OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

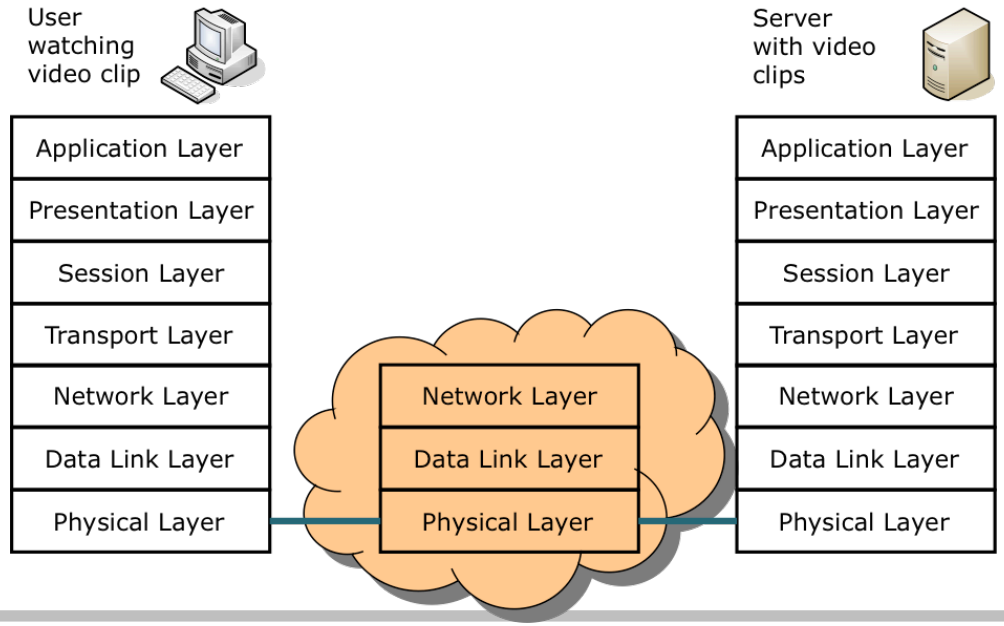
FAKULTÄT FÜR INFORMATIK

Communication and Networked Systems

Computer Networks

Chapter 5: Medium Access Control Sublayer

Prof. Dr. Mesut Güneş
Communication and Networked Systems (ComSys)
OVGU Magdeburg
comsys.ovgu.de | mesut.guenes@ovgu.de



Contents

- Design Issues
- Network Topologies
- The Channel Allocation Problem
- Multiple Access Protocols
- Ethernet
- IEEE 802.2 – Logical Link Control
- Network Infrastructure
- Structured Cabling
- Virtual LANs

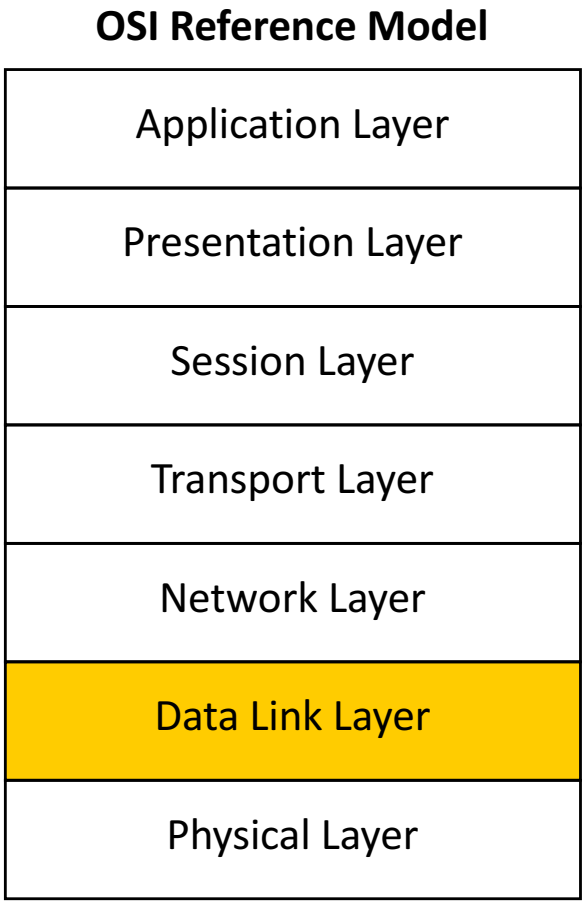
Design Issues

Design Issues

- **Two kinds of connections in networks**
  - Point-to-point connections
  - Broadcast
    (Multi-access channel, Random access channel)

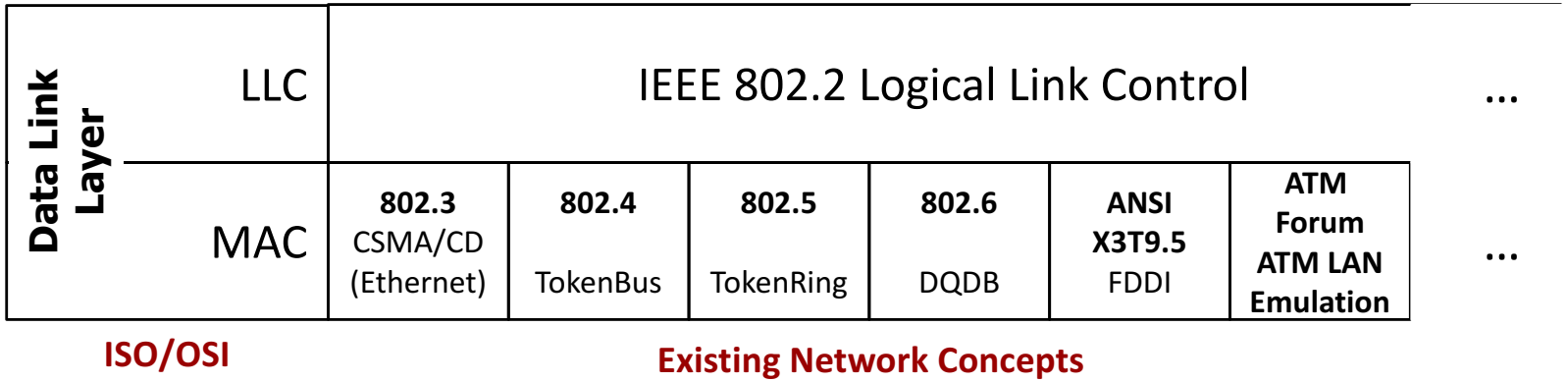
- **In a network with broadcast connections**
  - Who gets the channel?

- **Protocols used to determine who gets next access to the channel**
  - Medium Access Control (MAC) sublayer



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:

1. Packing data into frames: error detection during frame transmission and receipt

2. Media Access Control: who gets the access to the medium

Standardization: IEEE

www.ieee.org

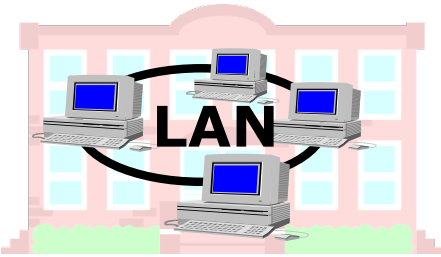
Institute of Electrical and Electronic Engineers (IEEE)

- Standardization of the IEEE 802.X-Standards for Local Area Networks (www.ieee802.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)
  - Wireless LAN (WLAN, up to a few 100 m)

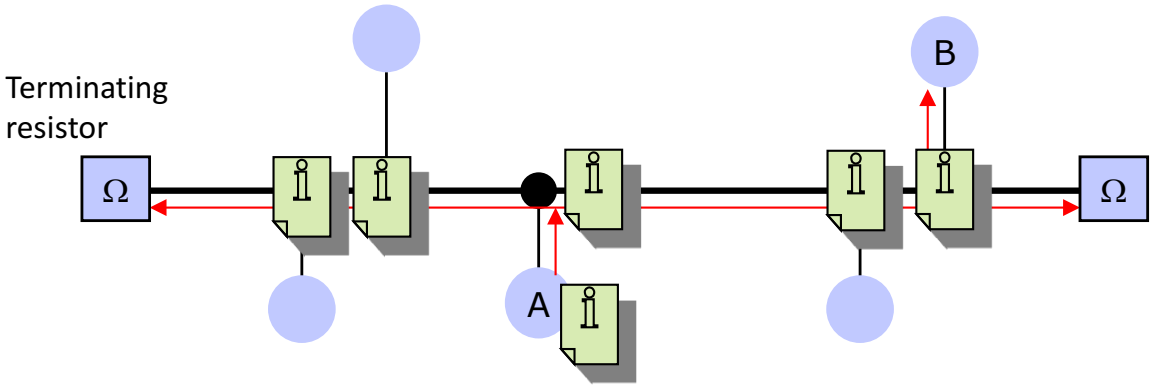


- **Metropolitan Area Network (MAN): 10-100 km**
  - City range
  - DQDB
  - FDDI II
  - Resilient Packet Ring
  - [also used: Gigabit Ethernet]

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

Network Topologies

Bus

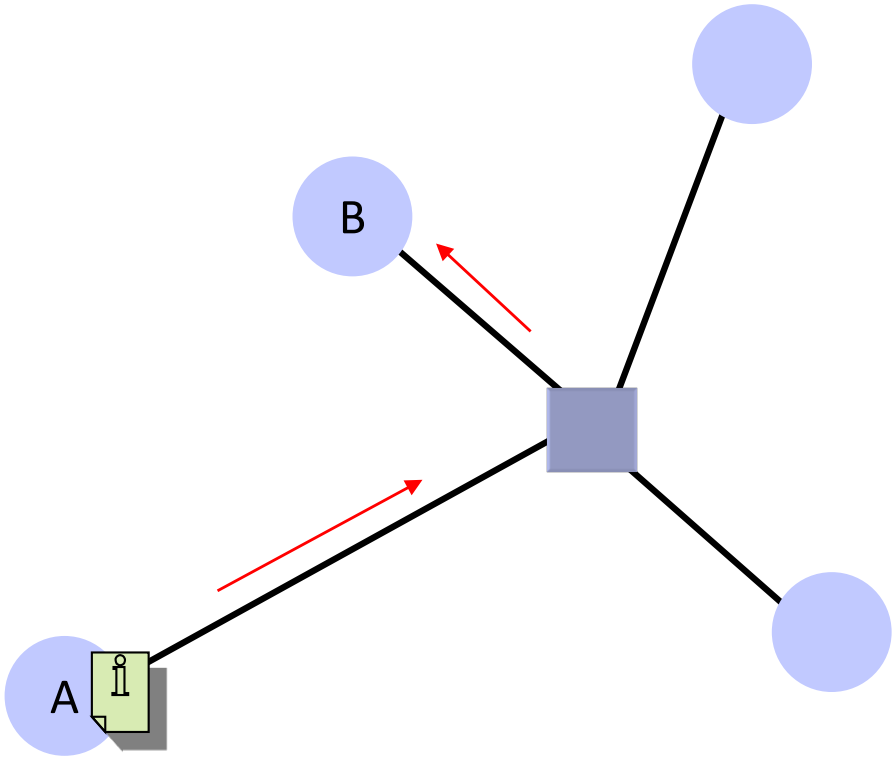


Example: **Ethernet**

- **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

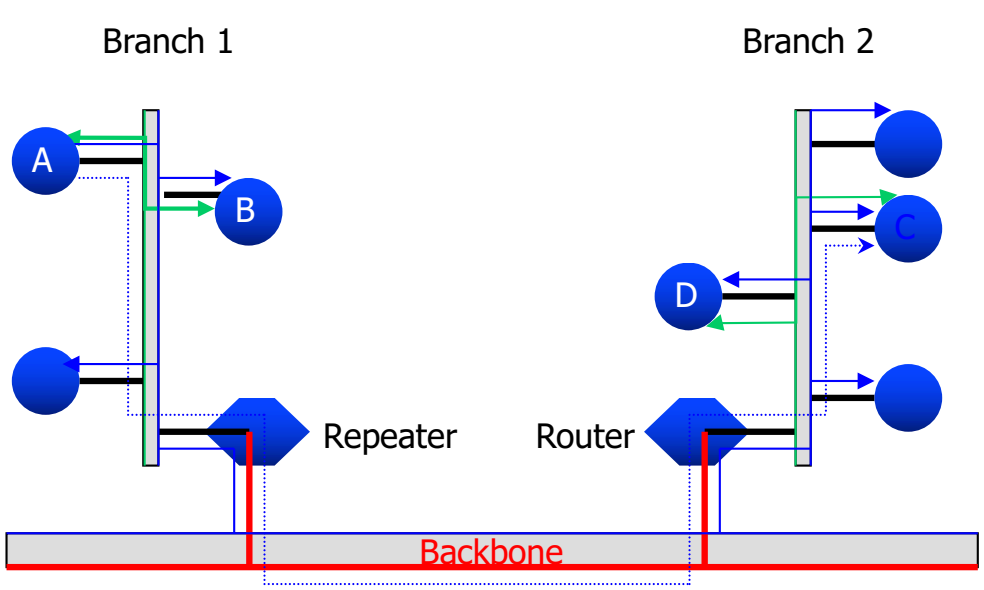
- **Star**
  - Designated computer as central station: a message of station A is forwarded to station B via the central station
  - Broadcast network (Hub) or point-to-point connections (Switch)
  - Expensive central station
  - Vulnerability through central station (Redundancy possible)
  - N connections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

