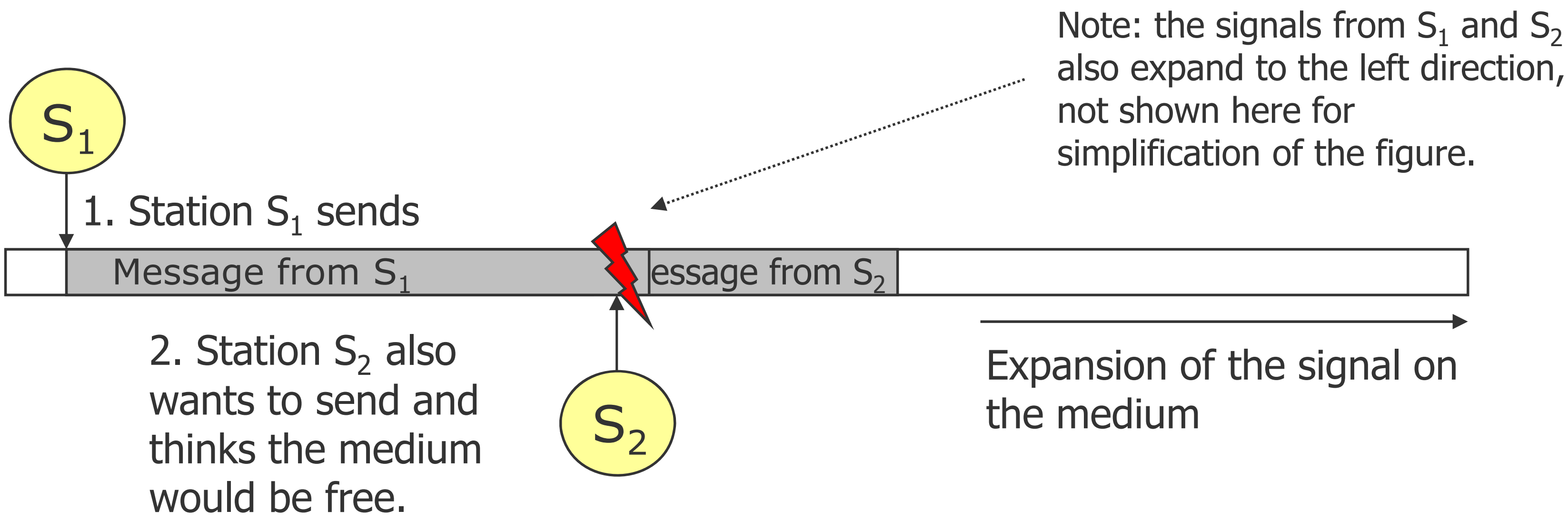
- listen to the medium before sending
- send only if the medium is free



- Advantages: simple, since no mechanisms are needed for the coordination; with some extensions nevertheless a good utilization of the network capacity
- Disadvantage: no guaranteed access, a large delay before sending is possible

Problem with CSMA

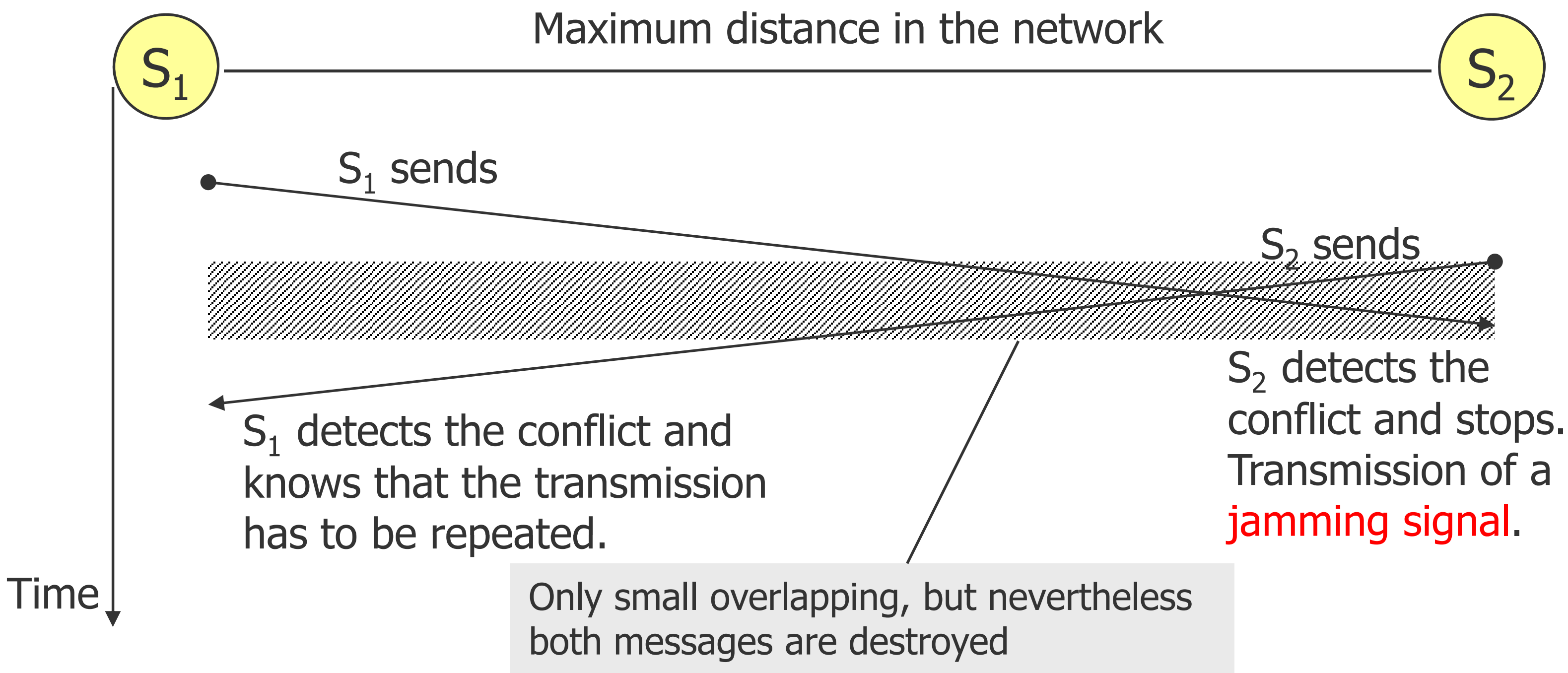
Problem: the message which is sent by S_1 spreads with finite speed on the medium. Therefore, it can be that S_2 only thinks that the medium would be free, although S_1 already has begun with the transmission. It comes to a collision: both messages overlap on the medium and become useless.



Detection of Collisions

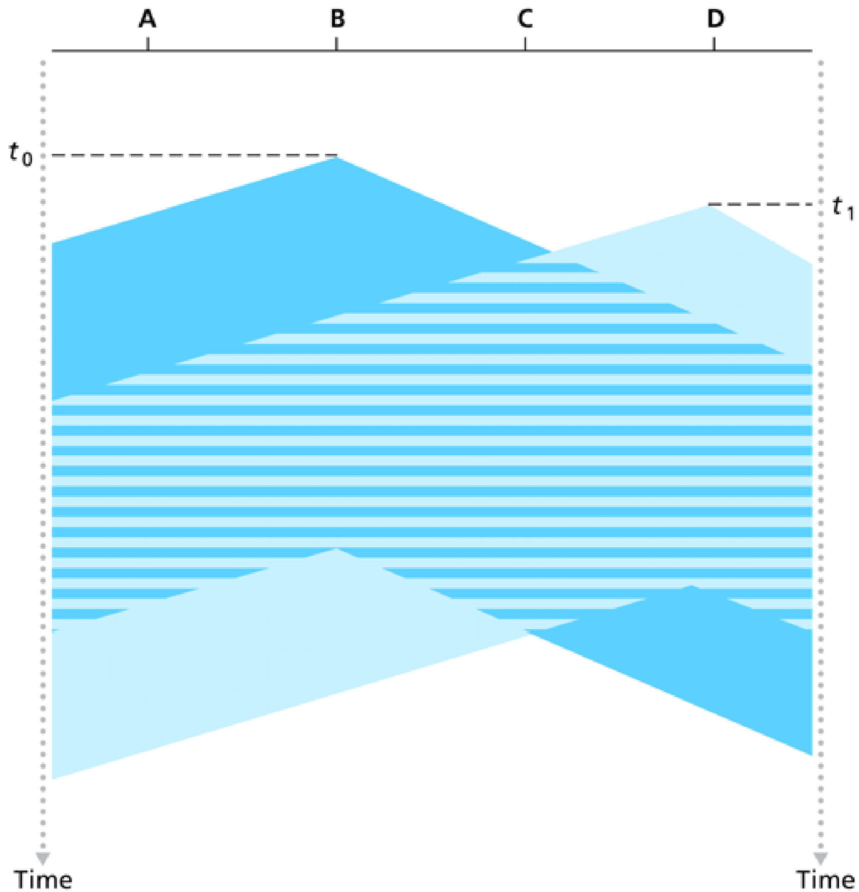
Carrier Sense Multiple Access with Collision Detection (**CSMA/CD**)

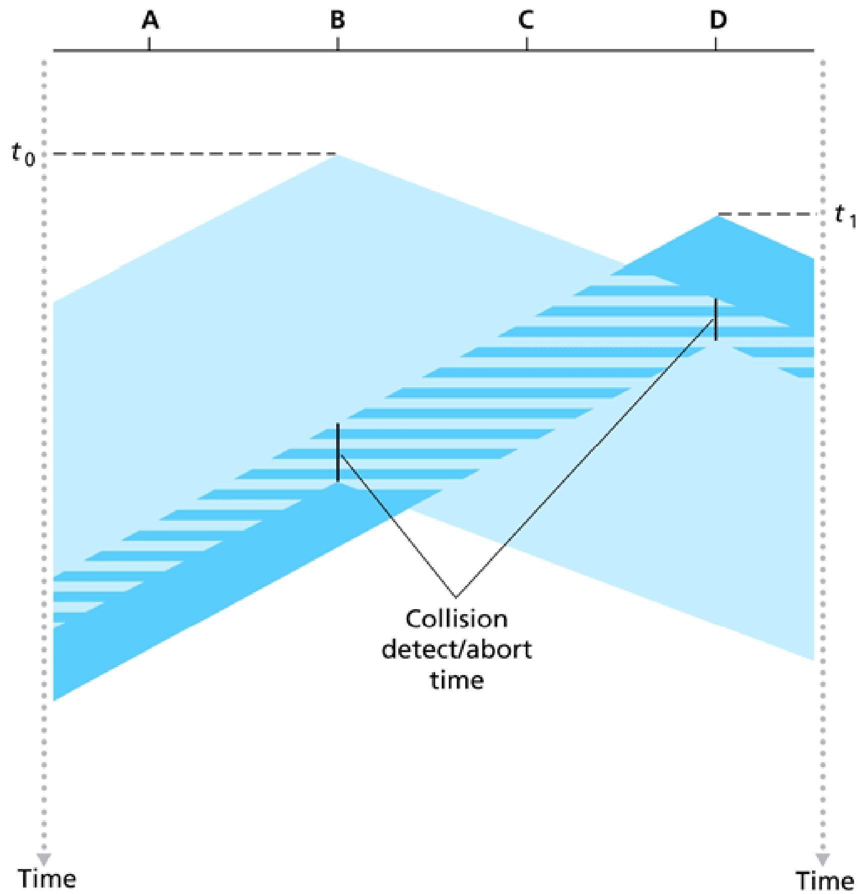
- Principle:
  - like CSMA
  - additionally: stop the transmission if a collision occurs



Note: with increasing expansion of the network the risk of a conflict also increases. Therefore, this technology is suitable only for "small" networks (Ethernet)

Detection of Collisions



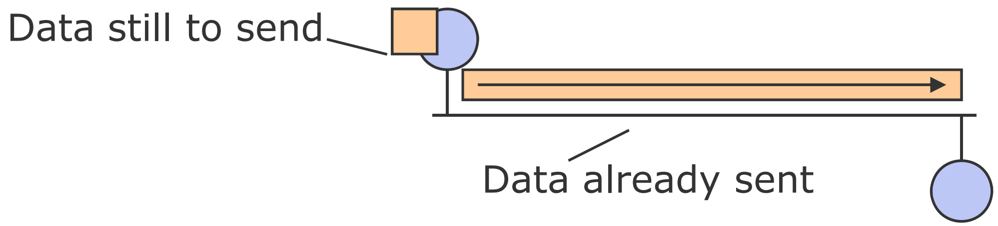


Data transmission with CSMA/CD

- When does the collision detection in CSMA/CD work correctly?
  - The maximum time for the detection of a collision is about twice as long as the signal propagation delay on the medium.
  - First compromise: one wants to create large networks, but although to have a small probability of collisions …
    - Result: the maximum expansion of the network is specified as 2,500m.
  - At a signal speed of approximately 2,00,000 km/s (5 µs/km) the maximum signal propagation delay (with consideration of the time in repeaters) is less than 25 µs.
  - The maximum conflict duration thereby is less than 50 µs. To be sure to recognize a collision, a sending station has to listen to the medium at least for this time.
  - Arrangement: a station only listens to the medium as long as it sends data.
  - Based on a transmission rate of 10 Mbps a minimum frame length (64 byte) was defined in order to make a collision detection possible.
    - The 64 bytes need the maximum conflict duration of 50 µs

Performance of CSMA/CD

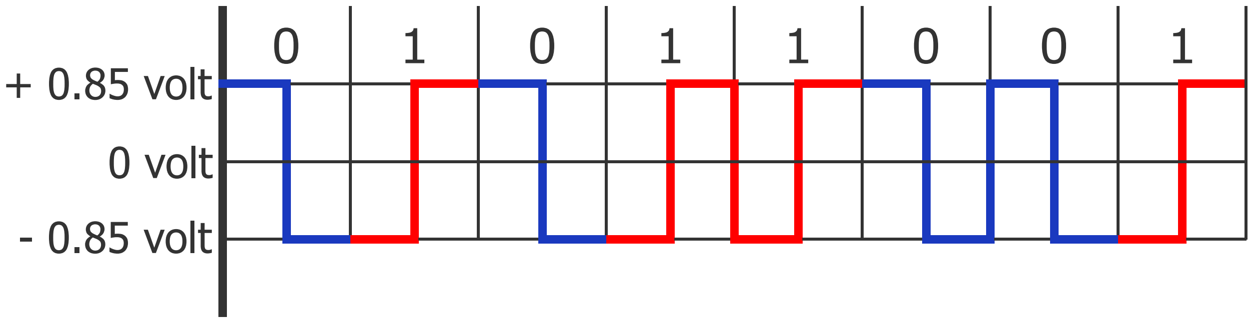
- The performance of Ethernet systems depends on the vulnerability part α:



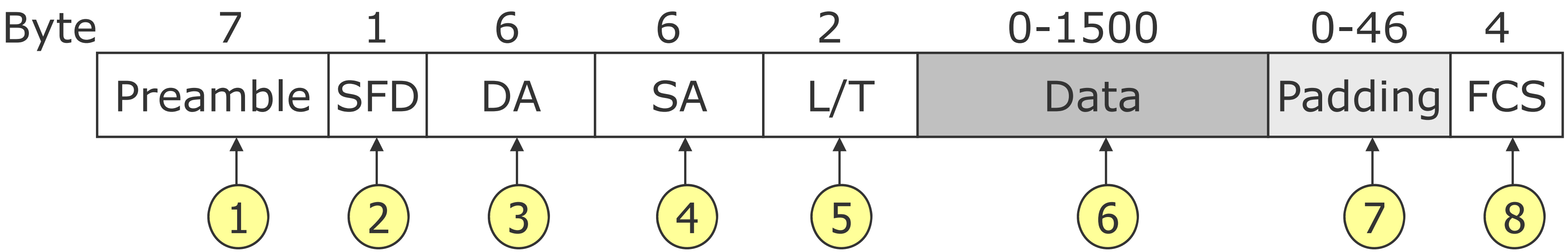
- α is the fraction of a frame which the sender has to transmit until the first bit crossed the whole network
- If someone begins to send during the time α needs to cross the whole network, a conflict arises
- The smaller α is, the better is the performance of the network
- α is small …
  - when the network is small
  - when frames are large
  - when capacity is low
- Conclusion: the best network has nearly zero size, nearly zero capacity, and a station should never stop sending.

Ethernet: Encoding on the Physical Layer

- No directly usage of binary encoding with 0 volts for a 0-bit and 5 volts for a 1-bit
  - Synchronization problems
- Manchester Encoding
  - Transition in the middle of a bit
  - The high signal is at +0.85 volts and the low signal at -0.85 volts
  - Disadvantage: twice bandwidth, i.e., to send 10Mbps, 20MHz is required



The Ethernet Frame



1: 7 byte synchronization
Each byte contains 10101010

2: 1 byte start frame delimiter (SFD)
Marking of the begin of the frame by the byte 10101011

3: 6 (2) byte destination address
MAC address of receiver

4: 6 (2) byte source address
MAC address of sender

5: 2 byte length (IEEE 802.3)/type (Ethernet)

- In 802.3: Indication of the length of the data field (range: 0 - 1500 byte)
- In Ethernet: identification of the upper layer protocol, e.g., IP, IPX, etc.

6: (0 – 1500) byte data

7: (0 – 46) byte padding

- Filling up of the frame to at least 64 byte (smaller fragments in the network are discarded, exception the jamming signal)

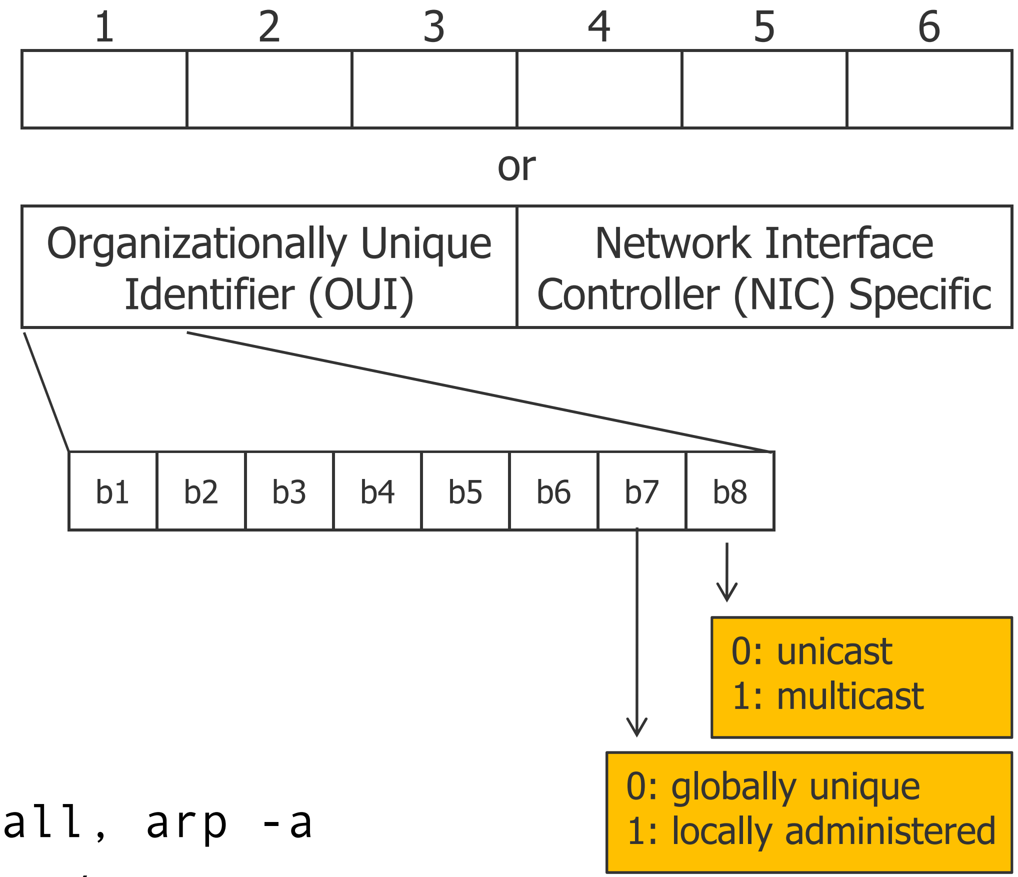
8: 4 byte Frame Check Sequence (FCS). Use of a cyclic code (CRC).

The Ethernet Frame

- Preamble: marks a following transmission and synchronizes the receiver with the sender.
- The Start-of-Frame-Delimiter (resp. the two successive ones) indicates that finally data are coming.
- Destination address: the first bit determines the kind of receiver:
  - First bit 0: an individual station
  - First bit 1: a group address (multicast)
  - Broadcast is given by 11…1
- Length(/Type): In IEEE 802.3 a value $\leq$1500 indicates the length of the data part.
  - In Ethernet, the meaning is changed, identifying the layer-3 protocol to which the data have to be passed.
  - For distinction from IEEE 802.3, only values from 1536 are permitted.
- FCS: Checksum, 32-bit (CRC).
  - It covers the fields DA, SA, length/type, data/padding.
  - Error detection

The Ethernet Frame: Addresses

- MAC address 6 byte
  - Originally invented at Xerox PARC
  - Unicast
  - Multicast
  - Broadcast

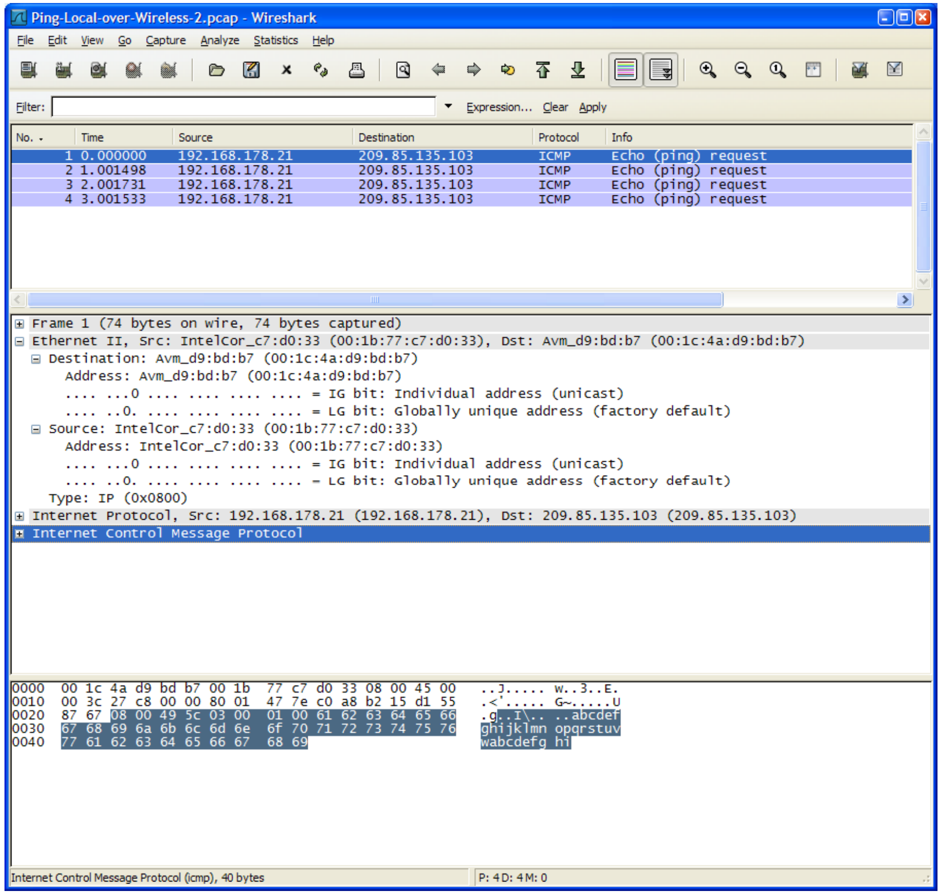


- Administrative
  - Globally unique, assigned by IEEE
  - Locally administered

- Tools
  - Windows: `getmac, ipconfig /all, arp -a`
  - Linux: `ifconfig, cat /proc/net/arp`
  - http://www.heise.de/netze/tools/mac-adressen

The Ethernet Frame: Network Analyzer

- Network packet analyzer: Wireshark
  - http://www.wireshark.org/



Ethernet

Resolving Transmission Conflicts

Resolving Transmission Conflicts

- What to do after a collision detection?
  - Different categories of reaction methods

- Non-persistent (example: ALOHA):
  - After a conflict, wait a random time afterwards start a new transmission
  - Problem: possibly inefficient utilization of the medium

- 1-persistent
  - Idea: it is very unlikely that during a current transmission two or more new messages appear
  - Start the next transmission attempt as soon as possible, thus as soon as the channel is free or becomes free after having been busy / after a conflict
  - Problem: Subsequent conflicts!

Resolving Transmission Conflicts

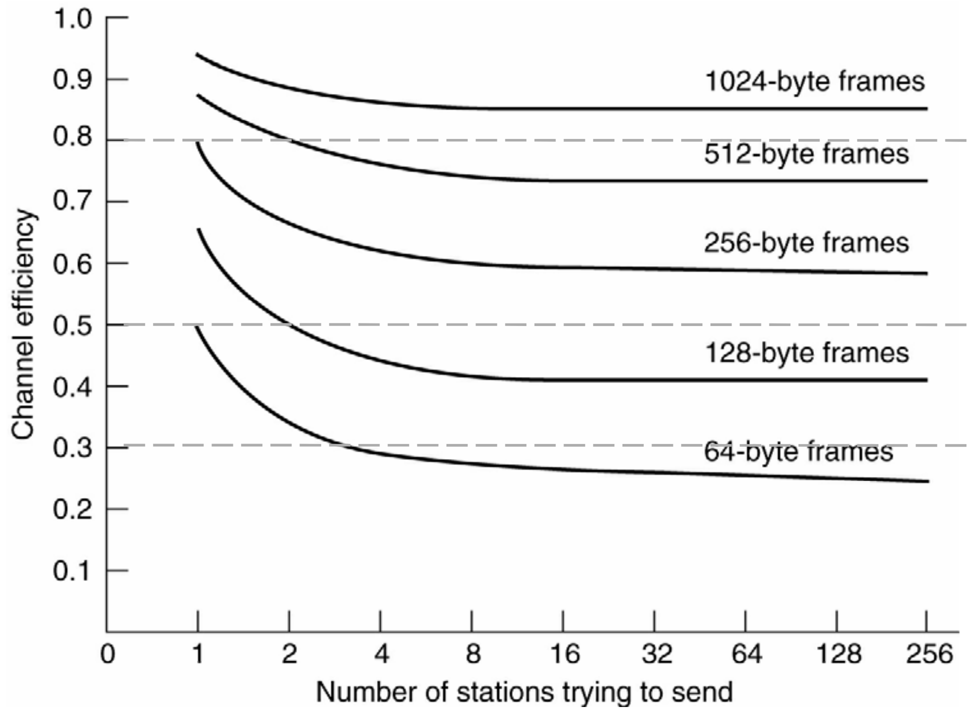
- p-persistence:
  - In this variant conflicts between concurrently waiting messages should be avoided
  - In a free channel transmission takes place only with probability p
  - In case of a conflict, a message needs on the average $1/p$ attempts

- But: how to select p?
  - p large ➨ high risk for subsequent conflicts
  - p small ➨ long waiting periods
  - $p = 0$ ➨ not possible
  - $p = 1$ ➨ 1-persistent

Resolving Transmission Conflicts

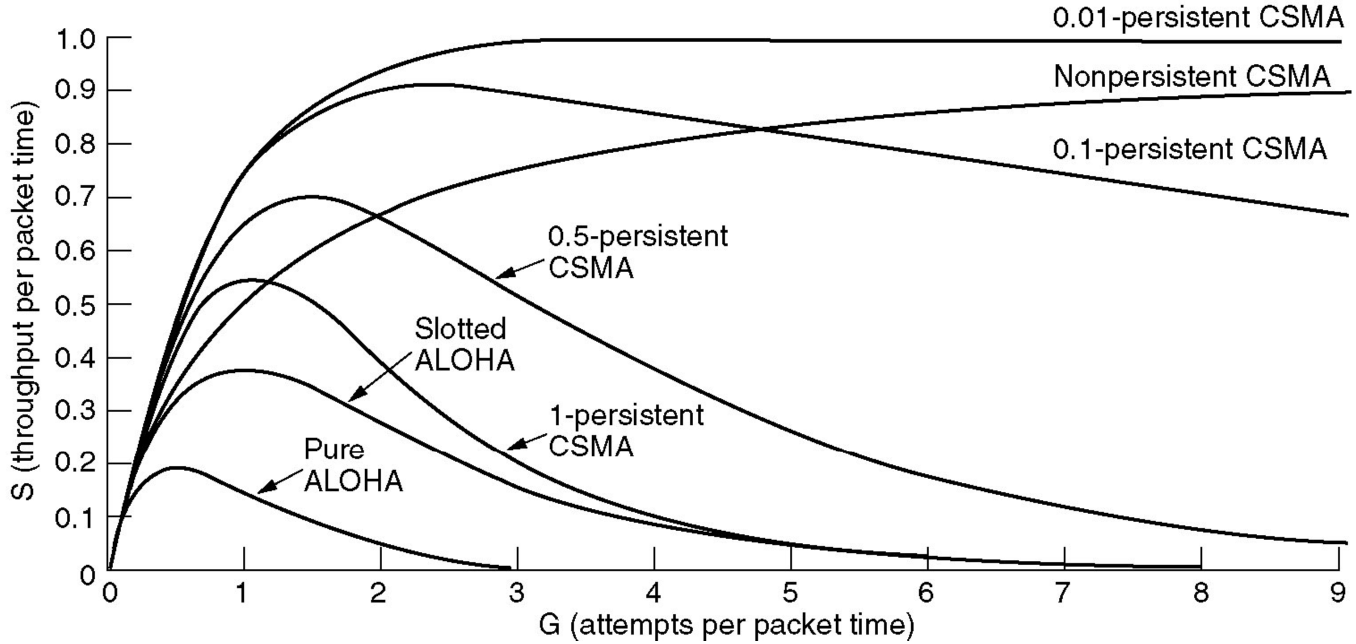
- Performance of Ethernet
  - Ethernet at 10 Mbps with 512-bit slot times
  - Assumptions
    - T : Time to transmit a frame
    - τ : Propagation on cable
    - A: Probability that a station gets the channel

$$\text{Channel efficieny} = \frac{T}{T + \frac{2\tau}{A}}$$



Resolving Transmission Conflicts

Compared to ALOHA, CSMA in any form has a good efficiency (based on a mathematical modeling of network traffic)



Nevertheless for Ethernet a further procedure was developed: the **Binary Exponential Backoff mechanism**

Resolving Collisions in Ethernet: Binary Exponential Backoff

- Binary Exponential Backoff (BEB)
  - In order to **avoid** the simultaneous **repetition** of transmissions **after a collision** (subsequent collision), a random **waiting period** is drawn from a given interval.
    - The interval is kept small, in order to avoid long waiting periods up to the repetition.
    - Thus, the risk of a subsequent conflict is high.
    - If it comes to a further collision, the interval before the next attempt is increased, in order to create more clearance for all sending parties.
- The **waiting period** is determined as follows:
  - After i collisions, a station throws a random number x from the interval $[0, 2^i\text{-}1]$
  - After 10 collisions, the interval remains fixed with $[0, 2^{10}\text{-}1]$
  - After the 16-th collision a station aborts the transmission completely
  - As soon as the medium is free, the sender waits for x time slots, whereby a time slot corresponds to the minimum Ethernet frame length of 512 bits (for a 10 Mbps Ethernet this corresponds to the maximum conflict period of 51,2 µs).
  - After the x-th time slot the station becomes active with carrier sense.

Resolving Collisions in Ethernet: Binary Exponential Backoff

- Advantage:
  - Short waiting periods (by small interval) if not much traffic is present
  - Distribution of repetitions (by large interval) if much traffic is present

- Disadvantage:
  - Stations having a subsequent conflict during a repetition have to draw a random waiting period from an interval twice as large. If they are having a further conflict, the interval again is doubled, …
  - Thus, single stations can be disadvantaged.

Ethernet

Types of Ethernet

Ethernet

Based on IEEE 802.3 "CSMA/CD" http://www.ethernetalliance.org

4 classes of Ethernet variants:

- Standard Ethernet ➡ 10 Mbps — Still partly in use
- Fast Ethernet ➡ 100 Mbps — Today the most common used variant
- Gigabit Ethernet ➡ 1,000 Mbps — Also used in MANs
- 10Gigabit Ethernet ➡ 10,000 Mbps — Standardized not long ago

Ethernet became generally accepted within the LAN range.
It is used in most LANs as infrastructure:

- It is simple to understand, to build, and to maintain
- The network is cheap in the acquisition
- The topology allows high flexibility
- No compatibility problems, each manufacturer knows and complies with the standard

Ethernet Parameters

Parameter	Ethernet	Fast Ethernet	Gigabit Ethernet
Maximum expansion	≤ 2500 meters	205 meters	200 meters
Capacity	10 Mbps	100 Mbps	1000 Mbps
Minimum frame length	64 byte	64 byte	520 byte
Maximum frame length	1526 byte	1526 byte	1526 byte
Signal representation	Manchester code	4B/5B code, 8B/6T code, …	8B/10B code,…
Max number of repeaters	5	2	1

Naming of Ethernet Variants

Indication of the used Ethernet variant by 3 name components:

1. Capacity in Mbps (10, 100, 1000, 10G)
2. Transmission technology (e.g. **Base** for baseband, Broad for broadband)
3. Maximum segment length in units of the medium used by 100 meters, resp. type of medium

Examples:

- 10Base-5: 10 Mbps, baseband, 500 meters of segment length
- 100Base-T2: 100 Mbps, baseband, two Twisted Pair cables (i.e. two cores)
- 1000Base-X: 1000 Mbps, baseband, optical fiber

Some parameters depend on the variant, e.g., the minimum frame length (because of different signal propagation delay):

- 1000Base-X: minimum frame length of 416 bytes
- 1000Base-T: minimum frame length of 520 bytes

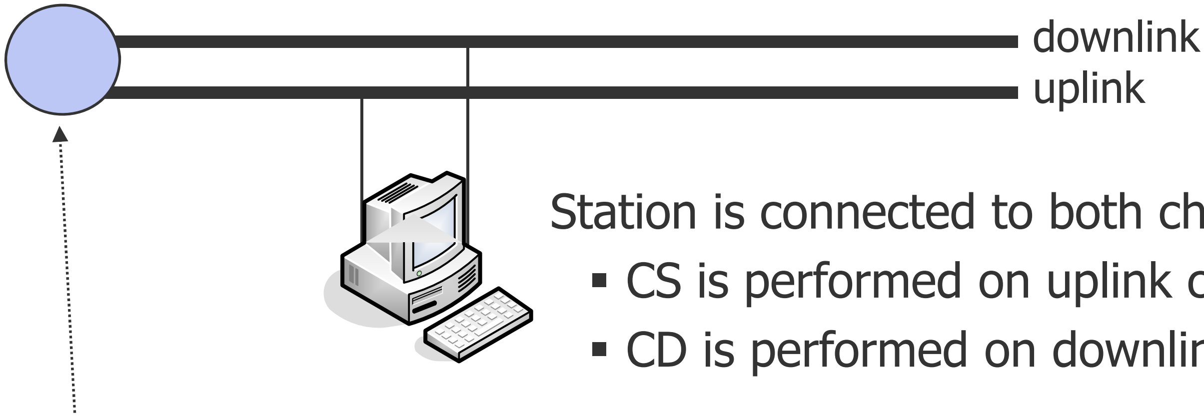
Ethernet

10Broad-36

10Broad-36

Broadband Ethernet has an analogy to CATV (Cable TV)

- Two channels: whole frequency range is divided into uplink and downlink



Station is connected to both channels:

- CS is performed on uplink channel
- CD is performed on downlink channel

retransformation for downlink, in CATV e.g.