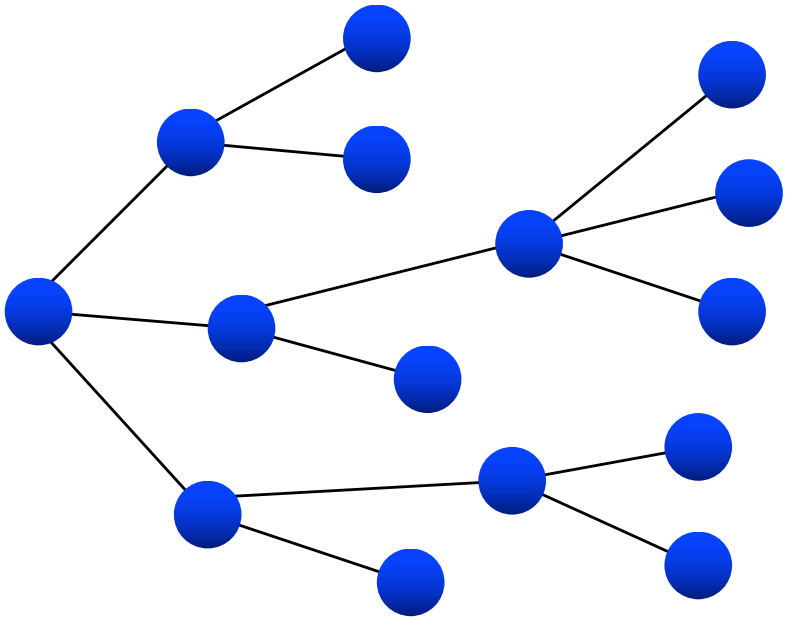


Example: **Fast Ethernet**

Tree

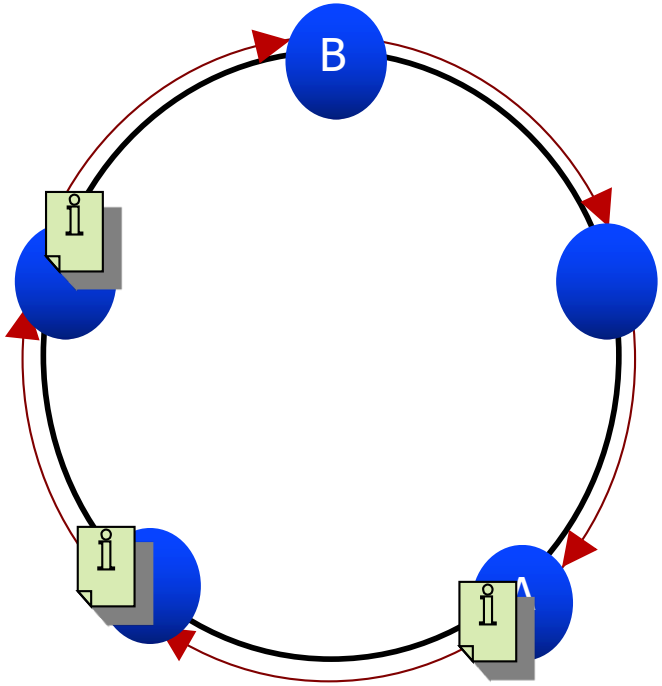
- **Tree**
  - Topology: Connection of several busses or stars
  - Branching elements can be active (Router) or passive (Repeater)
  - Bridging of large distances
  - Adaptation to given geographical structure
  - Minimization of the cable length possible





Ring

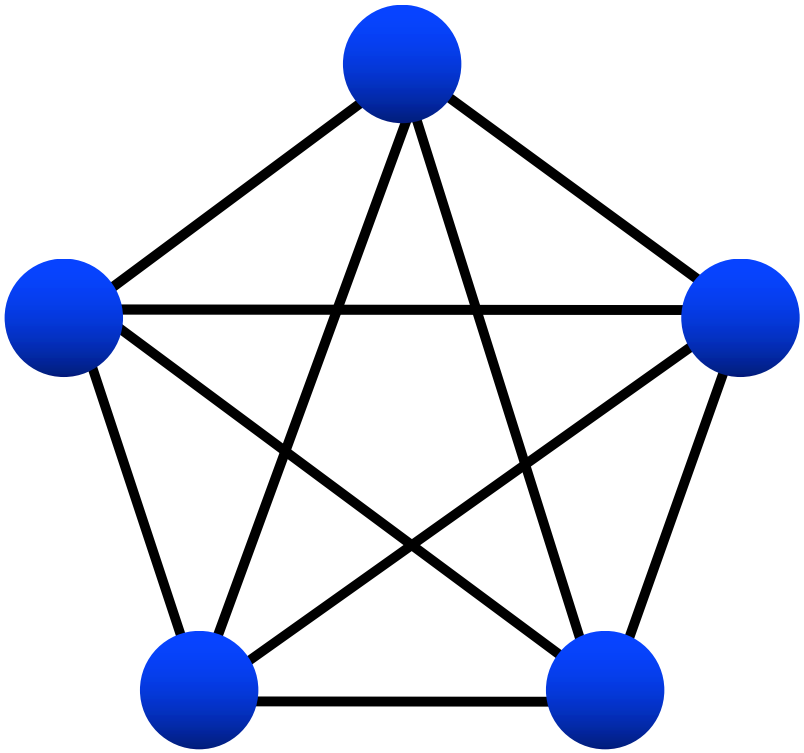
- **Ring**
  - Broadcast Network
  - Chain of point-to-point connections
  - Active stations: messages are regenerated by the stations (Repeater)
  - Breakdown of the whole network in case of failure of one single station or connection
  - Large extent possible
  - Easy connection of new stations
  -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



Example: **Token Ring, FDDI**

Meshed Networks

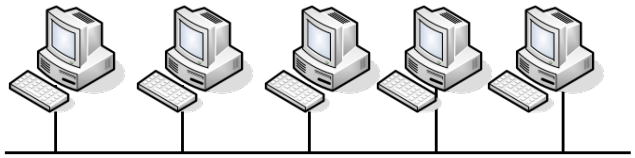
- **Fully Meshed Network**
  - Point-to-Point connections between all stations
  - For N stations, $\frac{N(N-1)}{2}$ connections are needed
  - Connecting a new station is a costly process
  - Redundant paths
  - Maximal connection availability through routing integration

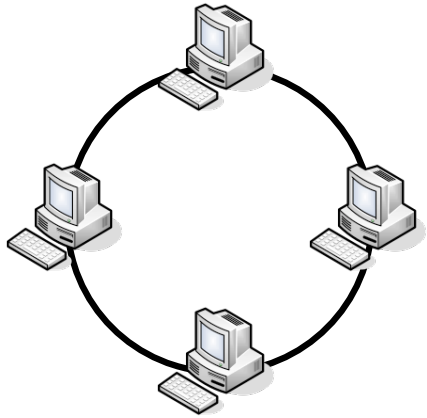


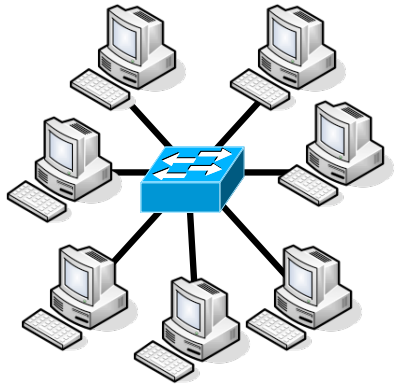
Partly meshed network: cheaper, but routing, flow control, and congestion control become necessary (Wide Area Networks)

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



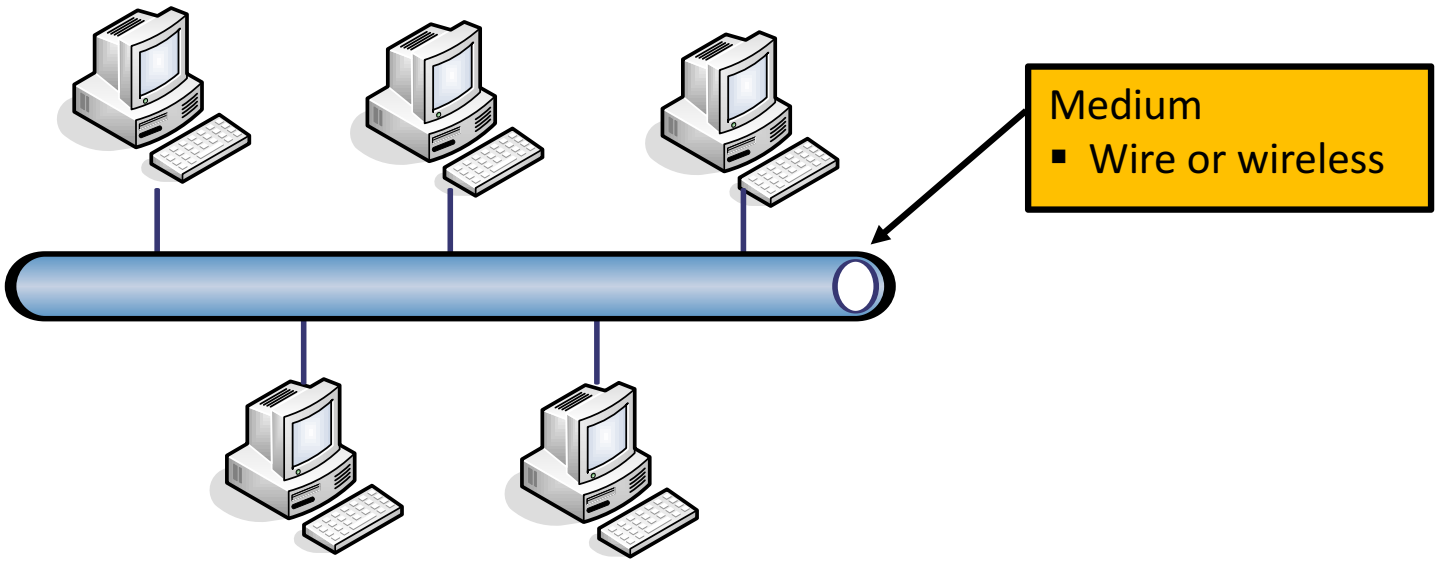




The Channel Allocation Problem

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

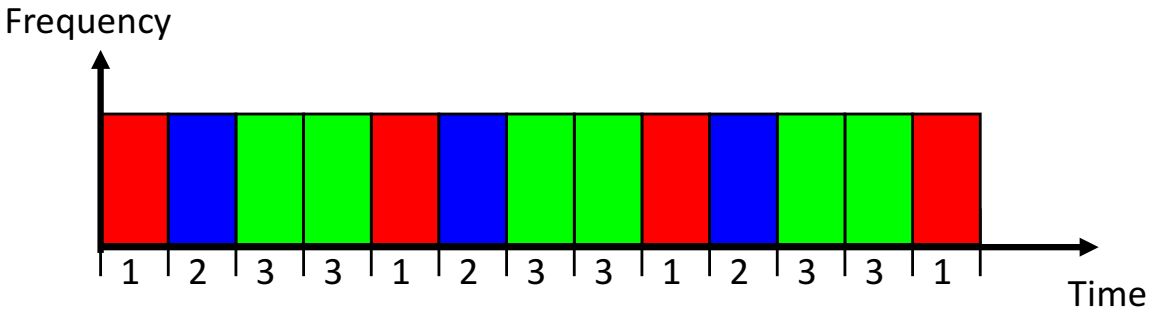


- **Approaches**
  - Static channel allocation
  - Dynamic channel allocation

Static Channel Allocation

- Controlling the competitive access of several users to a shared medium
- Simplest procedure: **static** assignment of a limited capacity

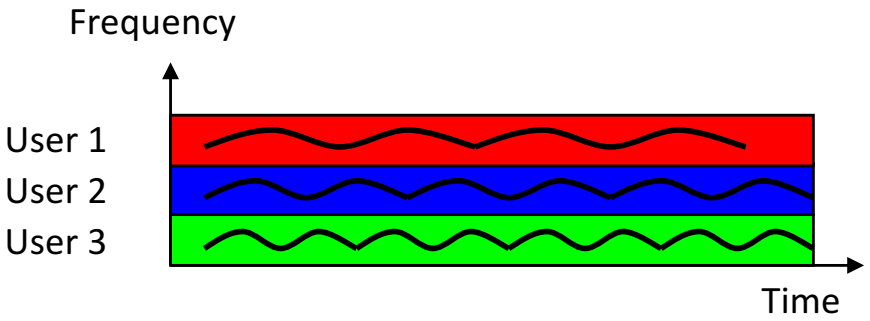
- Time Division Multiple Access (**TDMA**)



Each user gets the entire transmission capacity for a fixed time interval

(Baseband transmission)

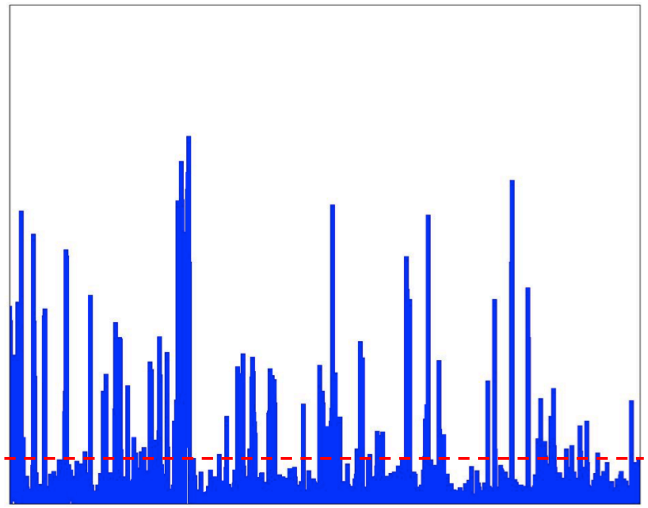
- Frequency Division Multiple Access (**FDMA**)



Each user gets a fixed portion of the transmission capacity (a frequency range) for the whole time (Broadband transmission)

Static Channel Allocation

- **Problems with static channel allocation**
  - Works only for a fixed number of users
    - When number of users changes, 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**

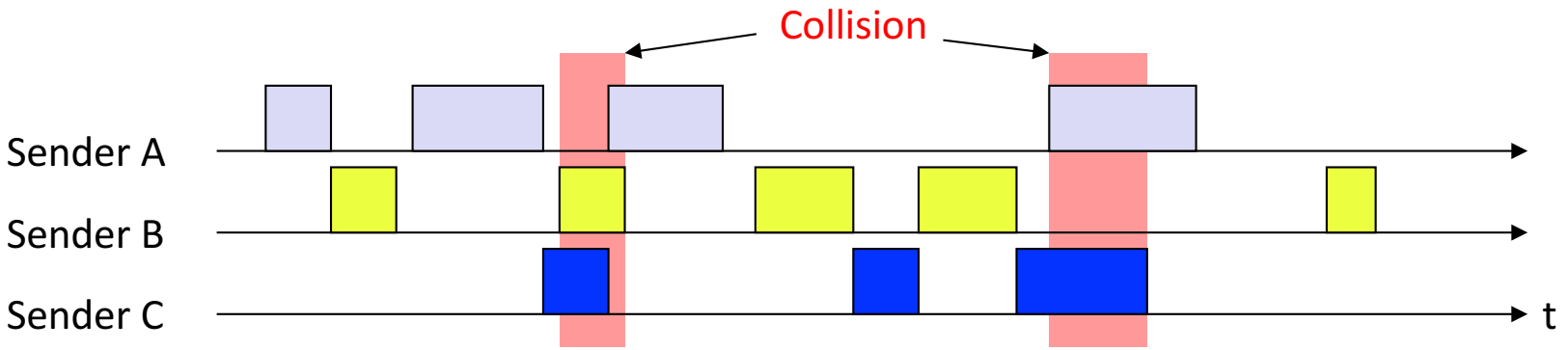
Dynamic Channel Allocation

- **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

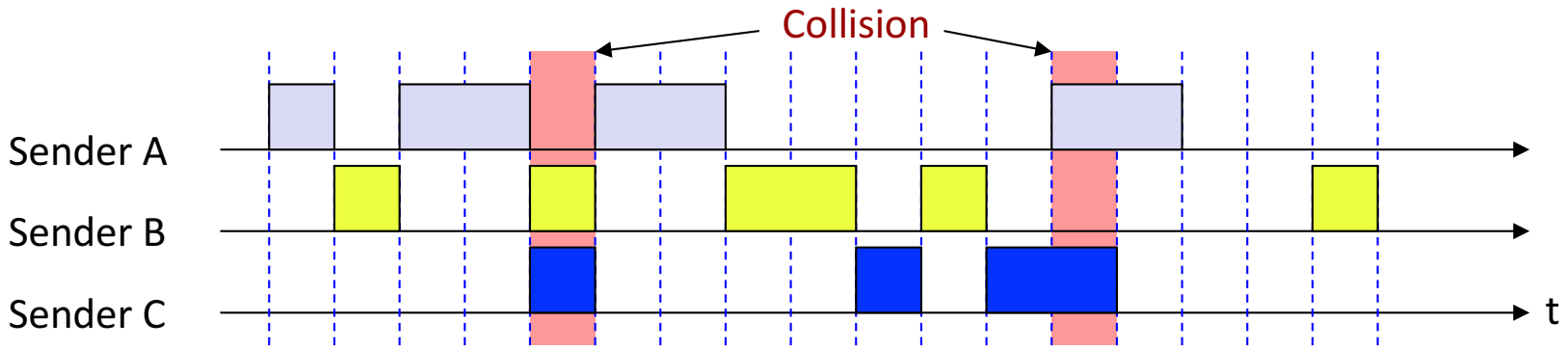
Multiple Access Protocols: ALOHA

- **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 stations use the same frequency
  - When two (or more) stations are sending at the same time, a collision occurs: all 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 (1 bit) result in transmission conflicts. Therefore, often collisions arise resulting in many retransmissions:**
  - 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 with mean N frames/s
  - Collided frames are retransmitted
  - Probability of k transmission trials per frame time is according to a Poisson distribution with mean G

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

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

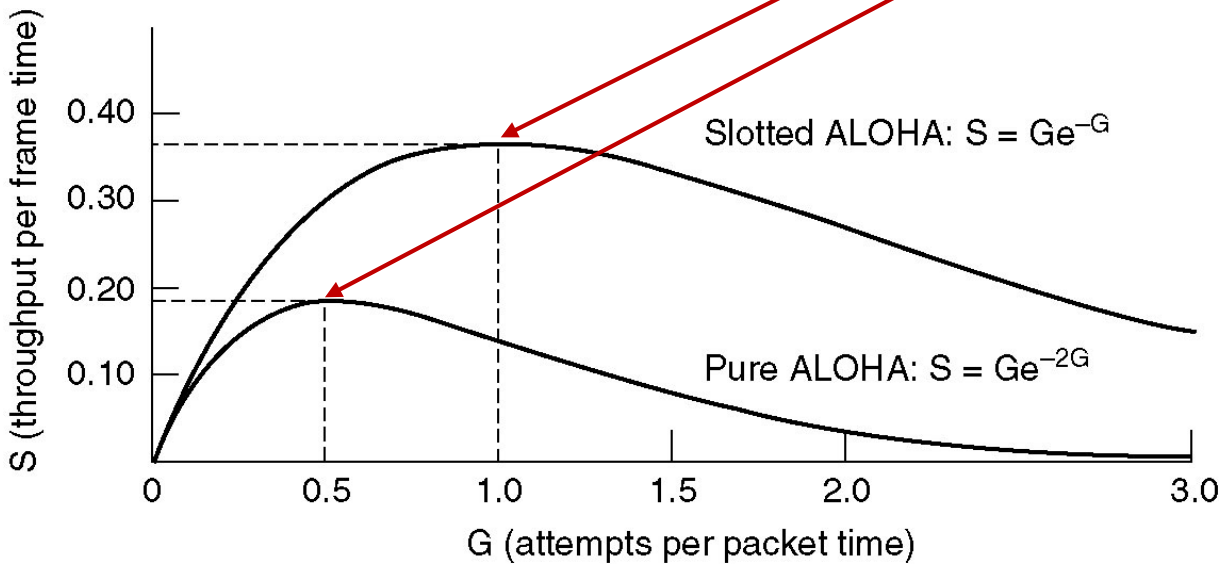
$$S = G\, P_0$$

- **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:** $P(k=0) = e^{-G}$
- **Collision time**
  - ALOHA: $2t$
  - Slotted ALOHA: t
- **Throughput**
  - ALOHA: $S = G\,P_0 = \mathrm{G}\ \mathrm{e}^{-2\mathrm{G}}$
  - Slotted ALOHA: $S = G\,P_0 = \mathrm{G}\ \mathrm{e}^{-\mathrm{G}}$

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



Multiple Access Protocols: CSMA

- **Variant of ALOHA for networks with small range**
  - Similar to ALOHA: no coordination of the stations
  - But: each station, which wants to send, first examines whether already another station is sending
  - If no sending takes place, the station begins to send
    → **Carrier Sense Multiple Access (CSMA)**
  - Notice: this principle only works with networks with a short transmission delay. This principle does not work for satellite (wireless) systems, because there is no chance to know whether a conflict occurred before the end of the transmission
  - **Advantages:** simple, since no master station and no tokens are needed. Nevertheless good utilization of the network capacity.
  - **Disadvantage:** no guaranteed medium access, a large delay until the begin of a transmission is possible.

Multiple Access Protocols: CSMA

Persistent and Nonpersistent CSMA

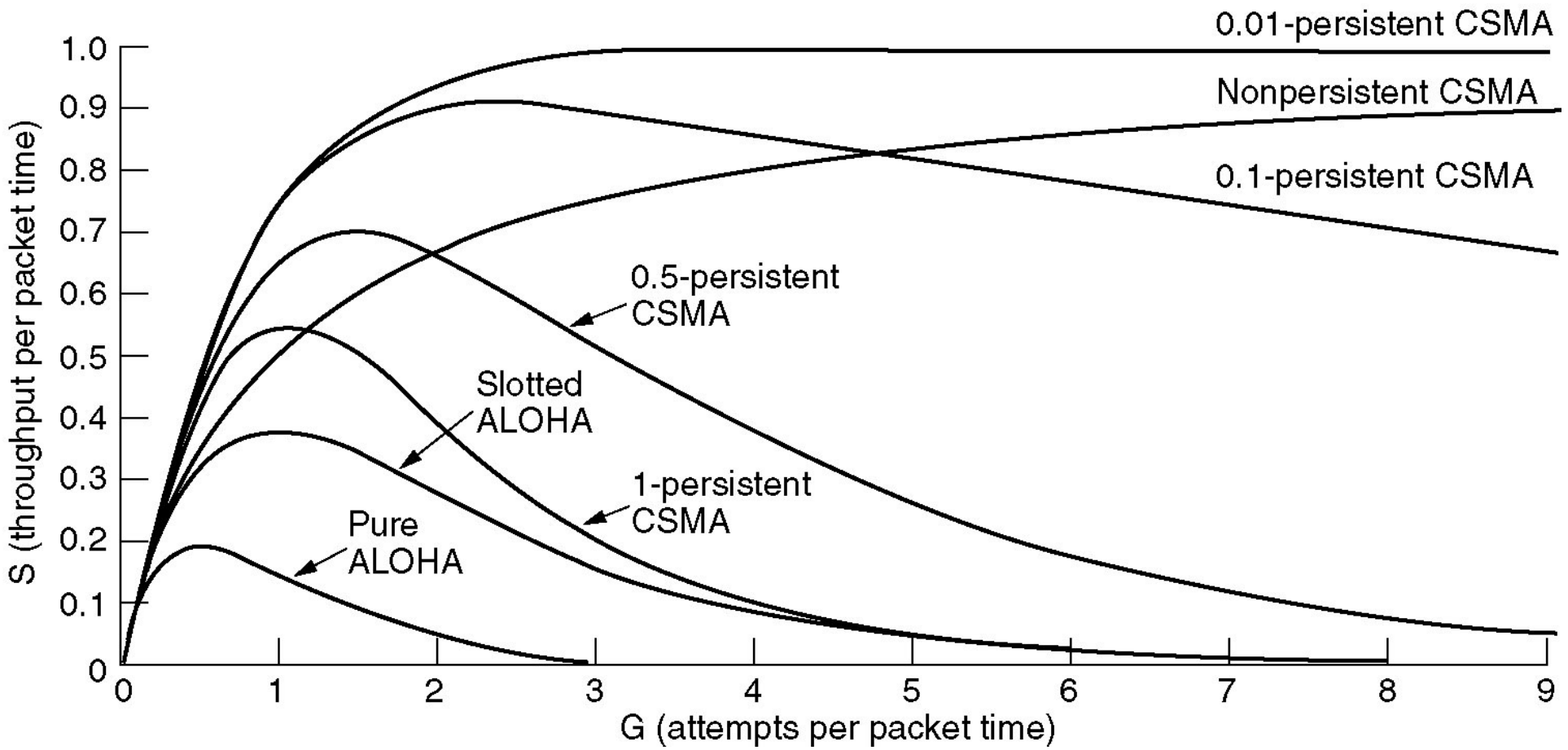
- **1-persistent CSMA**
  - When a station has data to send, it first listens to the channel.
  - If channel busy, the station waits until it becomes idle.
  - When channel is idle, station transmits a frame.
  - When a collision occurs, the station waits a random amount of time and starts all over again.
  - 1-persistent = station transmits with probability of one if channel idle.

- **Non-persistent 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 $(1\text{-}p)$ it defers until next slot.
  - If the next slot is idle, the station again transmits with probability p and defers with $(1\text{-}p)$.

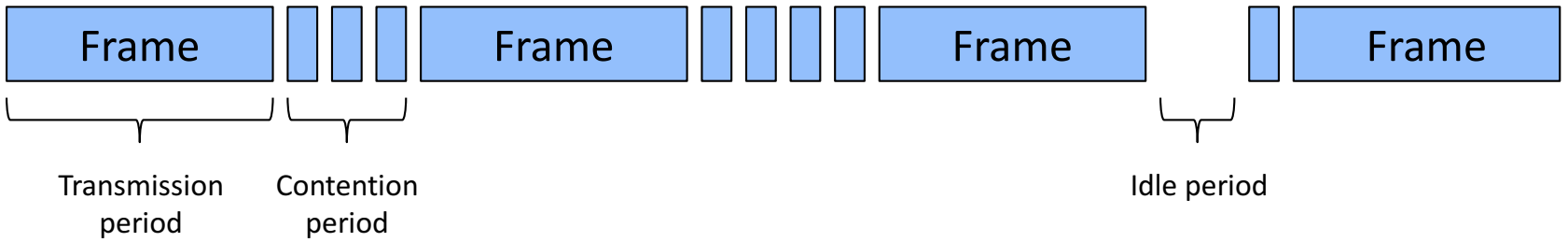
Multiple Access Protocols: CSMA

Comparison of ALOHA and variants of CSMA



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):**
  - 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)
  - 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 periodically polls all stations for sending data. Master station assigns sending rights.