- channel 21 -> 41
- channel 22 -> 42

you need “single side” amplifiers and modulator/demodulator components to send the digital signal over the analogous medium

➡ makes broadband Ethernet too expensive

10Broad-36

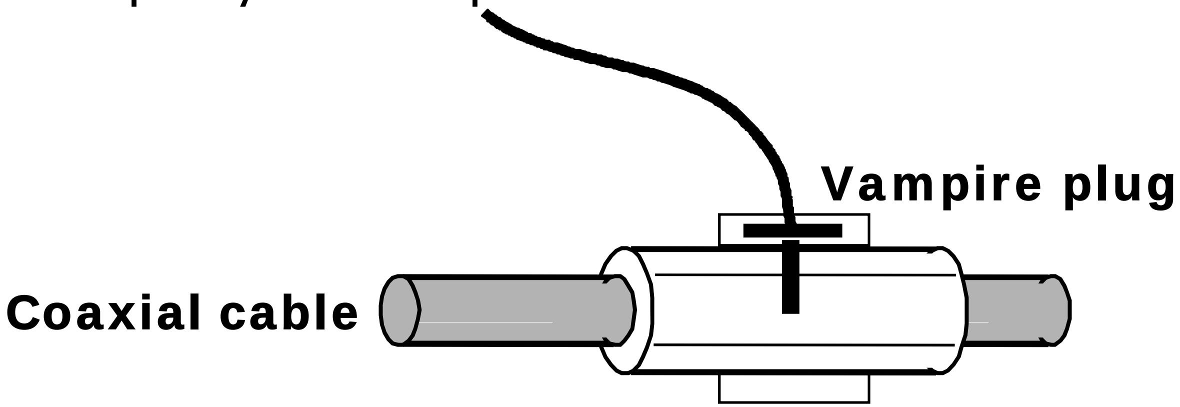
- Data rate of 10 Mbps
- Maximum segment length of 1800 meters (3600 meters is maximum range!)
- Uses CATV technology, mostly with bus topology, but also tree topology is possible (but then “carrier sense” is restricted; it is only possible if both stations are on the same branch of the tree)
- Up to 100 stations per segment
- In difference to the baseband variants, NRZ-coded signals are modulated on a specific frequency, and receiving is made demodulating incoming signals on another frequency.
- A head-end at the end of the cable has to translate incoming signals from one frequency to the other frequency

Ethernet

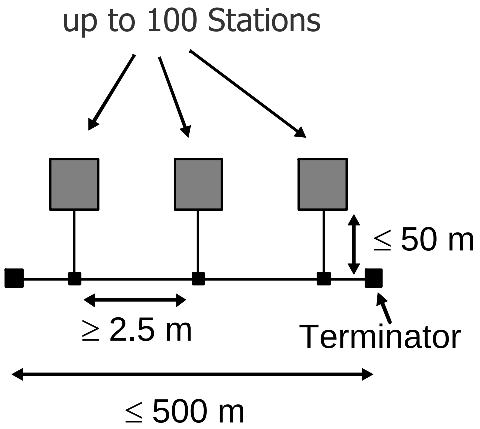
Basic Ethernet (10Base)

10Base-5 (Yellow Cable)

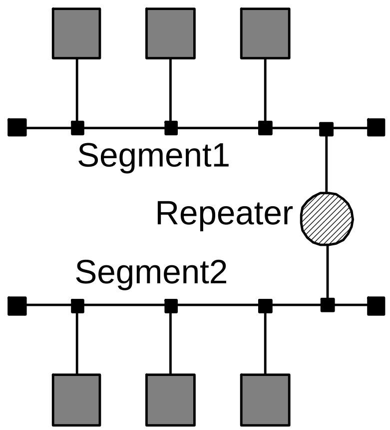
- Uses classical coaxial cable (expensive, inflexible)
  - Thick Ethernet, since cable looks like a yellow garden hose
- Terminals are attached over transceivers (vampire plug)
- Max. 5 segments (connected by repeaters)
- Max. 100 stations per segment
- At least 2.5 m distance between plugs
- Max. 500 m segment length
- Max. 50 m connection cable to a station
- Max. expansion 2.5 km (without connection cables)
- Also possible: partly line of optical fiber without stations



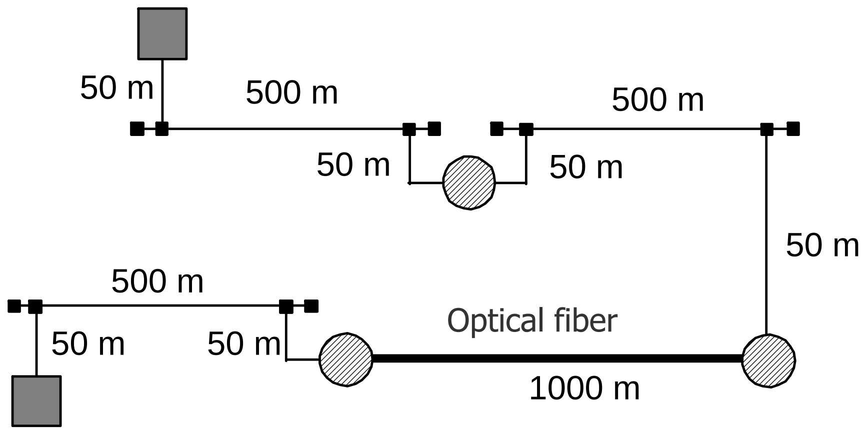
Ethernet - Configurations



Basic configuration: segment



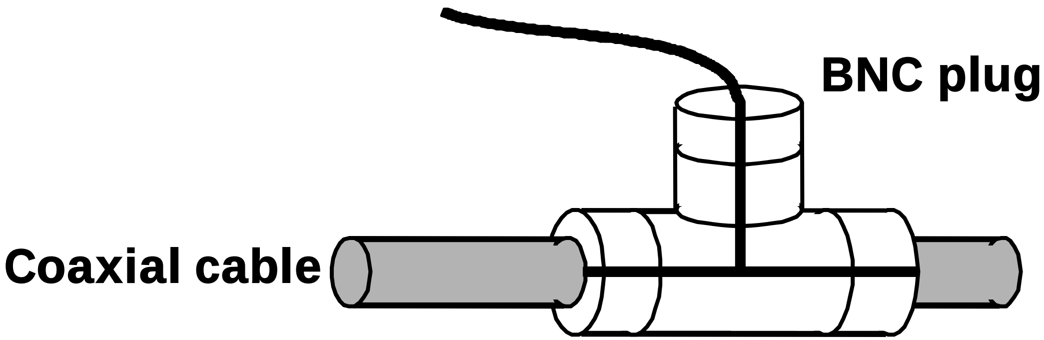
Connection of segments through a repeater



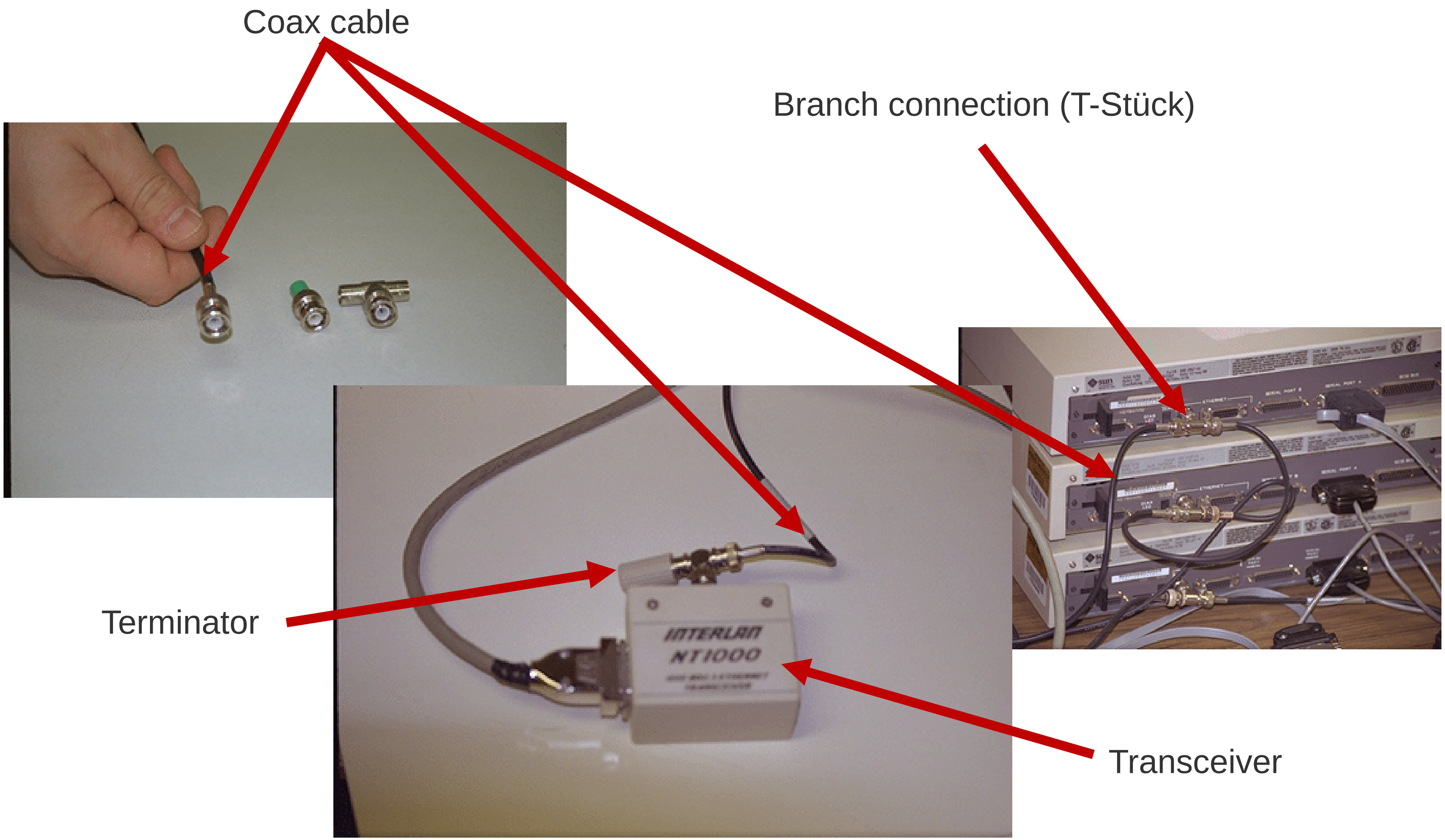
Ethernet with maximum range

10Base-2 (Cheapernet)

- Cheap coaxial cable (flexible)
  - Thin Ethernet
- Terminals are attached with BNC connectors
- Max. 5 segments (connected by repeaters)
- Max. 30 stations per segment
- At least 0.5 m distance between connections
- Max. 185 m segment length
- Maximum expansion 925 m

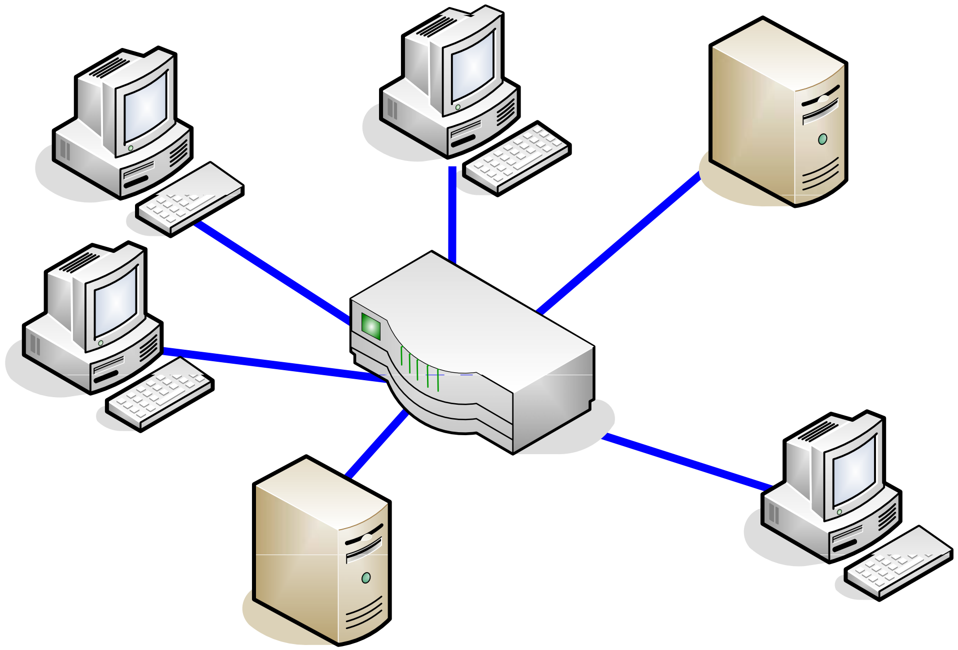


10Base-2 (Cheapernet)



10Base-T (Twisted Pair)

- Star topology using twisted pair: several devices are connected by a hub
- Devices are attached by a RJ-45 plug (Western plug), however only 2 of the 4 pairs of the cables are used
- Cable length to the hub max. 100 m
- Total extension thereby max. 200 m
- Long time the most commonly used variant



10Base-F

- Ethernet with Fiber optics
  - Expensive
  - Excellent noise immunity
  - Used when distant buildings have to be connected
  - Often used due to security issues, since wiretapping of fiber is difficult

Ethernet

Fast Ethernet

Fast Ethernet

- Principle: still use the Ethernet principles, but make it faster:
  - Compatibility with existing Ethernet networks
  - 100 Mbps as data transmission rate, achieved by better technology, more efficient codes, utilization of several pairs of cables, switches,…
  - Result: **IEEE 802.3u**, 1995
- Problem:
  - The **minimum frame length** for collision detection with Ethernet is 64 byte.
  - With 100 Mbps the frame is sent about 10 times faster, so that a collision detection is not longer ensured.
  - Result: for Fast Ethernet the expansion had to be reduced approx. by the factor 10 to somewhat more than 200 meters …
  - Therefore, its concept is based on **10Base-T** with a central **hub/switch**.
- Auto configuration
  - Negotiation of speed
  - Negotiation on communication mode (half-duplex, full-duplex)

100Base-T (Fast Ethernet)

- 100Base-T4
  - Twisted pair cable (UTP) of category 3 (cheap)
  - Uses all 4 cable pairs: one to the hub, one from the hub, the other two depending upon the transmission direction
  - Encoding uses 8B/6T (8 bits map to 6 trits)
- 100Base-TX
  - Twisted pair cable (UTP) of category 5 (more expensive, but less absorption)
  - Uses only 2 cable pairs, one for each direction
  - Encoding uses 4B/5B
  - The most used 100 Mbps version
- 100Base-FX
  - Optical fiber, uses one fiber per direction
  - Maximum cable length to the hub: 400 meters
  - Variant: Cable length up to 2 km when using a switch. Hubs are not permitted here, since with this length no collision detection is possible anymore. In the case of using a good switch, no more collisions arise!

Ethernet

Gigabit Ethernet

Gigabit Ethernet

- 1998 the IEEE standardized the norm **802.3z**, “Gigabit Ethernet”
- Again: compatibility to (Fast) Ethernet has to be maintained!
- Problem: for collision detection a reduction of the cable length to 20 meters would be necessary … “Very Local Area Network”
- Auto configuration as in Fast Ethernet (data, half-duplex, duplex, …)
- Therefore, the expansion remained the same as for Fast Ethernet – instead a new **minimum frame length of 512 byte** was specified by extending the standard frame by a ‘nodata’ field (after the FCS, because of compatibility to Ethernet). This procedure is called **Carrier Extension**.
  - It is added by the hardware, the software part does not know
  - When a frame is passed on from a Gigabit Ethernet to a Fast Ethernet, the ‘nodata’ part is simply removed and the frame can be used like a normal Ethernet frame.

PRE	SFD	DA	SA	Length /Type	DATA	Padding	FCS	nodata
Preamble 7 byte	Start Del. 1 byte							

Gigabit Ethernet

- With Gigabit Ethernet the sending of several successive frames is possible (**Frame Bursting**) without using CSMA/CD repeatedly.
- The sending MAC controller fills the gaps between the frames with "Interframe-bits" (IFG), thus for other stations the medium is occupied.

MAC frame (including nodata field)	IFG	MAC frame	IFG	....	MAC frame

- Under normal conditions, within Gigabit Ethernet no more hubs are used. In the case of using a switch no more collisions occur, therefore the **maximum cable length** is only determined by the signal absorption.
  ➡ usage for backbone connections in the MAN area

1000Base-T/X (Gigabit Ethernet)

- 1000Base-T
  - Based on Fast Ethernet
  - Twisted pair cable (Cat. 5/6/7, UTP); use of 4 pairs of cables
  - Segment length: 100 m
- 1000Base-CX
  - Shielded Twisted Pair cable (STP); use of 2 pairs of cables
  - Segment length: 25 m
  - Not often used
- 1000Base-SX
  - Multimode fiber with 550 m segment length
  - Transmission on the 850 nm band
- 1000Base-LX
  - Single- or multimode over 5000 m
  - Transmission on 1300 nm

Added later:

1000Base-LH

- Single mode on 1550 nm
- Range up to 70 km
- MAN!

Future of the Ethernet: 10-Gigabit Ethernet

- … latest specification: 10-Gigabit Ethernet, **IEEE 802.3ae**
  - (First) only specified for optical fiber (LX or SX)
  - Star topology using a switch
  - CSMA/CD is **no longer used** since no collisions can occur (but nevertheless implemented for compatibility with older Ethernet variants regarding frame format and size …)
  - It may also be used also in the MAN/WAN range: 10 - 40 km (Mono mode)
  - Most important change: two specifications on physical layer (PHY):
    - One PHY for LANs with 10 Gbps
    - One PHY for WANs with 9,6215 Gbps (for compatibility with SDH/SONET, see Wide Area Networks)

10G Ethernet: Variants

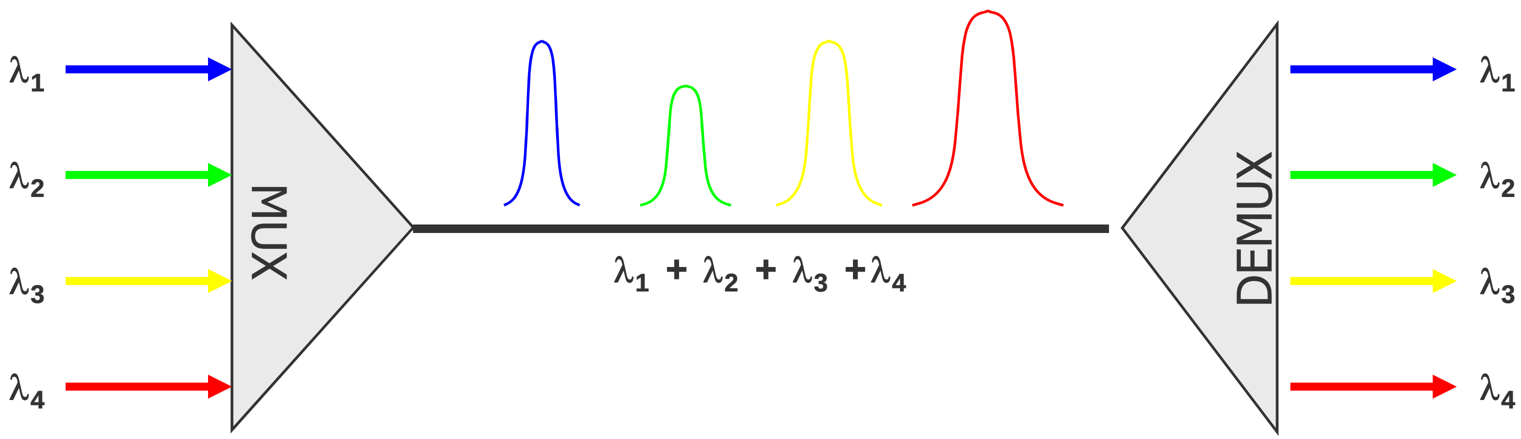
Name	Type	Wavelength [nm]	PHY	Coding	Fiber	Range [m]
10GBase-SR	serial	850	LAN	64B/66B	Multimode	26 – 65
10GBase-LR	serial	1310	LAN	64B/66B	Singlemode	10,000
10GBase-ER	serial	1550	LAN	64B/66B	Singlemode	40,000
10GBase-LX4	WWDM	1310	LAN	8B/10B	Singlemode Multimode	10,000 300
10GBase-SW	serial	850	WAN	64B/66B	Multimode	26 – 65
10GBase-LW	serial	1310	WAN	64B/66B	Singlemode	10,000
10GBase-EW	serial	1550	WAN	64B/66B	Singlemode	40,000

S: short
L: long
E: extended

serial: "normal" transmission
WWDM: Wide Wavelength Division Multiplex

Wavelength Division Multiplexing (WDM)

Technical principle **Wavelength Division Multiplexing**: transmit data using four different wavelengths in parallel:



Data are distributed to four wavelengths – how to apply this concept to copper cables?

Are Variants for Twisted Pair possible?

- Some years ago: no, impossible!
- But now:
  - **IEEE 802.3ak**: 10GBASE-CX4 (Coax)
    - Four pairs of cable for each direction
    - Cable length of up to 15 meters …
  - **IEEE 802.3an**: 10GBASE-T (Cat. 6/7 TP)
    - Cat6 (50 meters) or Cat7 (100 meters) cabling
    - Use of all 8 lines in the TP cable – in both directions in parallel!
- Filters for each cable to separate sending and receiving signal
  - Layer 1: Variant of Pulse Amplitude Modulation (PAM) with 16 discrete levels between -1 and +1 Volt (PAM16)
  - MAC-Layer: keep old Ethernet-Formats …

And what's next?

- Maybe in future: Resilient Packet Ring (RPR)?
  - IEEE 802.17, first standard version from 2004
  - Topology: double ring for metropolitan area
  - Range of several 100 km
  - Based on Ethernet, but additional management functionalities oriented at SDH/SONET (fast reaction to faults, reservation of capacity, …)

- Maybe combined with full optical networks?
  - Optical multiplexers, optical switches
  - But at the moment only tested in labs, expensive

- 100G-Ethernet under work (http://www.ethernetalliance.org)
  - Data rates from 40G to 100G
  - Variants for 100 m and 10 km with duplex communication

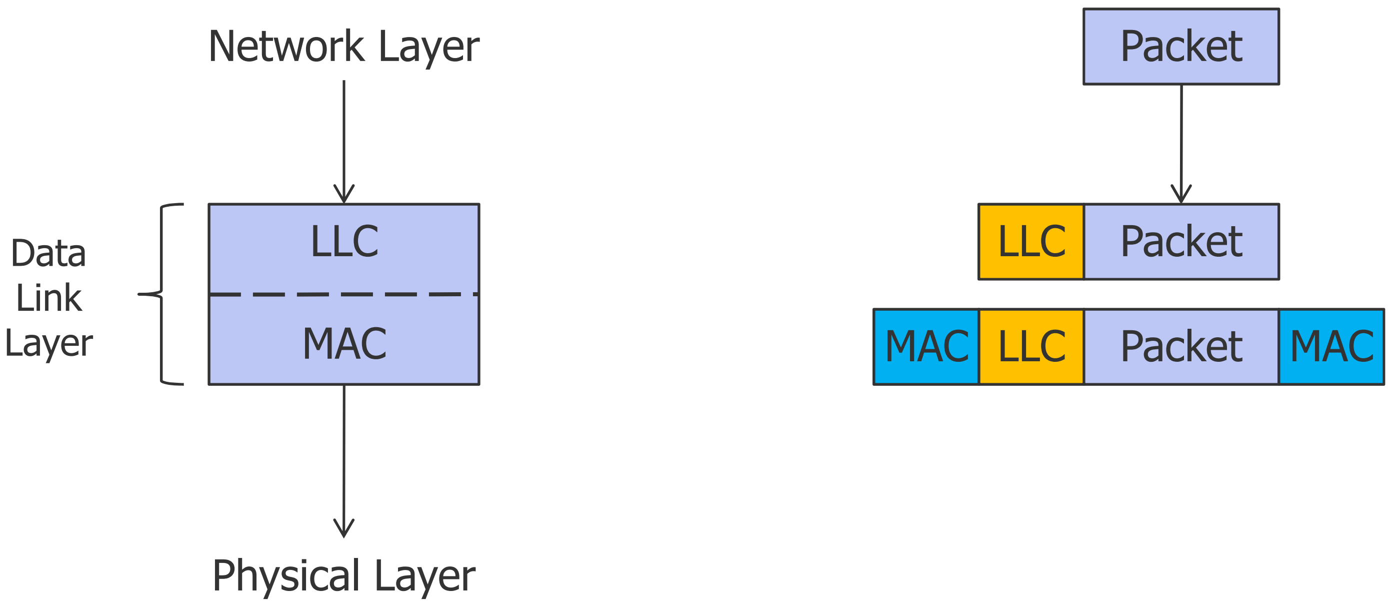
IEEE 802.2: Logical Link Control

IEEE 802.2: Logical Link Control

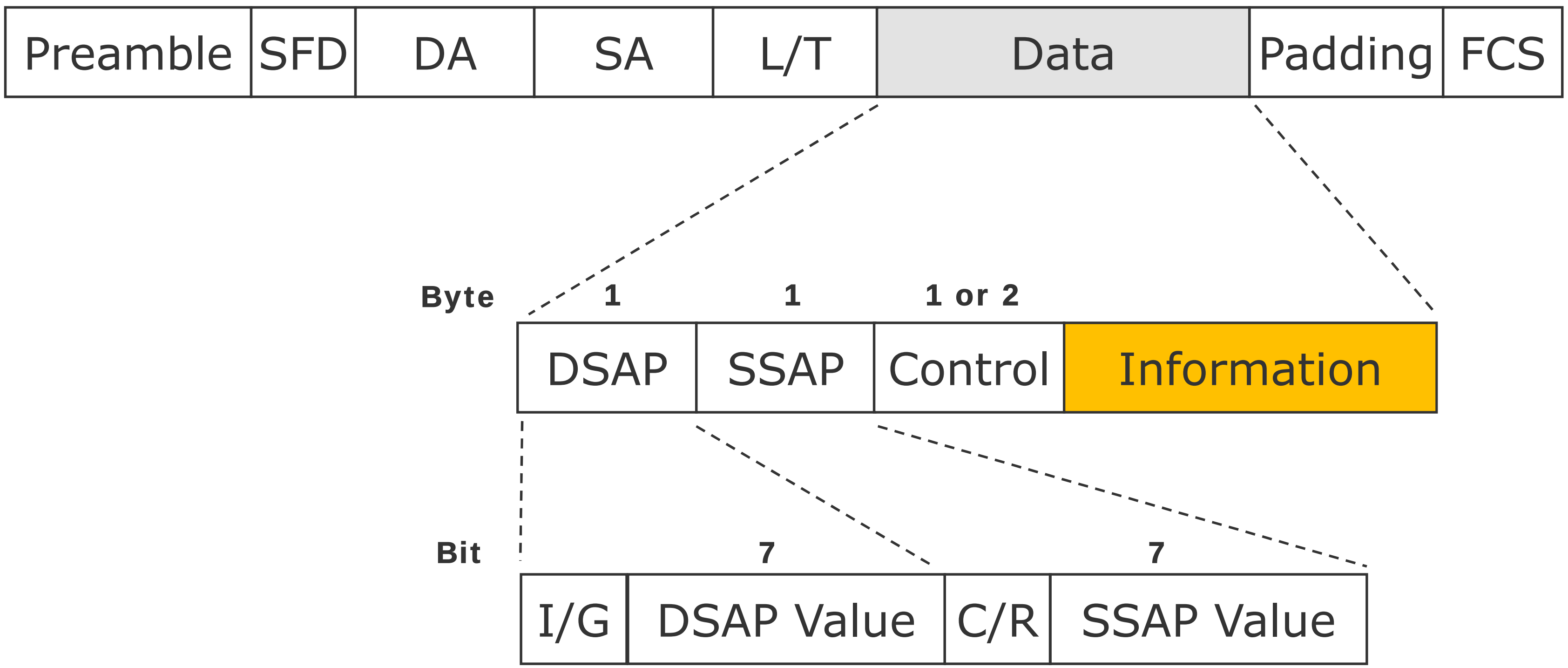
- Ethernet and IEEE 802.3 protocols offer only best effort
  - Unreliable datagram service (No acks)
  - What to do if error-control and flow-control is required?
- Logical Link Control (LLC)
  - Runs on top of Ethernet and other IEEE 802.3 protocols
  - Provides a single frame format and interface to the network layer
    - Hides differences between the protocols
    - Based on HDLC
- LLC provides
  - Unreliable datagram service
  - Acknowledged datagram service
  - Reliable connection oriented service
- LLC header contains
  - Destination access point ➡ Which process to deliver?
  - Source access point
  - Control field ➡ Seq- and ack-numbers

IEEE 802.2: Logical Link Control

- Relationship between Network Layer, LLC, and MAC
  - Network layer passes packet to LLC
  - LLC adds header with sequence number and ack number
    ➡ packet is inserted into the payload of a frame



IEEE 802.2: Logical Link Control

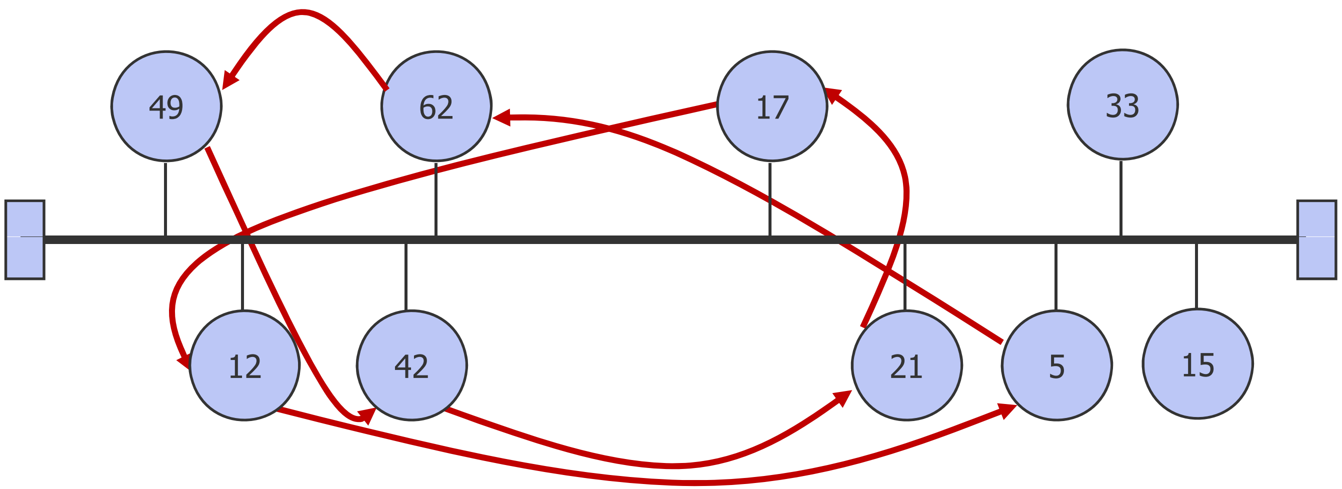


DSAP	Destination Service Access Point
SSAP	Source Service Access Point
I/G	Individual/Group
C/R	Command/Response

Token Bus

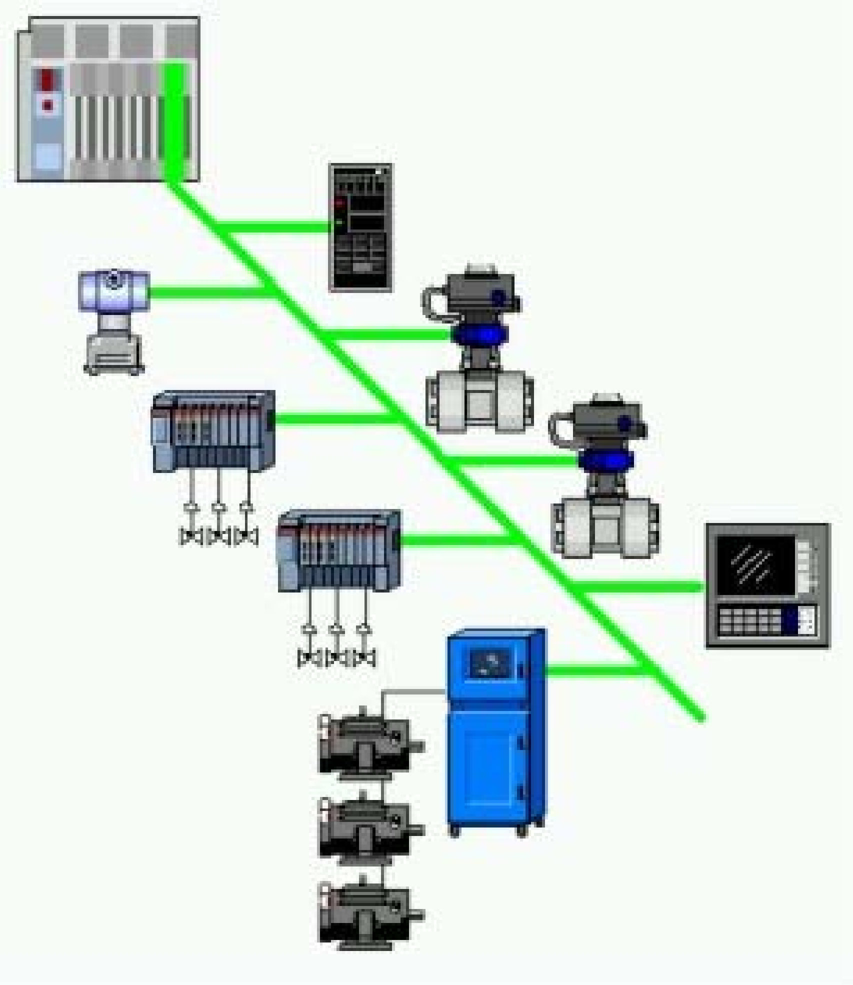
Token Bus

- Token Bus
  - LAN with ring topology
  - Token = Small frame, that circulates
    - Only the node who possesses the token may send
  - One example for a token network: IEEE 802.4 “Token Bus”
  - All stations should be treated equally, i.e., they have to pass the token cyclically
  - For this: logical ordering of all stations into a ring
  - In a bus topology, ordering is made regarding station addresses:



Token Bus

- Application Area
  - Mainly for industrial applications
  - Forced by General Motors for their Manufacturing Automation Protocol standardization effort
  - Usage e.g. as a field bus (Feldbus in German) in industrial environments with a high degree of noise.
  - Purpose: e.g. roboter control; a few masters, many slaves (they only listen).
  - Data rate is not that important, but guarantees in response times are necessary (not possible with Ethernet).



Message Exchange in Token Bus

Two types of messages are used:

- Token messages $T_{ID,\ nextID}$

ID	nextID

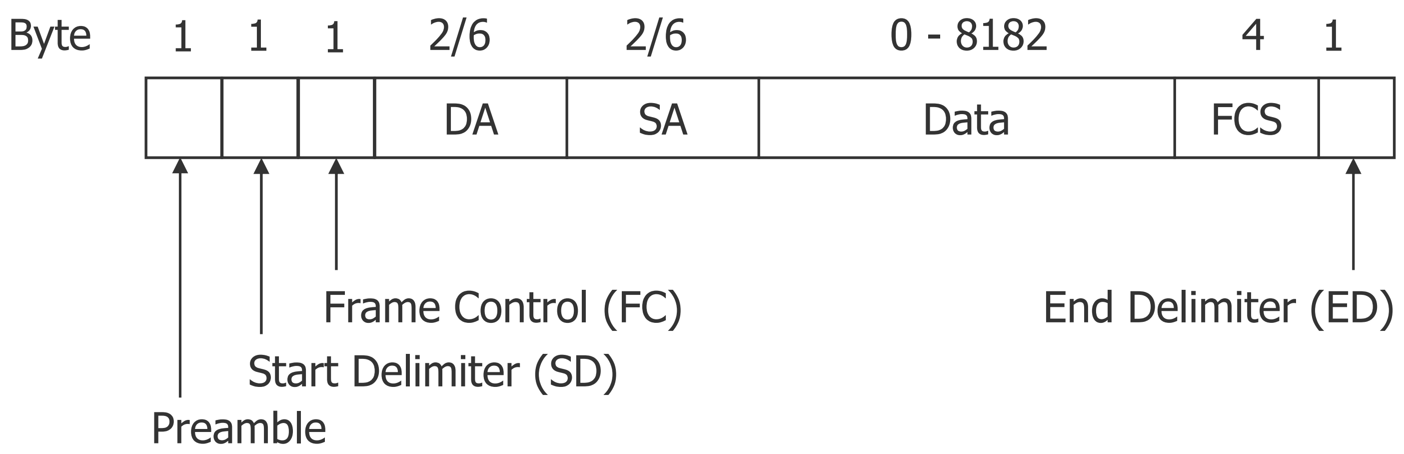
- Data messages M_{ID}

ID	Data

- Token messages are used for passing on the sending permission from station ID to station nextID
- Data messages contain the data to be sent
- Having the token, a station is allowed to send a message. After this (or if nothing is to be sent) the token is passed on.
- Traffic on the bus e.g.:
  - T5,17 → M17 → T17,21 → M21 → T21,22 → T22,42 → T42,63 → M63 → T63,149 → T149,5 → M5 → T5,17 → …
- High overhead for token exchange: 512 Bit for each token message (a full small size Ethernet frame)!
- Thus, the number of participating stations should be small or the number of masters should be small, but many slaves can be tolerated

Token Bus: Frame Format

- Token Bus supports priorities
  - Four classes of priorities are provided (0, 2, 4, and 6)
  - A station is assumed to consist of four substations, i.e., four different queues
  - Data of the highest priority gets first service (highest priority is 6)
  - A station may send during the token hold time (timer based)
    - A fix part of the time may be reserved for priority 6 data
    - Supporting of voice and realtime data



Problems with Token Bus

- First problem: a station leaves the logical ring
  - Easy solution: the leaving station sends a message to its predecessor indicating the new successor
- Second problem: a station comes into the logical ring
  - To allow new stations to join in, in periodically intervals a “window” is opened between neighbors, e.g., between 12 and 5.
  - New stations with IDs from 6 to 11 can now apply.
  - Problem: conflict risk! Several stations could apply to join in in this window
  - Conflict resolution: survival of the fittest. Consider last 2 bits of the IDs:
    send a request to join in with a duration specified by the last 2 bits of your ID:

    00 send short

    01 send longer

    10 send even longer

    11 send longest
  - If you hear anybody else sending longer than you, give up. If you survive without conflict, join. If there is no resolution (two or more stations are sending for the same time, no one is sending longer), repeat with the second-last bit pair, etc.

Example

Assume a global window.

Competitors:

15	**63**	**22**	**4**	**35**
00001111	00111111	00010110	00000100	00100011
↓	↓	↓	↓	↓
11	11	~~1~~0	~~0~~0	11
↓	↓			↓
11	11			~~0~~0
↓	↓			
~~0~~0	11			
	↓			
	Winner!			

In case of some configuration error, two identical IDs are present: after checking all pairs of the IDs, continue by adding random bit pairs.