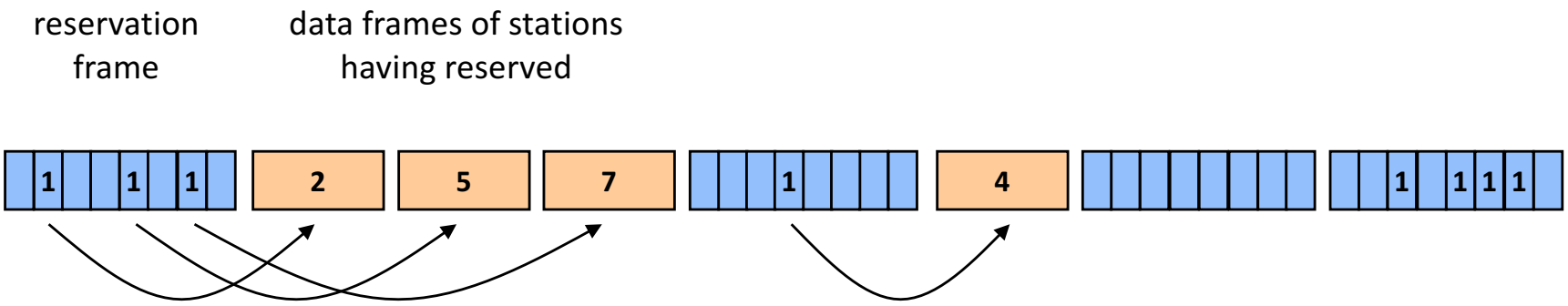
- **Techniques for »easy« reservation without master station:**
  - Explicit reservation
  - Implicit reservation

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
- User k is assigned the k-th slot in the reservation frame. If he wants to send data, he sets the k-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.



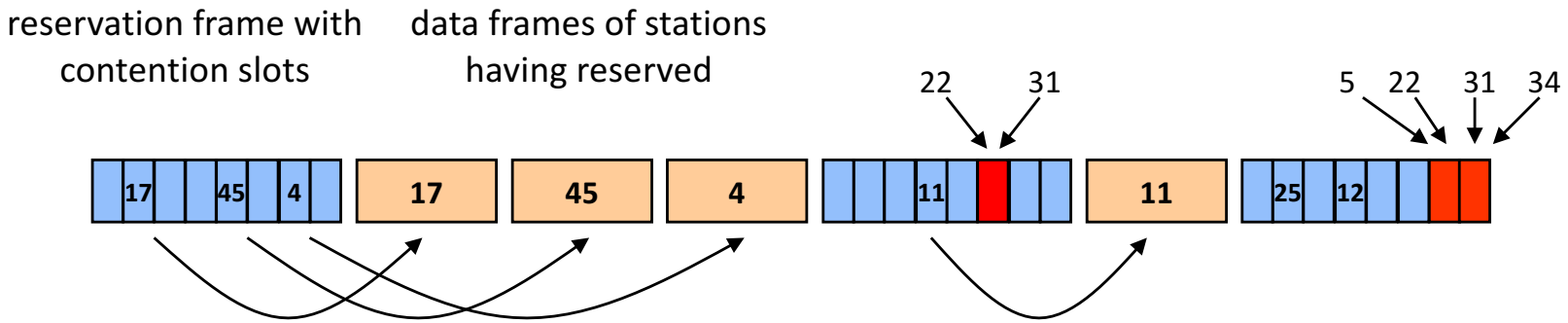
This procedure is called **Bit-Map Protocol**

Collision-Free Protocols: Bit-Map Protocol

- Uses two frame types:
  - reservation frame (very small) in the first phase
  - data frame (constant length) in the second phase

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: Binary Countdown

- **Binary Countdown**
  - For large number of stations
  - Binary station addresses, all addresses to be the same length
  - A station that wants to use the channel broadcasts its address as a binary string starting with the high-order bit
  - The bits from different stations are OR-ed
  - 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			
	0	1	2	3
0010	0			
0100	0			
1001	1	0	0	
1010	1	0	1	0
Result	1	0	1	0

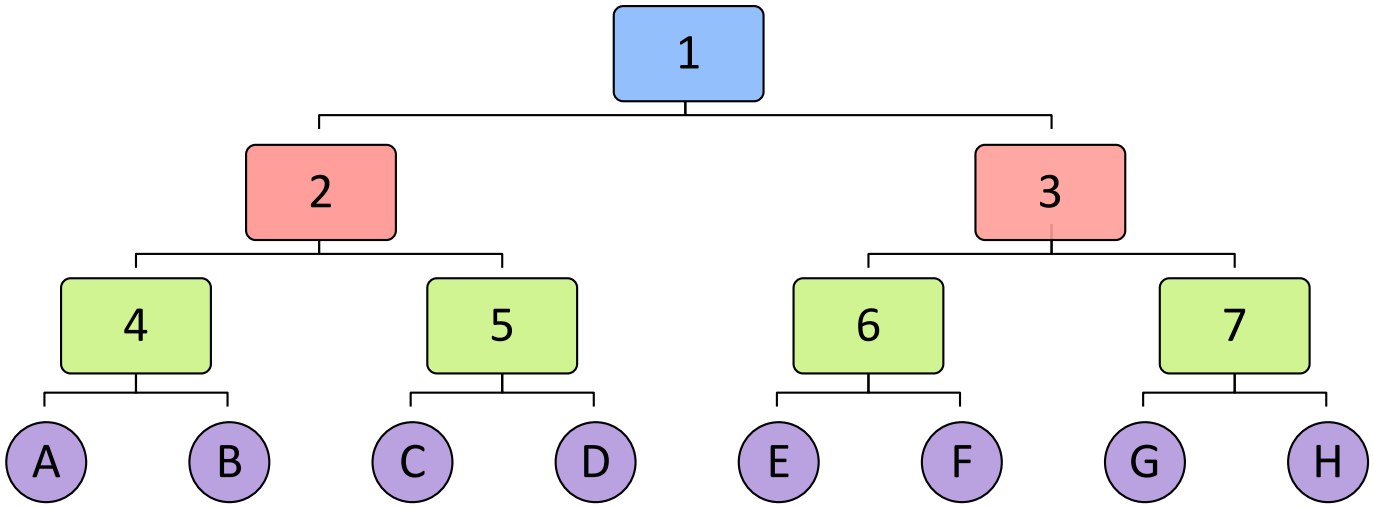
Multiple Access Protocols

Limited Contention Protocols

Limited Contention Protocols

Adaptive Tree Walk

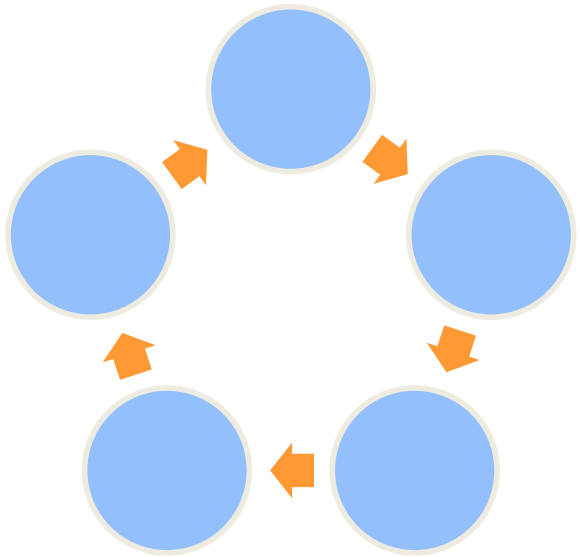
- **Adaptive Tree Walk Protocol**
  - Stations are the leaves of a binary tree
  - In the first contention slot following a successful frame, slot 0, all stations (A-H) are permitted to try to acquire the channel
  - If collision, during slot 1 only stations under node 2 (A-D) may compete
    - If one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

- **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



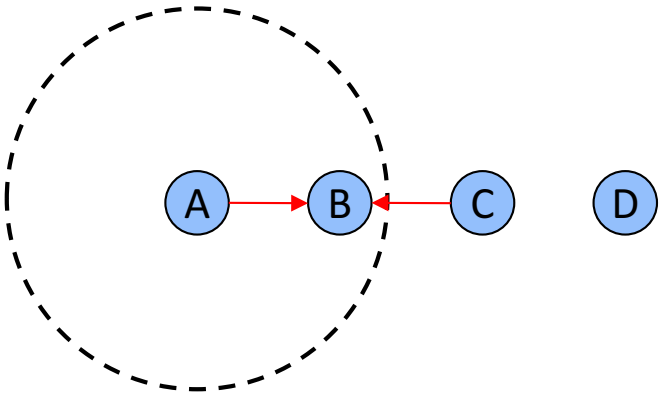
Passing on of the token

Multiple Access Protocols

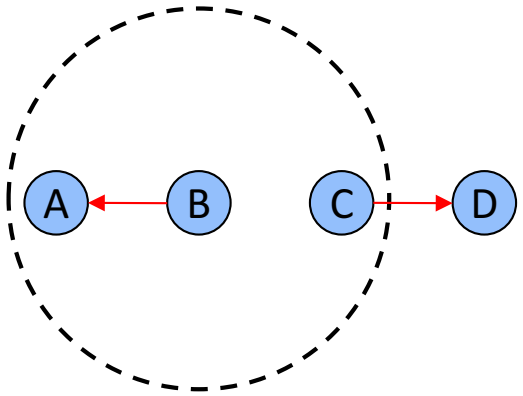
MAC for Wireless Networks

MAC for Wireless LANs

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



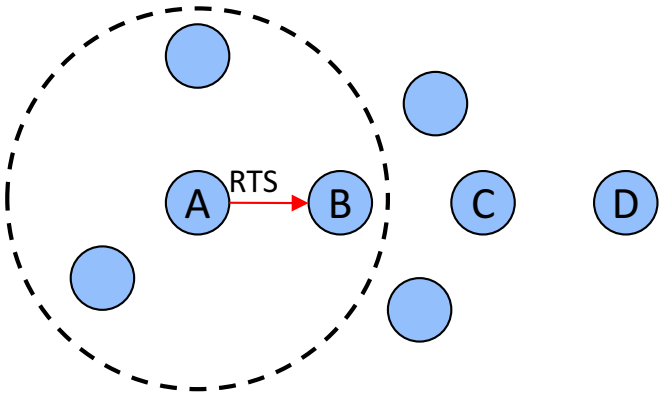
Hidden Station Problem

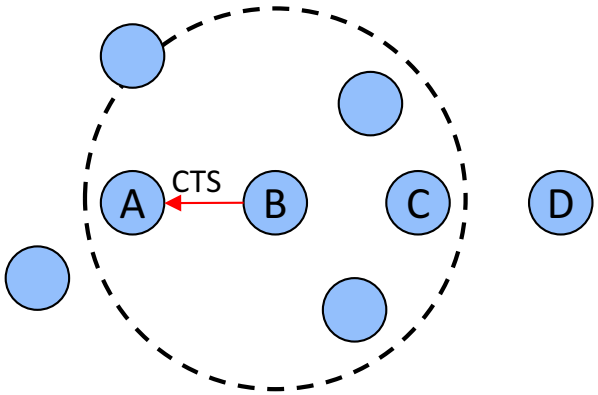


Exposed Station Problem

MAC for Wireless LANs

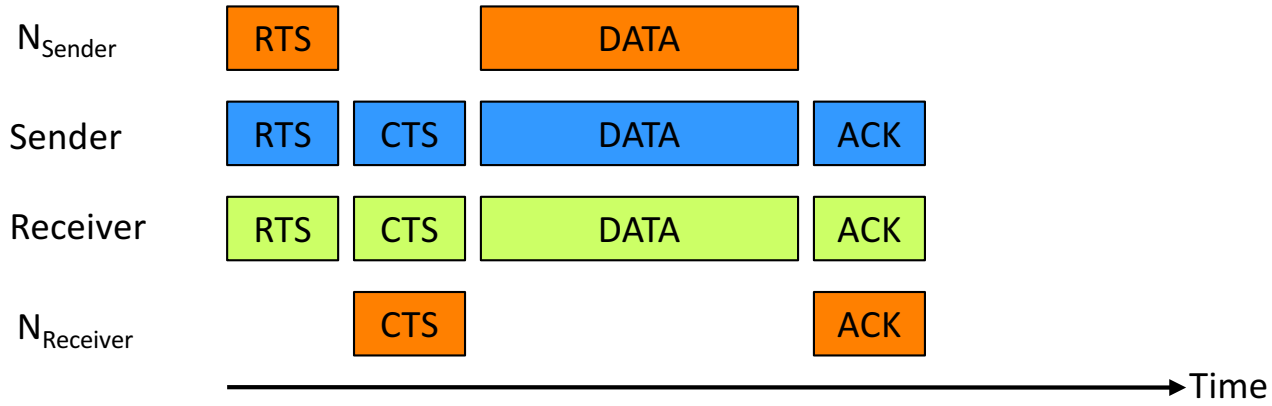
- **Multiple Access with Collision Avoidance (MACA)**
  - Idea: Inform stations in the neighborhood about the transmission
  - Ready To Send (RTS)
    - Informs the neighbors of the sender
  - Clear To Send (CTS)
    - Informs the neighbors of the receiver
  - Collision can occur, e.g., A and C could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

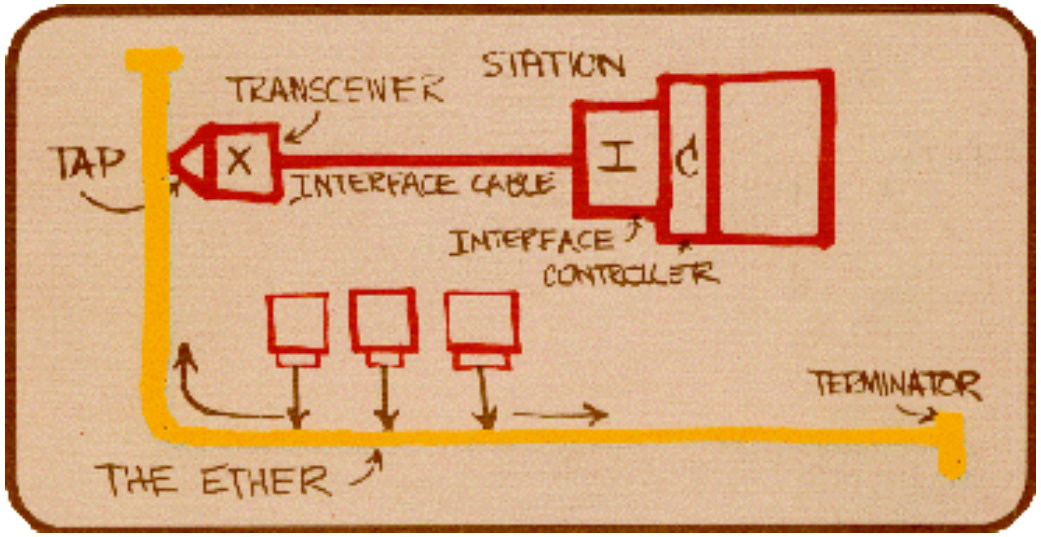
Ethernet

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 poor under heavy load
- **1970's: experimental network based on 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 millions of Ethernet adapters
- **Original Ethernet structure:**
  - **Bus topology** with a maximum segment length of 500 meters, connection of a maximum of 100 stations.
  - **Repeaters** are used to connect several segments.

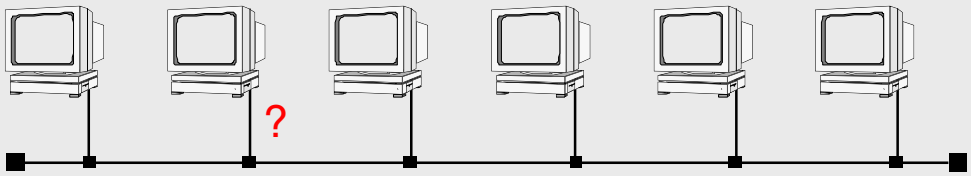


- **Most common medium: Copper cable.**
  - In addition, optical fibers are used (the segment length increases).
- **Early 90's: the bus topology is displaced more and more by a star topology, in which a central hub or switch (based on Twisted Pair or Optical Fiber) realizes connections to all stations.**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

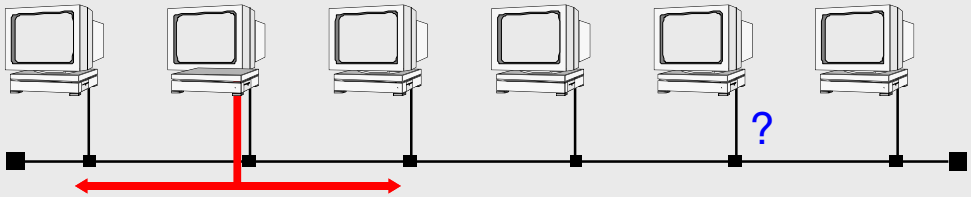
Ethernet

- 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)

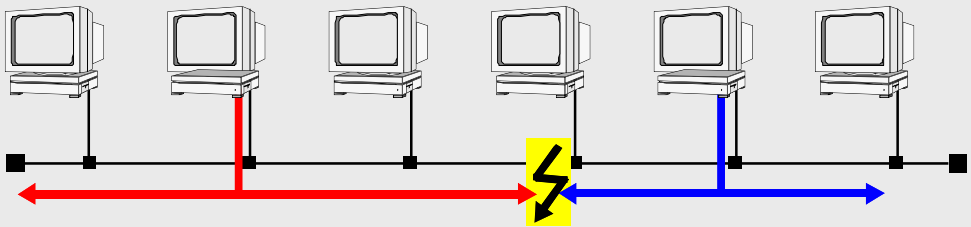


2. Data transmission



3. Check for collisions
   (Collision Detection)

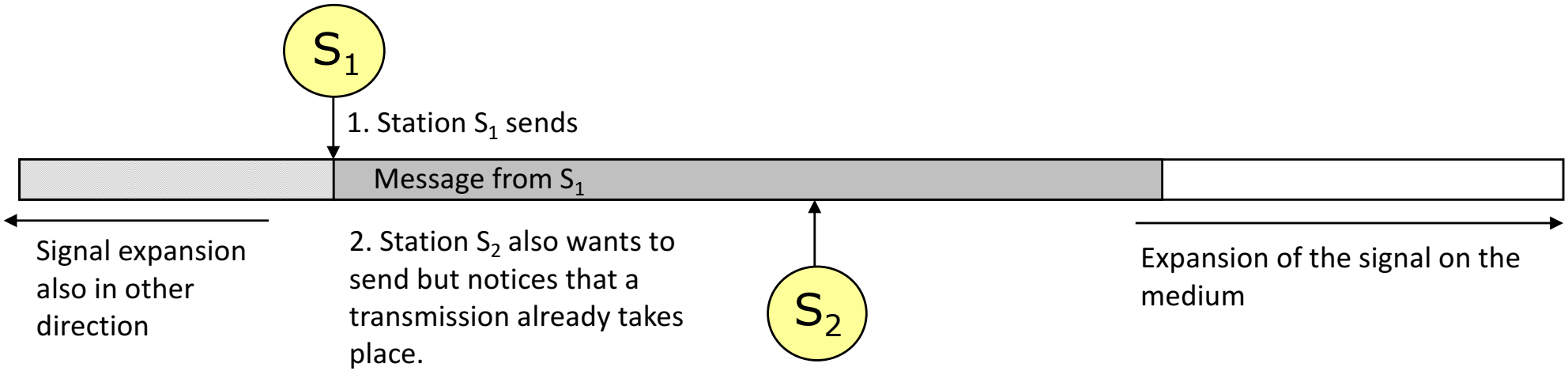
   If so: send jamming signal and stop transmission.
   Go on with binary exponential backoff algorithm



Carrier Sense Multiple Access

Principle:

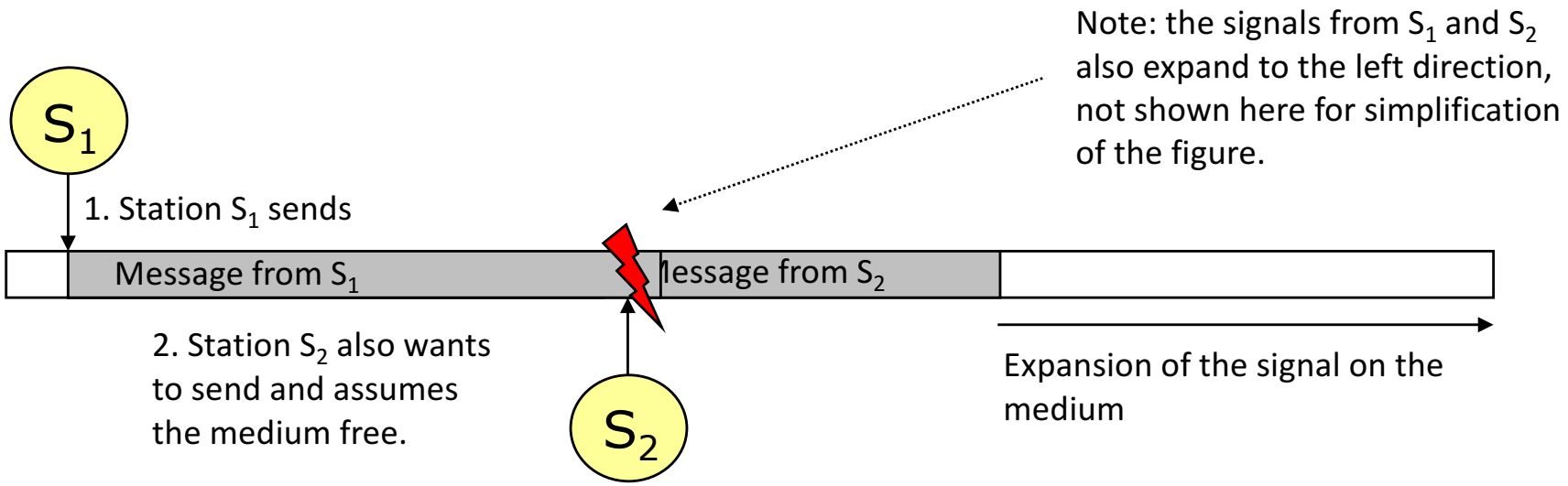
- listen to the medium before sending
- send only if the medium is free



- Advantages
  - simple, since no coordination mechanisms required
  - with extensions a good utilization of the network capacity
- Disadvantage: no guaranteed access, a large delay before sending is possible

Problem with CSMA

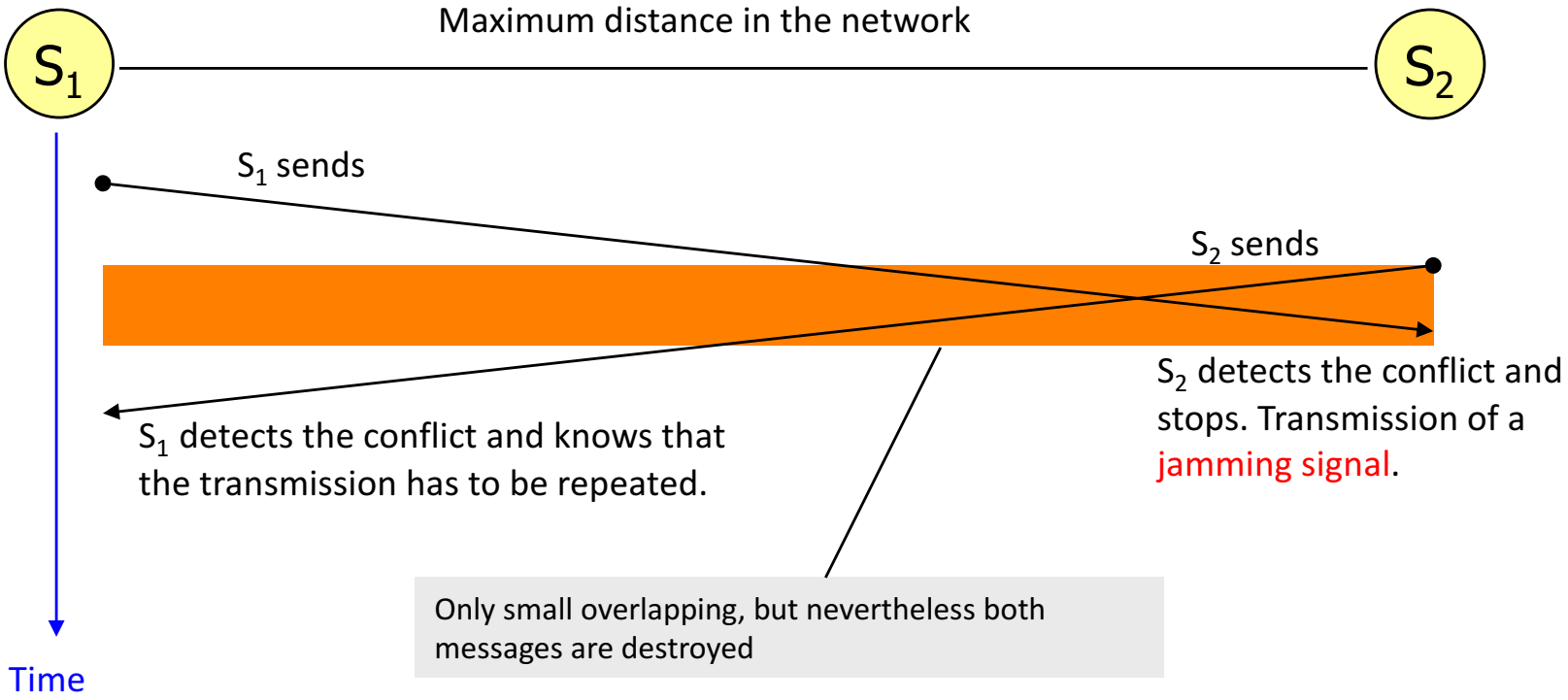
Problem: the message which is sent by S_1 spreads with finite speed on the medium. Therefore, it can be that S_2 assumes that the medium would be free, although S_1 already has begun with the transmission. It comes to a collision: both messages overlap on the medium and become useless.