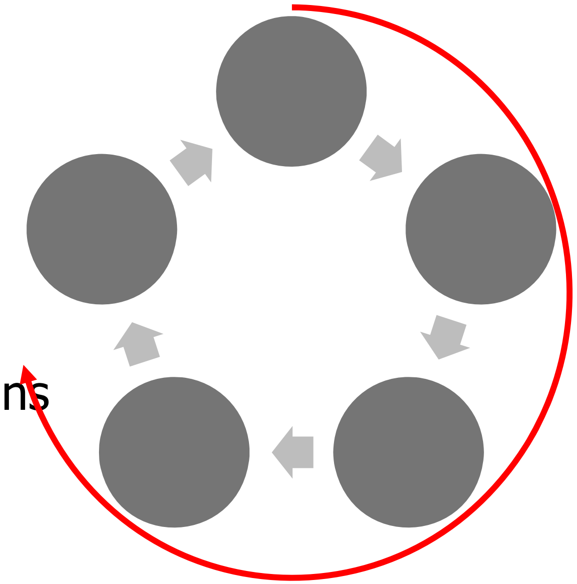
But… “Industrial Ethernet”

- The Token-Bus approach is more and more displaced by Ethernet variants, e.g.:
- EtherCAT (since 2003, http://www.ethercat.org/)
  - Fast Ethernet based on a bus, star, or tree topology (very flexible)
  - Uses TP or optical fiber as medium
  - Synchronization necessary between all stations
  - A master station polls the other stations with a single Ethernet frame – each station has its one time slot to read out /write in data
- Ethernet Powerlink (http://www.ethernet-powerlink.org/)
  - Introduction of time slots and a cyclic timing schedule
  - Whole time axis is divided into isochronous and asynchronous phases
  - Isochronous: for time-critical data transfer
  - Asynchronous: for non-time-critical data transfer
  - A managing node assigns time slots (in both phases!): in the isochronous phase to all stations, in the asynchronous phase to one particular station

Token Ring

Token Ring

- Token Ring
  - LAN with ring topology
  - Token = Small frame, that circulates
    - Only the node who possesses the token may send
  - Based on the standard IEEE 802.5 "Token Ring"
  - The stations share a ring of **point-to-point** connections
  - The token is cyclically passed on
    - particularly suitable for rings
    - Token Ring (4/16/100 Mbps)
  - Mainly supported by IBM
- Characteristics:
  - Guaranteed access, no collisions
  - Fair, guaranteed response times
  - Possible: multiple tokens
  - However: complex and expensive



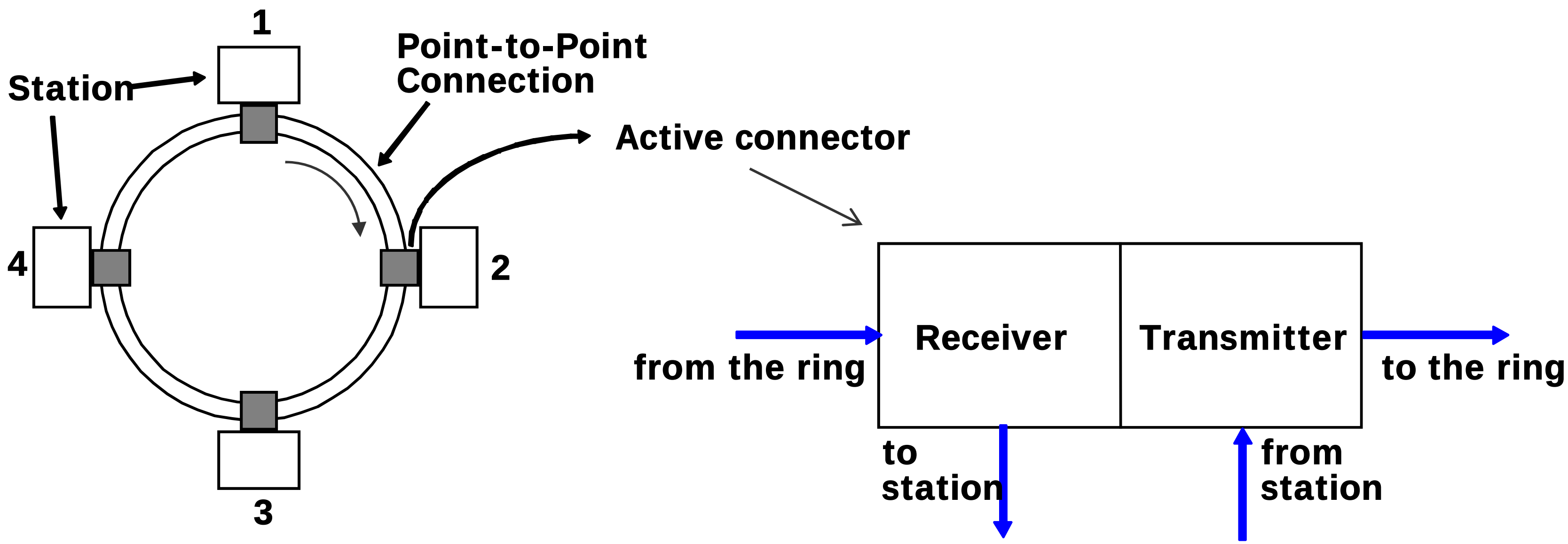
Passing on the token

Token Ring

- Performance
  - Under light load: inefficient, since a station has to wait for the token
  - Under heavy load: efficient and fair
    - Round robin fashion transmission of stations
- Disadvantage
  - Token maintenance
  - Lost token can block the network
  - Duplication of token
  - Monitor station observes the ring
    - Central entity

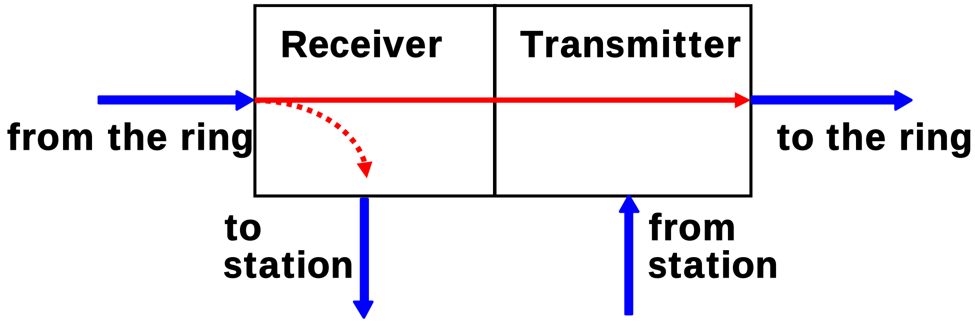
Token Ring

- Characteristics
  - Medium: twisted pair, coaxial cable, or optical fiber
  - Capacity of 4 resp. 16 Mbps (100 Mbps with optical fiber)
  - Differential Manchester Code on layer 1
  - The stations are actively attached, i.e., received signals are regenerated (same principle as for repeaters, therefore no restriction of the ring's expansion)

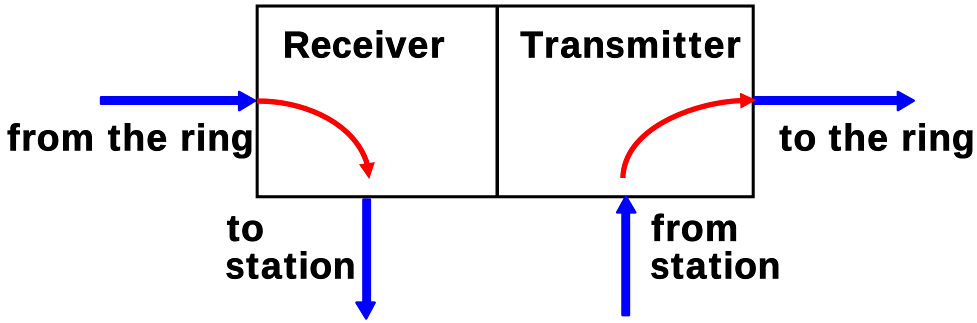


Sending and Receiving

- Initial state
  - Data are received from the ring serially
  - Data addressed to a connector's station are copied
  - Data are serially passed on along the ring

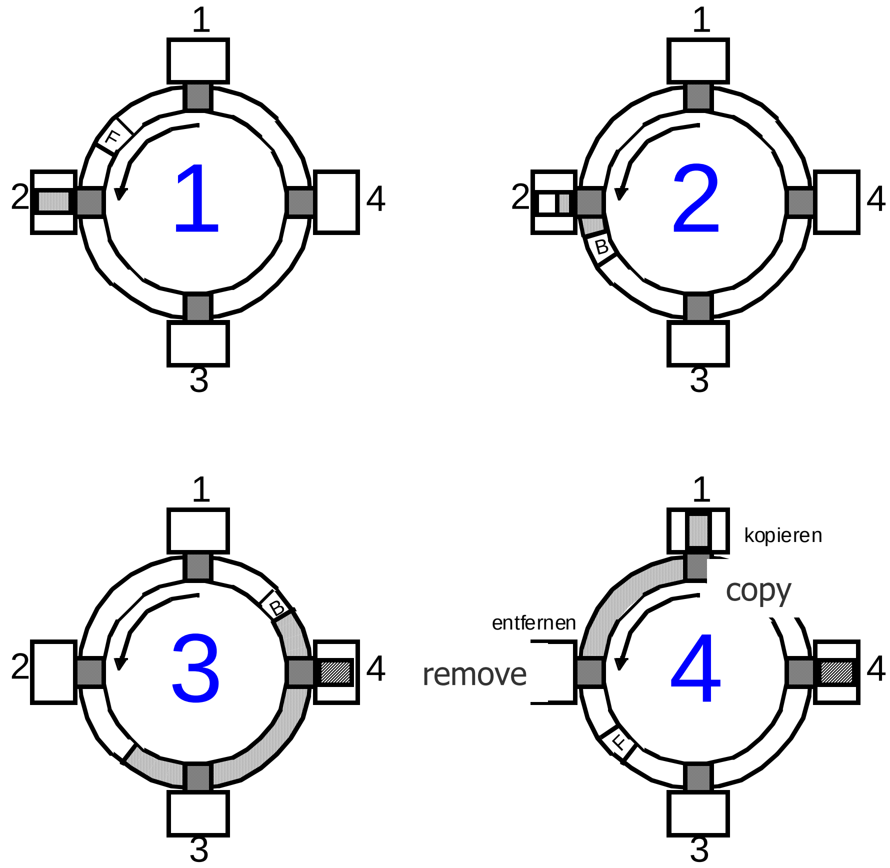


- Transmission state
  - The ring is divided
  - Own data are sent serially
  - Data coming in from the ring are evaluated by the station



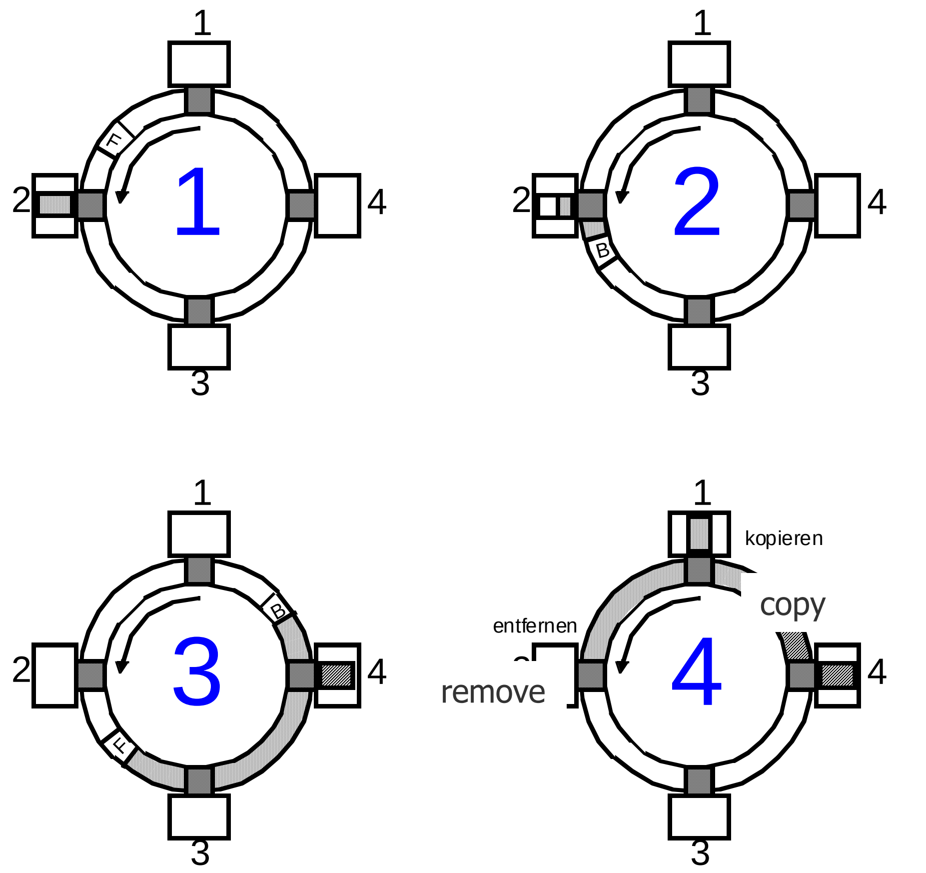
Access within a Token Ring

- Example: Station 2 sends to station 1
  1. Station 2 waits for free token (transmission authorization, 3-Byte-Token).
  2. Station 2 changes free token into an occupied one (occupied token = frame header).
     Afterwards, station 2 sends the frame.
     - Station 2 may send further frames, if the **token holding timer** (default 10 ms) is not exceeded
  3. Station 2 terminates the frame and waits until the frame passed the whole ring and arrives again.
  4. Station 1 copies the frame. Station 2 removes it from the ring and produces a new, free token.



Access within a Multiple Token Ring

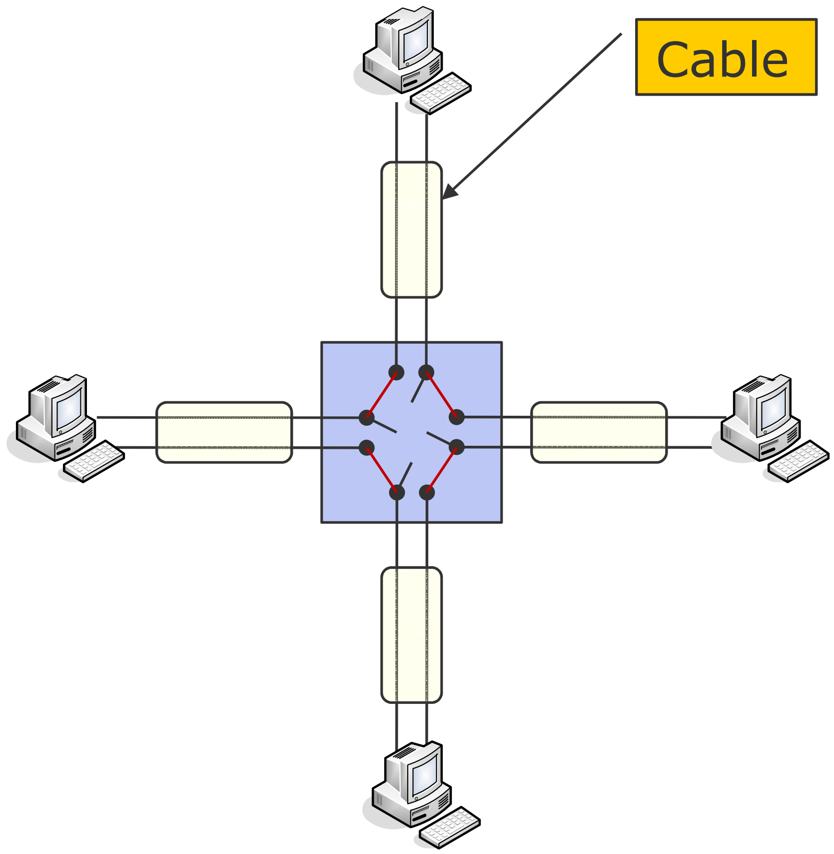
- Same example: Station 2 sends to 1
  1. Station 2 waits for free token (transmission authorization).
  2. Station 2 changes free token into an occupied one (occupied token = frame header).
     Afterwards, 2 sends the frame.
     - Station 2 may send further frames, if the **token holding timer** (default 10 ms) is not exceeded
  3. Station 2 terminates the frame and produces a new, free token immediately.
  4. Station 1 copies the frame. Station 2 removes it from the ring.



Wire Center for Robust Rings

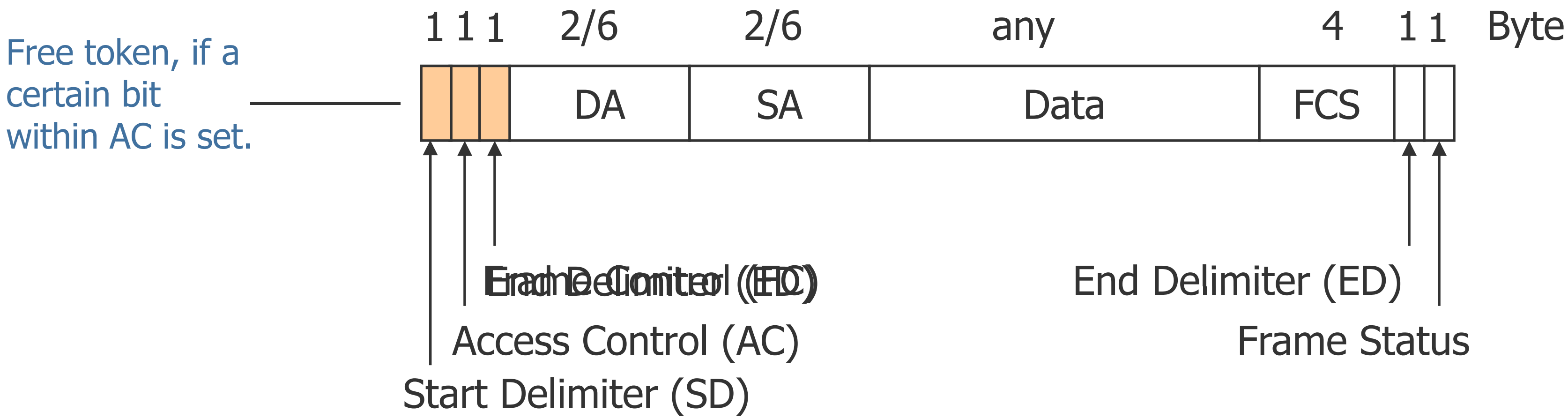
- High risk in ring networks
  - When a cable breaks the network may not work any more

- Wire Center
  - Each station is connected to the Wire-Center
  - Logically still a ring
  - Wire Center contains bypass-switches which connects the internal connection when a station does not respond
    - Can be controlled via software



Frame Format for Token Ring

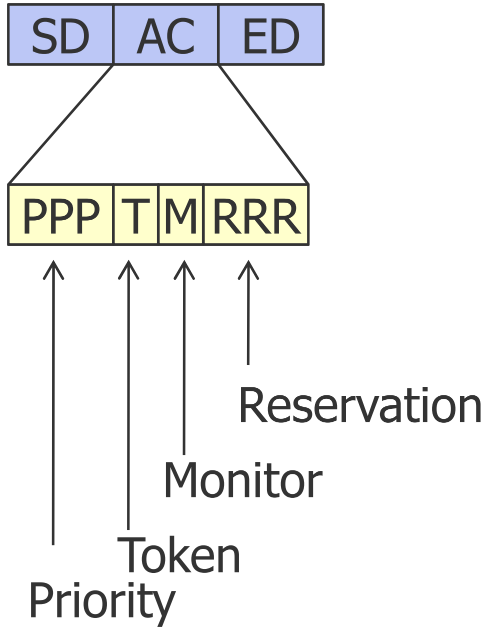
If the ring is inactive, only the 3-Byte-Token (SD, AC, ED) circulates. If a station wants to send, it sets the “token” bit in this token from 0 to 1.



- SD and ED serve for marking the frame. They contain invalid sequences of the Differential Manchester code.
- Access control contains the **token bit**, further a monitor bit, priority bits, and reservation bits.
- Frame control marks the kind of the frame: Data, control,…

Frame Format for Token Ring

- Token frame format



Frame Format for Token Ring

- Acknowledgement in Token Ring
  - Frame status contains confirmation bits A and C. If a frame arrives at the station with the destination address, bit A is set. If the station processes the frame, also bit C is set. When the sending station gets the frame back, it can see:
    - A=0, C=0: the receiving station is not working
    - A=1, C=0: station is working, but frame was not accepted
    - A=1, C=1: frame was received correctly
    - To protect against bit errors, both bits are doubly present.
  - The addresses and the checksum are identical to Ethernet.
- Access Control Bits
  - The monitor bit serves for recognition of a second frame circulation
  - The priority bits provide several priorities. They indicate the priority of the token. If a station wants to send with priority n, it must wait for a token of priority n or higher.
  - The reservation bits permit a station to reserve the next frame for itself. If a station wants to do this, it registers its priority into the reservation bits. This is only possible, if not already a higher priority is registered. During the next token generation, the priority is copied into the priority bits.

Ring Maintenance

- Monitor Station
  - To check the correct function of the ring, a monitor station is introduced. If this station crashes, another station is raised as monitor station: if a station recognizes that the monitor is inactive, this station sends a certain token (CLAIM_TOKEN). This can be done by several stations simultaneously.
  - If such a message arrives with a smaller ID then suppress it.
  - If a message arrives with larger ID then pass it on.
  - If a CLAIM_TOKEN message arrives with own ID: this station is the new monitor.
- Tasks of the Monitor Station
  - Generation of a new token after a token loss
  - Reaction to ring collapse
  - Removal of frame fragments
  - Deletion of old, circulating frames
- For each problem an own token is defined. Additionally – if necessary – also timers are used.

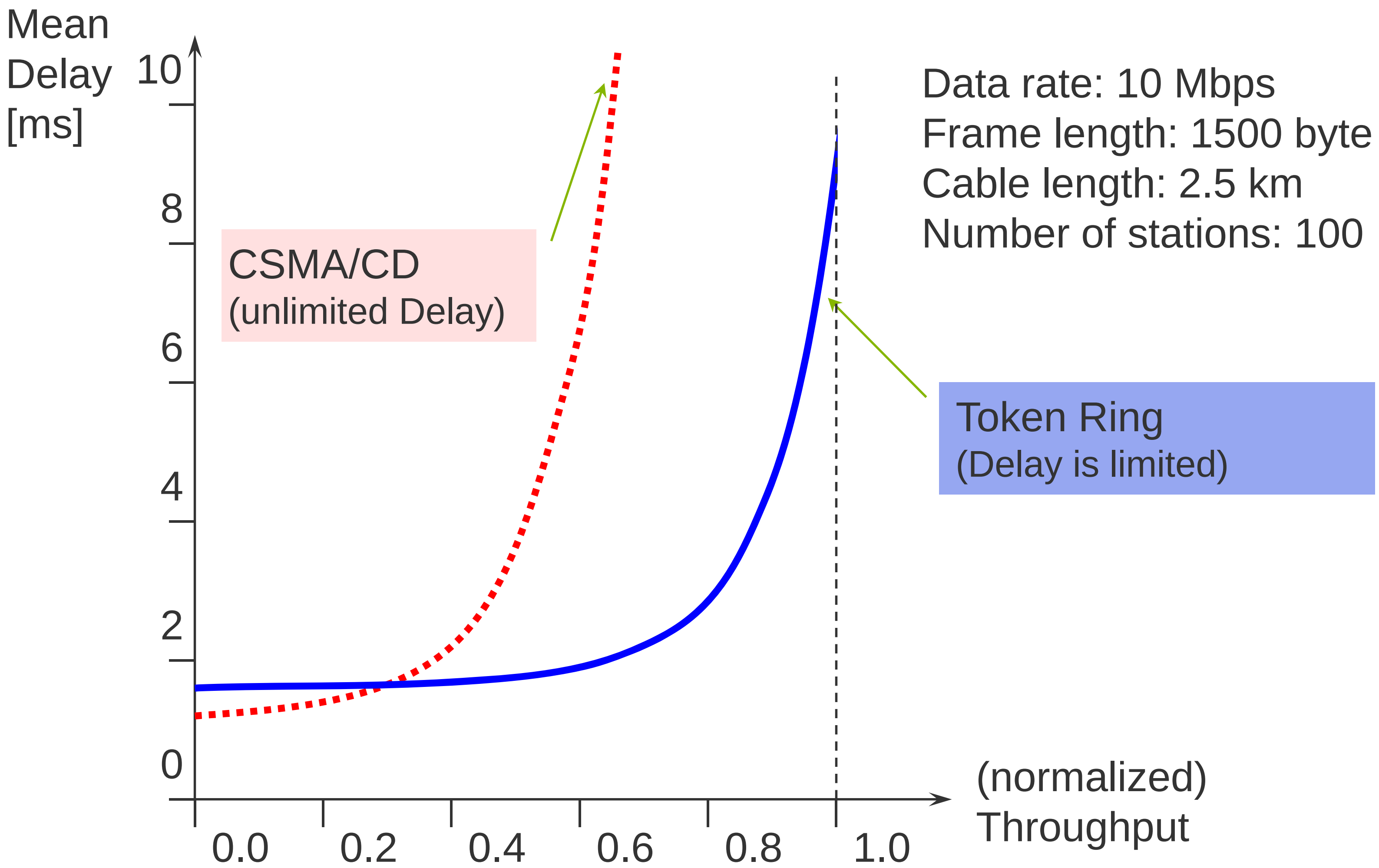
Token Ring vs. CSMA/CD

- CSMA/CD
  - Advantages
    - Widely deployed, high expertise and experience
    - Simple protocol
    - Installation of stations during operation (plug-and-play)
    - Passive cable
    - Low delay by low traffic
  - Disadvantages
    - Analogous components, minimum frame length of 64 byte, maximum frame length 1,500 byte
    - Probabilistic, no priorities
    - Limited cable length
    - Poor performance by high load
- Token Ring
  - Advantages
    - full digital
    - Automatic recognition and elimination of cable problems by wiring-centers
    - Provides priorities
    - Short frames possible, frame length restricted by token hold time
    - Good performance by high load
  - Disadvantages
    - Central monitor
    - Delay by low load
    - Problems at the monitor may affect the whole ring

CSMA/CD vs. Token Bus vs. Token Ring

- CSMA/CD
  - Advantages
    - Widely deployed, high expertise and experience
    - Simple protocol
    - Installation of stations during operation (plug-and-play)
    - Passive cable
    - Low delay by low traffic
  - Disadvantages
    - Analogous components, min. frame length 64 byte, max. frame length 1500 byte
    - Probabilistic, no priorities
    - Limited cable length
    - Poor performance by high load
- Token Bus
  - Advantages
    - More deterministic than CSMA/CD
    - Short frames possible
    - Provides priorities
    - Provides guarantees
  - Disadvantages
    - Protocol is complicated
    - Lost tokens may cause big problems
    - Analog components
    - Long delay due to token exchange
- Token Ring
  - Advantages
    - full digital
    - Automatic recognition and elimination of cable problems by wiring-centers
    - Provides priorities
    - Short frames possible, frame length restricted by token hold time
    - Good performance by high load
  - Disadvantages
    - Central monitor
    - Delay by low load
    - Problems at the monitor may affect the whole ring

Token Ring vs. CSMA/CD

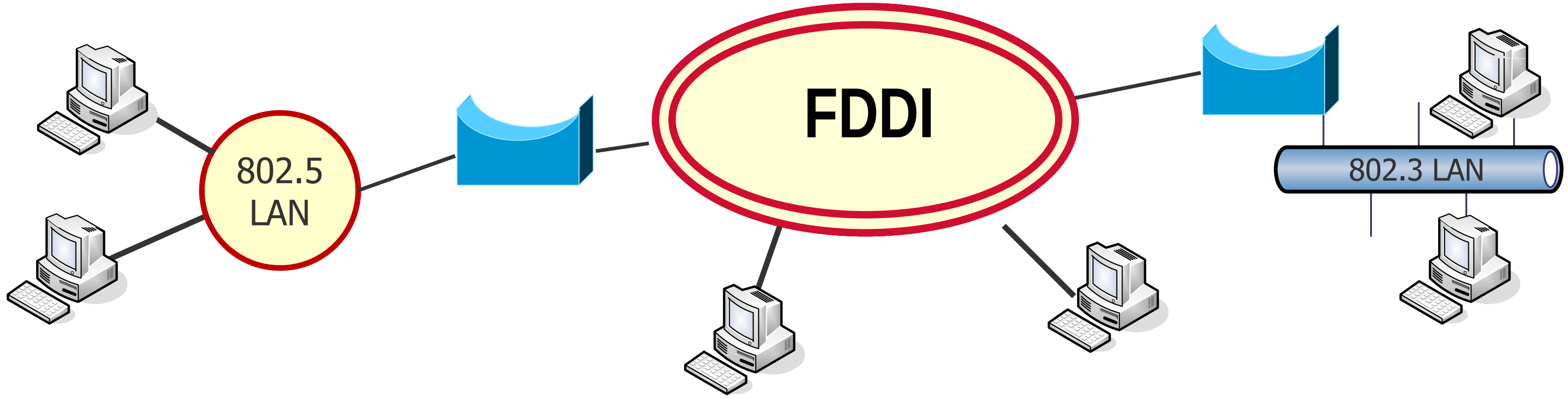


Data rate: 10 Mbps
Frame length: 1500 byte
Cable length: 2.5 km
Number of stations: 100

Fiber Distributed Data Interface (FDDI)

Fiber Distributed Data Interface (FDDI)

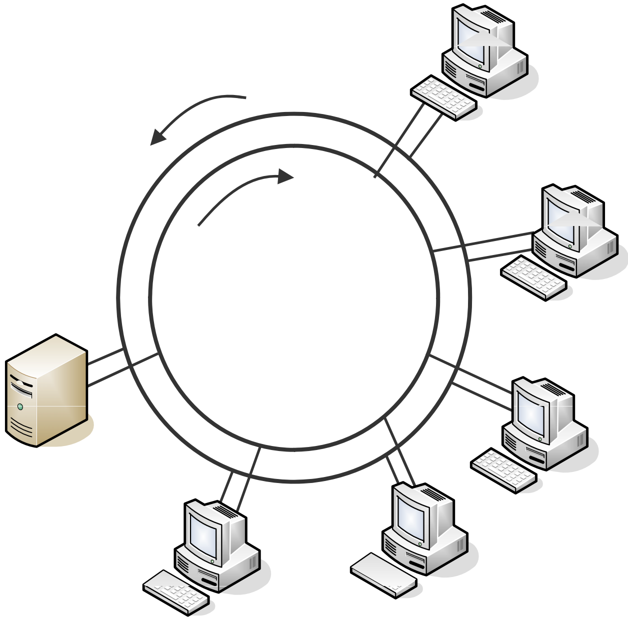
- FDDI is a high performance token ring LAN based on optical fibers
- ANSI standard X3T9.5
- Data rates of 100 Mbps
- Range of up to 200 km (MAN?)
- Support of up to 1000 stations, with distances of maximally 2 km
- Often used as Backbone for small LANs



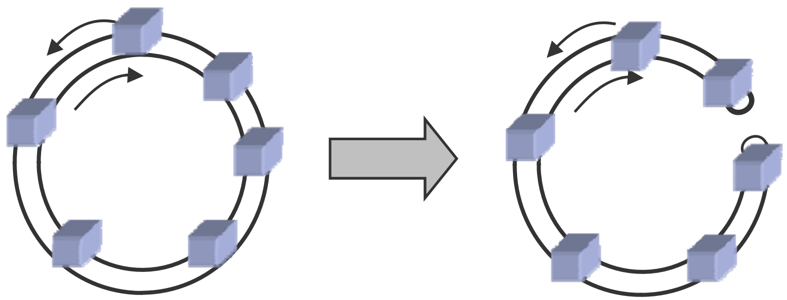
- Successor: FDDI-II, supports besides normal data also synchronous circuit switched PCM data (speech) and ISDN traffic
- Variant: CDDI (Copper Distributed Data Interface), with 100 Mbps over Twisted Pair

Structure of FDDI

Wiring within FDDI: **2** optical fiber rings with opposite transmission direction



- During normal operation, only the primary ring is used, the secondary ring remains in readiness
- If the ring breaks, the other one (also called protection ring) can be used.
- If both rings break or if a station fails, the rings can be combined into only one, which has double length:

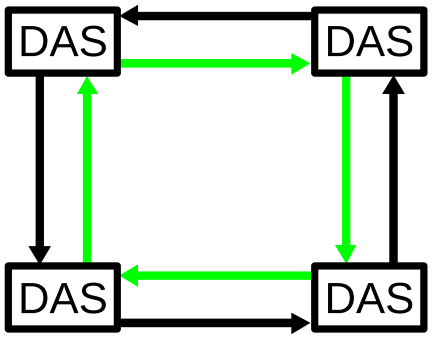


Two classes of stations exist: **DAS** (Dual Attachment Station) can be attached to both rings, the cheaper **SAS** (Single Attachment Station) are only attached to one ring.

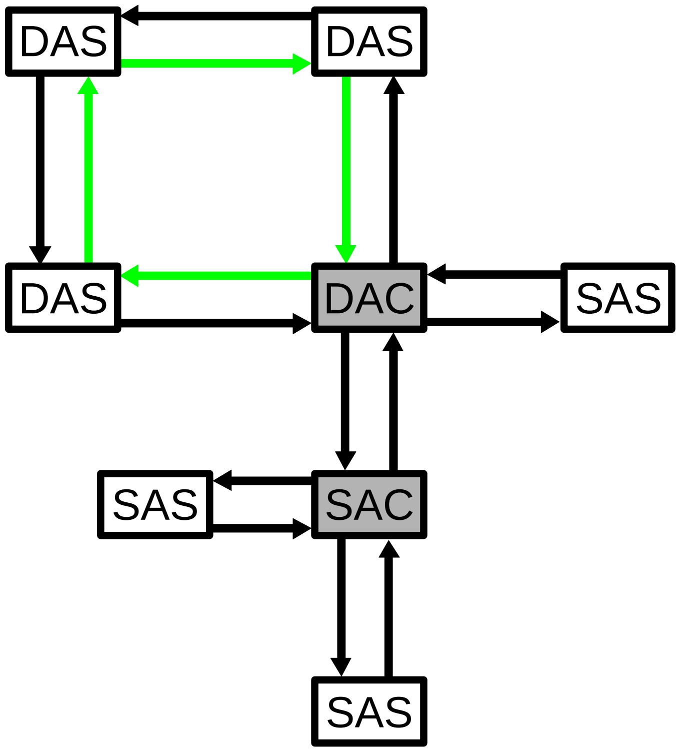
Freie Universität Berlin

FDDI Configurations

Basic double ring

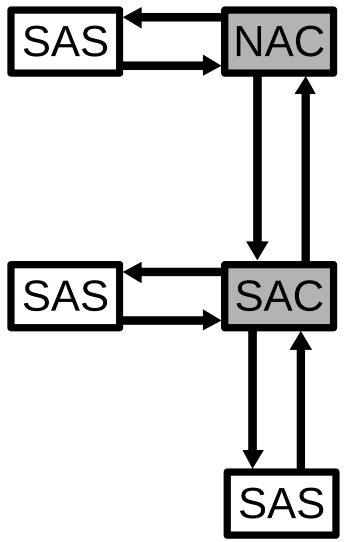


Double ring with connected single ring



"Simple" FDDI ring

NAC is used to create a simple FDDI ring



DAS = Dual Attachment Station

SAS = Single Attachment Station

DAC = Dual Attachment Concentrator

NAC =Null Attachment Concentrator

SAC = Single Attachment Concentrator

By means of the concentrators several rings can be linked.

Transmission within FDDI

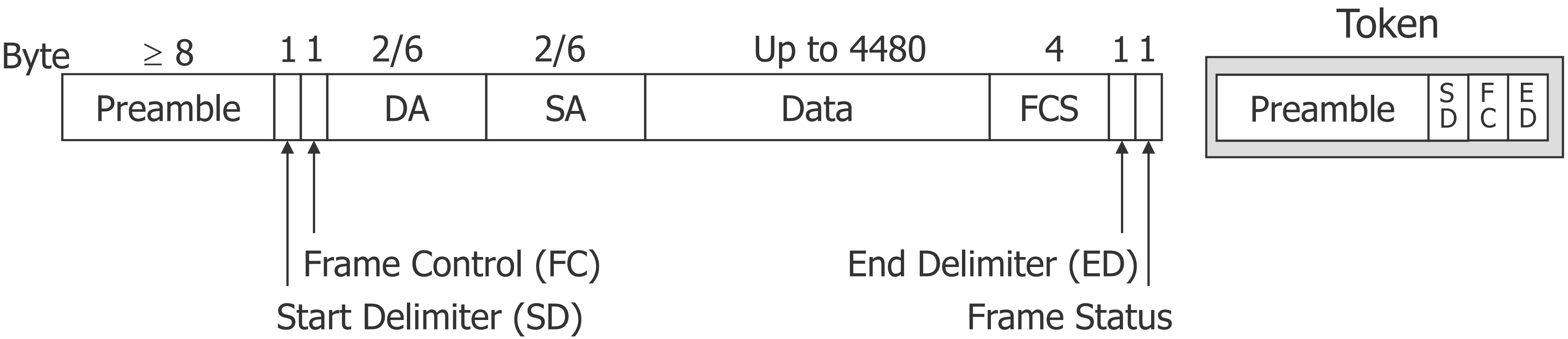
- Coding
  - 4B/5B code, thus coding of 4 bits of data in 5 bits which are transferred
- Synchronization
  - Transmission of a long preamble in order to synchronize the receiver to the sender clock. The clocks of all stations must run stable on at least 0.005%. With such a stability, frames with up to 4500 byte of data can be transferred without the receiver losing the clock pulse.
- Protocols
  - The fundamental protocols of FDDI are similar to IEEE 802.5 (token ring): in order to transmit data, a station must acquire the token. Then it transfers its frame and takes it from the ring when it returns to it. Due to the expansion of FDDI, a single token is unpractical. Therefore, FDDI transfers in the multiple token mode.
- Ring and station management also are similar to IEEE 802.5, additionally a function for deviating traffic to the protection ring is included.

Synchronous Transmission of Data

- Original transmission principle within FDDI: Use of asynchronous frames, i.e., sending can be started any time.
- Additionally, with FDDI-II also the use of synchronous frames for circuit switched PCM or ISDN data (telephony) is possible:
  - every 125 μs a master station produces synchronous frames for reaching the 8000 samples / second necessary for PCM.
  - every frame consists of 16 byte for non-circuit-switched data and up to 96 byte for circuit switched data (up to 96 PCM channels per frame).
  - if a station once uses fixed slots in a frame, these are considered for it as reserved until the station releases them expressly (implicit reservation).
  - unused synchronous slots of the frame are assigned on request to any station.

Data Frames in FDDI

The data frames are similar to those used in Token Ring:



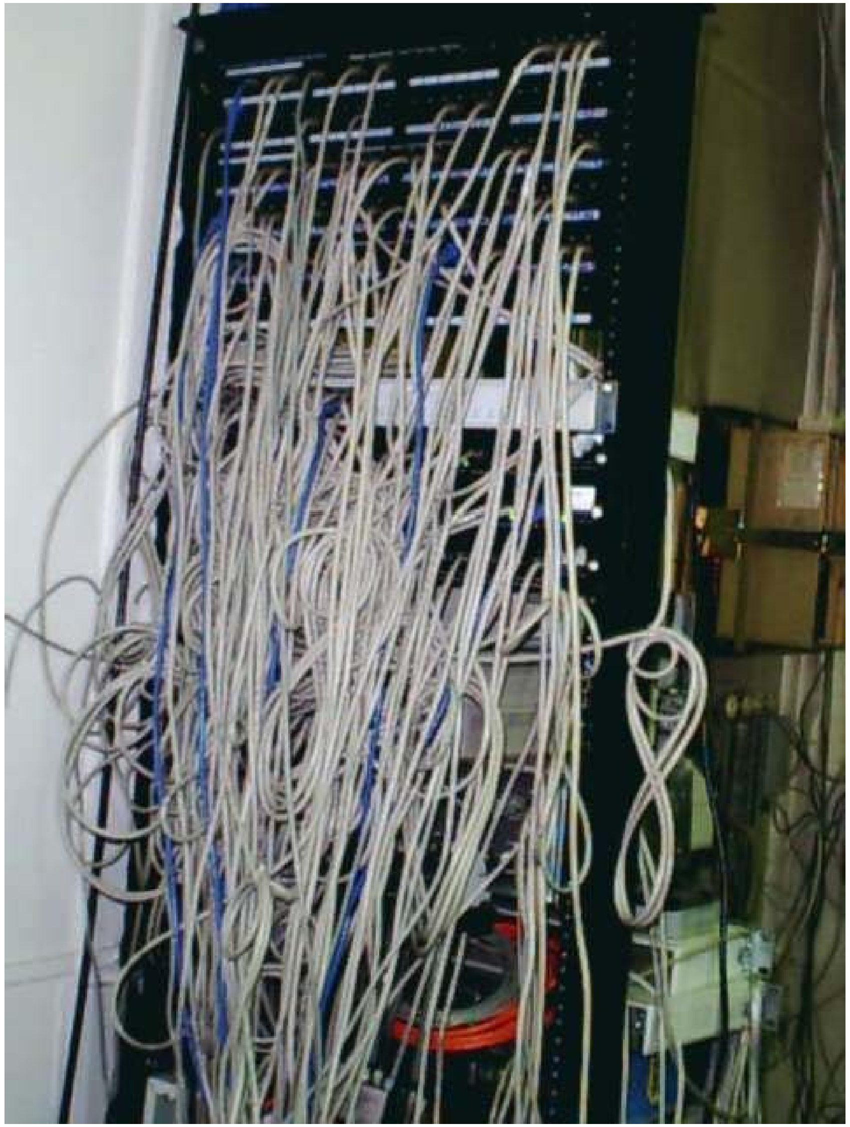
- The **preamble** is used for the synchronization as well as for the preparation of the stations to a following transmission
- **Start** and **end delimiter** are being used for marking the frame
- **Frame control** specifies the type of the frame: data, control, synchronous/asynchronous,…
  - Several tokens are distinguished for different traffic types.
- **Frame status** contains confirmation bits as in IEEE 802.5
- **Addresses** and the **FCS** are as in IEEE 802.5

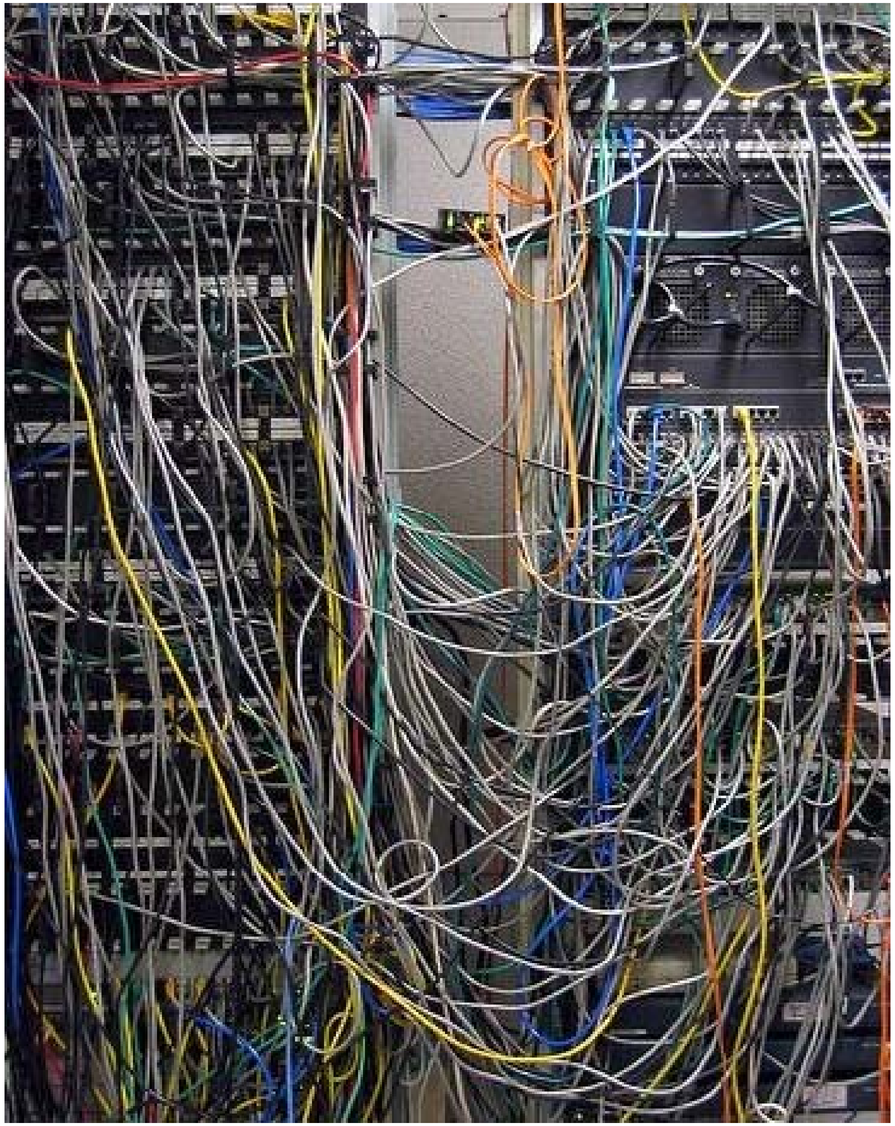
Structured Cabling

Structured Cabling

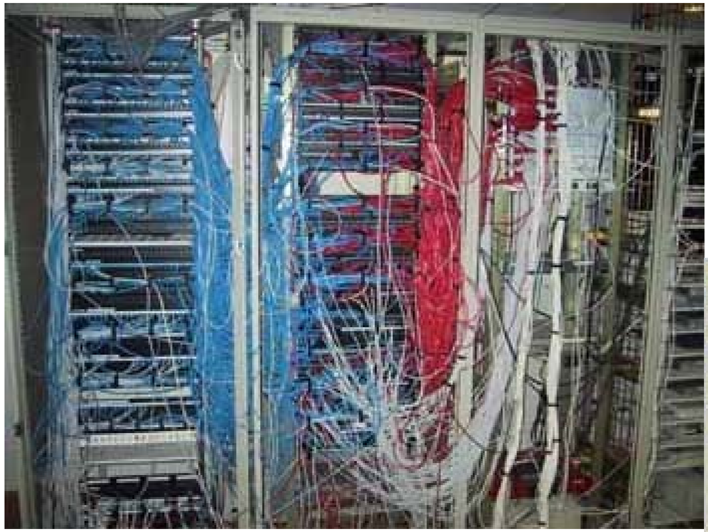
- Why we need a structured cabling?

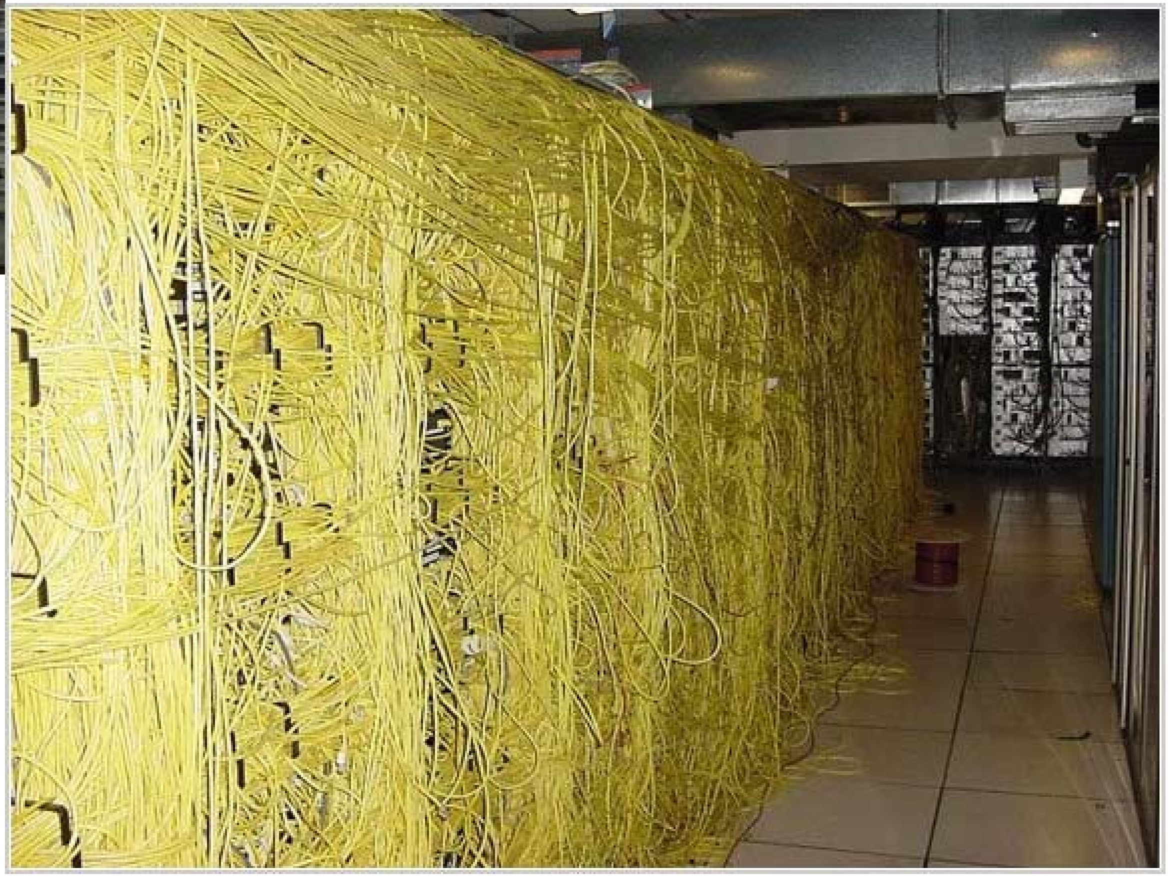
Structured Cabling



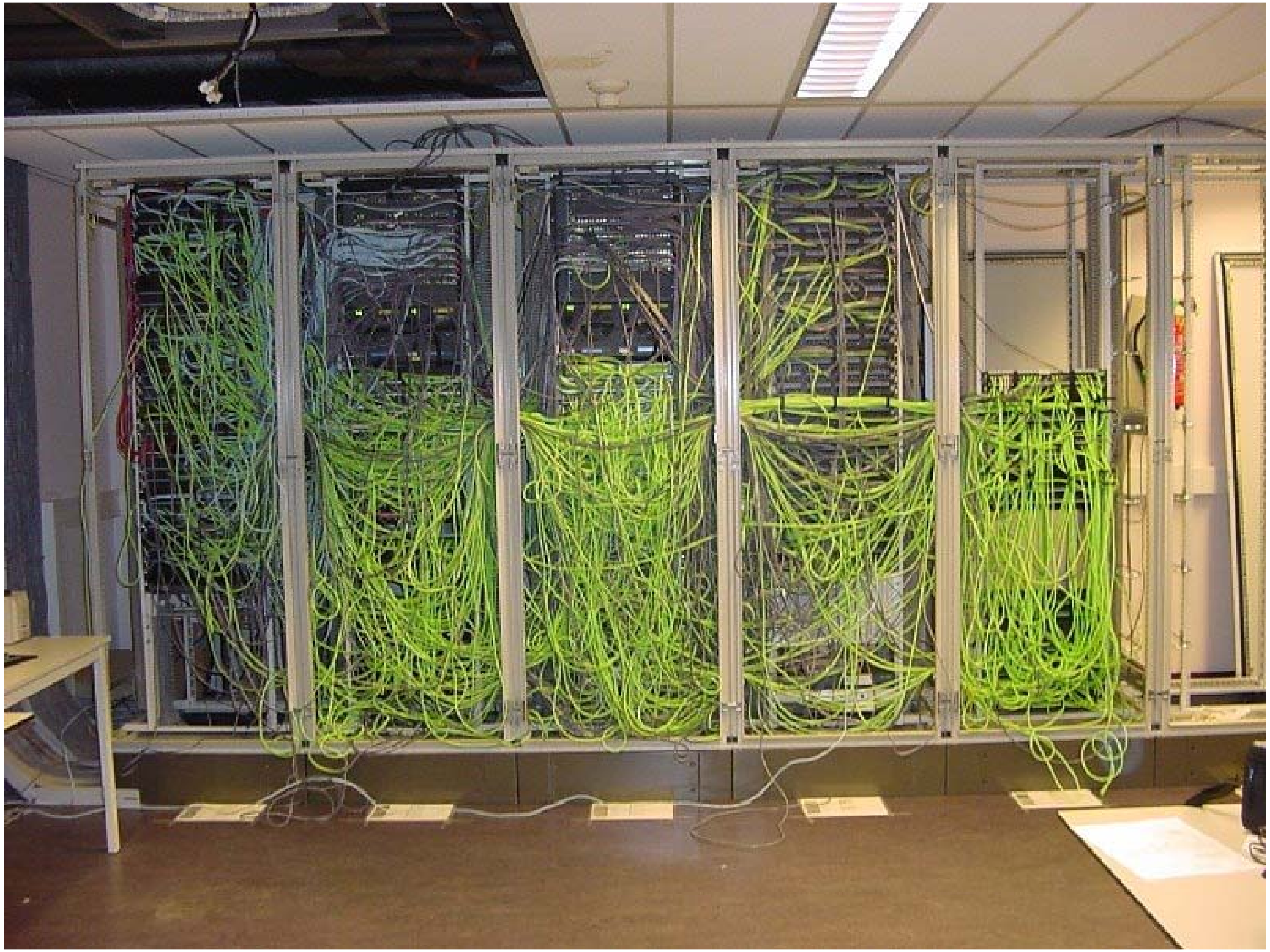


Structured Cabling

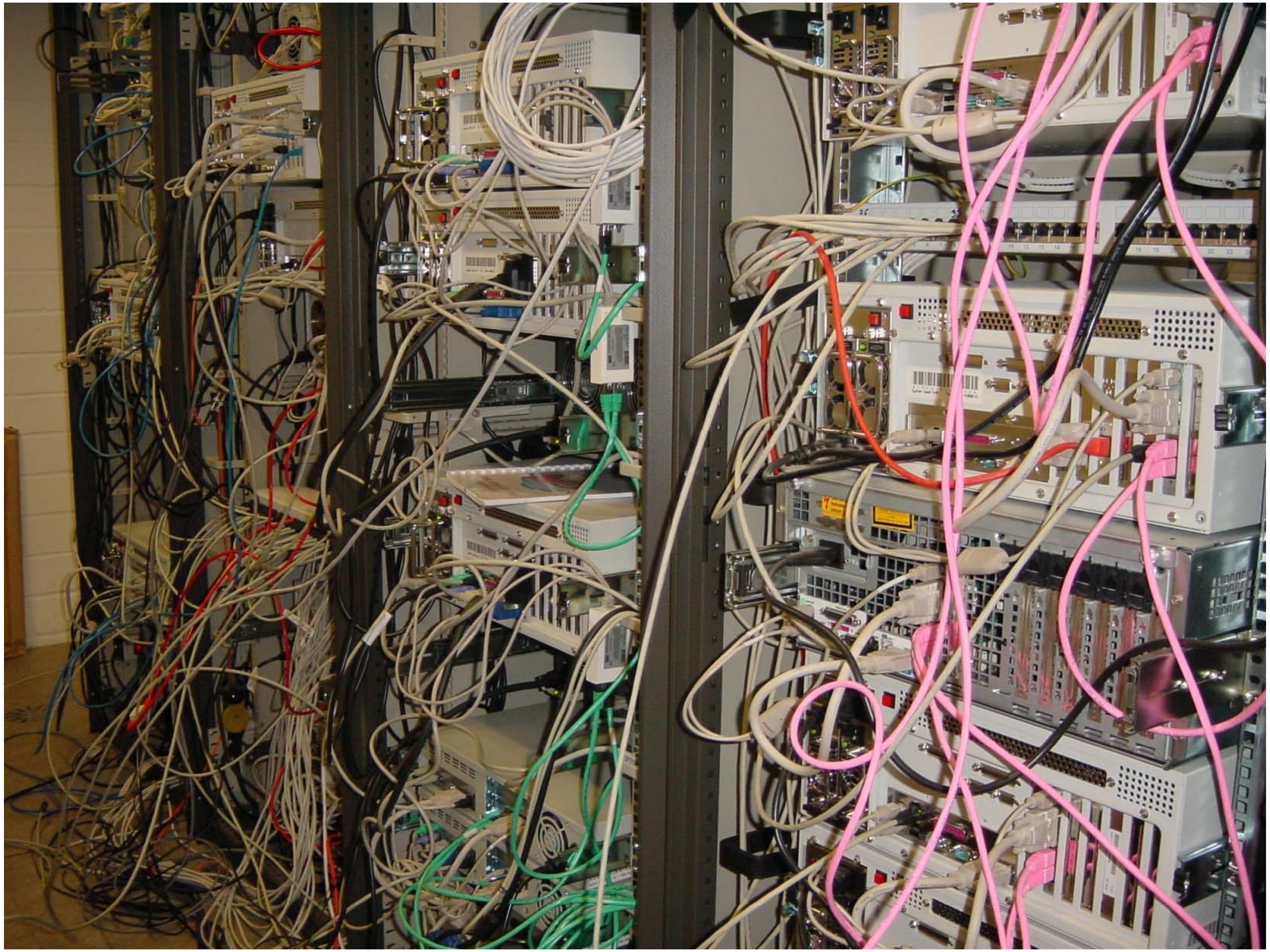




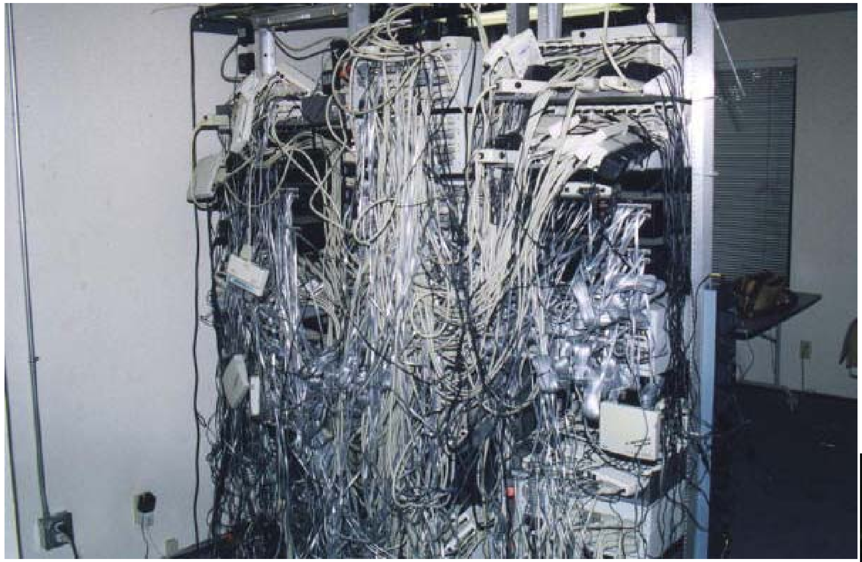
Structured Cabling

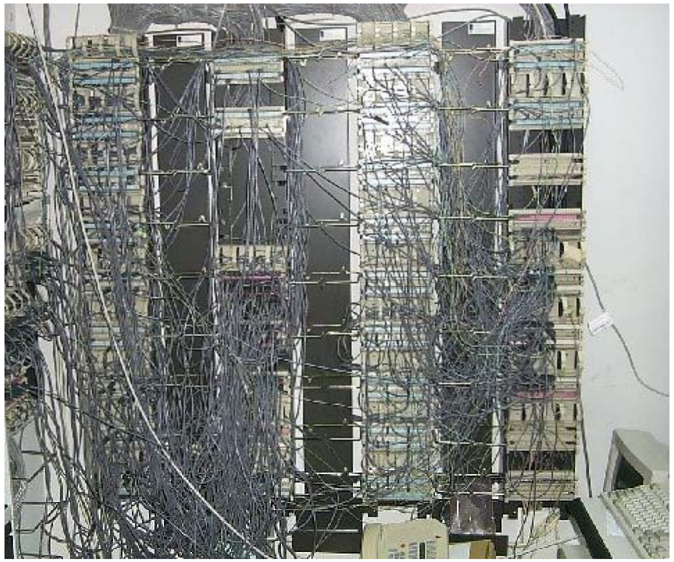


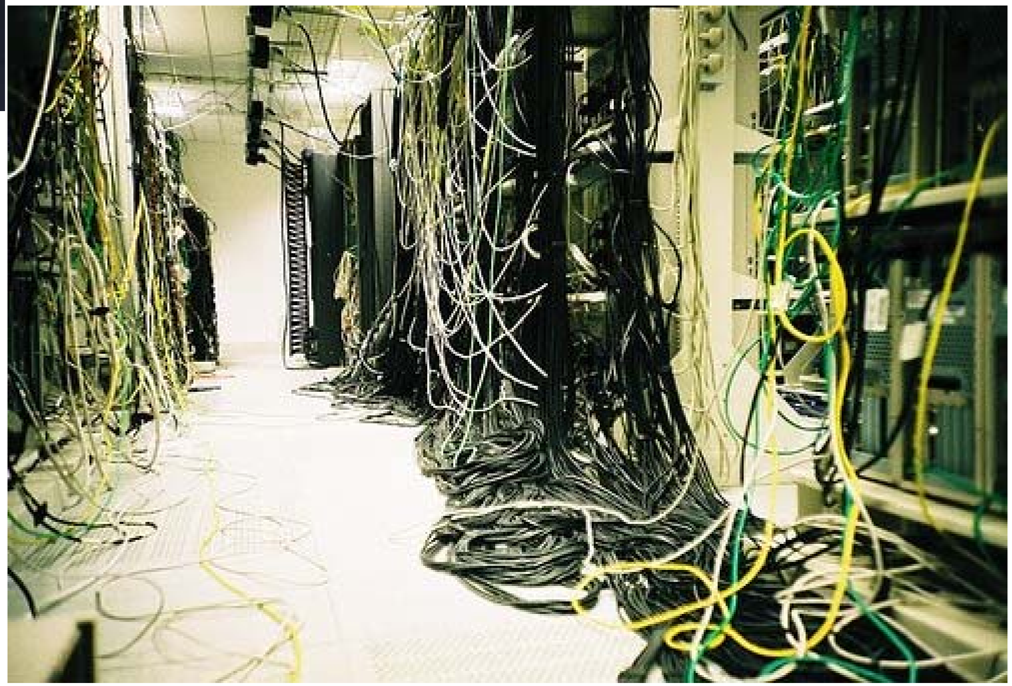
Structured Cabling



Structured Cabling

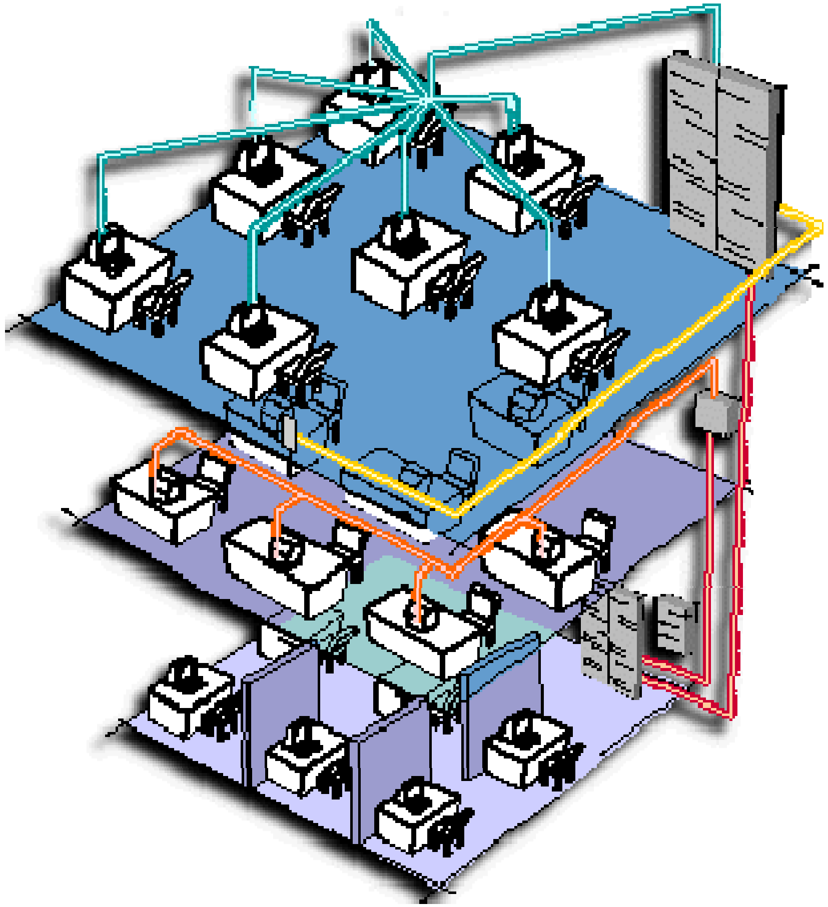






Structured Cabling

- Structured cabling: Partitioning of a network, i.e., cabling infrastructure, which is connected to a backbone or a central switch
  - Each user outlet is cabled to a communications closet using individual cables
  - In the communications closet the user outlets terminate on patch panels
  - Patch panels are mounted usually on 19" racks



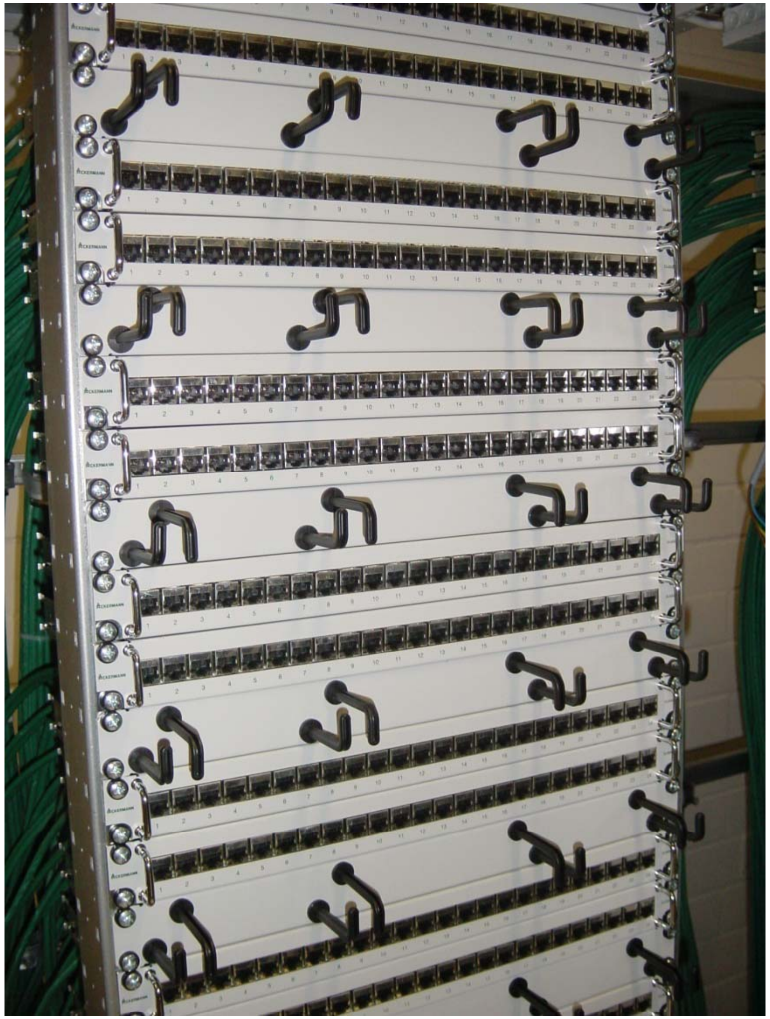
Structured Cabling

- Advantages of structured cabling
  - Consistency
    - Usage of the same cabling systems for data, voice, and video
  - Support for multi-vendor equipment
    - A standard based cable system will support equipment from different vendors
  - Simplify modifications
    - Supports the changes in within the system, e.g., adding, changing, and moving of equipment
  - Simplify troubleshooting
    - Problems are less likely to down the entire network and simplifies the isolation and fixing of problems
  - Support for future applications
  - Support for fault isolation
    - By dividing the entire infrastructure into simple manageable blocks, it is easy to test and isolate specific points of fault and correct them

Structured Cabling

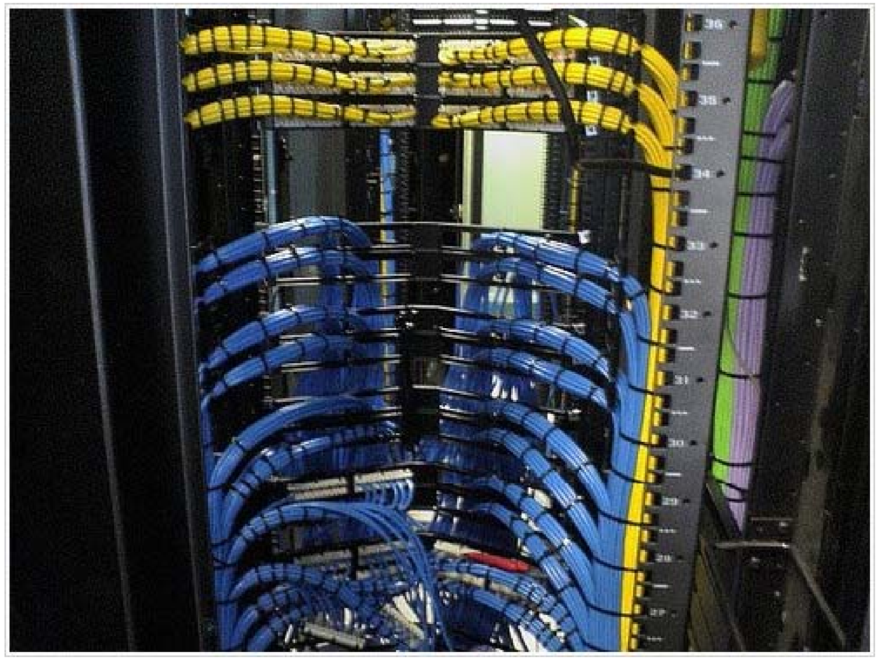
Structured Cabling

Structured Cabling



Structured Cabling

Structured Cabling



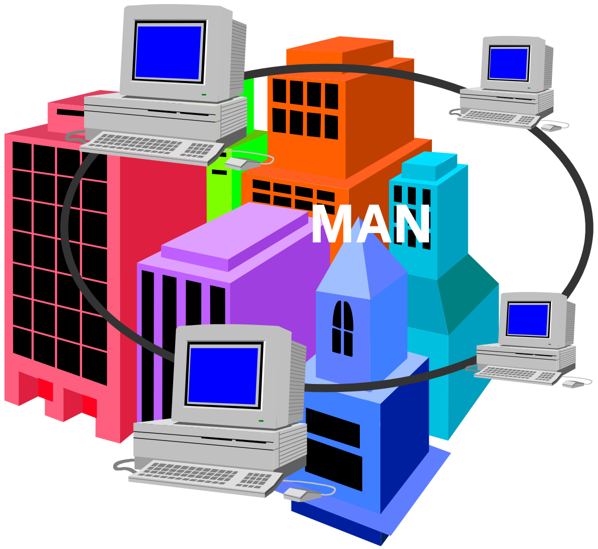
Structured Cabling

Structured Cabling

Metropolitan Area Networks (MAN)

Metropolitan Area Networks

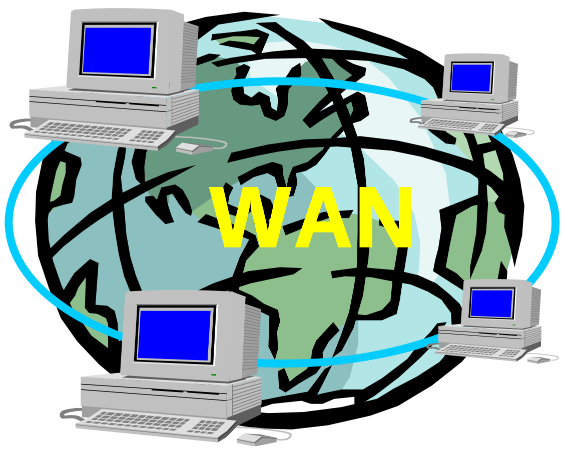
- Properties of MAN
  - Bridges larger distances than a LAN, usage e.g. within the city range or on a campus
  - Only one or two cables, no switching elements. Thus a simple network design is achieved
  - All computers are attached to a broadcast medium
  - Main difference between LAN and MAN: utilization of a clock pulse
- Examples:
  - Distributed Queue Dual Bus (DQDB)
  - Gigabit Ethernet



Wide Area Networks (WAN)

Wide Area Networks

- Characteristics of Wide Area Networks
  - Bridging of any distance
  - Usually for covering of a country or a continent
  - Topology is normally irregular due to orientation to current needs.
    - Therefore, not the shared access to a medium is the core idea, but the thought “how to achieve the fast and reliable transmission of as much data as possible over a long distance”.
  - Usually quite complex interconnections of sub-networks which are owned by different operators
  - No broadcast, but point-to-point connections
  - Range: several 1000 km
- Examples:
  - Frame Relay
  - Asynchronous Transfer Mode (ATM)
  - Synchronous Digital Hierarchy (SDH)

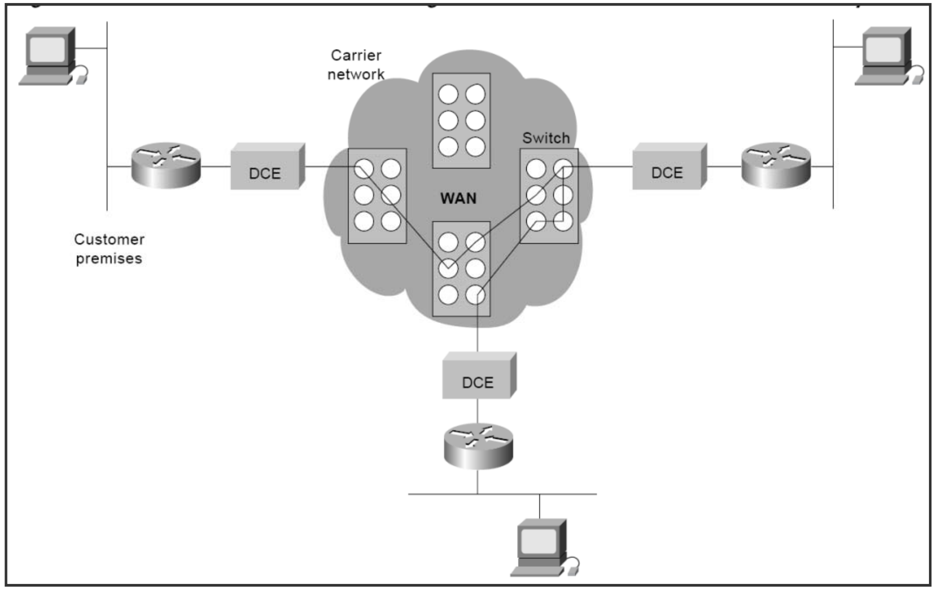


Transmission Technologies for WANs

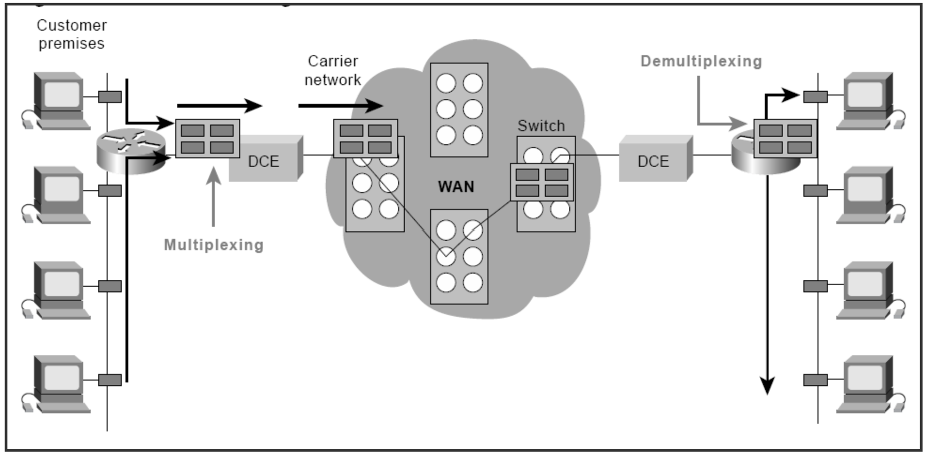
- Point-to-Point Links
  - Provision of a single WAN connection from a customer to a remote network
  - Example: telephone lines. Usually communication resources are leased from the provider.
  - Accounting is based on the leased capacity and the distance to the receiver.
- Circuit Switching
  - A connection is established when required, communication resources are reserved exclusively. After the communication process, the resources are released.
  - Example: Integrated Services Digital Network (ISDN)
- Packet Switching
  - "Enhancement" of the "Circuit Switching" and the Point-to-Point links.
  - Shared usage of the resources of one provider by several users, i.e., one physical connection is used by several virtual resources.
  - Shared usage reduces costs

Transmission Technologies for WANs

- Circuit Switching
  - Reservation of resources for the time of the connection



- Packet Switching
  - Sharing of the resources



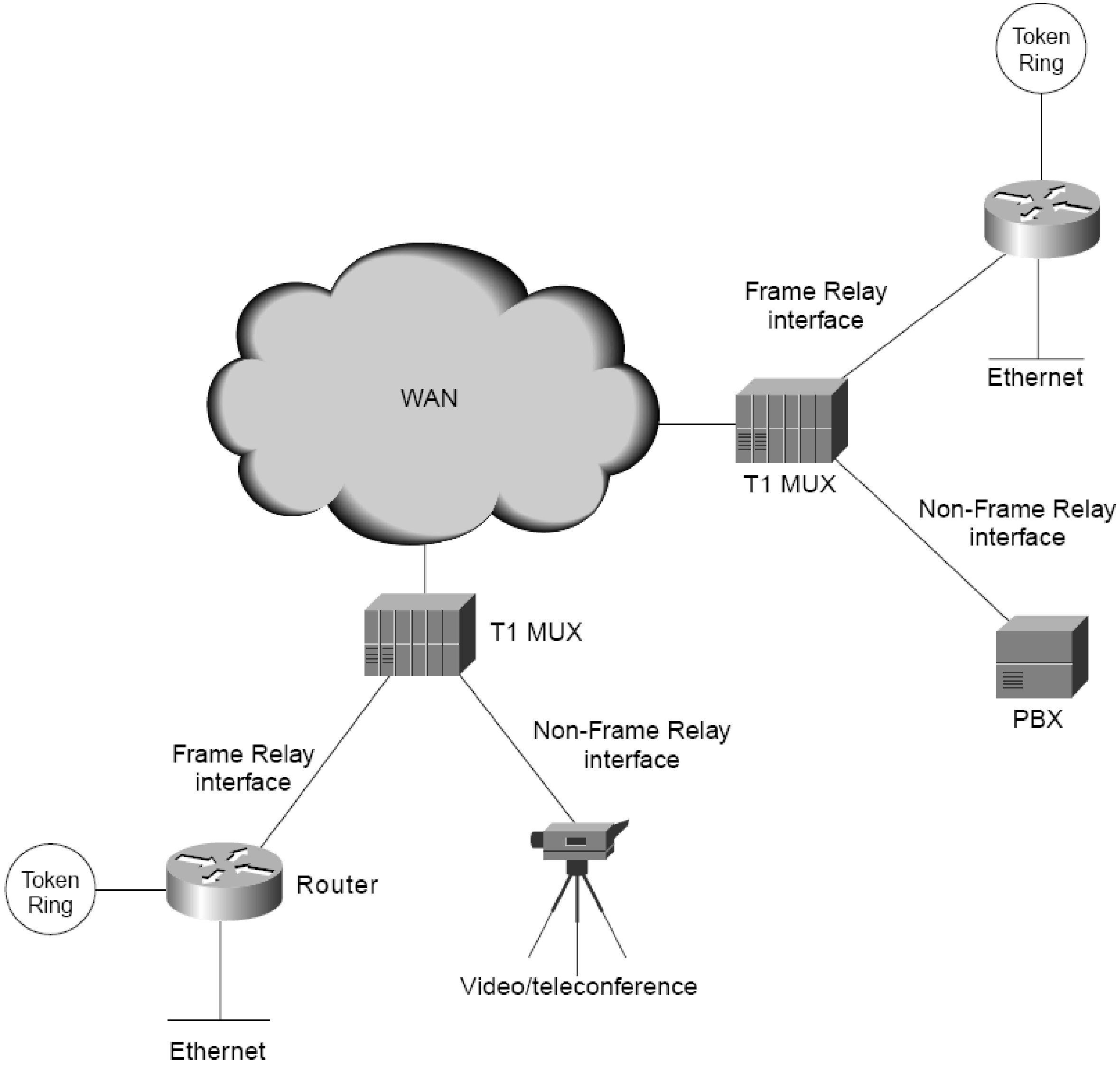
Packet Switching

- Packet Switching is the most common communication technology in WANs today
  - The provider of communication resources provides virtual connections (virtual circuits, circuit switching) between remote stations/networks, the data are transferred in the form of packets.
  - Examples: Frame Relay, ATM, OSI X.25

- Two types of Virtual Circuits:
  - Switched Virtual Circuits (SVCs)
    - Useful for senders with sporadic transmission wishes.
    - A virtual connection is established, data are transferred, after the transmission the connection is terminated and the resources are released.
  - Permanent Virtual Circuits (PVCs)
    - Useful for senders which need to transfer data permanently.
    - The connection is established permanently, there exists only the phase of the data transfer.