Detection of Collisions

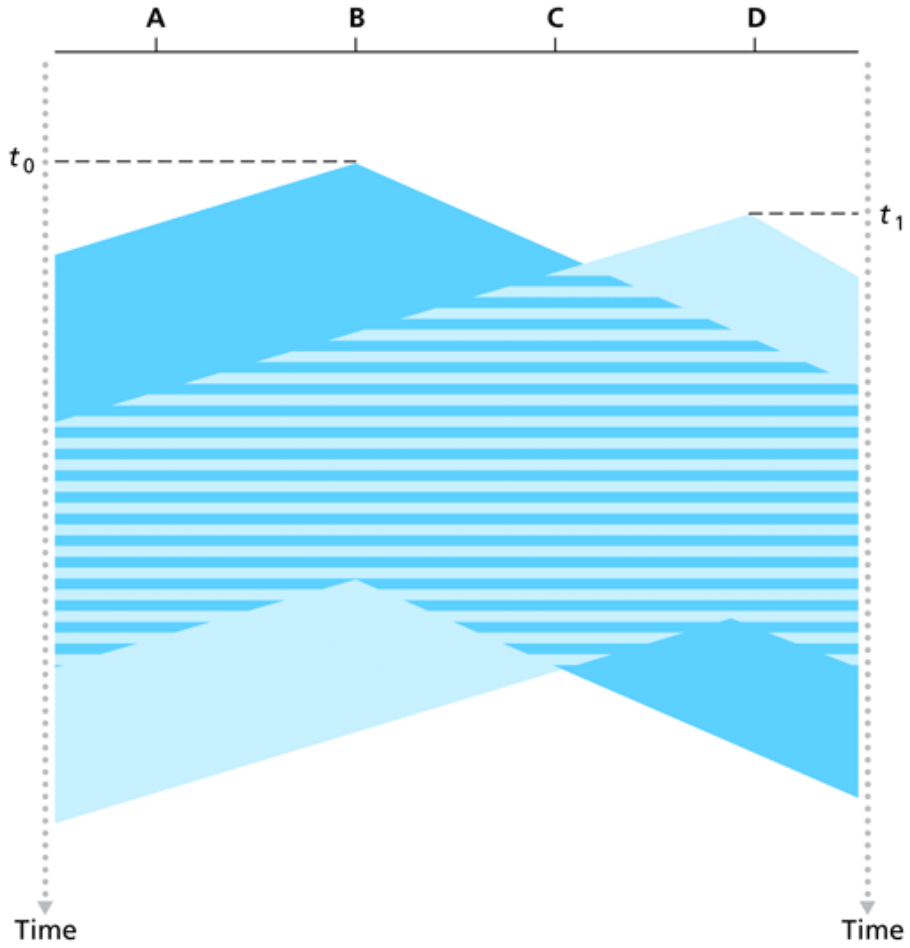
Carrier Sense Multiple Access with Collision Detection (**CSMA/CD**)

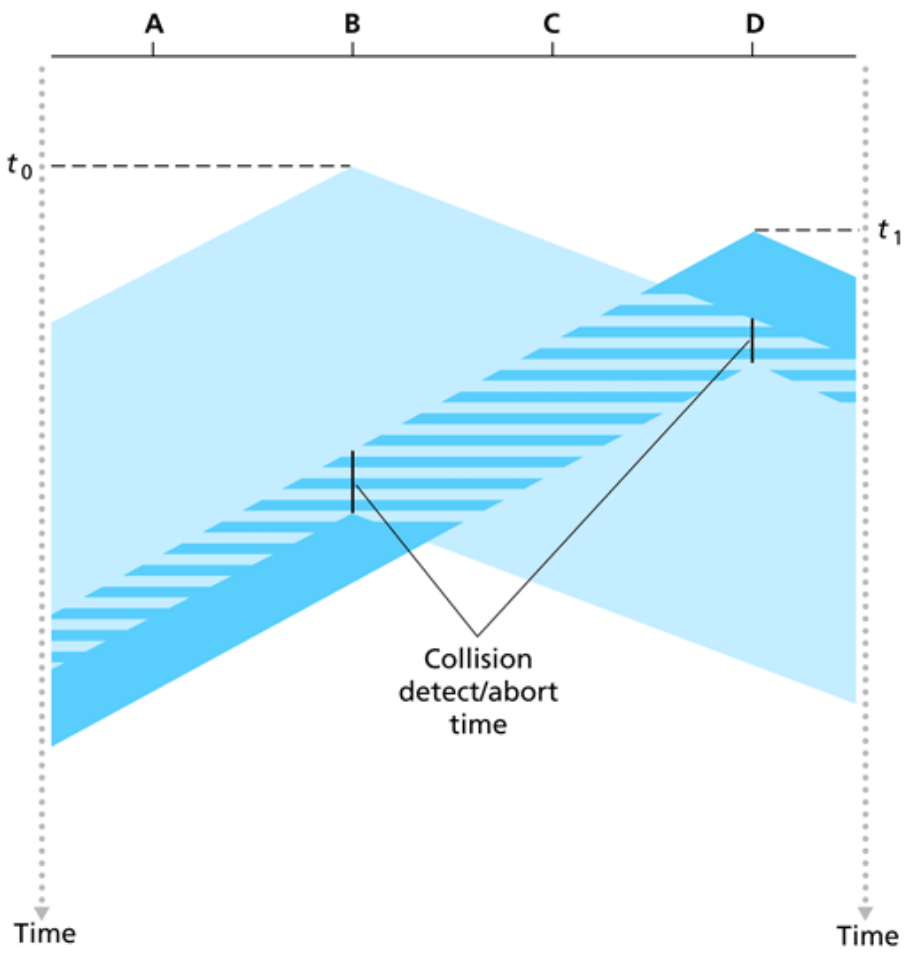
- Principle:
  - like CSMA
  - additionally: stop the transmission if a collision occurs



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



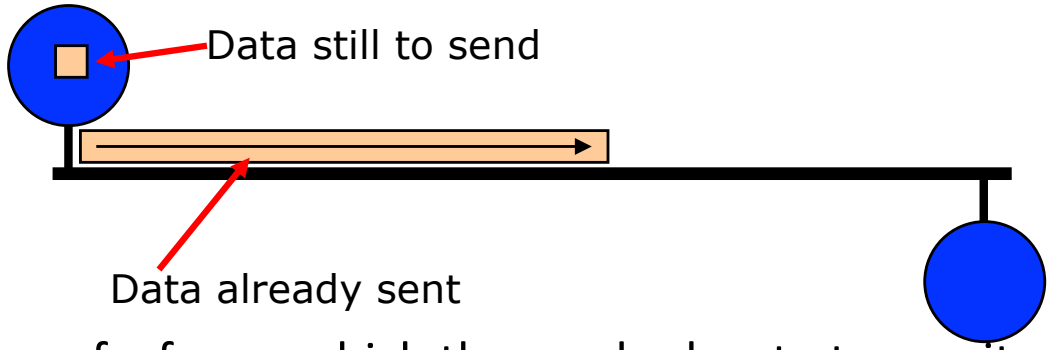


Data transmission with CSMA/CD

- **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 …
    - ➢ 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:**

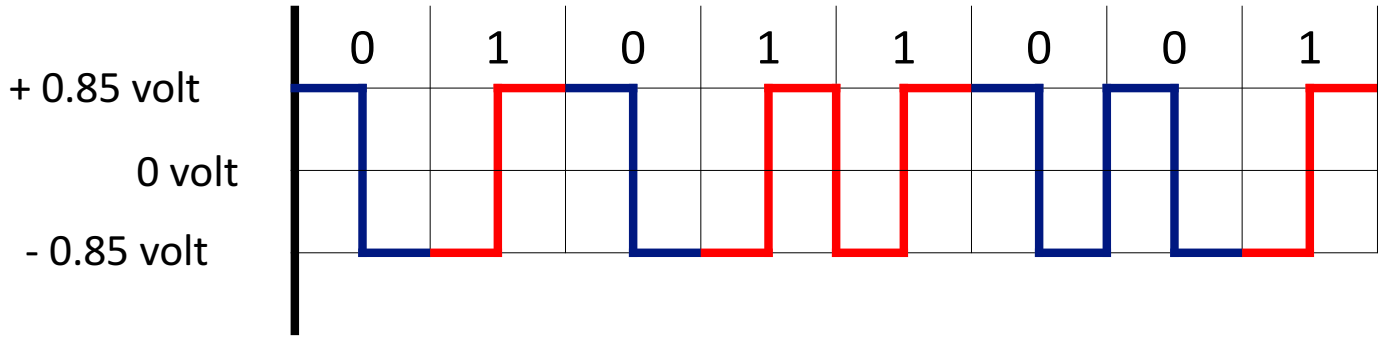


  - α is the fraction of a frame which the sender has to transmit until the first bit crosses the whole network
  - If someone begins to send during the time α, a conflict arises
  - The smaller α is, the better is the performance of the network
  - α is small …
    - when the network is small
    - when frames are large
    - when capacity is low

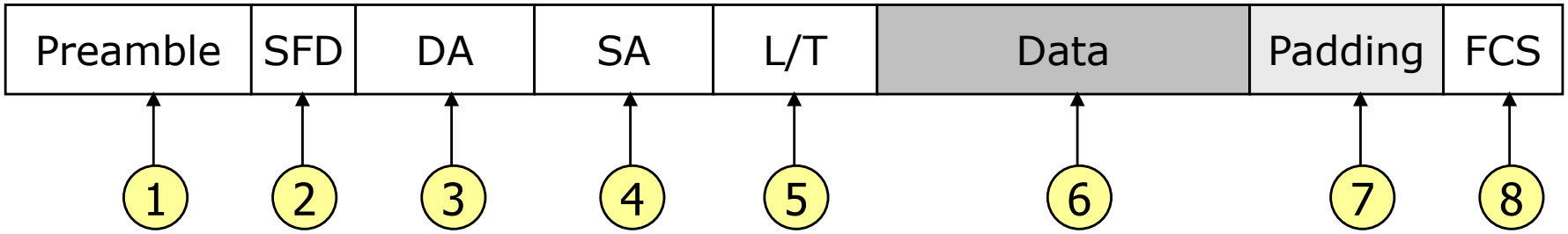
➢ Conclusion: the best network has nearly zero size, nearly zero capacity, and a station should never stop sending.

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 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 (0 – 1500) byte data

7: ≥ 0 (0 – 46) byte padding

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

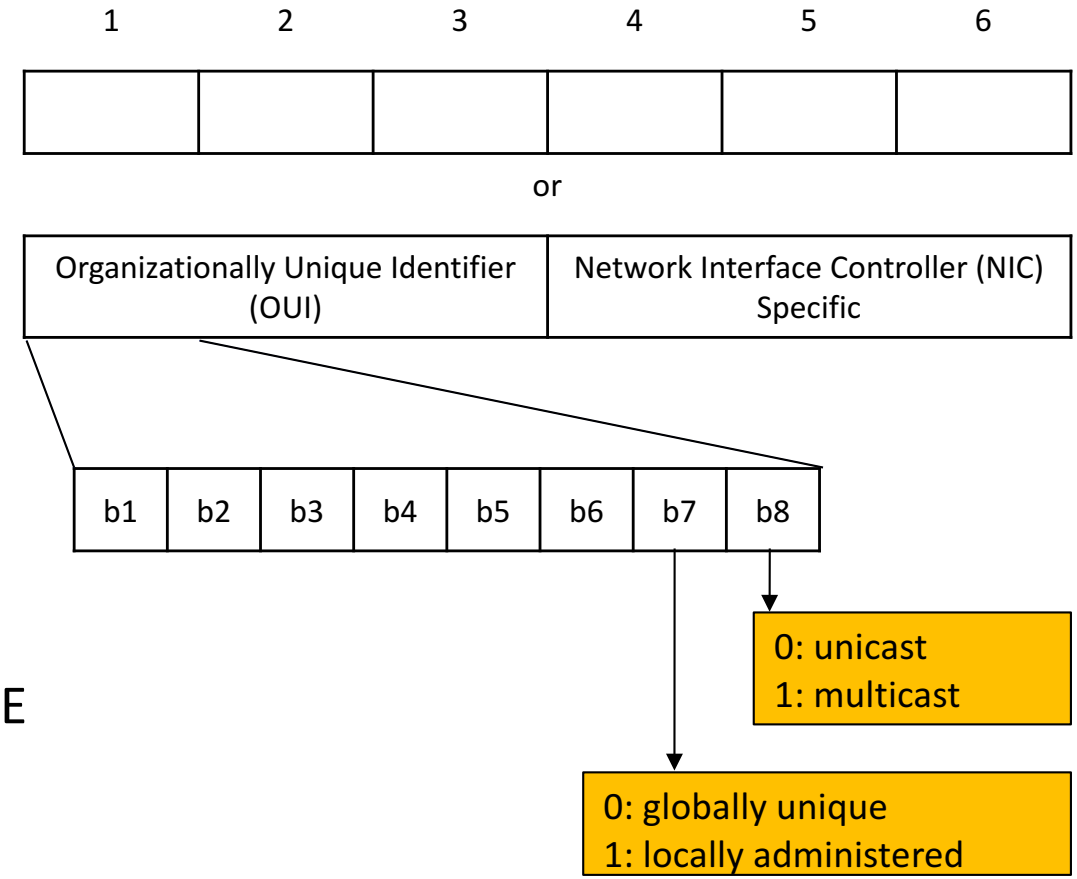
8: 4 byte Frame Check Sequence (FCS, checksum).
Use of a cyclic code (CRC).