Frame Relay

Frame Relay Network Implementation

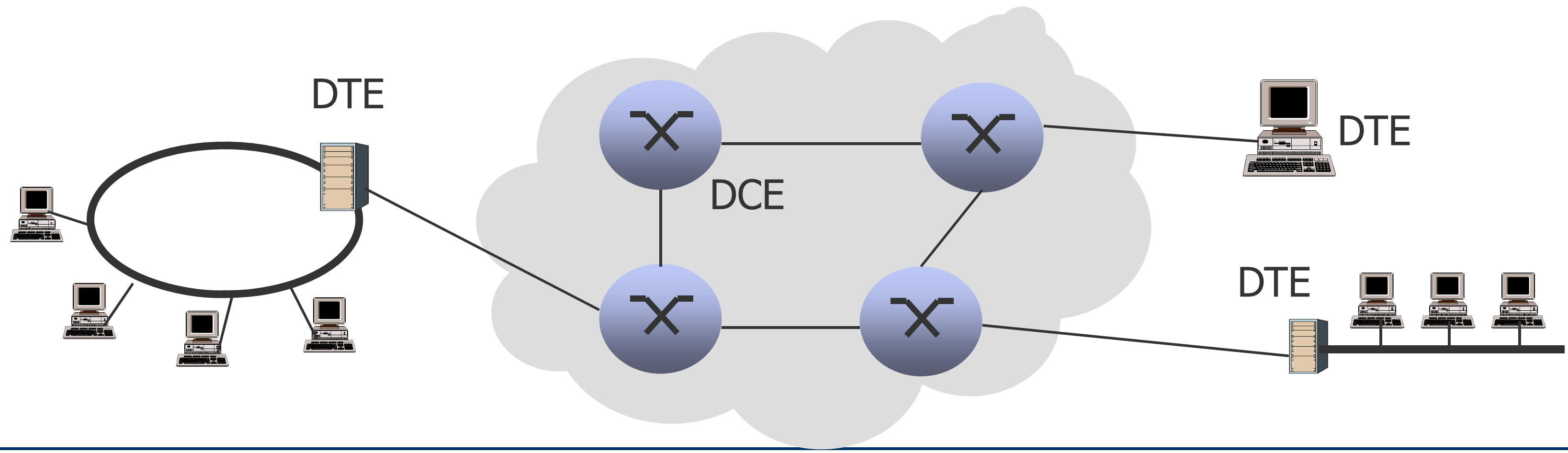


Frame Relay

- Based on Packet Switching, i.e., the **transmission** of data **packets**
- Originally designed for the use **between** ISDN devices, usage has spread further
- The packets can have **variable length**
- **Statistical Multiplexing** (i.e. "mixing" of different data streams) for controlling the network access.
    - This enables a flexible, efficient use of the available bandwidth
- A first standardization took place 1984 by the CCITT. However, it did not result in a complete specification.
- Therefore, in 1990 Northern Telecom, StrataCom, Cisco, and DEC formed a consortium that build up upon the incomplete specification and developed some extensions to Frame Relay which should make a usage in the complex Internet environment possible.
  ➡These extensions were called Local Management Interface (LMI)
  ➡Due to their success, ANSI and CCITT standardized own LMI variants
- Frame Relay finally became internationally standardized by the **ITU-T**, in the USA by **ANSI**.

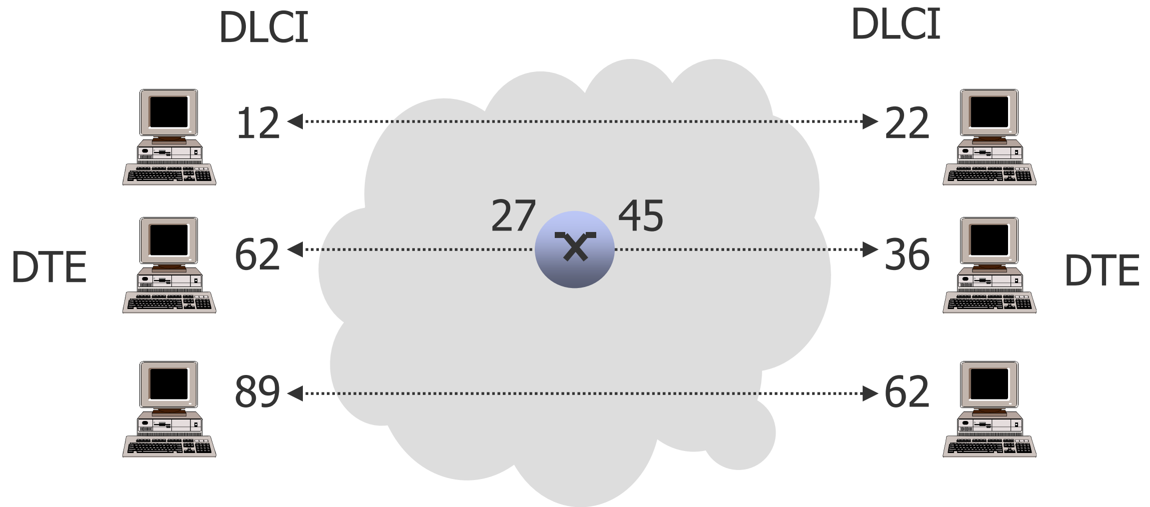
Structure of Frame Relay

- Purpose: simple, **connection-oriented** technology for economic transmission of data with acceptable speed
  - Data transmission rates of 56 Kbps up to 45 Mbps can be leased
  - Mostly used for **permanent virtual connections** for which no signaling for the connection establishment is necessary
- Two device categories can be distinguished:
  - **Data Terminal Equipment (DTE)**
    typically in the possession of the end user, for example PC, router, bridges, …
  - **Data Circuit-Terminating Equipment (DCE)**
    in the possession of a provider. DCEs realize the transmission process. Usually they are implemented as packet switches.



Communication within Frame Relay

- Frame Relay offers connection-oriented communication on the LLC layer:
  - Between two DTEs a virtual connection is established. It is identified by a unique connection identifier (**Data-Link Connection Identifier, DLCI**).
    - Note: DLCIs only refer to one hop, not to the entire connection; in addition they are only unique in a LAN, not globally:



  - The virtual connection offers a bidirectional communication path.
  - Several virtual connections can be **multiplexed** to a **single physical** connection (reduction of equipment and network complexity).

Communication within Frame Relay

- Frame Relay offers two types of connections
- Switched Virtual Circuits (SVC)
  - Temporary connections used when sporadic data transfer between DTEs is required
  - Four states
    - Call setup: Establish virtual circuit between two DTEs
    - Data transfer: Transmit data
    - Idle: Connection is active, but no data to transfer
    - Call termination: Bring down the virtual circuit
- Permanent Virtual Circuits (PVC)
  - Permanent established connections for consistent data transfers between DTEs
  - Do not require a call setup, two states
    - Data transfer: Transmit data
    - Idle: No data to transfer
- ➡ Small protocol overhead, high data transmission rates

Flow Control within Frame Relay

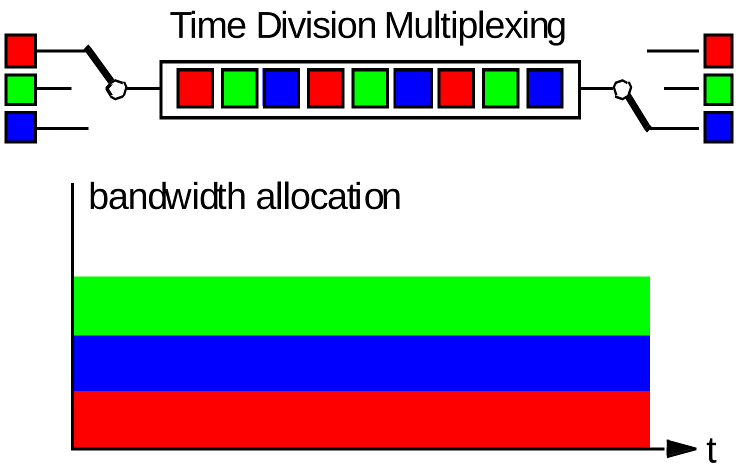
- Flow Control in Frame Relay
  - Frame Relay does not possess an own flow control mechanism for controlling the traffic of each virtual connection.
  - Frame Relay is used typically on reliable network media, therefore flow control can be left over to higher layers.
  - Instead: Notification mechanism (Congestion Notification) to report bottlenecks to higher protocol layers, if a control mechanism on a higher layer is implemented.
- There are two mechanisms for Congestion Notification:
  - Forward-Explicit Congestion Notification (FECN)
    - Initiated, when a DTE sends frames into the network
    - In case of overload, the DCEs (switches) in the network set a special FECN bit to 1
    - If the frame arrives at the receiver with set FECN bit, it recognizes that an overload on the virtual connection is present. The information is relayed to **higher layers**.
  - Backward-Explicit Congestion Notification (BECN)
    - Similarly to FECN, but the BECN bit is set in frames which are transmitted in the opposite direction from frames with set FECN bit

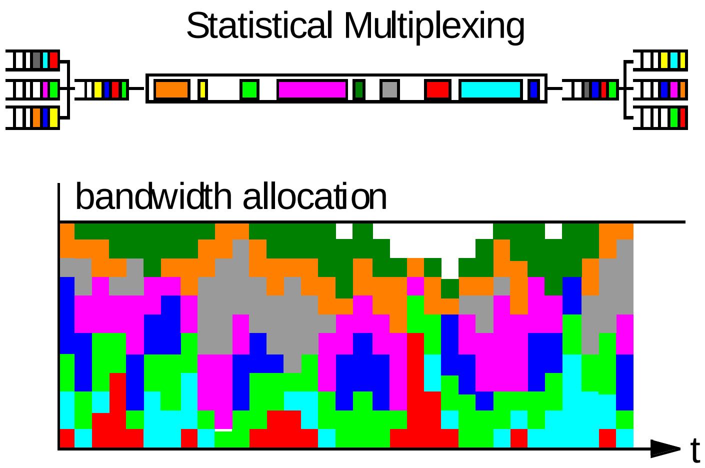
Asynchronous Transfer Mode (ATM)

ATM for the Integration of Data and Telecommunication

- **Telecommunication**
- Primary goal: Telephony
  - Connection-oriented
  - Firm dispatching of resources
  - Performance guarantees
  - Unused resources are lost
  - Small end-to-end delay

- **Data communication**
- Primary goal: Data transfer
  - Connectionless
  - Flexible dispatching of resources
  - No performance guarantees
  - Efficient use of resources
  - Variable end-to-end delay





ATM

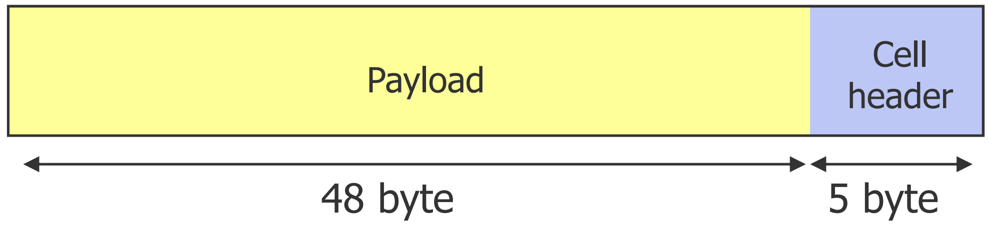
- Different Error Rates
  - Bit Error Rate (BER)
  - Packet Error Rate (PER)
  - Packet Loss Rate (PLR)
  - Packet Insertion Rate (PIR)

Characteristics of ATM

- Characteristics of ATM
  - ITU-T standard (resp. ATM forum) for **cell transmission**
  - Integration of data, speech, and video transmissions
  - Combines advantages of
    - Circuit Switching (granted capacity and constant delay)
    - Packet Switching (flexible and efficient transmission)
  - Cell-based Multiplexing and Switching technology
  - Connection-oriented communication: virtual connections are established
  - Guarantee of quality criteria for the desired connection (bandwidth, delay, …)
    - For doing so, resources are being reserved in the switches.
  - No flow control and error handling
  - Supports PVCs, SVCs, and connection-less transmission
  - Data rates: 34, 155, or 622 Mbps (optical fiber)

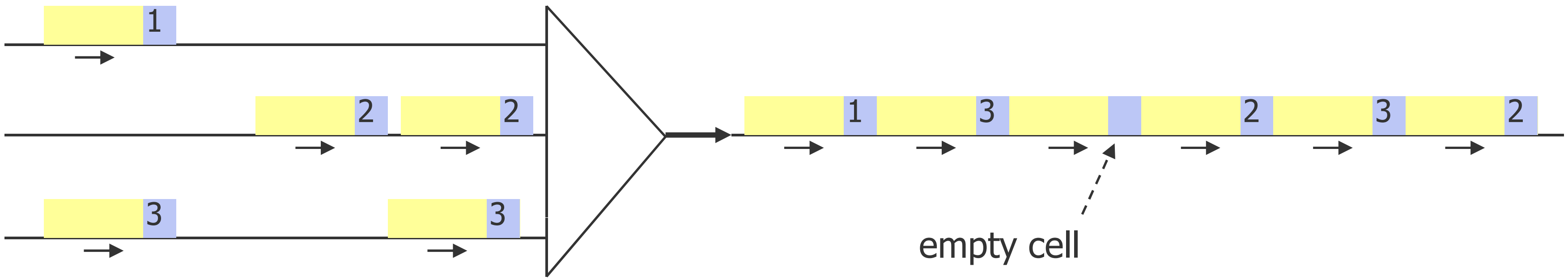
ATM Cells

- No packet switching, but **cell switching**: like time division multiplexing, but without reserved time slots
- Fix cell size: 53 byte



Cell multiplexing on an ATM connection:

- Asynchronous time multiplexing of several virtual connections
- Continuous cell stream
- Unused cells are sent empty
- In overload situations, cells are discarded

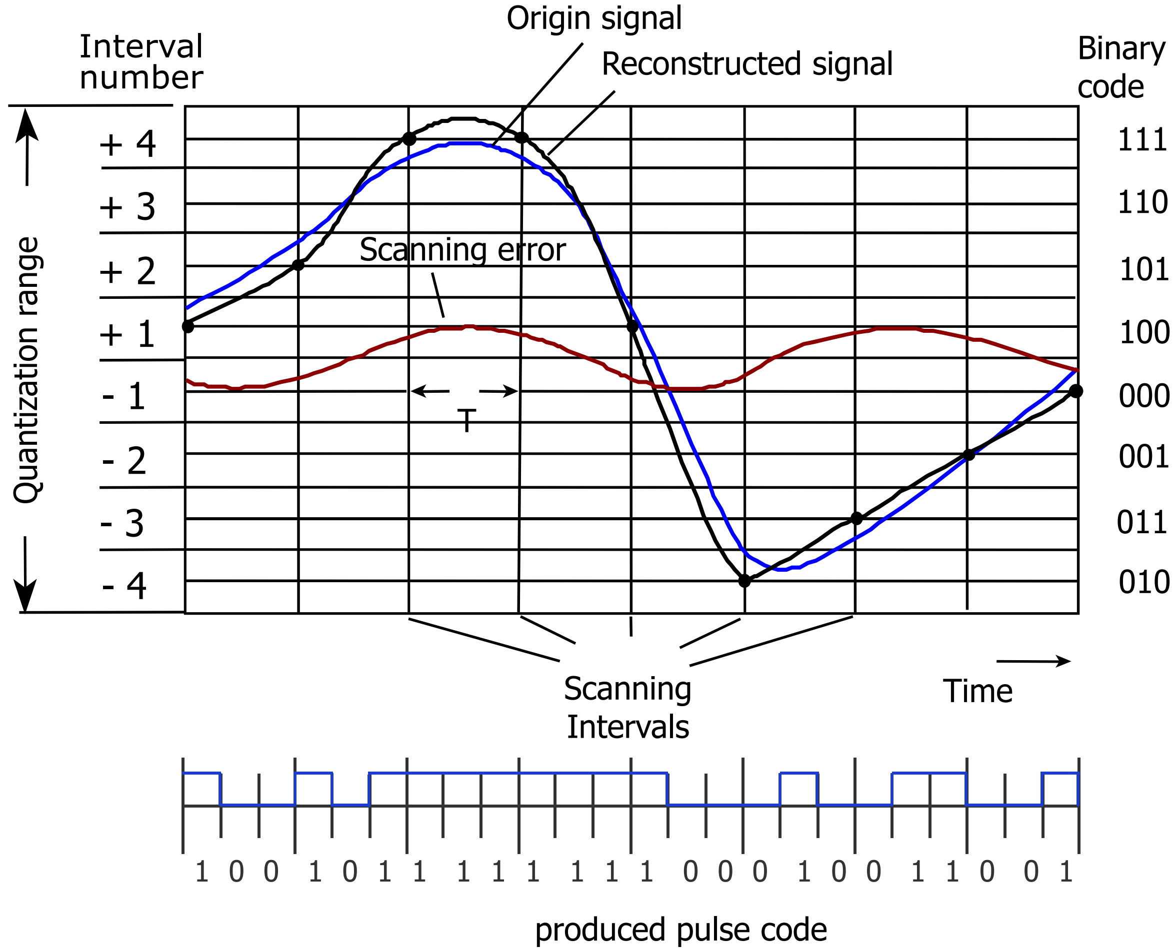


Cell Size: Transmission of Speech

Coding audio: **Pulse-code modulation (PCM)**

- Transformation of analogous into digital signals
- Regular scanning of the analogous signal
- **Scanning theorem (Nyquist):**
  Scanning rate ≥ 2×cutoff frequency of the original signal
  Cutoff frequency of a telephone: 3.4 kHz
  ➡ scanning rate of 8000 Hz
- Each value is quantized with 8 bits (i.e. a little bit rounded).
- A speech data stream therefore has a data rate of
  8 bits × 8000 1/s = 64 kbps

Example (simplification: Quantization with 3 bits)



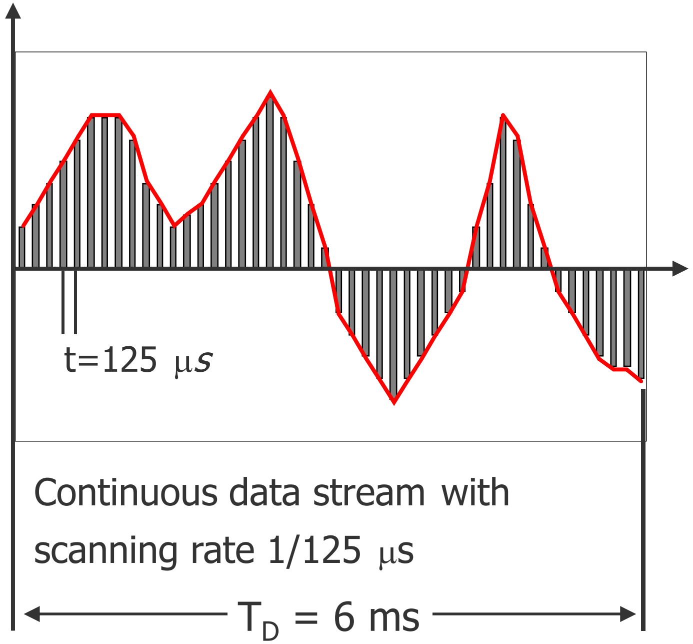
Cell Size within ATM

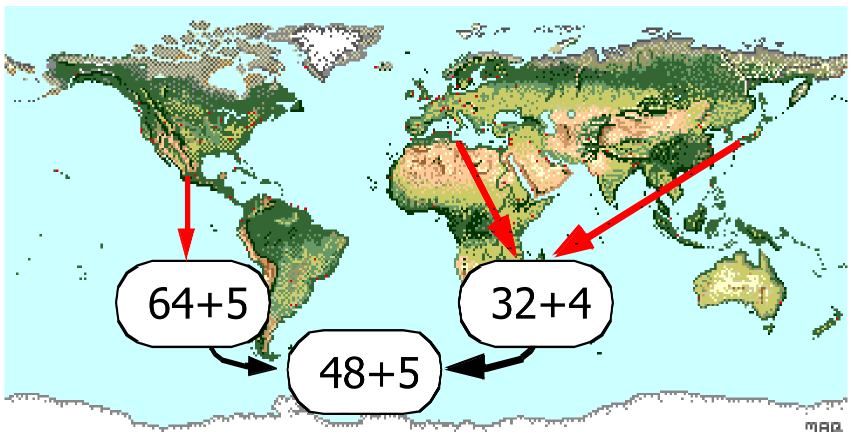
Problem: Delay of the cell stream for speech is 6 ms

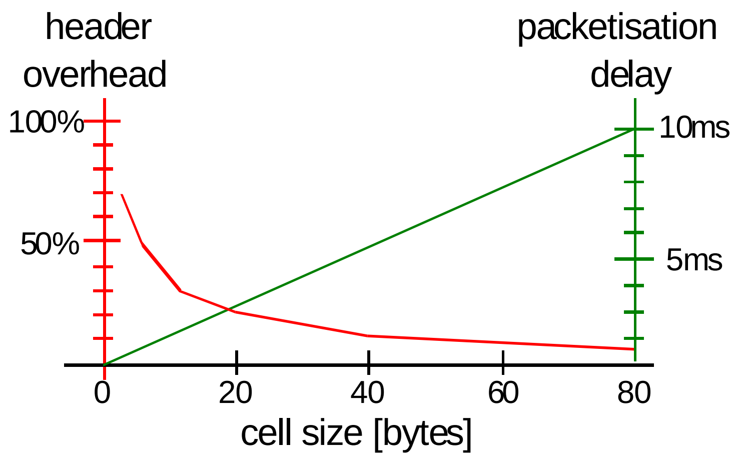
48 samples with 8 bits each
= 48 byte
= Payload for an ATM cell

- Larger cells would cause too large delays during speech transmission
- Smaller cells produce too much overhead for "normal" data (relationship Header/Payload)

i.e. 48 byte is a compromise.

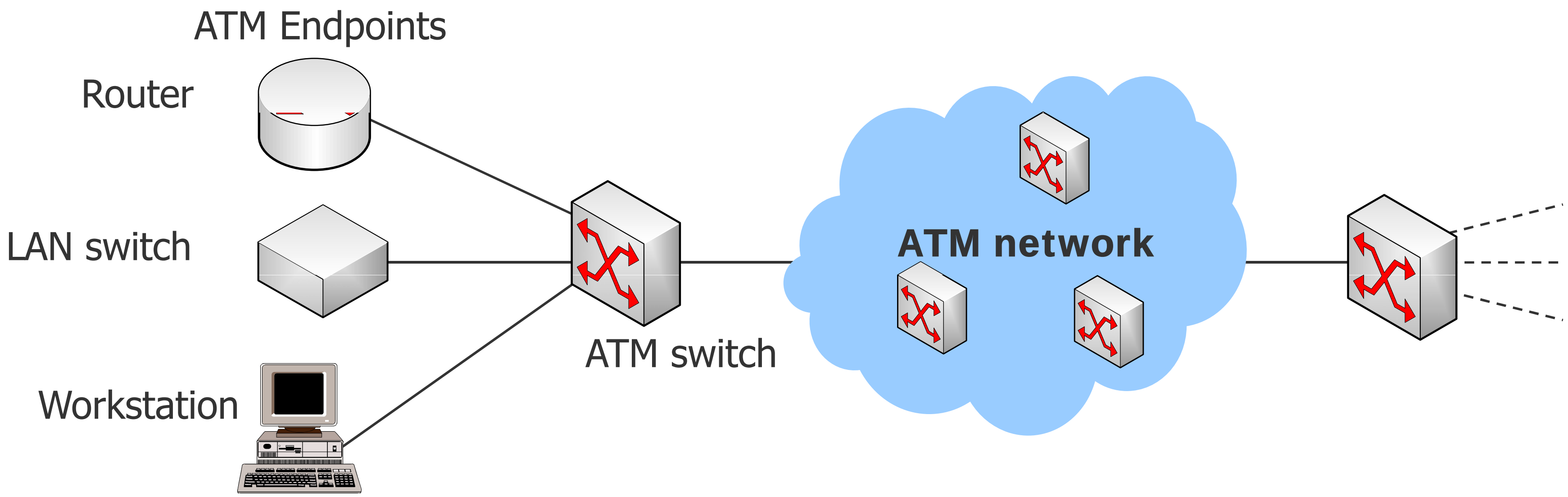






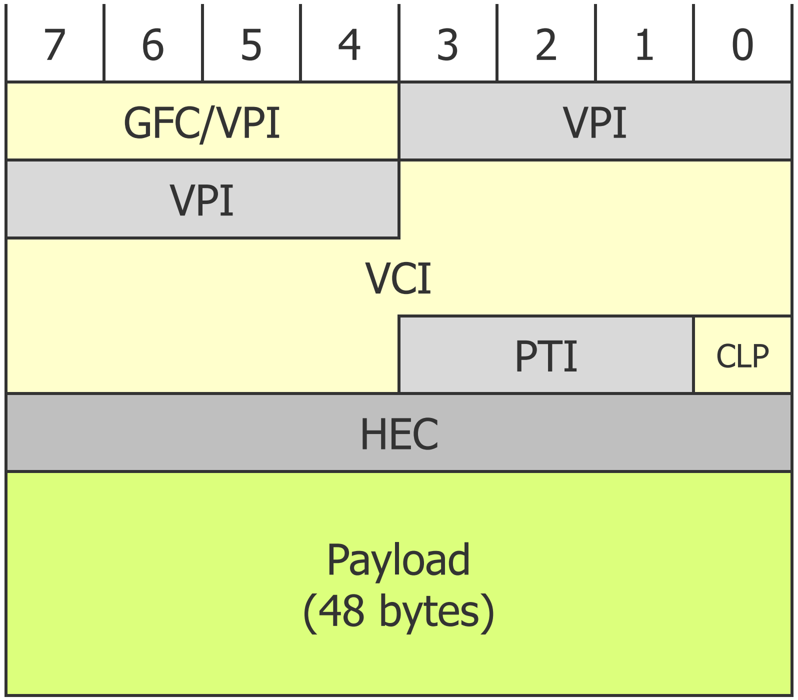
ATM Network

- Two types of components:
  - ATM Switch
    - Dispatching of cells through the network by switches. The cell headers of incoming cells are read and information is updated. Afterwards, the cells are switched to the destination.
  - ATM Endpoint
    - Contains an ATM network interface adapter to connect different networks with the ATM network.



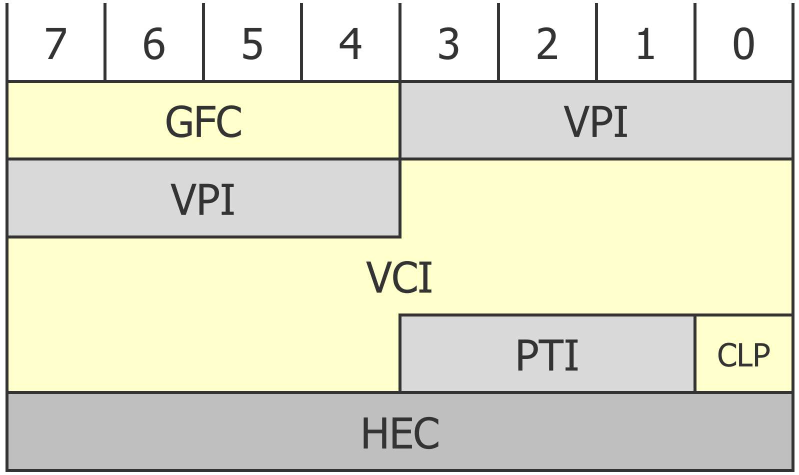
Structure of ATM cells

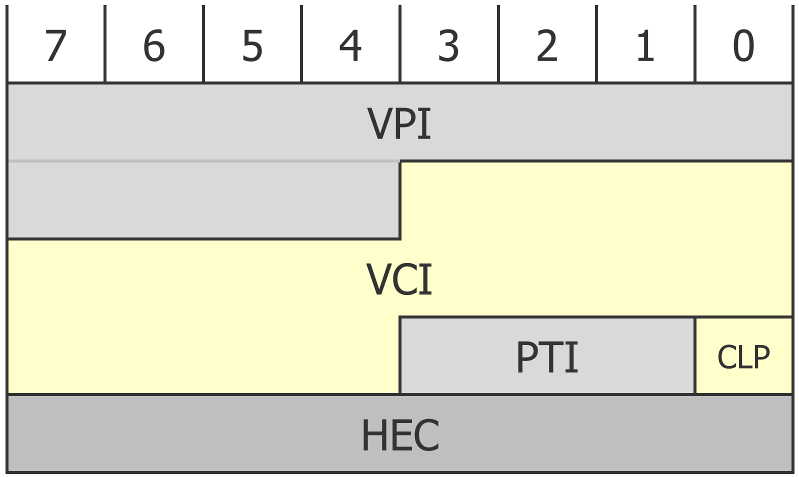
- Two header formats:
  - Communication between switches and endpoints: User-Network Interface (UNI)
    - Communication between ATM switches in private networks
  - Communication between two switches: Network-Network Interface (NNI)



Structure of ATM cells

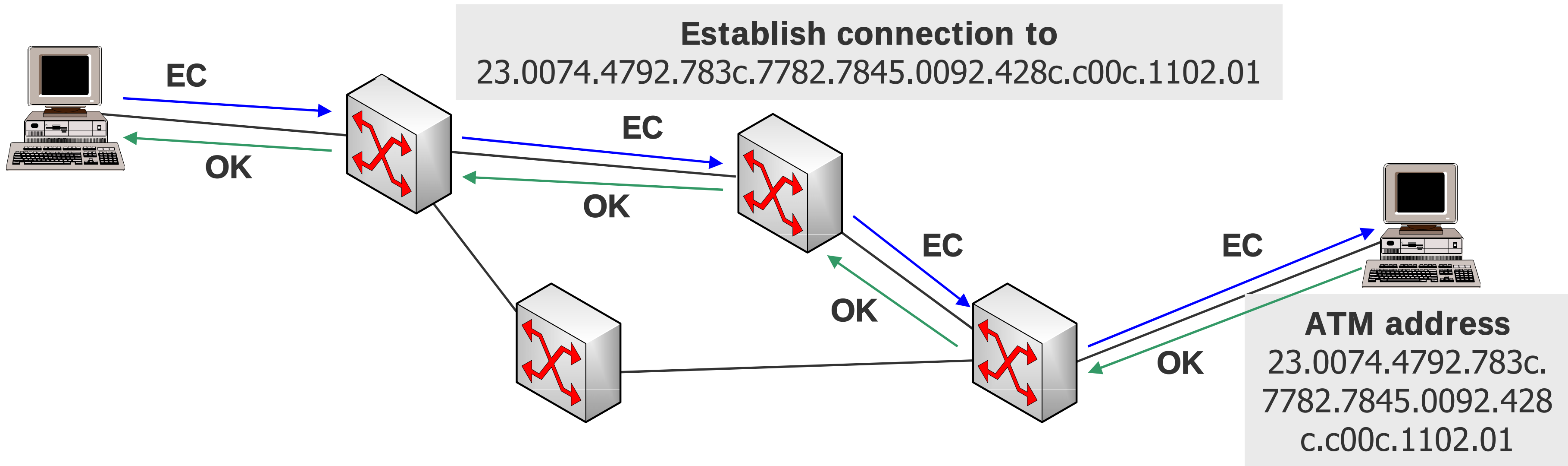
- Header Fields
  - Generic Flow Control (GFC)
    - Only with UNI, for local control of the transmission of data into the network.
  - Virtual Path Identifier (VPI)/ Virtual Channel Identifier (VCI)
    - Identification of the next destination of the cell
  - Payload Type Identifier (PTI)
    - Describes content of the data part, e.g., user data or different control data
  - Cell Loss Priority (CLP)
    - If the bit is 1, the cell can be discarded in overload situations.
  - Header Error Control (HEC)
    - CRC for the first 4 bytes; single bit errors can be corrected.





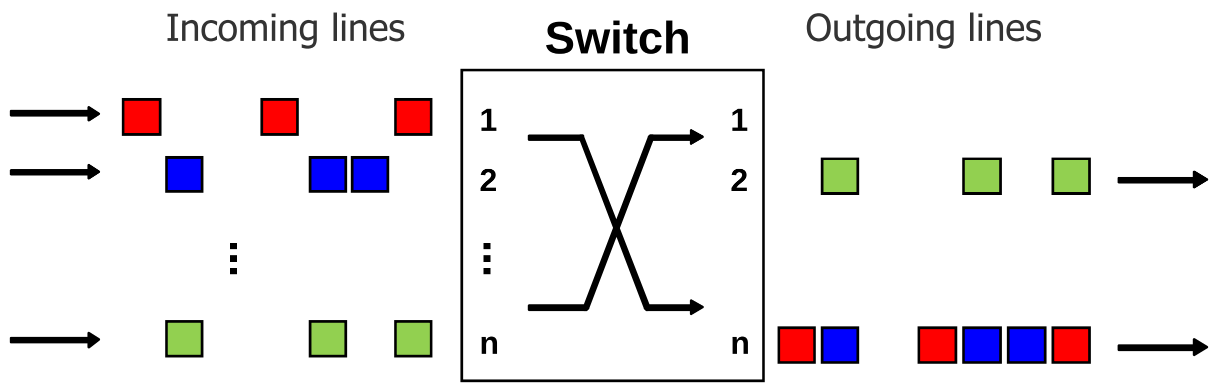
Connection Establishment in ATM

- The sender sends a connection establishment request to its ATM switch, containing the ATM address of the receiver and demands about the quality of the transmission.
- The ATM switch decides on the route, establishes a virtual connection (assigning a connection identifier) to the next ATM switch and forwards (using cells) the request to this next switch.
- When the request reaches the receiver, it sends back the established path and acknowledgement.
- After establishment, ATM addresses are no longer needed, only virtual connection identifiers are used.



ATM Switching

- Before the start of the communication a virtual connection has to be established. The switches are responsible for the forwarding of arriving cells on the correct outgoing lines. For this purpose a switch has a switching table.



Switching Table

In	Old Header	Out	New Header
1	a	n	a
2	c	n	d
⋮	⋮	⋮	⋮
n	b	2	e

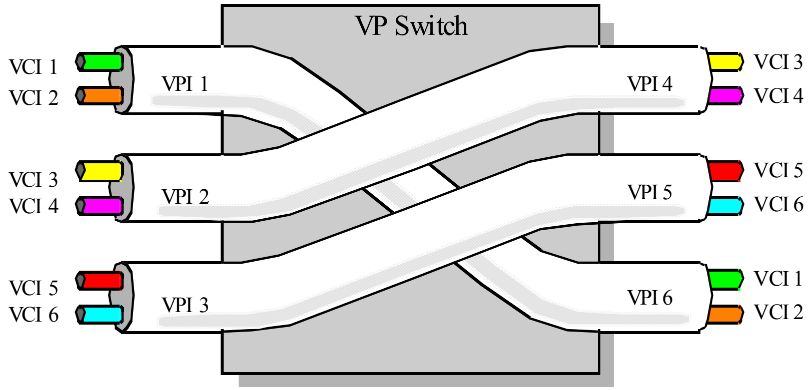
- The header information, which are used in the switching table are **VPI** (Virtual Path Identifier) and **VCI** (Virtual Channel Identifier).
- If a connection is being established via ATM, VPI, and VCI are assigned to the sender. Each switch on the route fills in to where it should forward cells with this information.

Path and Channel Concept of ATM

- Physical connections "contain" **Virtual Paths** (VPs, a group of connections)
- VPs "contain" **Virtual Channels** (VCs, logical channels)
- VPI and VCI only have local significance and can be changed by the switches.
- Distinction between VPI and VCI introduces a hierarchy on the path identifiers. Thus: Reduction of the size of the switching tables.

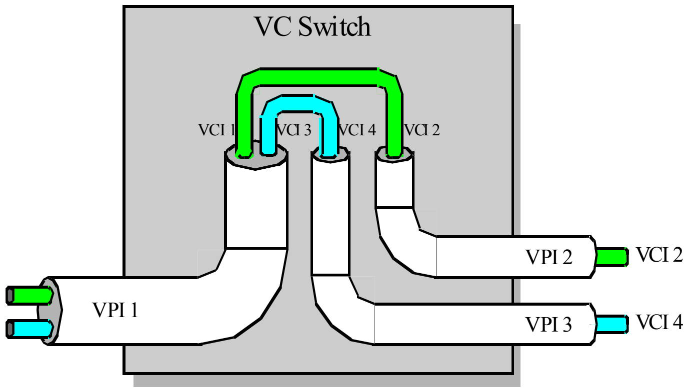
There are 2 types of switches in the ATM network:

Virtual Path Switching



VP-SWITCH

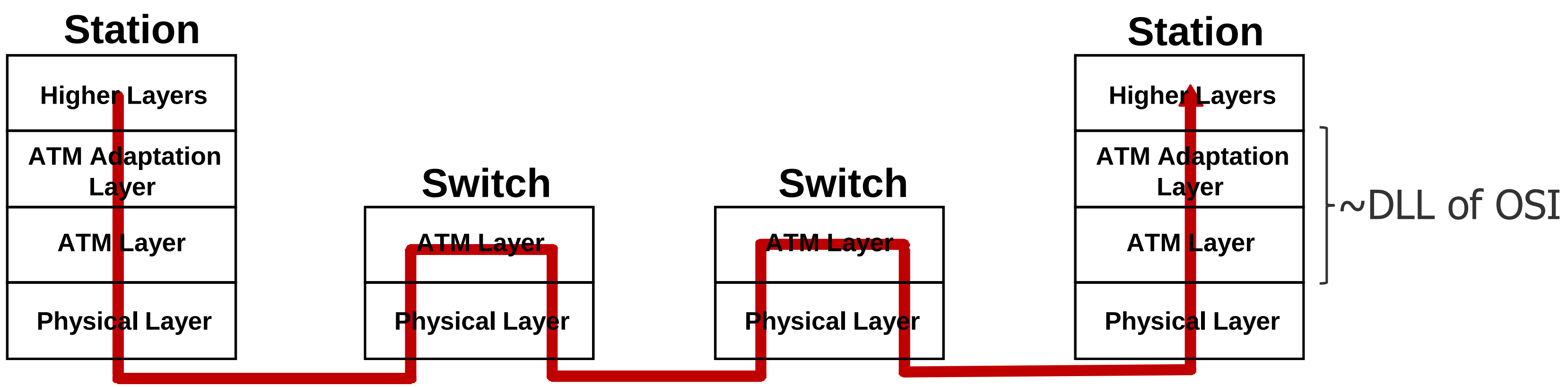
Virtual Channel Switching



VP/VC-SWITCH

Layers within ATM

- Physical Layer
  - Transfers ATM cells over the medium
  - Generates checksum (sender) and verifies it (receiver); discarding of cells
- ATM Layer
  - Generates header (sender) and extract contents (receiver), except checksum
  - Responsible for connection identifiers (Virtual Path and Virtual Channel Identifier)
- ATM Adaptation Layer (AAL)
  - Adapts different requirements of higher layer applications to the ATM Layer
  - Segments larger messages and reassembles them on the side of the receiver



Service Classes of ATM

Criterion	Service Class			
	A	B	C	D
Data rate	Negotiated maximum cell rate	Maximum and average cell rate	Dynamic rate adjustment to free resources	"Take what you can get"
Synchronization (source - destination)	Yes		No	
Bit rate	constant	variable		
Connection Mode	Connection-oriented			Connectionless

Applications:

Classes A and B:
- Moving pictures
- Telephony
- Video conferences

Classes C and D:
- Data communication
- File transfer
- Mail

Adaptation Layer (AAL):

A	B	C	D
AAL 1	AAL 2	AAL 3	AAL 4
		AAL 5	

AALs

AAL 1: **Constant Bit Rate (CBR)**

- Deterministic service
- Characterized by guaranteed fixed bit rate
- Parameter: Peak Cell Rate (PCR)

AAL 2: **Variable Bit Rate (VBR)**

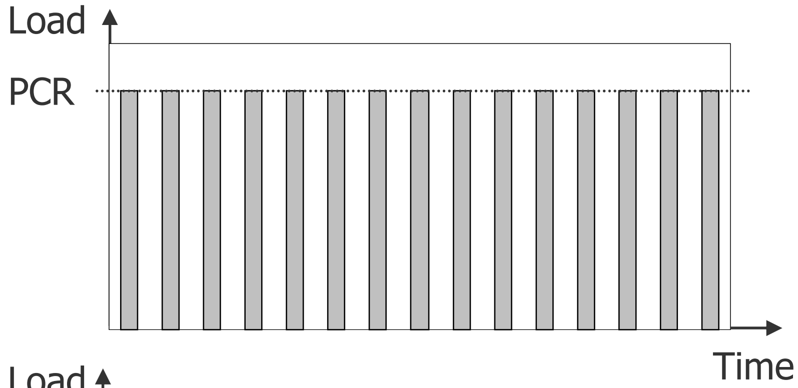
- Real time/non real time, statistical service
- Characterized by guaranteed average bit rate. Thus also suited for bursty traffic.
- Parameter: Peak Cell Rate (PCR), Sustainable Cell Rate (SCR), Maximum Burst Size

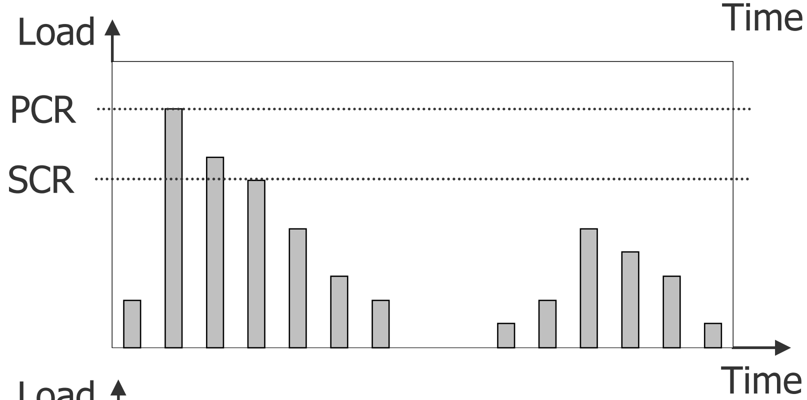
AAL 3: **Available Bit Rate (ABR)**

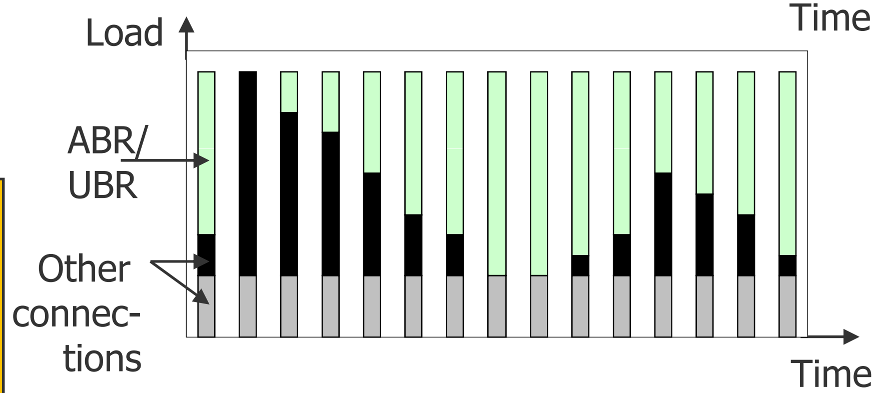
- Load-sensitive service
- Characterized by guaranteed minimum bit rate and load-sensitive, additional bit rate (adaptive adjustment)
- Parameter: Peak Cell Rate, Minimum Cell Rate

AAL 4: **Unspecified Bit Rate (UBR)**

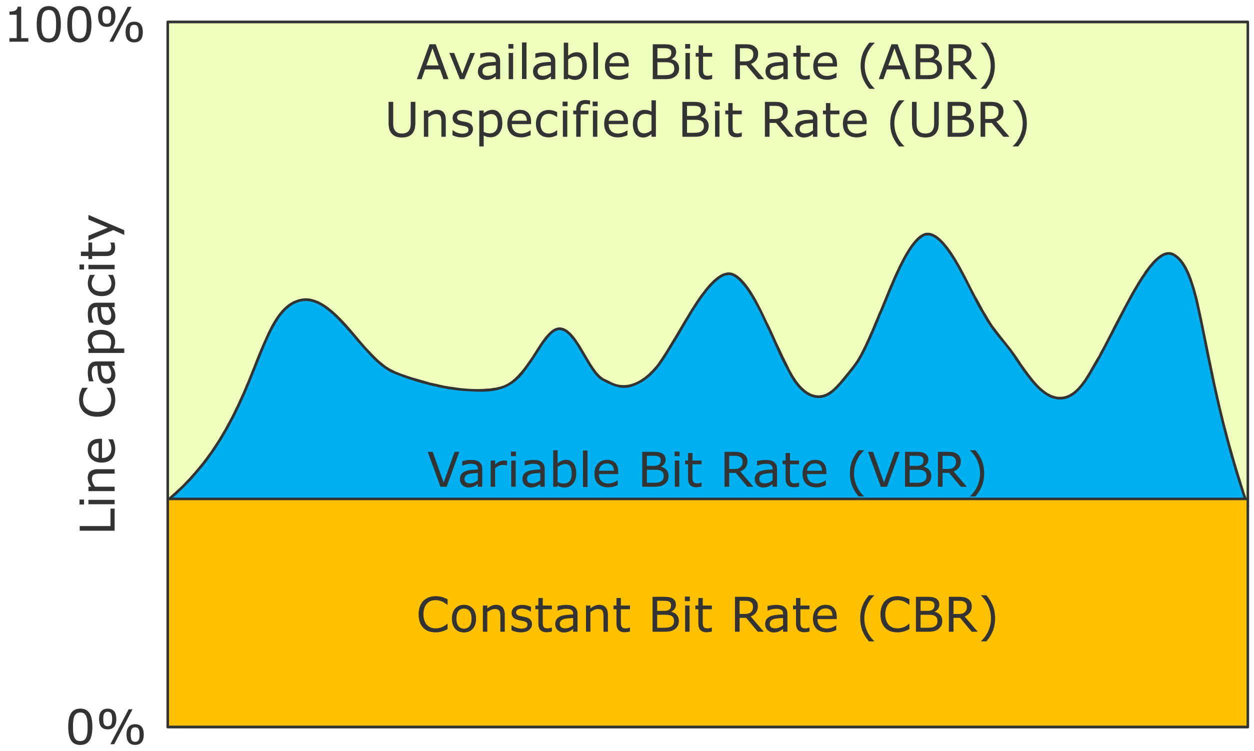
- Best Effort service
- Characterized by no guaranteed bit rate
- Parameter: Peak Cell Rate







Services Classes of ATM



Traffic Management

- Connection Admission Control (CAC)
  - Reservation of resources during the connection establishment (signaling)
  - Comparison between connection parameters and available resources
  - Traffic contract between users and ATM network
- Usage Parameter Control/Network Parameter Control
  - Test on conformity of the cell stream in accordance with the parameters of the traffic contract at the user-network interface (UNI) or network-network interface (NNI)
  - Generic Cell Rate Algorithm/Leaky Bucket Algorithm
- Switch Congestion Control (primary for UBR)
  - Selective discarding of cells for the maintenance of performance guarantees in the case of overload
- Flow Control for ABR
  - Feedback of the network status by resource management cells to the ABR source, for the adjustment of transmission rate and fair dispatching of the capacity

Integration of ATM into Existing Networks

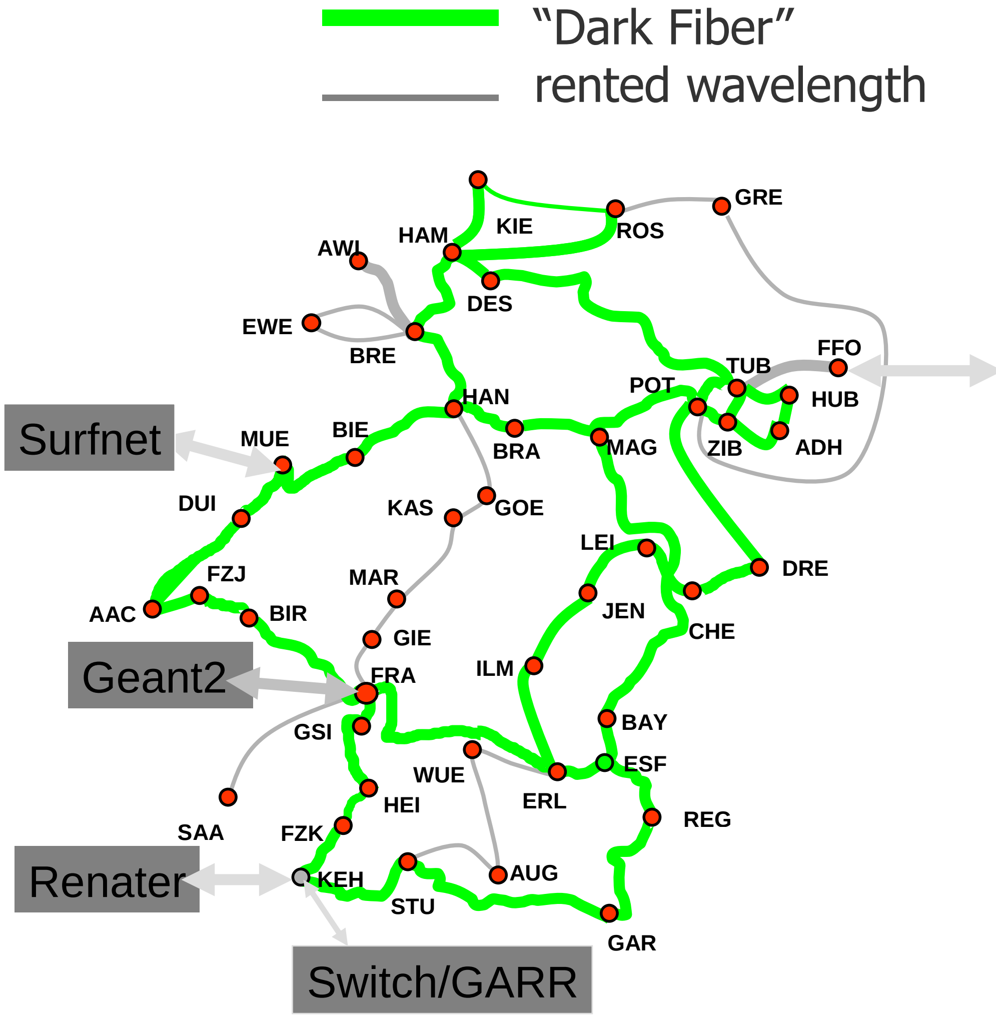
- What does ATM provide?
  - ATM offers an interface to higher layers (similar to TCP in the Internet protocols)
  - ATM additionally offers QoS guarantees (Quality of Service)
- ATM had problems during its introduction
  - Very few applications which build directly upon ATM
  - In the interworking of networks TCP/IP was standard
  - Without TCP/IP binding, ATM could not be sold!
- Therefore different solutions for ATM were suggested, e.g.
  - IP over ATM (IETF)
  - LAN emulation (LANE, ATM forum)

- Today: ATM still is in use in some regions, but SDH (as a technology coming from the telecommunication sector) took over the leading role in WAN technology

Synchronous Digital Hierarchy (SDH)

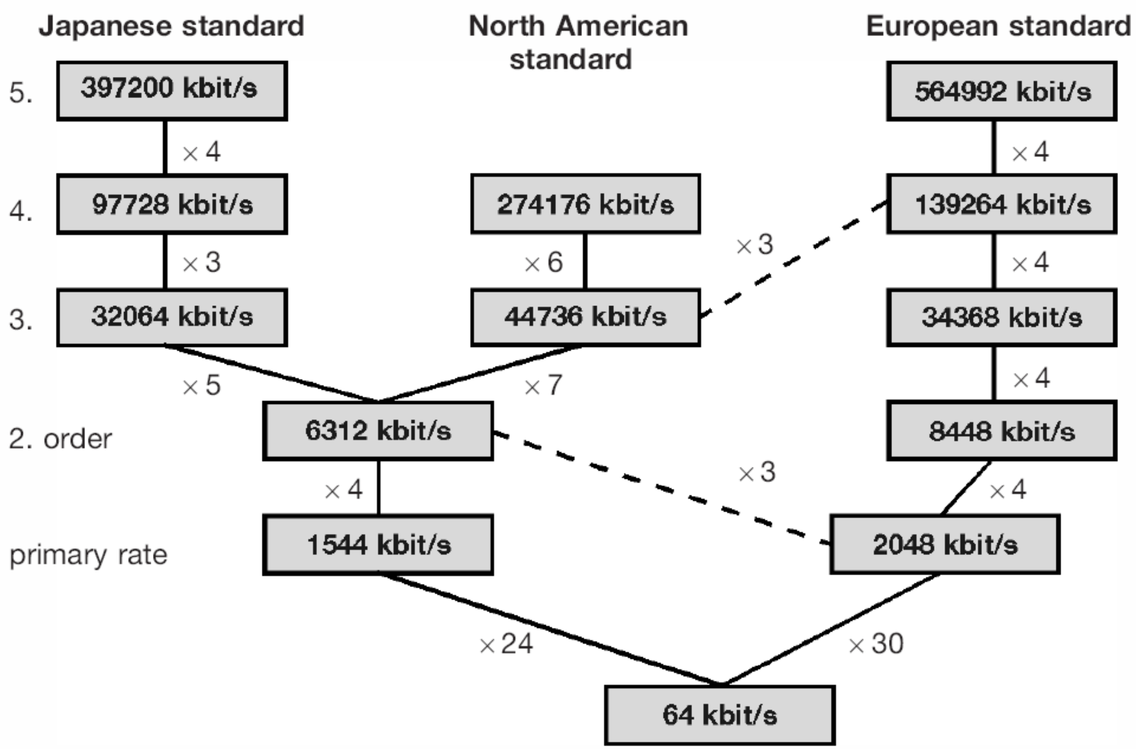
Synchronous Digital Hierarchy (SDH)

- All modern networks in the public area are using the SDH technology
- Example: the German B-WIN (ATM) was replaced by the G-WIN (Gigabit-Wissenschaftsnetz) on basis of SDH
- Since 2006: X-WIN – complete redesign of topology, additionally integration of DWDM (dense wavelength division multiplexing): up to 160 parallel transmissions over a fiber, giving 1.6 Tbps capacity!
- Also used within the MAN range (Replaced by Gigabit Ethernet?)
- Analogous technology in the USA: Synchronous Optical Network (SONET)



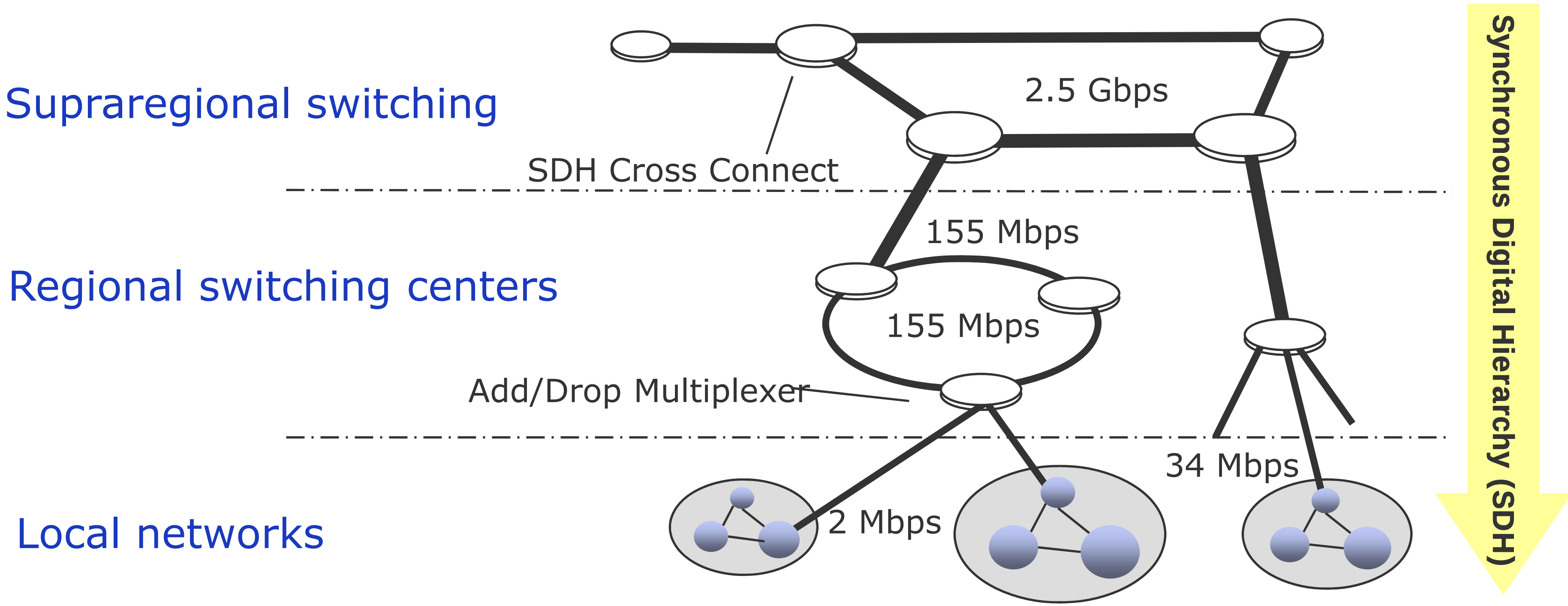
Synchronous Digital Hierarchy (SDH)

- Introduction of PCM in the 1960s
  - Digital telephone system
- Before SDH was introduced Plesiochronous Digital Hierarchy (PDH) was used
  - Europe: Combination of 30 channels of 64kbps
  - USA, Canac

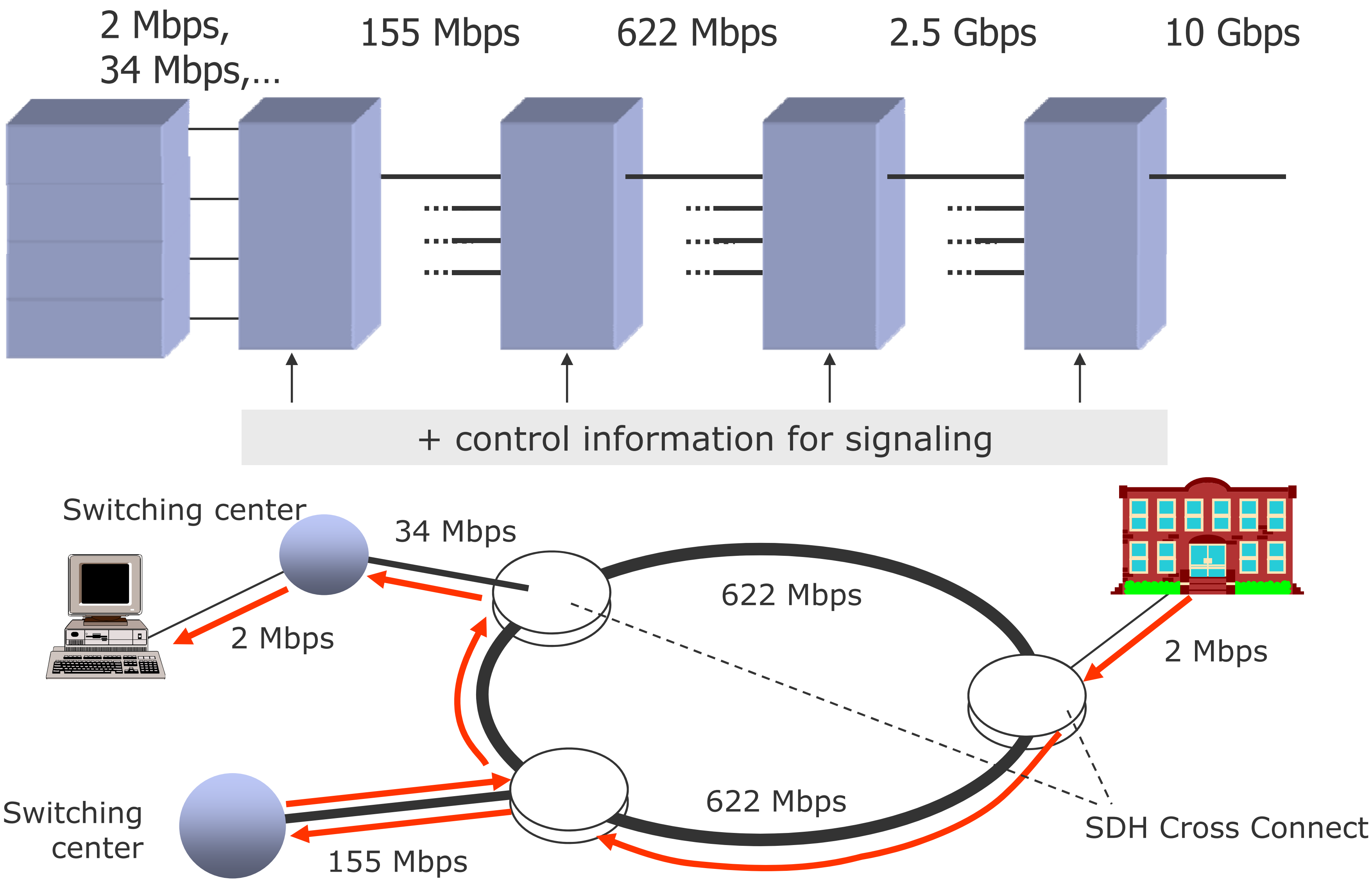


SDH Structure

- SDH achieves higher data rates than ATM (at the moment up to about 40 Gbps)
- Flexible capacity utilization and high reliability
- Structure: arbitrary topology, meshed networks with a switching hierarchy (exemplarily 3 levels):



Multiplexing within SDH

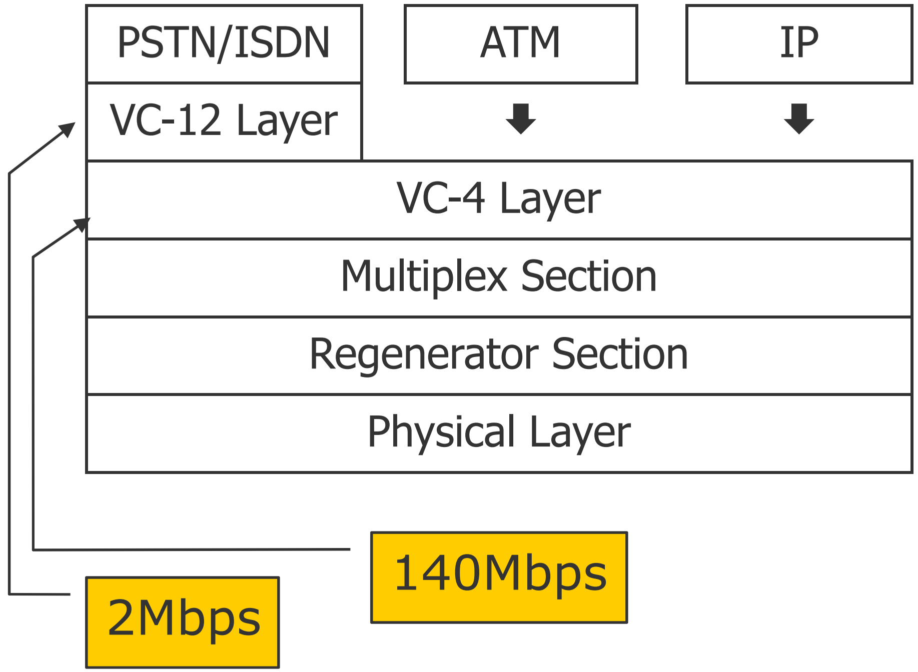


Characteristics of SDH

- World-wide standardized bit rates on the hierarchy levels
- Synchronized, centrally clocked network
- Multiplexing of data streams is made byte-by-byte, simple multiplex pattern
- Suitable for speech transmission:
  - Since on each hierarchy level four data streams are mixed byte-by-byte and a hierarchy level has four times the data rate of the lower level, everyone of these mixed data streams has the same data rate as on the lower level. Thus the data experience a constant delay.
- Direct access to signals by cross connects without repeated demultiplexing
- Short delays in inserting and extracting signals
- Additional control bytes for network management, service and quality control,…
- Substantial characteristic: Container for the transport of information

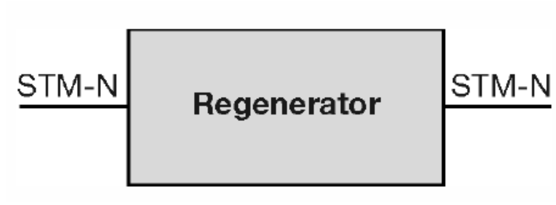
SDH Architecture

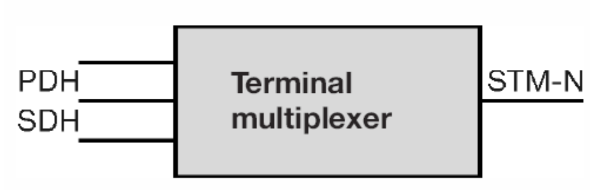
- Physical Layer
  - Transmission medium, typically fiber optics
    - Radio and Satellite links
- Regenerator Section
  - Path between regenerators
- Multiplex Section
  - Link between multiplexers
- VC Layer (Virtual Container)
  - Part of the mapping procedure, i.e., packing of ATM and PDH signals into SDH

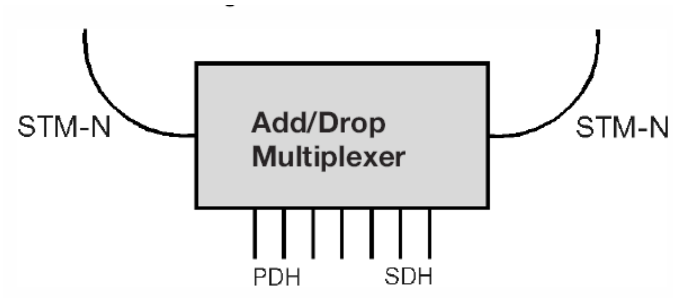


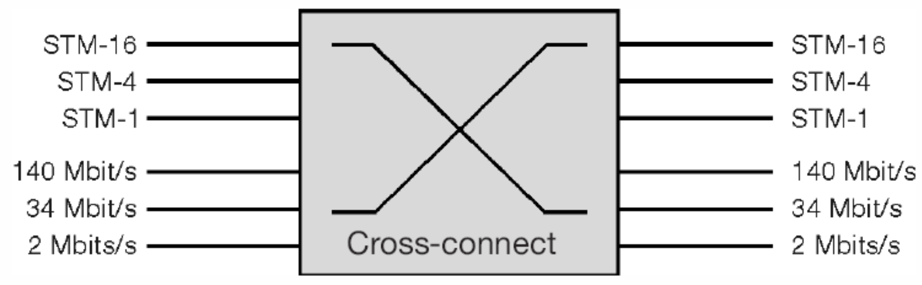
Components of a SDH Network

- Four different types of network elements
  - Regenerators
    - Regenerate incoming signal (clock and amplitude)
    - Clock signal is derived from incoming signal
  - Terminal multiplexer
    - Combine PDH and SDH signals into higher bit rate STM signals
  - Add/drop multiplexer
    - Insert or extract PDH and SDH lower bit rate signals
  - Digital cross connects
    - Mapping of PDH tributary signals into virtual containers
    - Switching of various containers

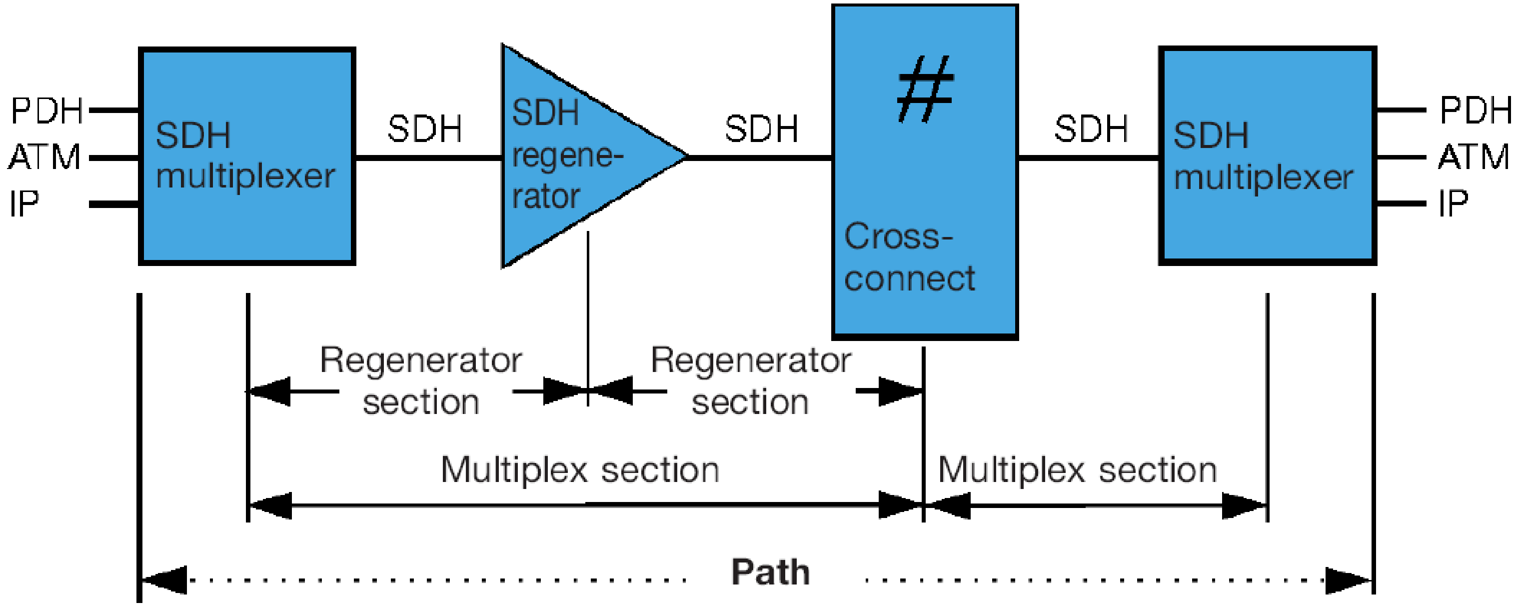






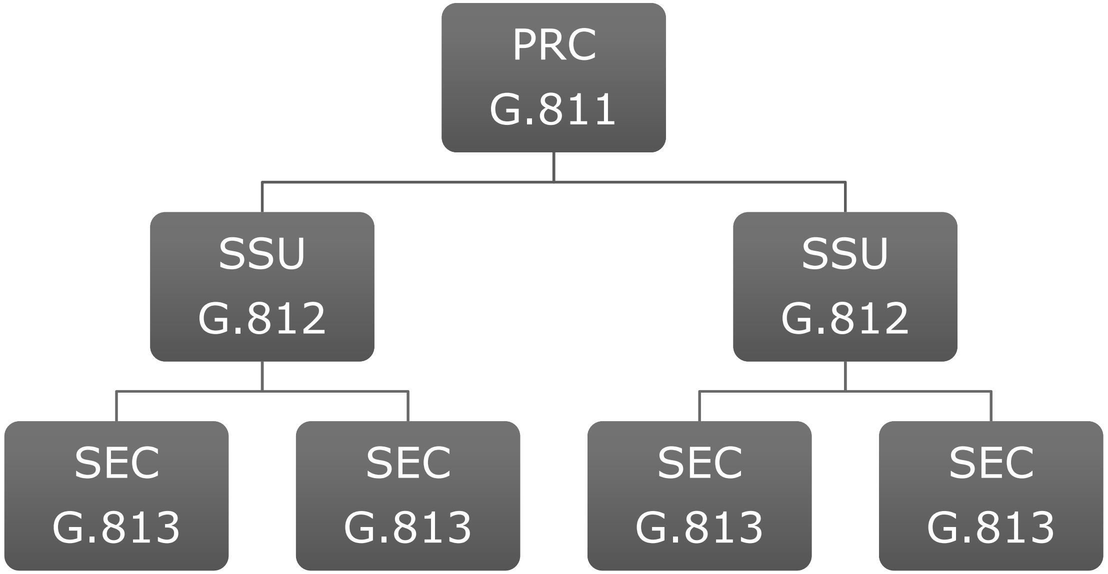


Components of a SDH Network



Synchronization in SDH

- All network elements have to be synchronized
  - Central clock with high accuracy, i.e., 1×10^{-11}
    - Primary Reference Clock (PRC)
    - Clock signal is distributed in the network
  - Hierarchical structure to distribute clock signals
    - Subordinate synchronization supply units (SSU)
    - Synchronous equipment clocks (SEC)
  - Synchronization path can be the same as for data

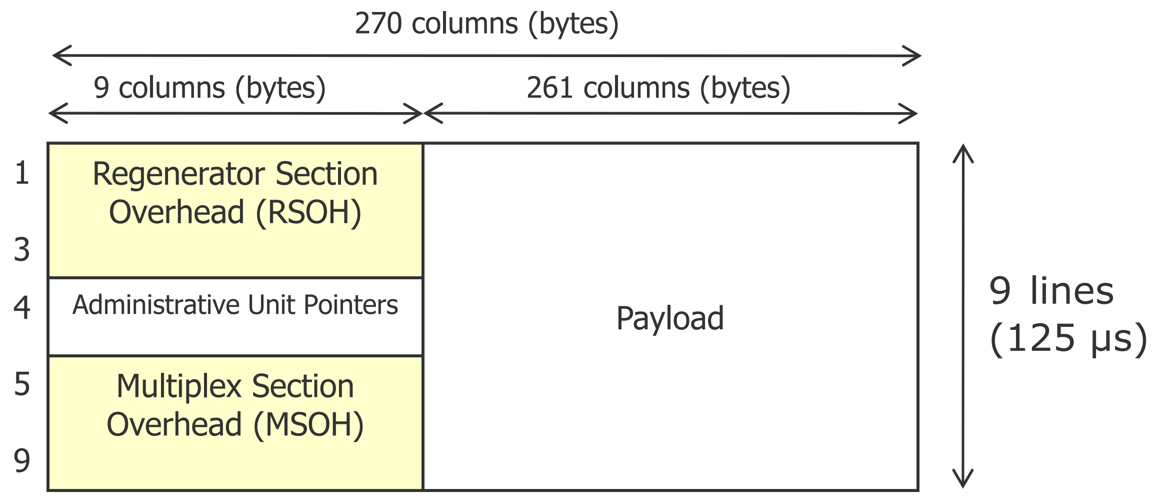


SDH Transport Module (Frame)

Synchronous Transport Module (STM-N, N=1,4,16, 64)

STM-1 structure:

- 9 lines with 270 bytes each
- Each byte in the payload represents a 64 kbps channel
- Basis data rate of 155 Mbps
  9x270x8x8000 bps = 155.52 Mbps



Administrative Unit Pointers

- Permit the direct access to components of the Payload

Section Overhead

- **RSOH**: Contains information concerning the route between two repeaters or a repeater and a multiplexer
- **MSOH**: Contains information concerning the route between two multiplexers without consideration of the repeaters in between.