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): One field to purposes ...**
  - IEEE 802.3: a value ≤ 1500 indicates the length of the following data part.
  - Ethernet: identification of 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.**

The Ethernet Frame: Addresses

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

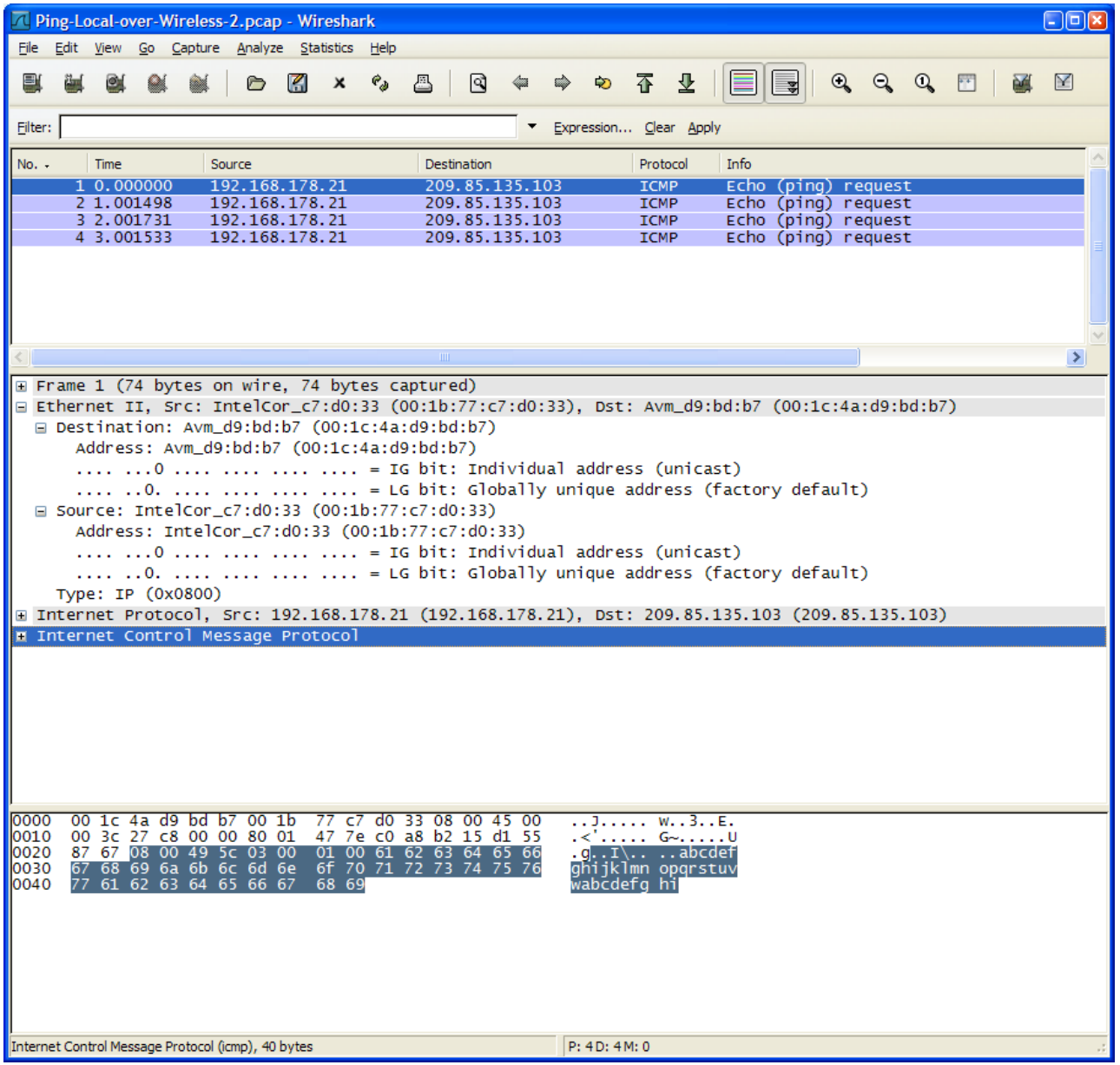


- **Administrative**
  - Globally unique, assigned by IEEE
  - Locally administered

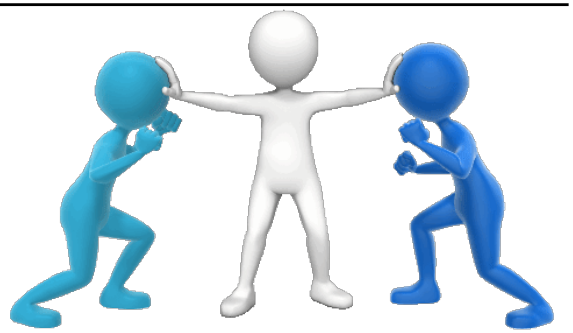
- **Tools**
  - Windows: `getmac, ipconfig /all, arp -a`
  - Linux: `ifconfig, cat /proc/net/arp`

The Ethernet Frame: Network Analyzer

Wireshark ➙ http://www.wireshark.org/



Resolving Transmission Conflicts



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

- **Non-persistent (example ALOHA)**
  - After a conflict, wait with a random waiting period chosen from a given interval until starting 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

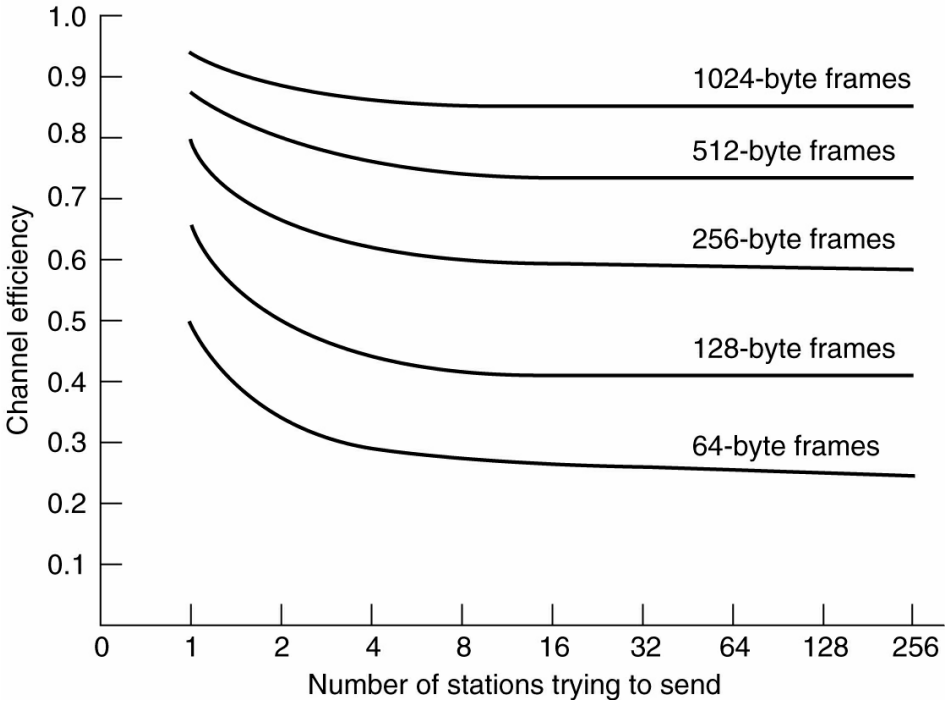
- ***p*-persistence**
  - In this variant conflicts between concurrently waiting messages should be avoided
  - In a free channel transmission takes place only with probability p
  - In case of a conflict, a message needs on the average $1/p$ attempts

- **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

Performance of Ethernet

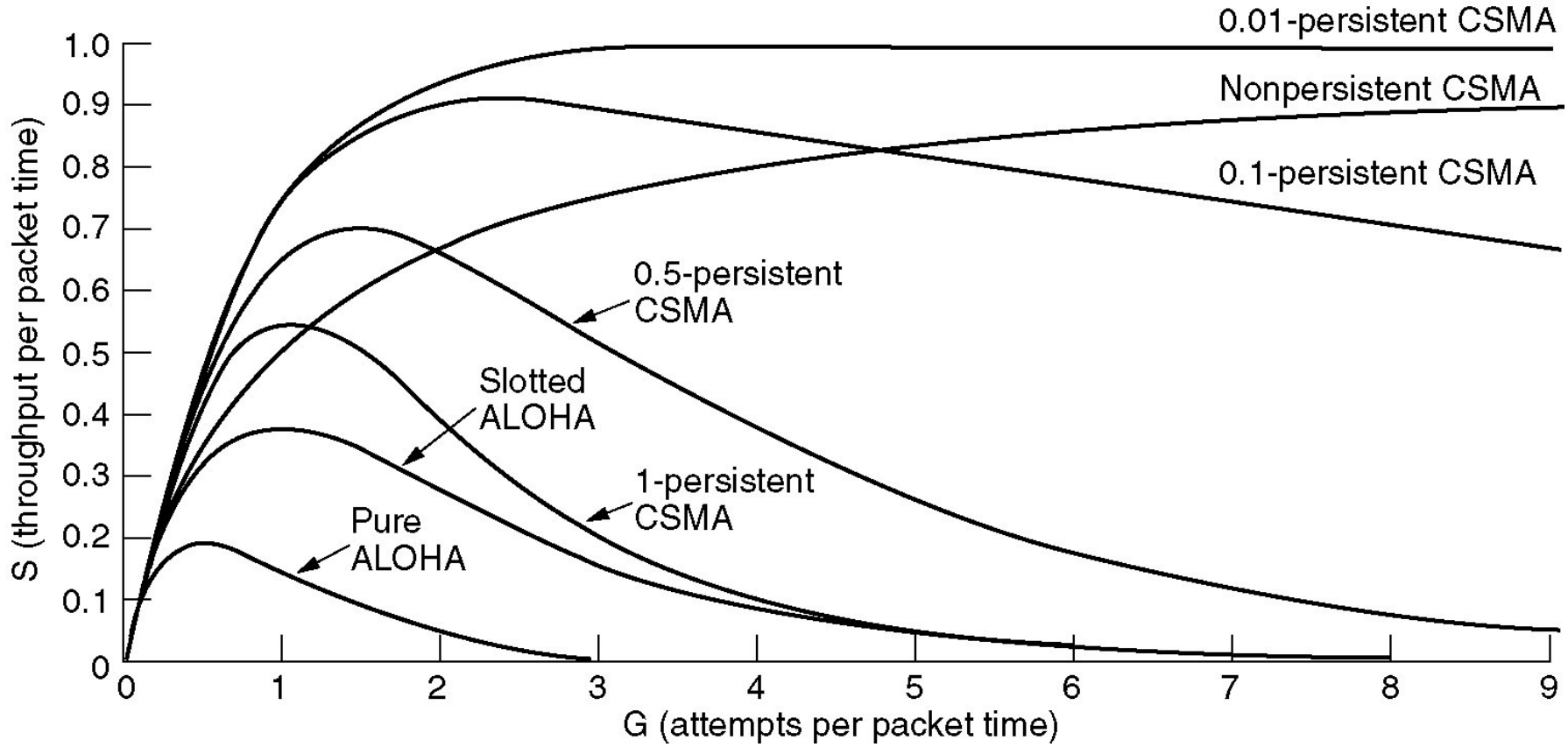
- **Ethernet at 10 Mbps with 512-bit slot times**
- **Assumptions**
  - T Time to transmit a frame
  - τ Propagation on cable
  - A Probability that a station gets the channel

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



Performance of Ethernet

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



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

Resolving Collisions in Ethernet

- **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 selects a random number x in the interval $[0, 2^i-1]$
  - After 10 collisions, the interval remains fixed with $[0, 2^{10}-1]$
  - 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 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.

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

Based on IEEE 802.3 “CSMA/CD”

4 classes of Ethernet variants:

- Standard Ethernet ➡ 10 Mbps — Not really used anymore
- 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	up to 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, …
Maximum number of repeaters	5	2	1

Additionally, for the jamming a 4 byte pattern is sent.