Payload

- Contains the utilizable data as well as further control data

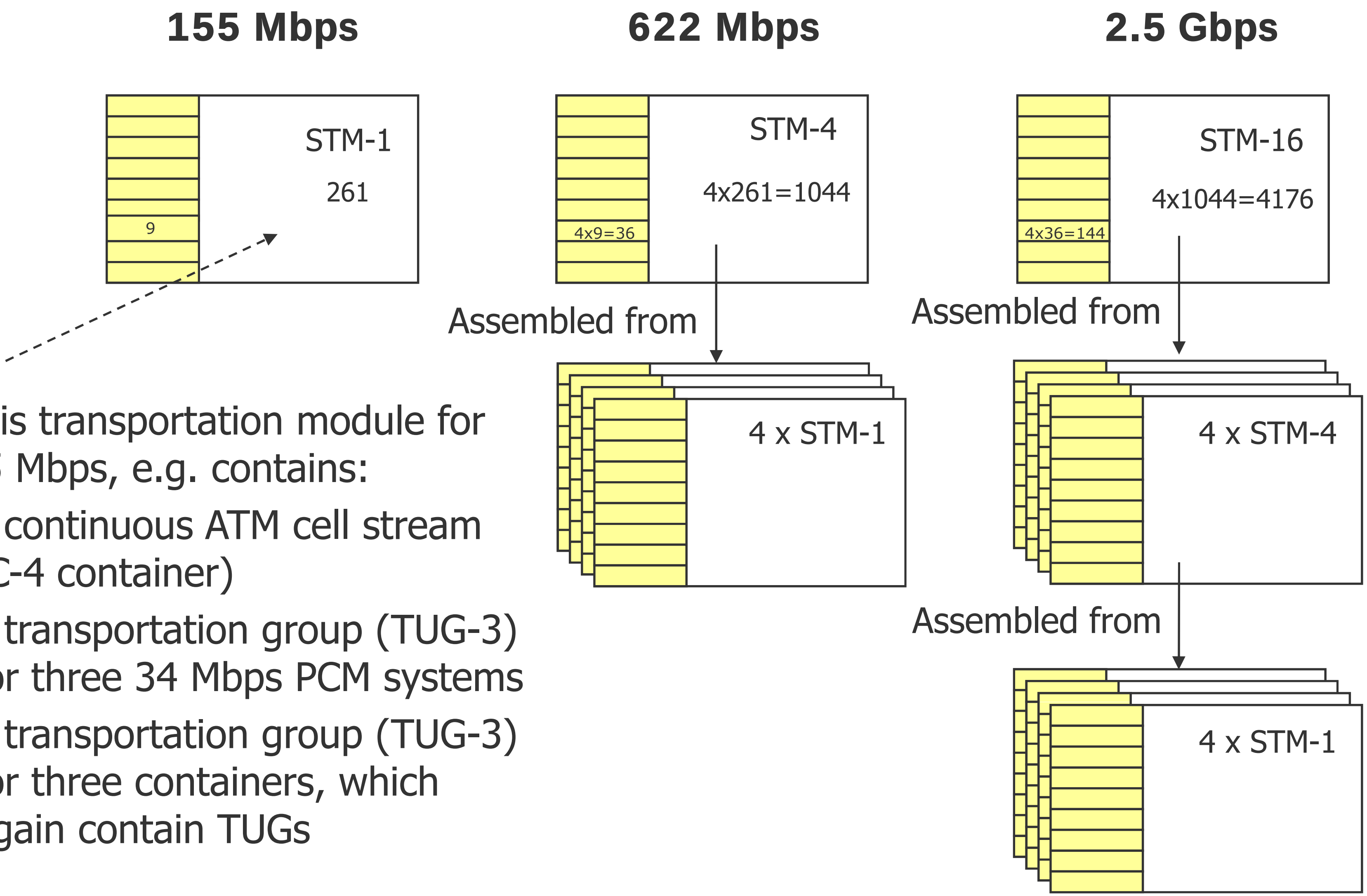
Creation of a STM

- Creation of a Synchronous Transport Module (STM)
  - Payload is packed into a container
  - A distinction of the containers is made by size: C-1 to C-4
  - Payload data are adapted if necessary by padding to the container size
  - Some additional information to the payload are added for controlling the data flow of a container over several multiplexers
    - Path Overhead (POH)
    - Control of single sections of the transmission path
    - Change over to alternative routes in case of an error
    - Monitoring and recording of the transmission quality
    - Realization of communication channels for maintenance
  - By adding the POH bytes, a container becomes a **Virtual Container** (**VC**)

Creation of a STM

- If several containers are transferred in a STM payload, these are multiplexed byte-by-byte in **Tributary Unit Groups** (**TUG**).
- By adding an Administrative Unit Pointer, the Tributary Unit Group becomes an **Administrative Unit** (**AU**).
- Then the SOH bytes are supplemented, the SDH frame is complete. RSOH and MSOH contain for example bits for
  - Frame synchronization
  - Error detection (parity bit)
  - STM-1 identifications in larger transportation modules
  - Control of alternative paths
  - Service channels
  - … and some bits for future use

SDH Hierarchy

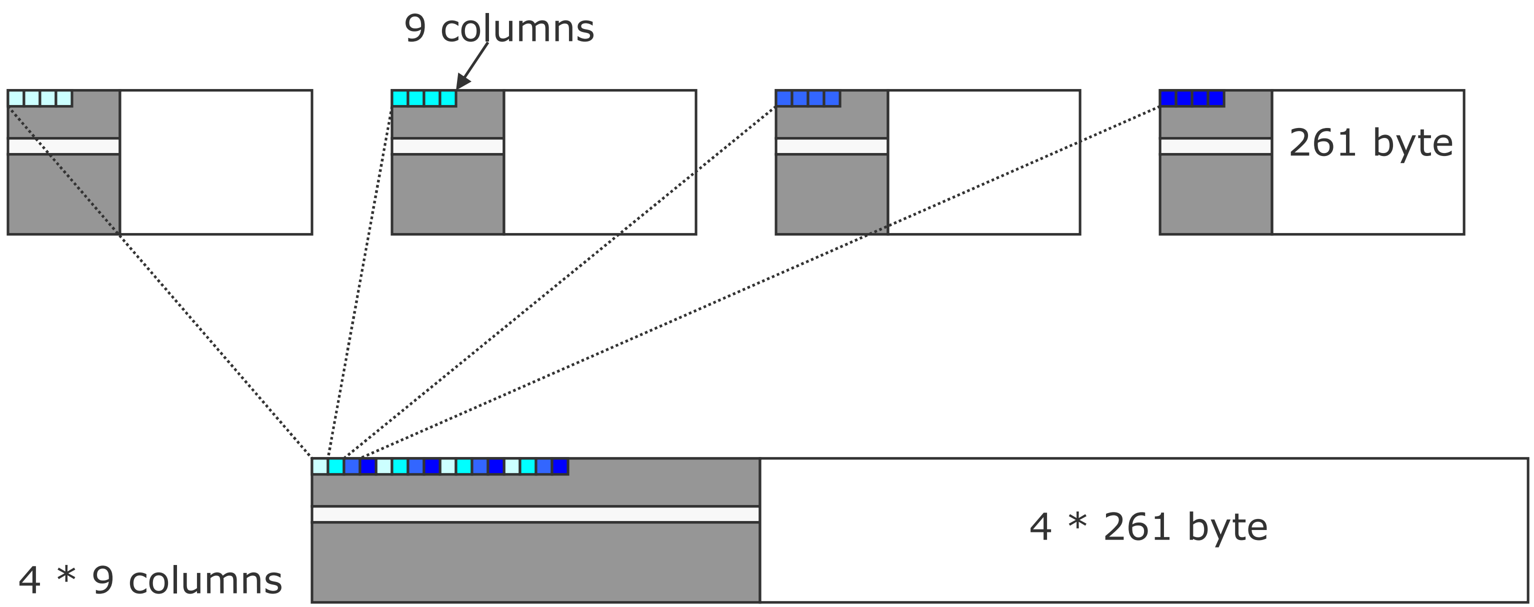


Basis transportation module for 155 Mbps, e.g. contains:

- a continuous ATM cell stream (C-4 container)
- a transportation group (TUG-3) for three 34 Mbps PCM systems
- a transportation group (TUG-3) for three containers, which again contain TUGs

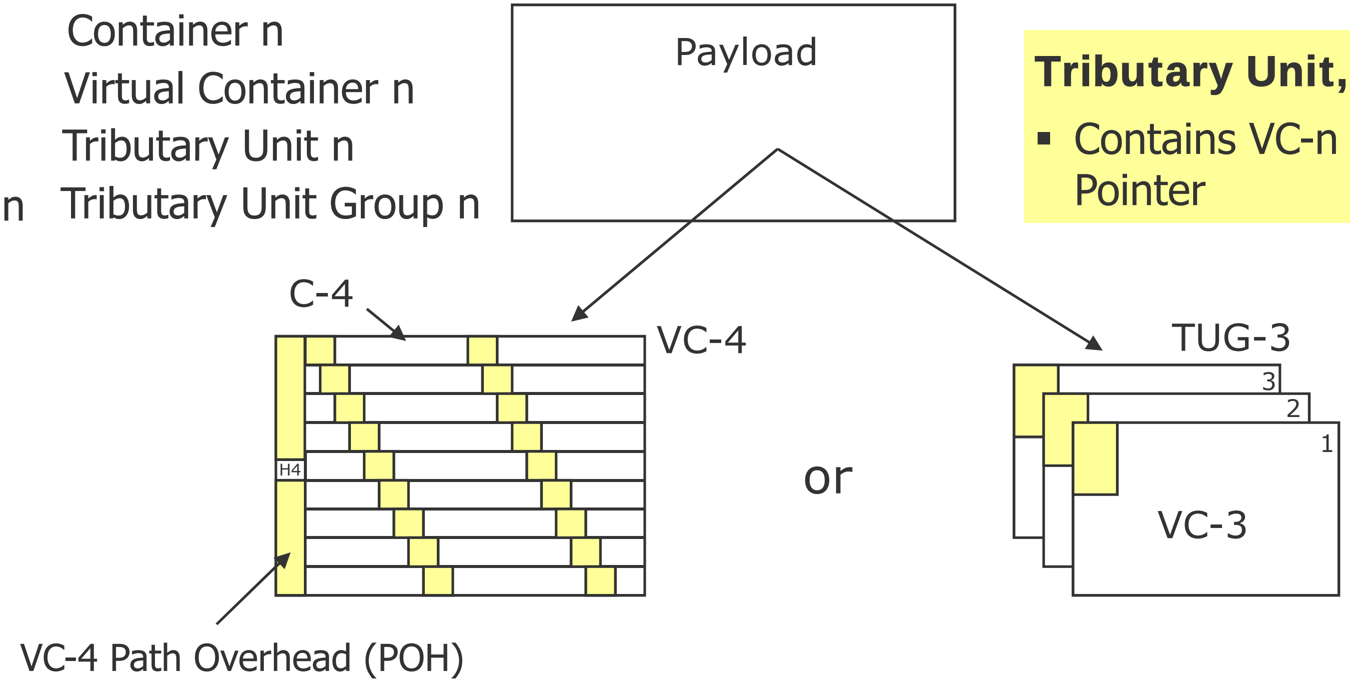
SDH Hierarchy

- Higher hierarchy levels assembling STM-1 modules
- Higher data rates are assembled by multiplexing the contained signals byte-by-byte
- Each byte has a data rate suitable of 64 kbps for the transmission of voice (telephony)
- Except STM-1, only transmission over optical fiber is specified



Types of SDH Containers

C-n	Container n
VC-n	Virtual Container n
TU-n	Tributary Unit n
TUG-n	Tributary Unit Group n



Tributary Unit, n (n=1 to 3)

- Contains VC-n and Tributary Unit Pointer

Container, C-n (n=1 to 4)

- Defined unit for payload capacity (e.g. C-4 for ATM or IP, C-12 for ISDN or 2 Mbps)
- Transfers all SDH bit rates
- Capacity can be made available for transport from broadband signals not yet specified

Virtual Container, VC-n (n=1 to 4)

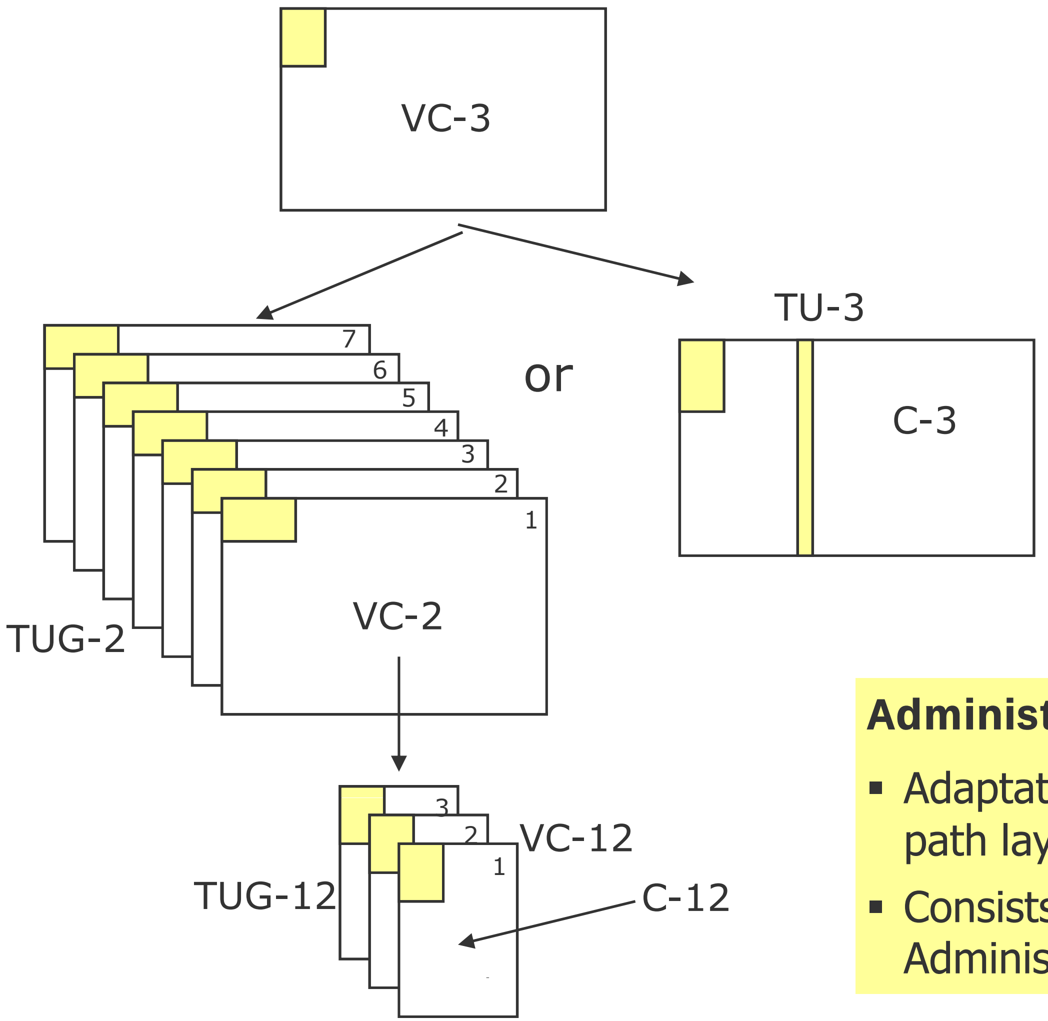
- Consists of container and POH
- Lower VC (n=1,2): single C-n plus basis Virtual Container Path Overhead (POH)
- Higher VC (n=3,4): single C-n, union of TUG-2s/TU-3s, plus basis Virtual Container POH

Types of SDH Containers

- Virtual Containers (VC)

SDH	Bit Rate [Mbps]	Size of VC Rows x Columns
VC-11	1,728	9 x 3
VC-12	2,304	9 x 4
VC-2	6,912	9 x 12
VC-3	48,960	9 x 85
VC-4	150,336	9 x 261

Types of SDH Containers

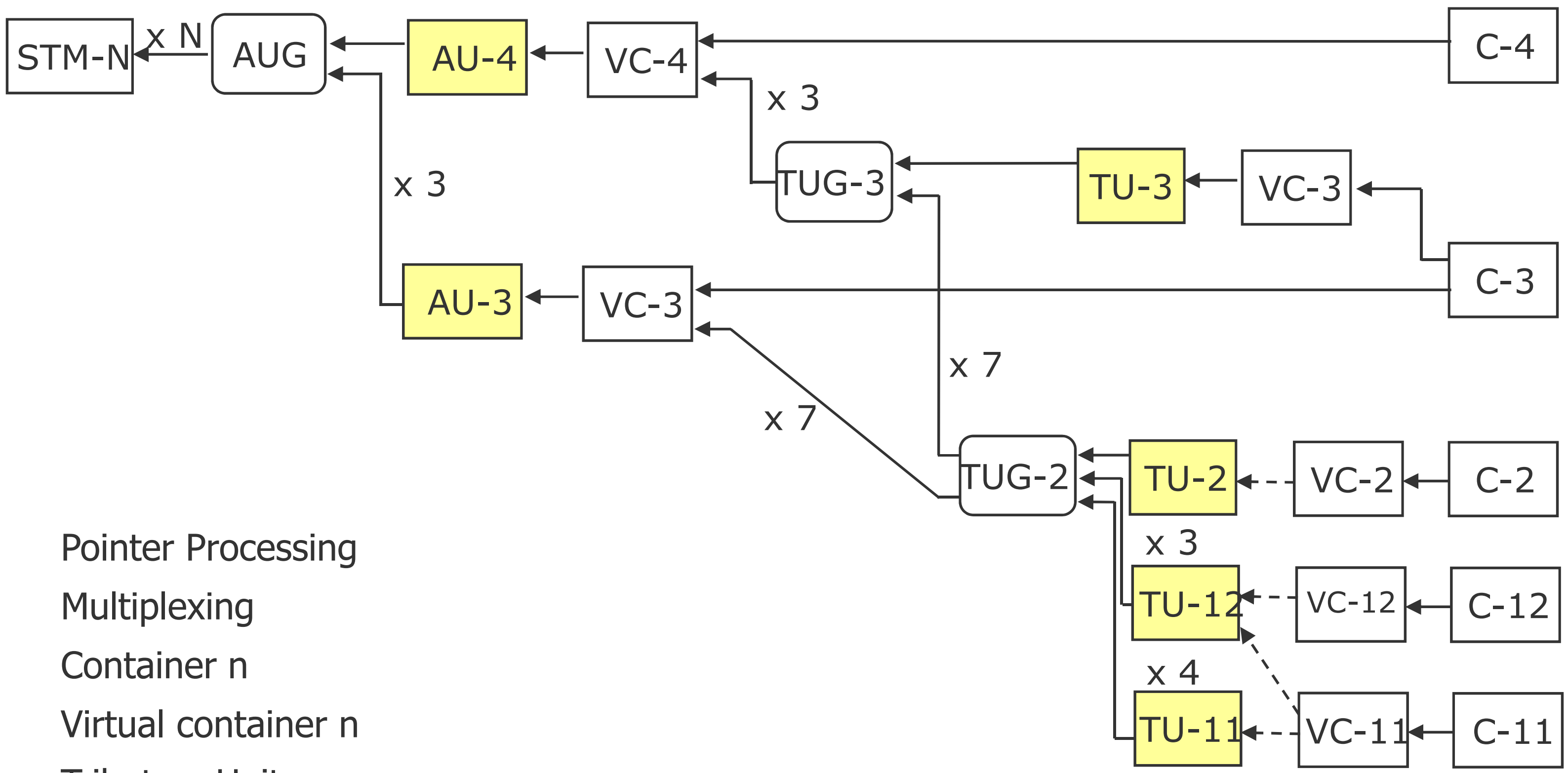


C-n	Container n
VC-n	Virtual Container n
TU-n	Tributary Unit n
TUG-n	Tributary Unit Group n
AU-n	Administrative Unit n
STM-N	Synchronous Transport Module N

Administrative Unit n (AU-n)

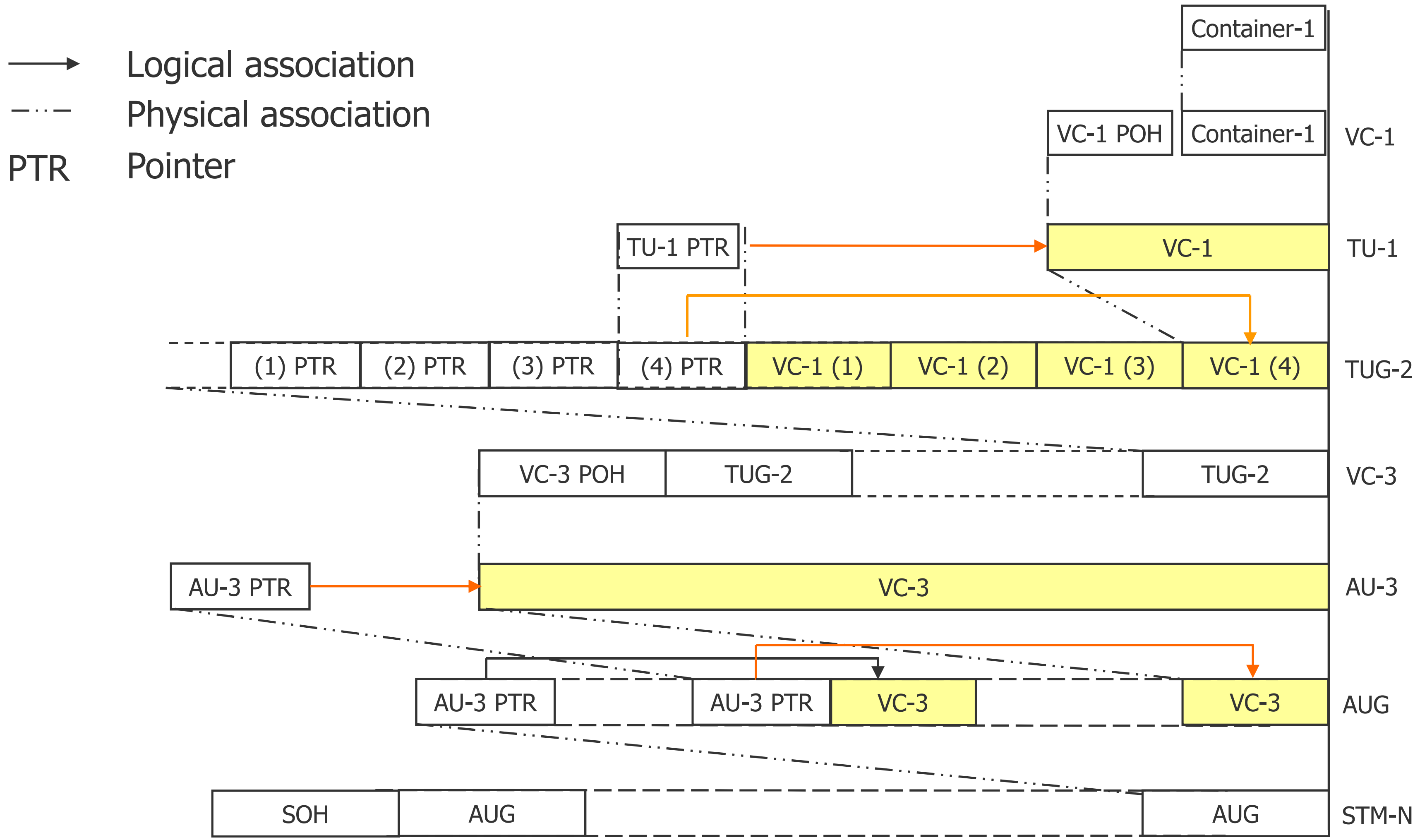
- Adaptation between higher order path layer and multiplex unit
- Consists of payload and Administrative Unit Pointers

SDH Multiplex Structure



(yellow box)	Pointer Processing
←	Multiplexing
C-n	Container n
VC-n	Virtual container n
TU-N	Tributary Unit n
TUG-n	Tributary Unit Group n
AU-n	Administrative Unit n
AUG	Administrative Unit Group
STM-N	Synchronous Transport Module N

SDH Multiplexing



What can SDH achieve?

SONET		SDH	Data rate (Mbps)	
Electrical	Optical	Optical	Gross	Net
STS-1	OC-1	STM-0	51.84	50.112
STS-3	OC-3	STM-1	155.51	150.336
STS-9	OC-9	(STM-3)	466.56	451.008
STS-12	OC-12	STM-4	622.08	601.344
STS-18	OC-18	(STM-6)	933.12	902.016
STS-24	OC-24	(STM-8)	1,244.16	1,202.688
STS-36	OC-36	(STM-12)	1,866.24	1,804.032
STS-48	OC-48	STM-16	2,488.32	2,405.376
STS-96	OC-96	STM-32	4,976.64	4,810.752
STS-192	OC-192	STM-64	9,953.28	9,621.504
STS-768	OC-758	STM-256	39,813.12	38,486.016

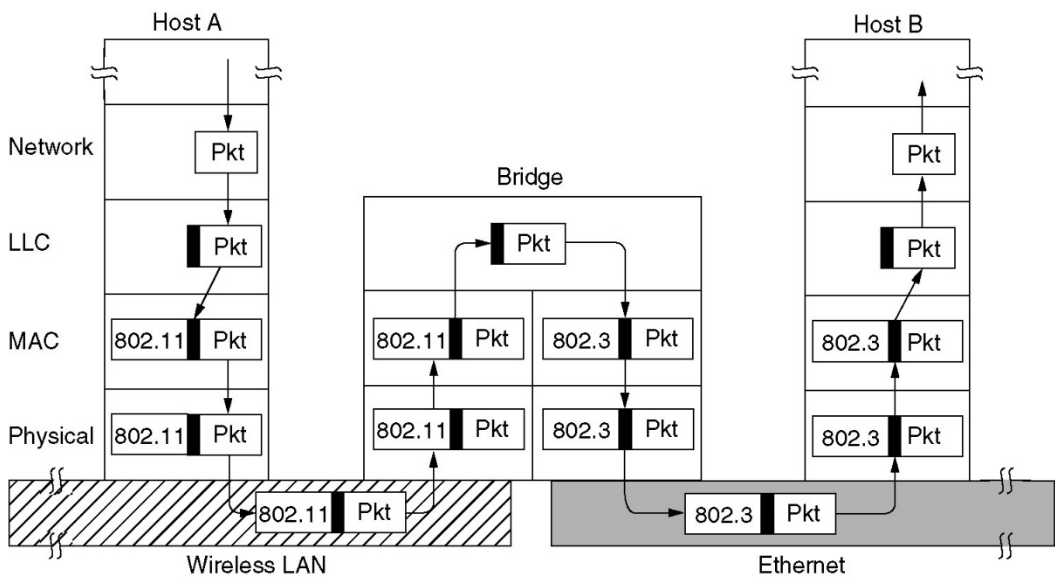
Network Infrastructure

Network Infrastructure

- Typically a LAN comes rarely alone
  - What to do if many LANs exist?
- Connect them by bridges
  - A bridge examines the data link layer address for routing
- Reasons why one organization could have multiple LANs
  - Autonomy of the owner
  - Several buildings with each having a LAN
  - Machines are too distant
    - Ethernet supports only up to 2.5 km
  - Load
  - Security
  - Reliability
- Requirements:
  - Bridges should be transparent
  - Moving of machines from one segment to another must not require the change of software or hardware

Network Infrastructure

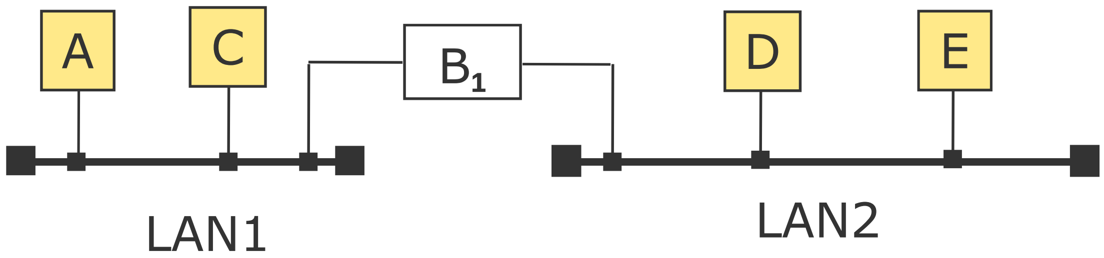
- Bridges from 802.x to 802.y



- Problems when moving frames between LANs
  - Different frame formats
  - Different data rates
  - Different max. frame length
  - Security: Some support encryption others do not
  - Quality of Service

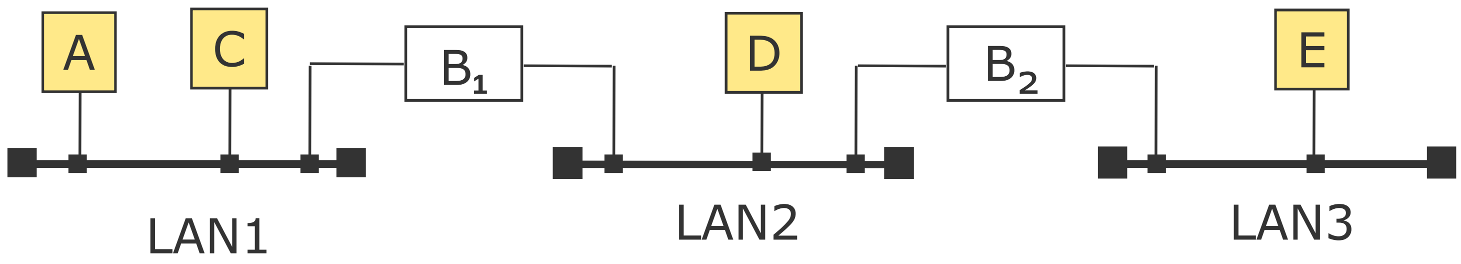
Infrastructure Components: Bridges

- With bridges, several LANs are connected on the link layer – possibly LANs of different types, i.e., having different header formats
- Major tasks:
  - Appropriate forwarding of the data
  - Adaptation to different LAN types
  - Reduction of the traffic in a LAN segment, i.e., packets which are sent from A to C are not forwarded by the bridge to LAN2. Thus, station D can communicate with E in parallel.
  - Increases physical length of a network
  - Increased reliability through demarcation of the LAN segments



Infrastructure Components: Bridges

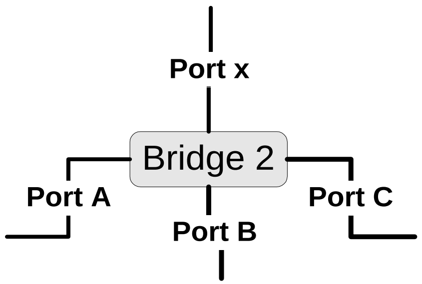
- Transparent bridges (e.g. for CSMA and Token Bus networks)



- Characteristics
  - Coupling of LANs is transparent for the stations, i.e., not visible
  - Hash tables contain the destination addresses
- Routing Procedure
  - Source and destination LAN are identical
    ➡ frame is rejected by bridge, e.g., B1 in case of a transmission from A to C
  - Source and destination LAN are different
    ➡ forward frames, e.g., in case of a transmission from D to E
  - Destination LAN unknown
    ➡ flood frame

Transparent Bridges

- To realize transparency, bridges have to learn in which LAN a host is located
- Each bridge maintains a forwarding database with entries
  <MAC address, port, age>
  - MAC address: host name
  - port: port number of bridge used to send data to the host
  - age: aging time of entry
- Assume a MAC frame arrives on port x:



Is MAC address of destination in forwarding database for ports A, B, or C?

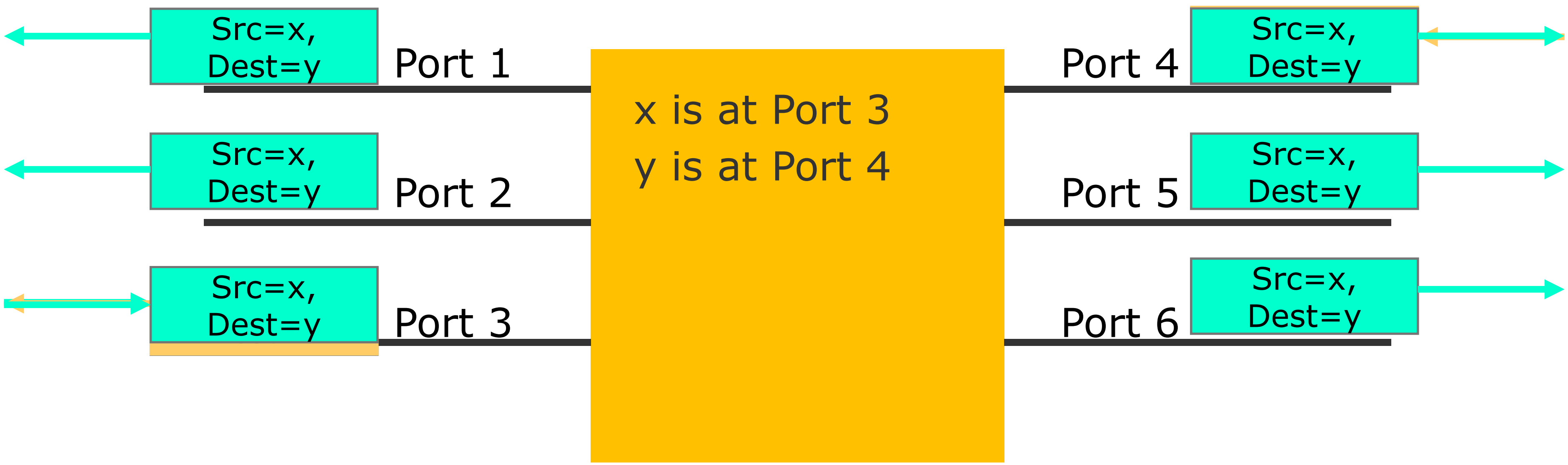
Found and ≠ x? → **Forward the frame on the appropriate port**

Found and = x? → **Ignore frame**

Not found ? → **Flood the frame,** i.e., send the frame on all ports except port x.

Transparent Bridges: Address Learning

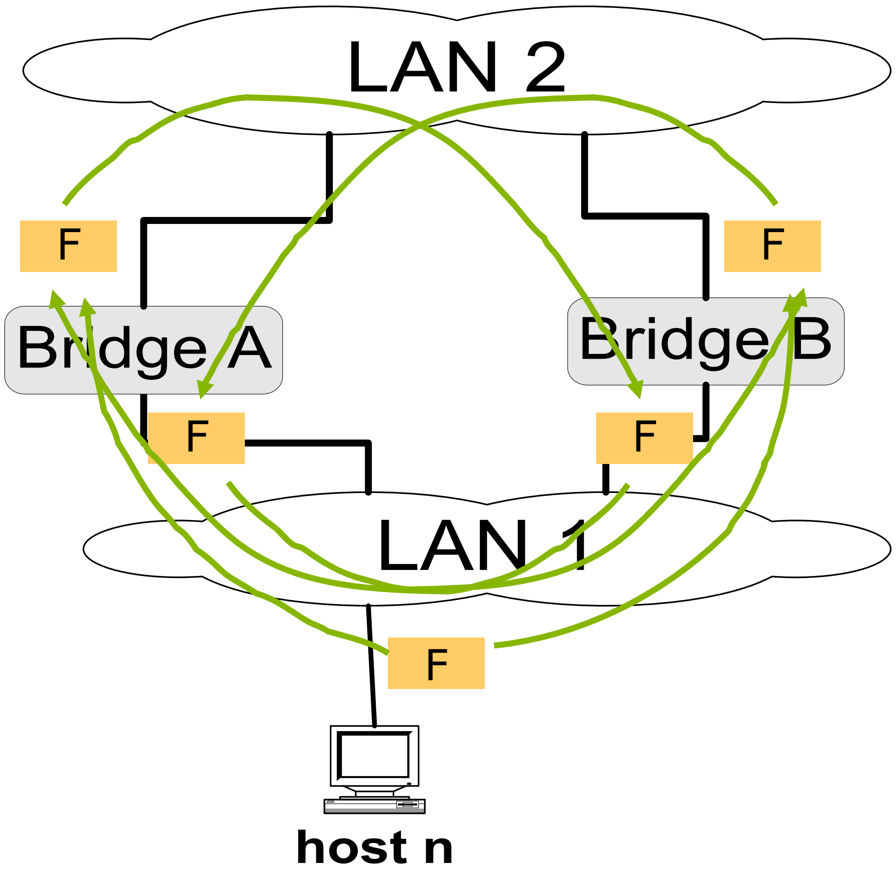
- Database entries are set automatically with a simple heuristic
  - the source field of a frame that arrives on a port tells which hosts are reachable from this port.
- Algorithm:
  - For each frame received, the source stores the source field in the forwarding database together with the port where the frame was received.
  - All entries are deleted after some time (default is 15 seconds).



Loops

- Consider two LANs that are connected by two bridges.
- Assume host n is transmitting a frame F with unknown destination.
- Bridges A and B flood the frame to LAN 2.
- Bridge B sees F on LAN 2 (with unknown destination), and copies the frame back to LAN 1
- Bridge A does the same.
- The copying continues

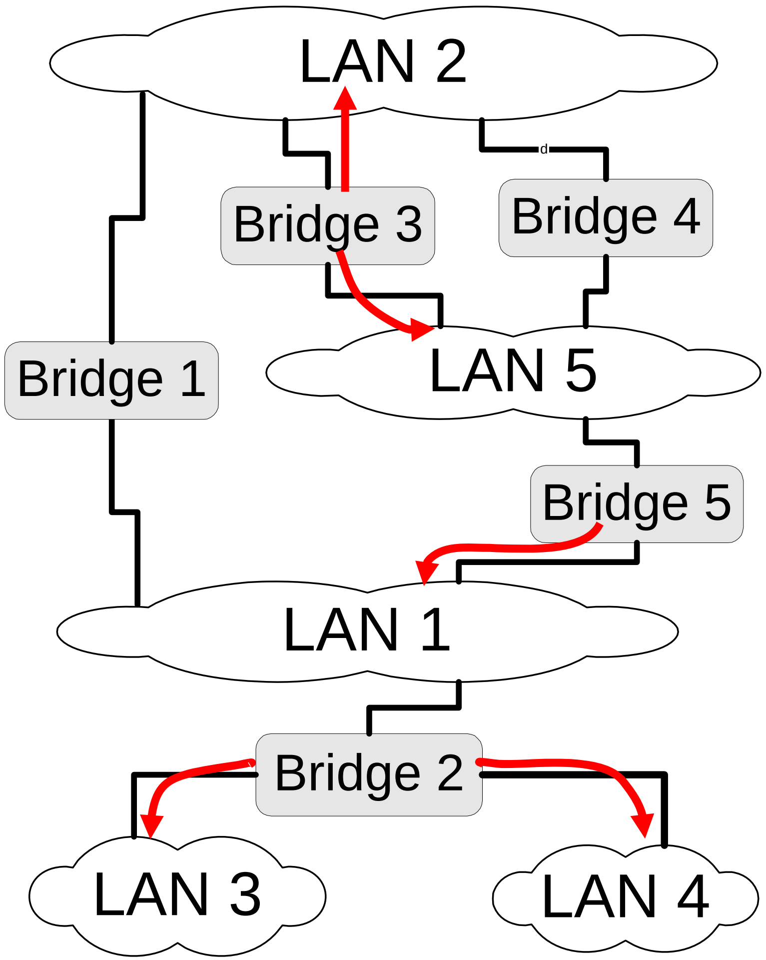
- Solution: Spanning Tree Algorithm



Spanning Tree Bridges

- Preventing loops: compute a spanning tree from all connected bridges

- Spanning Tree Algorithm:
  - Determine one root bridge
    - The bridge with the smallest ID
  - Determine a designated bridge for each LAN
    - The bridge which is nearest to the root bridge
  - Determine root ports
    - Port for the best path to root bridge considering costs for using a path, e.g., the number of hops.



Spanning Tree Algorithm

- At the beginning, all bridges assume to be root bridge and send out a packet containing their own ID and current costs (initialized with zero) over all of their ports:

root ID	costs	bridge ID	port ID

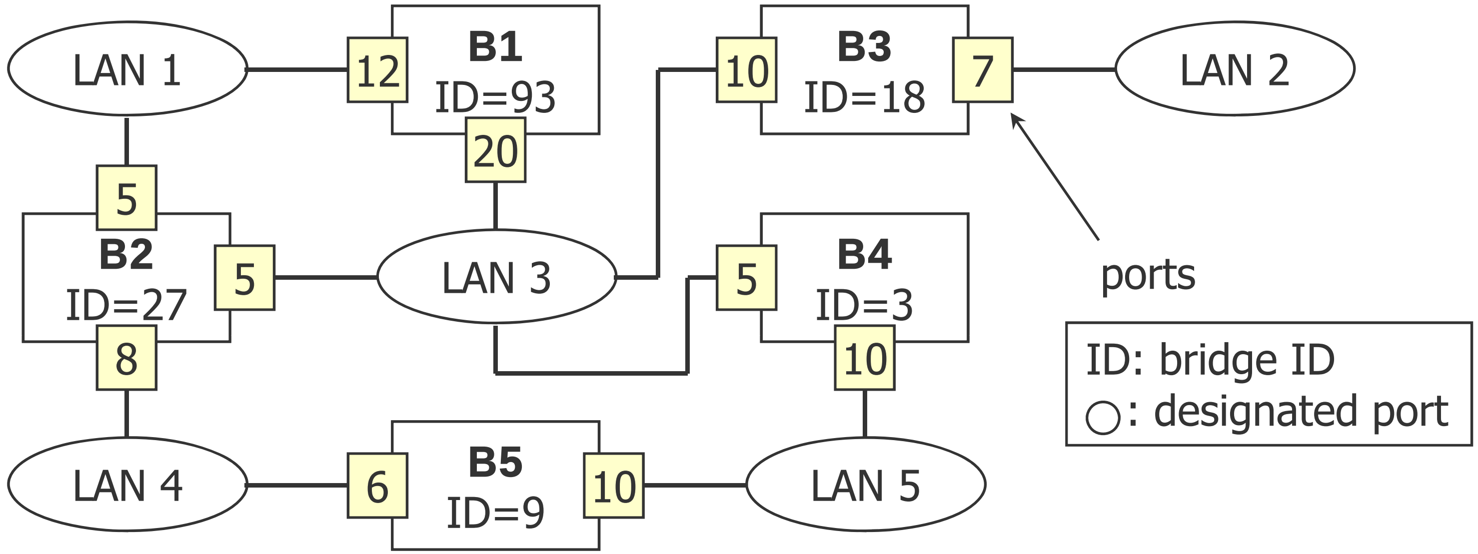
e.g. for station B on port P_1:

B	0	B	P_1

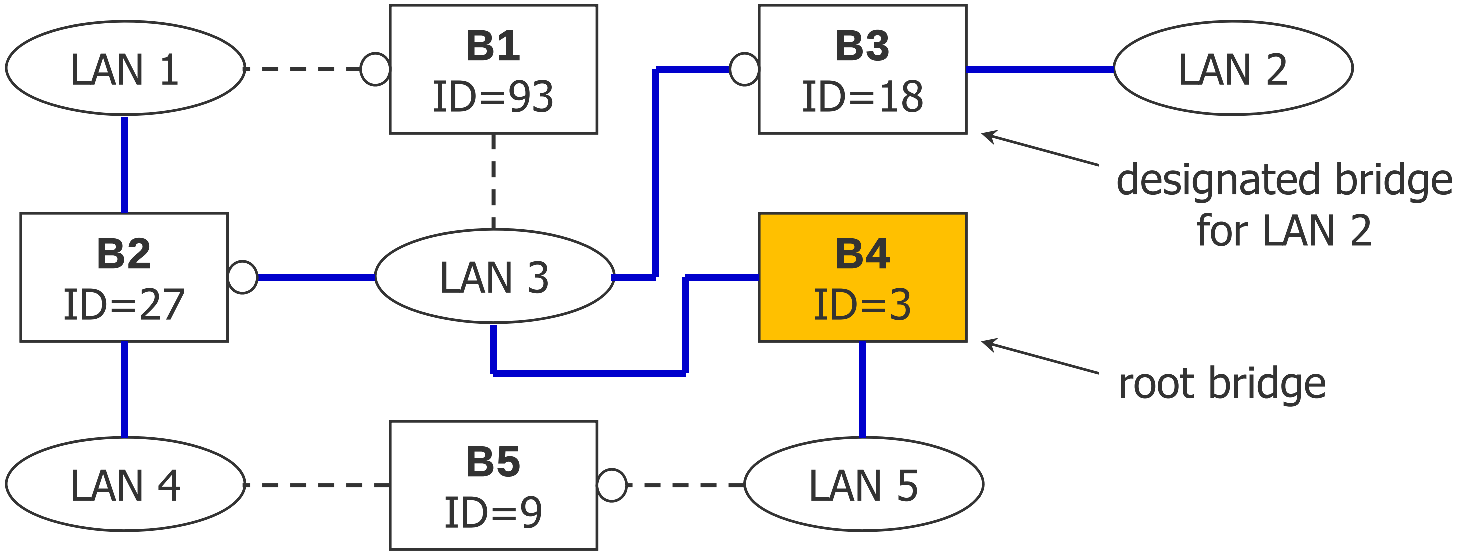
  - A bridge receiving such a packet checks the root ID and compares it with its own one. Root ID and costs are updated for received packets with smaller ID in the root bridge field and forwarded. Updating the costs is made by adding the own costs for the station from which the packet was received to the current costs value.
  - When the (updated) packets of all bridges have passed all other bridges, all bridges have agreed on the root bridge. The received packets containing the smallest costs value to the root bridge determine the designated bridge for a LAN and designated ports for the bridges to send out data.

Spanning Tree Algorithm: Example

Network:

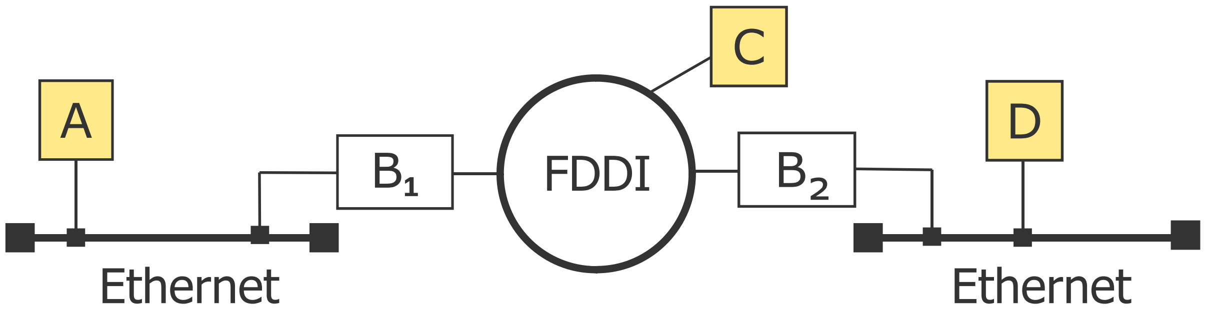


Spanning Tree:



Infrastructure Components: Bridges

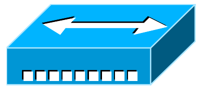
- Source Routing Bridges (e.g. for ring networks)



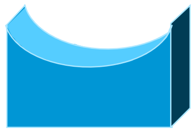
- Characteristics:
  - Sources must know (or learn), in which network segment the receivers are located
  - Large expenditure for determining the optimal route, e.g., via using a Spanning Tree algorithms or sending out Route Discovery Frames using broadcast
  - All LANs and Bridges on the path must be addressed explicitly
  - Connection-oriented, without transparency for the hosts

Network Infrastructure

- For building computer networks more complex than a short bus, some additional components are needed:
  - Repeater
    - Physically increases the range of a local area network
  - Hub
    - Connects several computers or local area networks of the same type (to a broadcast network)

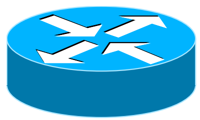


  - Bridge
    - Connects several local area networks (possibly of different types) to a large LAN

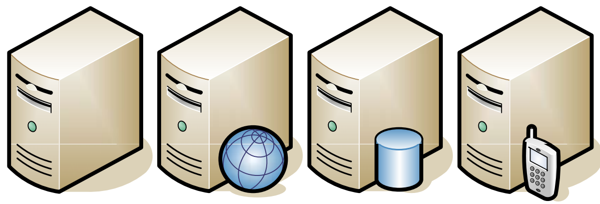


  - Switch
    - Like a hub, but without broadcast

  - Router
    - Connects several LANs with the same network protocol over large distances

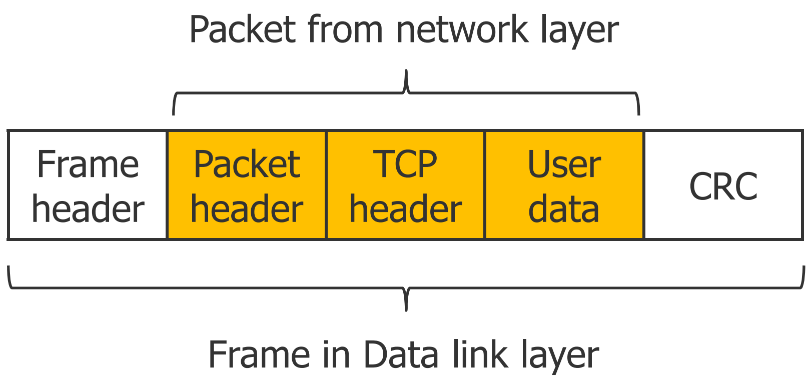


  - Gateway
    - Understands two different technologies and can convert the contents from one to the other and vice versa



Network Infrastructure

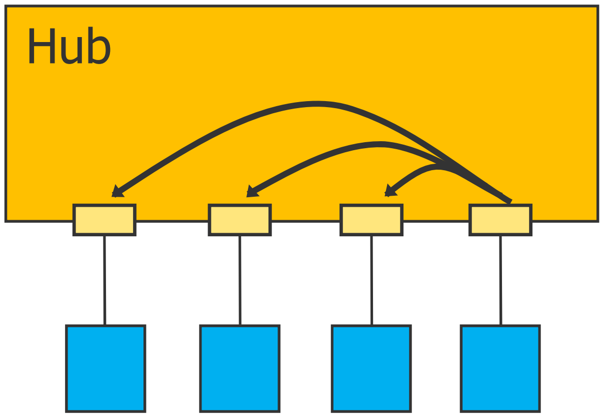
Application layer	Application gateway
Transport layer	Transport gateway
Network layer	Router
Data link layer	Bridge, Switch
Physical layer	Repeater, Hub



Infrastructure Components: Hub & Repeater

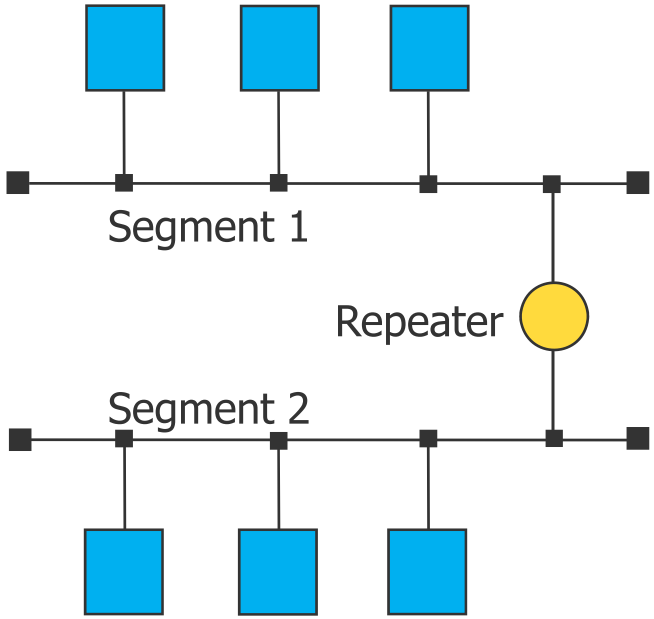
- Transmission of data on the physical layer
- Reception and refreshment of the signal, i.e., the signals received on one port are newly produced on the other(s)
- Do not understand frames, packets, or headers
- Increase of the network range
- Stations cannot send and receive at the same time
- One shared channel (Broadcast)
- Low security, because all stations can monitor the whole traffic
- Low costs

Layer 1

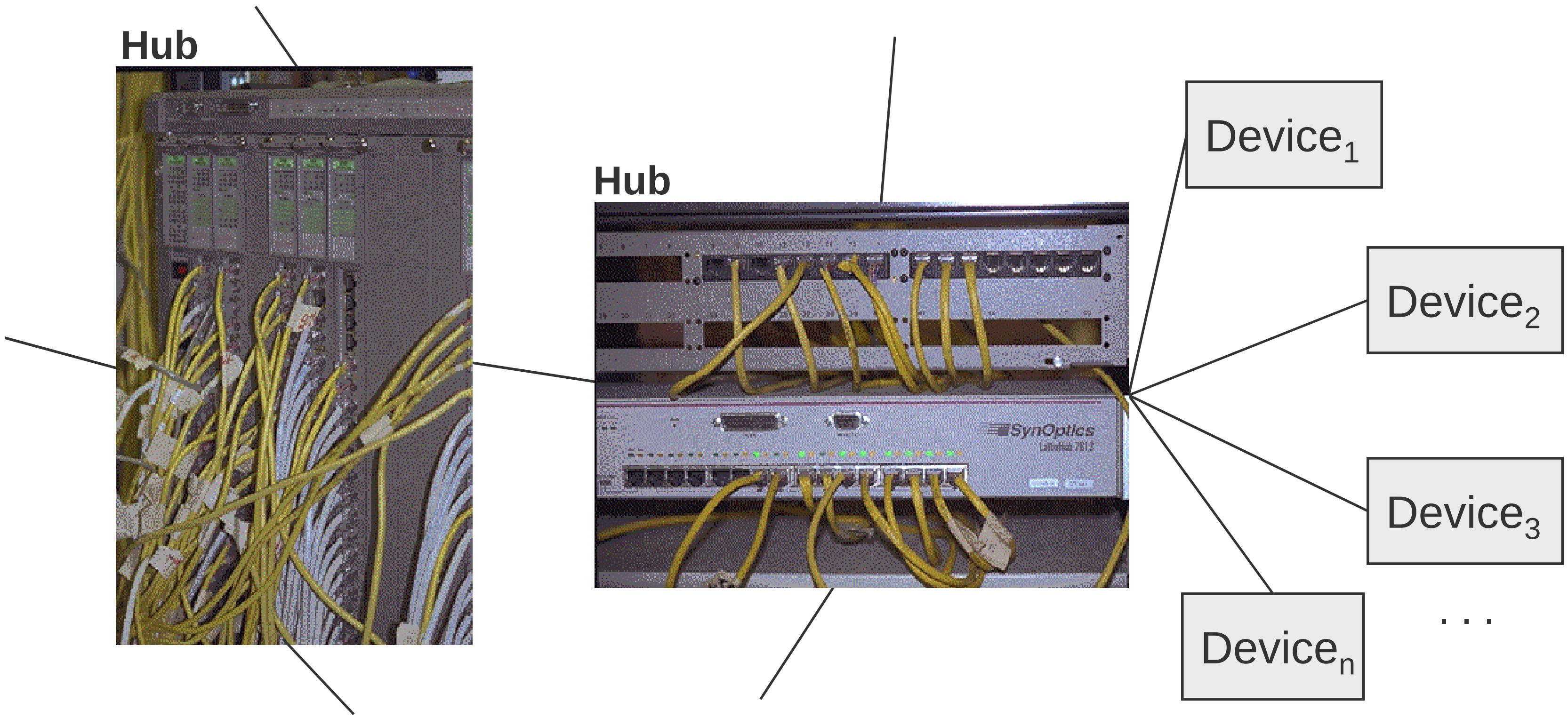


Hub: "one to all"

Repeater:
Linking of 2 networks



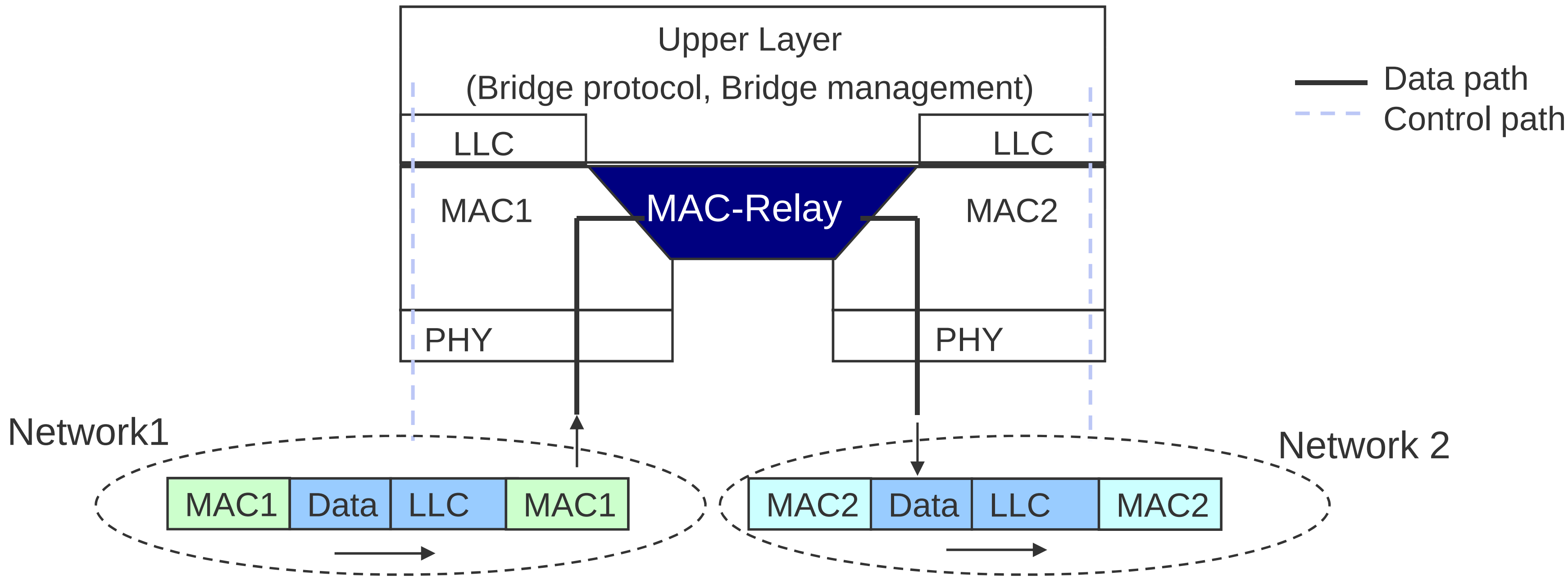
Infrastructure Components: Hub & Repeater



Infrastructure Components: Bridge

- Bridge
  - Bridge connects 2 or more LANs
  - Operates on frame addresses
  - Can support different network type

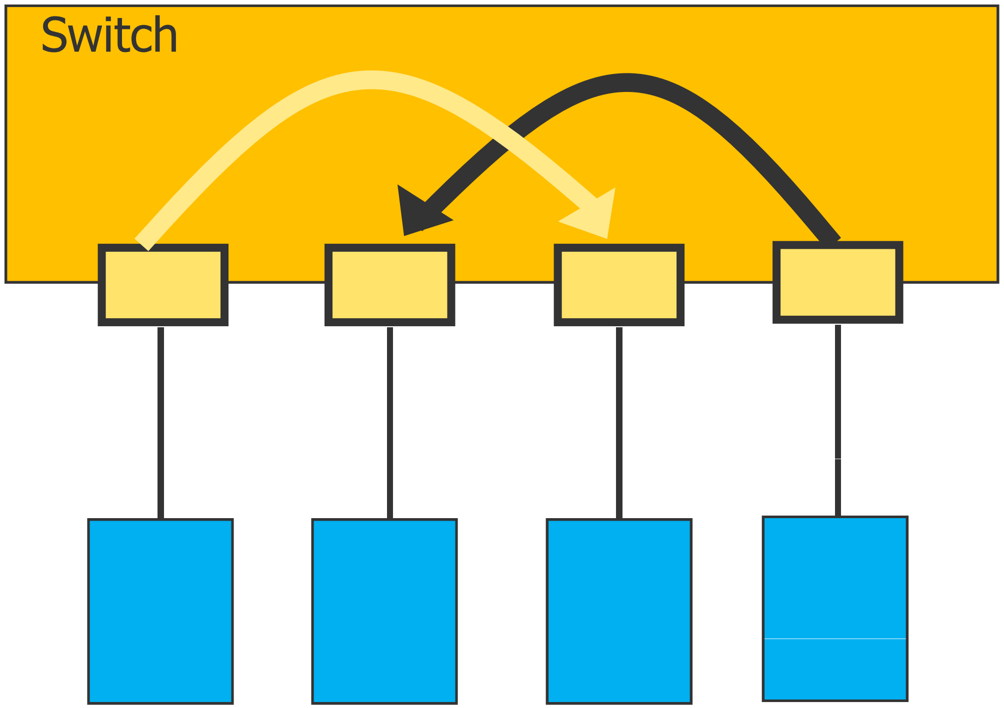
Layer 2



Infrastructure Components: Switch

Layer 2/3/4

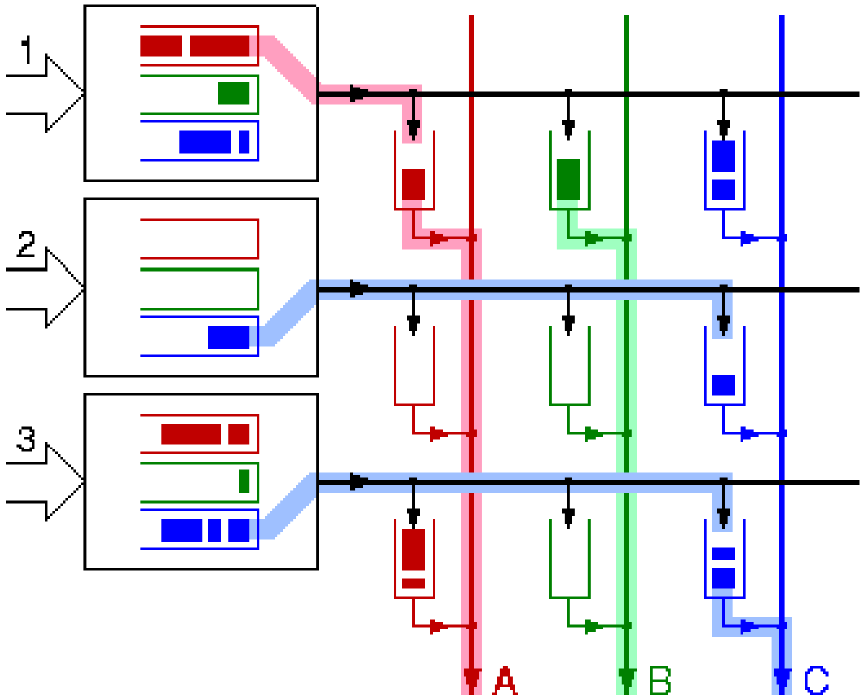
- Like a bridge, but:
  - Point-to-point communication, no broadcast
  - Switch learns the addresses of the connected computers
  - Stations can send and receive at the same time
  - No carrier control necessary
  - Buffer for each individual station/each port
  - Higher costs

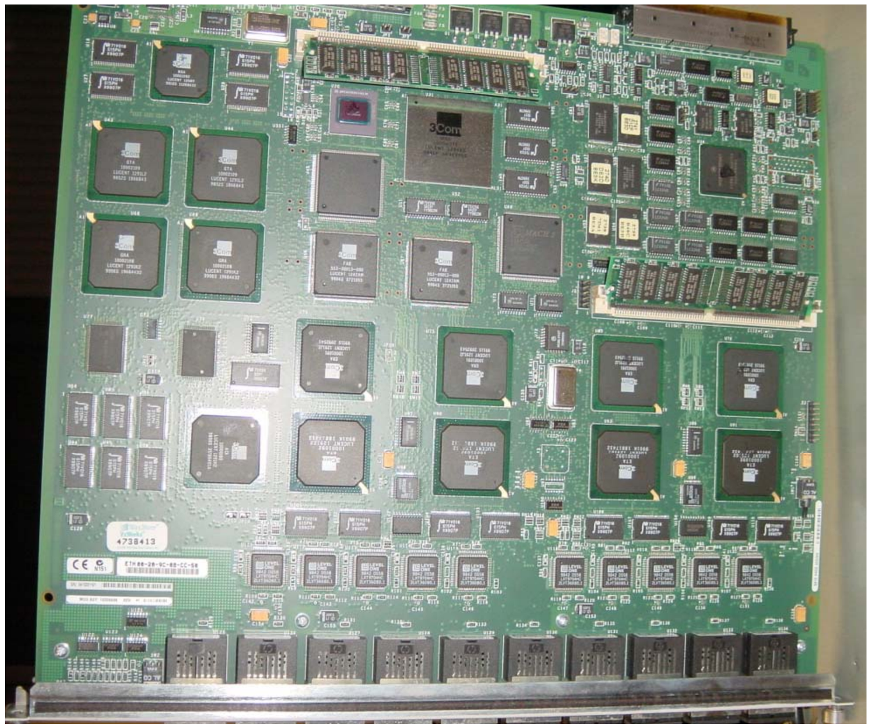


- "Layer 3-Switch": also has functionalities of level 3, i.e., it can e.g. take over the routing.
- "Layer 4-Switch": looks up additionally in the TCP-header, can therefore be used e.g. for load balancing.

Infrastructure Components: Switch – Realization

- Mostly used: buffered crossbar
  - For each input port, provide buffers for the output ports
  - At any time, only one input port can be connected to an output line
  - Additional speedup possible with small buffers at each cross-point
- With a buffered switch, nearly no more collisions are possible!





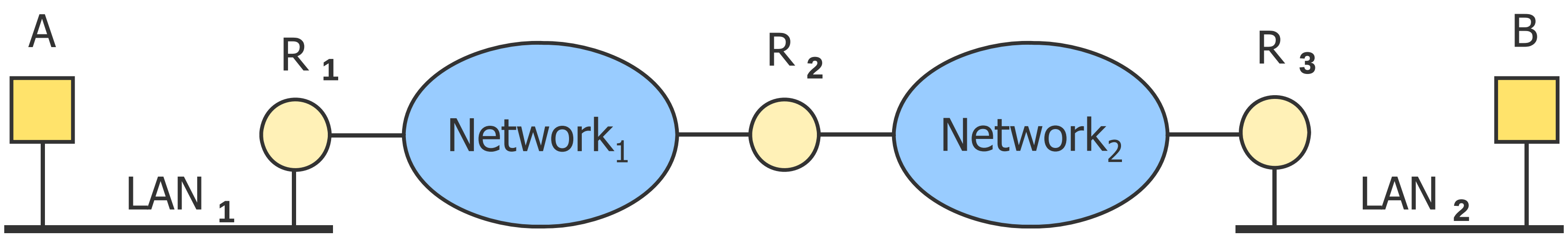
Infrastructure Components: Router

- What are the limitations of bridges?
  - Even though bridges are suitable to connect computers in several networks, there are also some disadvantages, e.g.:
    - Bridges can support only some thousand stations, which especially has the reason that addresses are used which do not have any geographical reference.
    - LANs coupled with bridges already form a “large LAN”, although a separation often would be desirable (e.g. regarding administration or errors).
    - Bridges pass broadcast frames on to all attached LANs.
      This can result in “Broadcast Storms”.
    - Bridges do not communicate with hosts, i.e., they do not hand over information about overload situations or reasons for rejected frames.
  - ➨ Router overcome these weaknesses

Infrastructure Components: Router

- Principal task of routers
  - Incoming packets are being forwarded on the best path possible to the destination on the basis of a global address
  - In principle no restriction concerning the number of hosts (hierarchical addressing)
  - Local administration of the networks (ends at the router), Firewalls are possible
  - Broadcasts are not let through by the routers, Multicast depending on the router
  - Communication between host and router improves performance

Layer 3



Infrastructure Components: Gateway

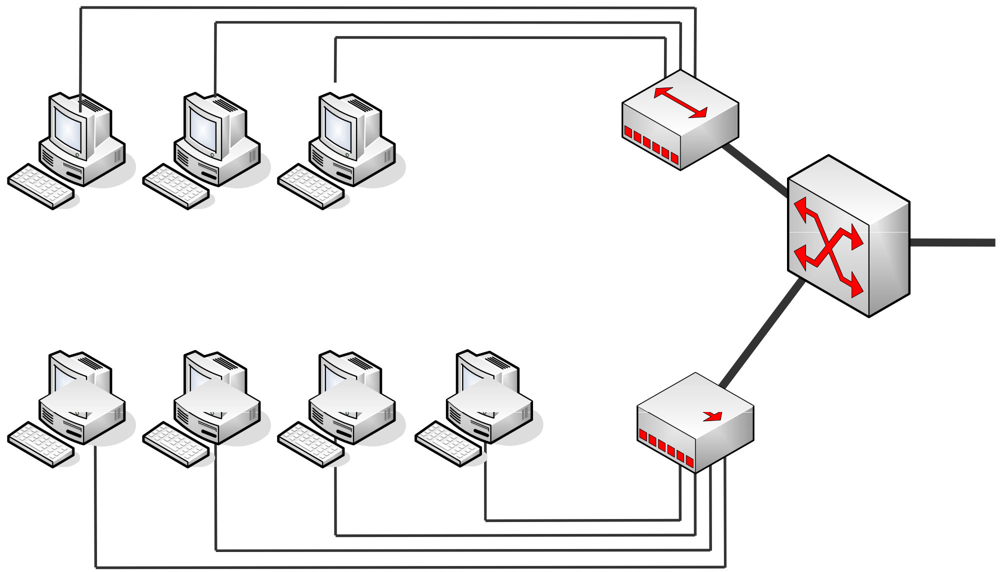
- Transport Layer Gateways
  - Connection of computers using different transport protocols, e.g., a computer using TCP/IP and one using ATM transport protocol
  - Copies packets from one connection to another

- Application Layer Gateways
  - Understand the format and contents of the data and translate messages from one format to another format, e.g., email to SMS

Virtual LANs

Virtual LANs

- Organization of LANs
  - In early Ethernet days all computers were on one LAN
  - With 10Base-T came new cabling in buildings
  - Configuration of LAN logically rather than physically
  - Requirement: Decoupling of the **logical topology** from the **physical topology**

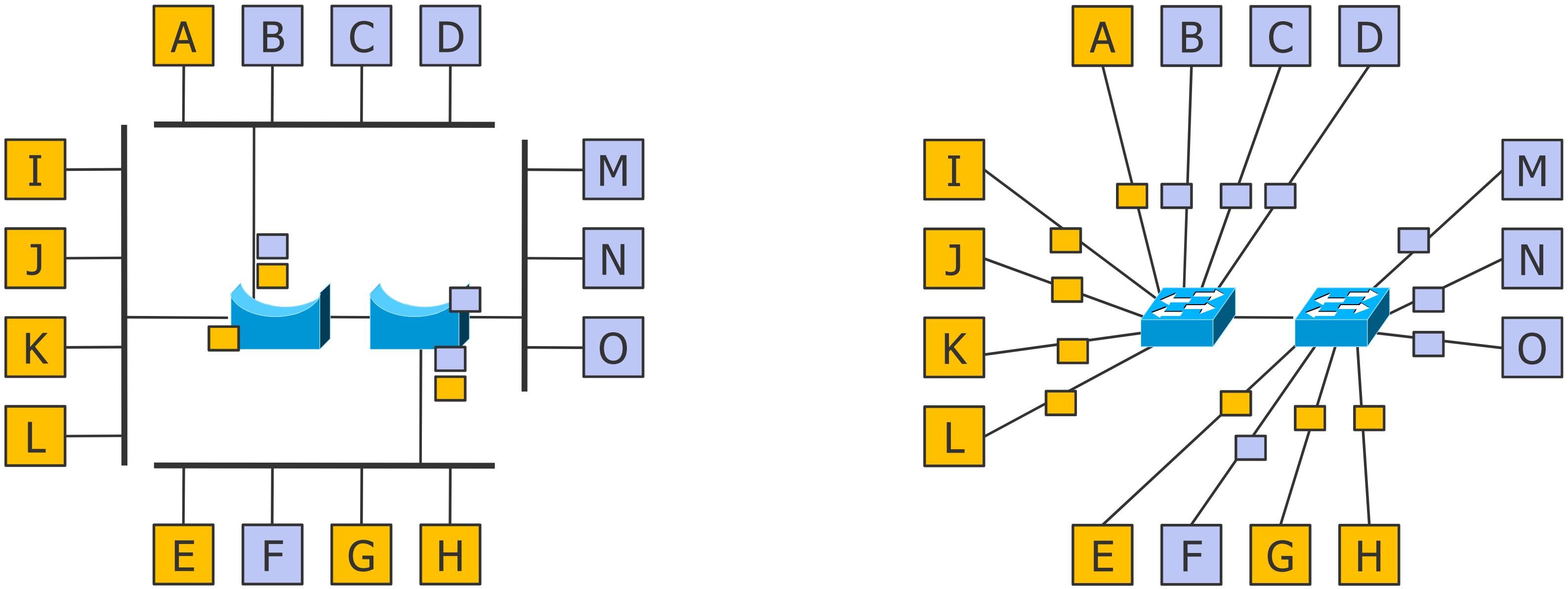


Virtual LANs

- Management often requires structuring of LANs due to
  - Different departments want different LANs
  - Security
  - Load
  - Broadcast (broadcast storm)

- What happens if users move from one department to another?
  - Rewire in hub/switch
  - VLANs with VLAN-aware switches

Virtual LANs



Virtual LANs

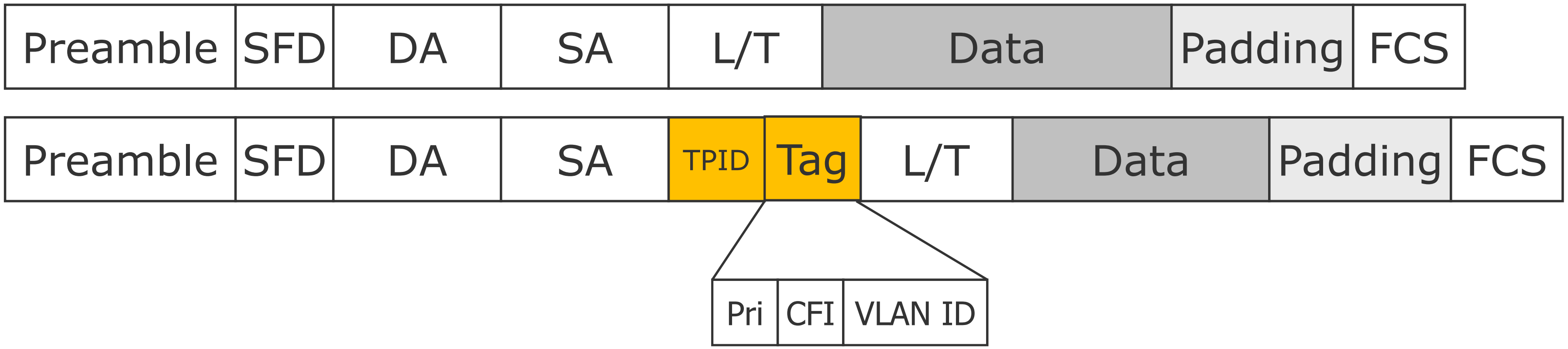
- Virtual LANs require VLAN-aware switches
  - VLANs are often named by colors (VLAN ID)
  - Allows colored diagrams which show logical and physical topology at the same time
- VLAN-aware devices have to know about the VLANs
  - Switch has a table which tells which VLAN is accessible via which port
  - A port may have access to multiple VLANs
- How do a VLAN-switch know the VLANs?
  - Assign every port of the device a VLAN ID
    - Only machines belonging to the same VLAN can be attached
  - Every MAC address is assigned to a VLAN
    - Device needs tables of the 48-bit MAC addresses assigned to VLANs
  - Every Layer 3 protocol (IP address) is assigned to a VLAN
    - Violates the independency of layers

Virtual LANs

- IEEE 802.1Q
  - Special field in frame header telling the VLAN assignment
  - Problems:
    - What happens with existing Ethernet cards?
    - Who generates the new field?
    - What happens with full frames (maximum length)?
  - Solution:
    - The first VLAN-aware device adds a VLAN-tag
    - The last VLAN-aware device removes the VLAN-tag

Virtual LANs

- IEEE 802.1Q Frame Format
  - Additional pair of 2-byte fields
  - TPID: Tag Protocol Identifier (0x8100)
  - Tag comprises three fields
    - Pri: 3-bit priority field, does not have anything to do with VLANs
    - CFI: Canonical Format Indicator
      - Indicates that payload has a IEEE 802.5 frame
    - **VLAN ID: 12-bit VLAN identifier**
      - **The only relevant field**



Virtual LANs

- Who inserts the VLAN-tag?
  - New cards (Gigabit Ethernet) support 802.1Q
  - Otherwise
    - First VLAN-aware switch adds the tag
    - The VLAN-aware switch removes the tag
  - How does the switch know which frame belongs to which VLAN?
    - First device has to decide based on the port or MAC address

Summary

- Layer 1 and 2: "How to physically transport data reliably from one computer to a neighbored one"?
  - Layer 1 defines transmission medium and bit representation on this medium
  - Layer 1 additionally specifies transmission mode, data rate, pin usage of connectors, …
  - Layer 2 protects against transmission errors (mostly CRC) and receiver overload (flow control, sliding window)
  - Layer 2 also defines medium access coordination for broadcast networks
  - Both layers together define how to transfer data from one computer to a **directly connected** one (maybe over a hub/switch) – on that reason both are implemented in one piece of software: the network interface card driver.
  - Bridges in principle allow to connect lots of LANs over long distances – is that the Internet?

Summary

- LANs
  - Ethernet as standard for local networks
  - 10G-Ethernet also possible for use in MANs
- WANs
  - SDH/Sonet as standard for wide area networks
  - 10G-Ethernet as access technology to the core network
  - Integration of DWDM – transmission on 160 wavelengths in parallel dramatically increases the capacity
  - Also possible: SDH with 40 Gbps, DWDM with 4096 channels – 164 Tbps!
  - Dream of “all optical network”: switch/route data streams with optical components (think of a prism)