Naming of Ethernet Variants

Indication of the used Ethernet variant by 3 name components:

1. Capacity in Mbps (10, 100, 1000, or 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, 2Twisted Pair cables (i.e. two cores)
- 1000Base-X: 1000 Mbps, baseband, optical fiber

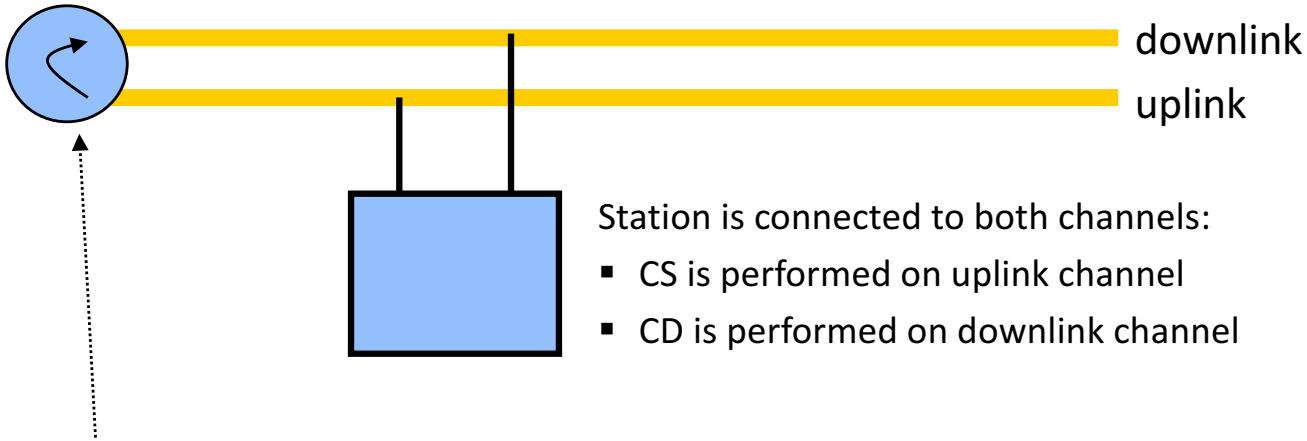
Some parameters depend on the variant, e.g., the minimum frame length (because of different signal propagation delay):

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

10Broad-36

Broadband Ethernet has an analogy to CATV (Cable TV)

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



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

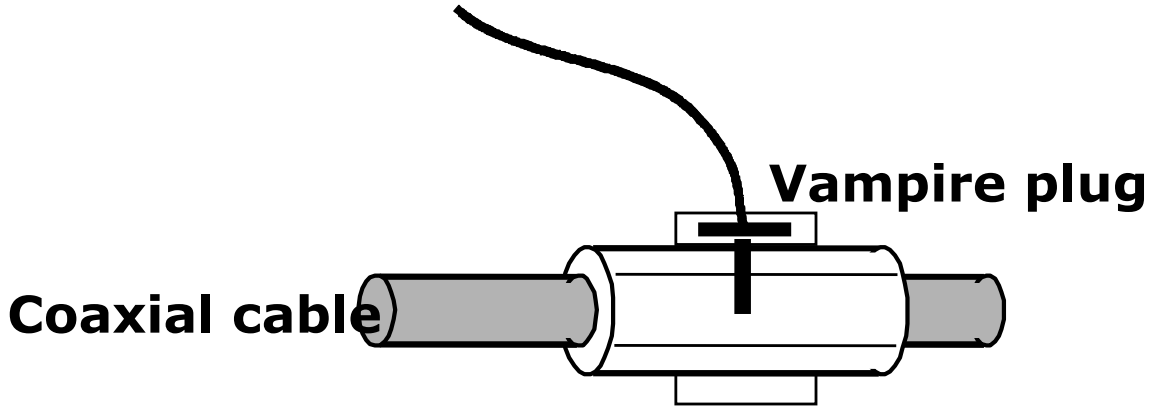
➡ makes broadband Ethernet too expensive

10Broad-36

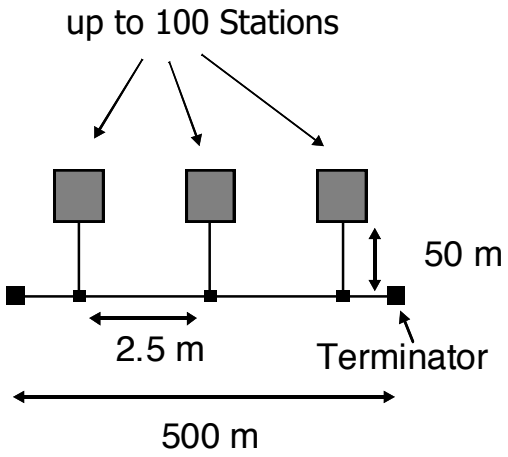
- Data rate of 10 Mbps
- Maximum segment length of 1800 meters (3600 meters is maximum range!)
- Uses CATV technology, mostly with bus topology, but also tree topology is possible (but then “carrier sense” is restricted; it is only possible if both stations are on the same branch of the tree)
- Up to 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

10Base-5 (Yellow Cable)

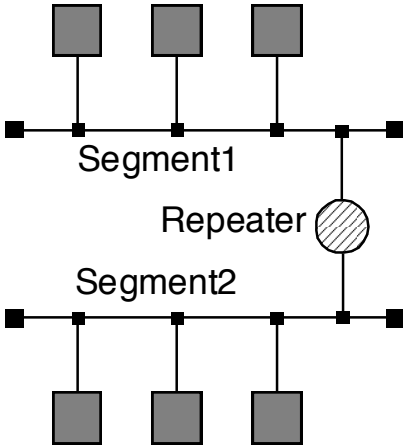
- **Uses classical coaxial cable (expensive, inflexible)**
  - Thick Ethernet, since cable looks like a yellow garden hose
- **Terminals are attached over transceivers (vampire plug)**
- **Max. 5 segments (connected by repeaters)**
- **Max. 100 stations per segment**
- **At least 2.5 m distance between 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**



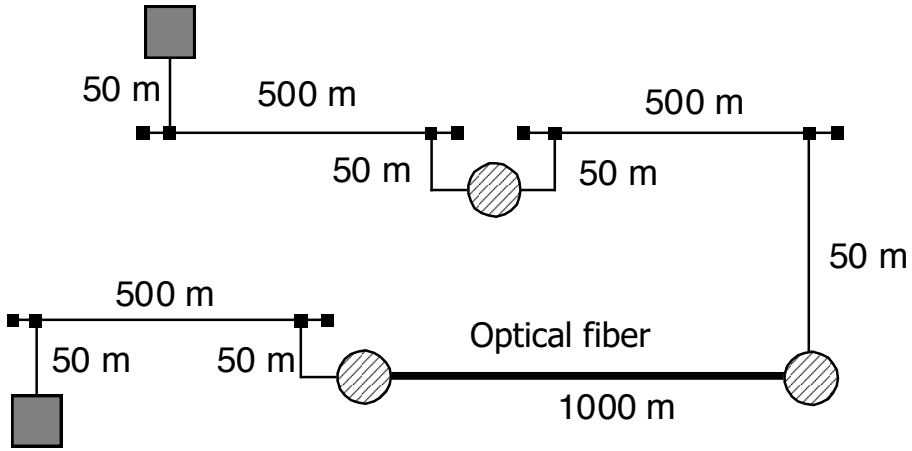
Ethernet: Configurations



Basic configuration: segment



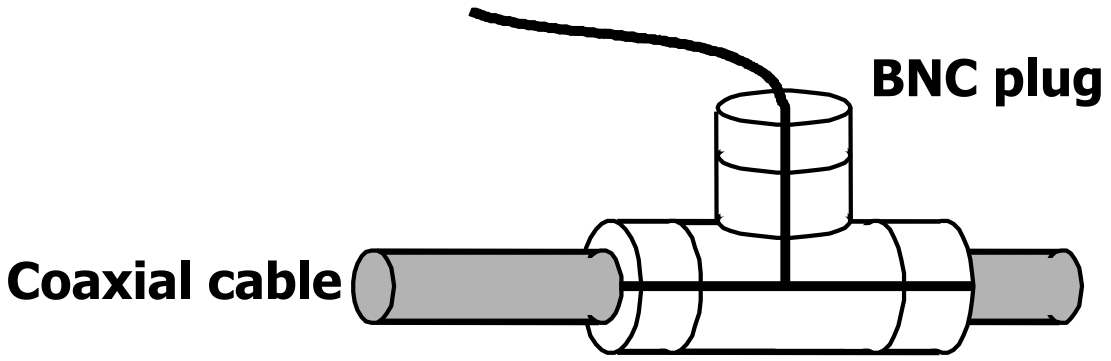
Connection of segments through a repeater



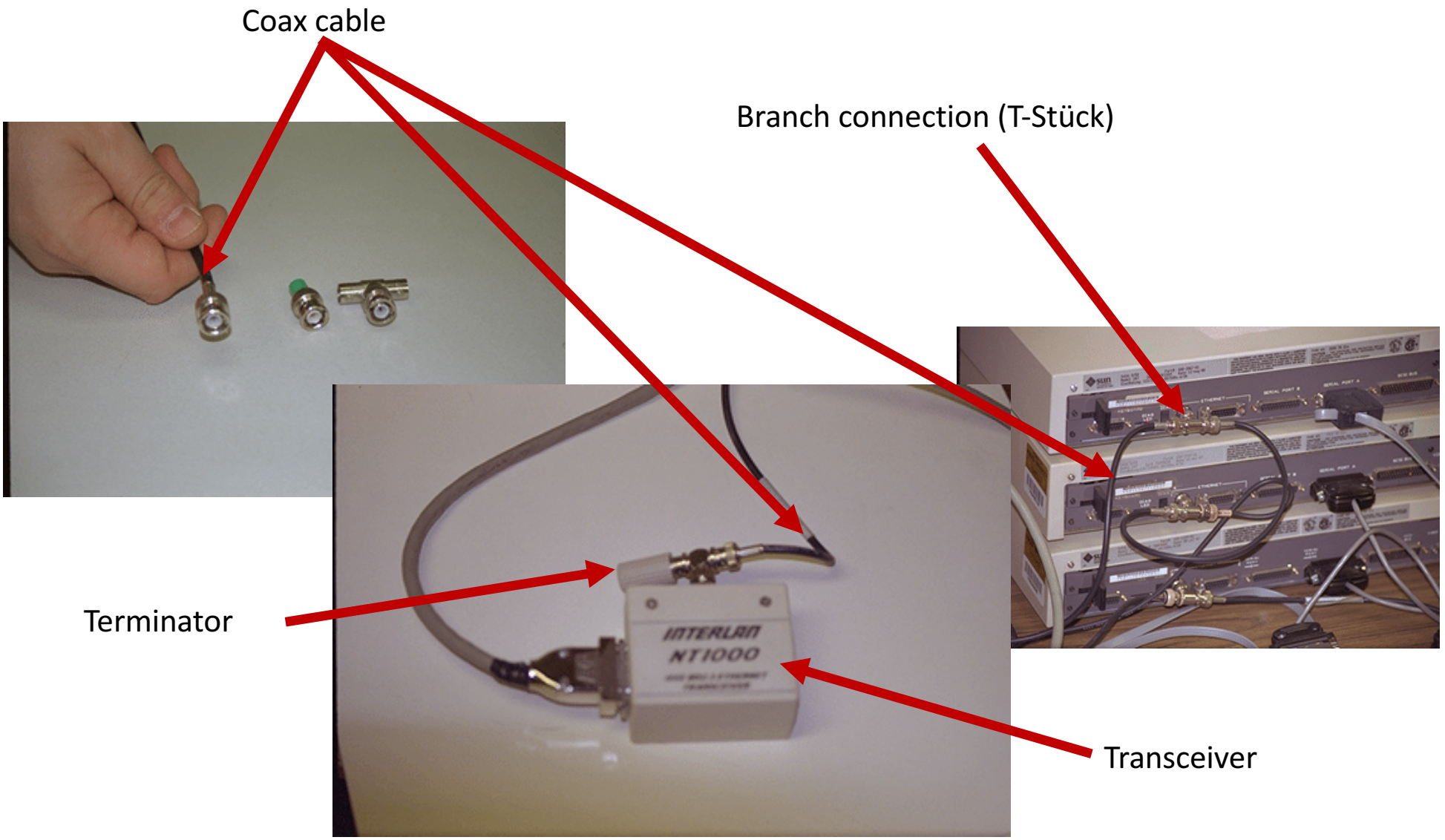
Ethernet with maximum range

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**

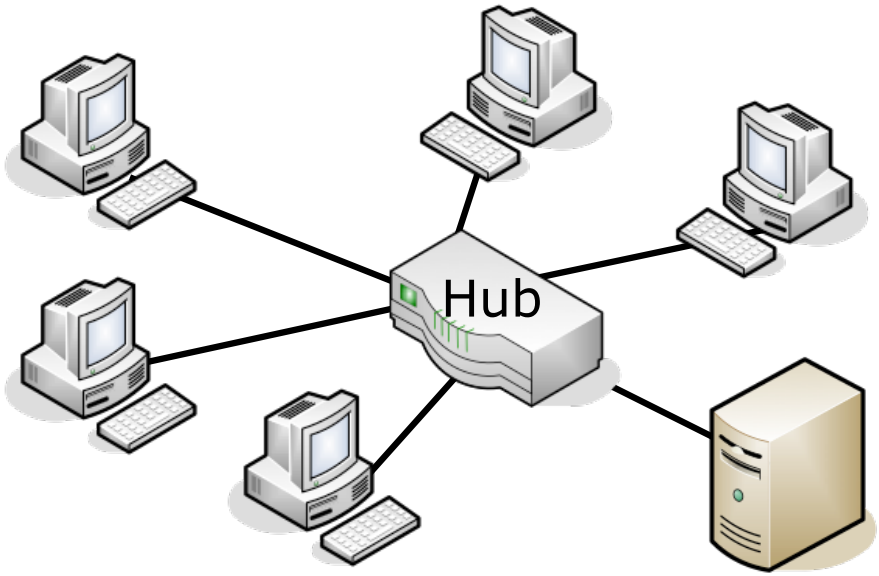


10Base-2 (Cheapernet)



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 within 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, …)**
- **Therefore, the expansion remained the same as for Fast Ethernet – instead a new minimal 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**
  - ‘Nodata’ is added and removed by the hardware, software 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.

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.**

- **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

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, …)

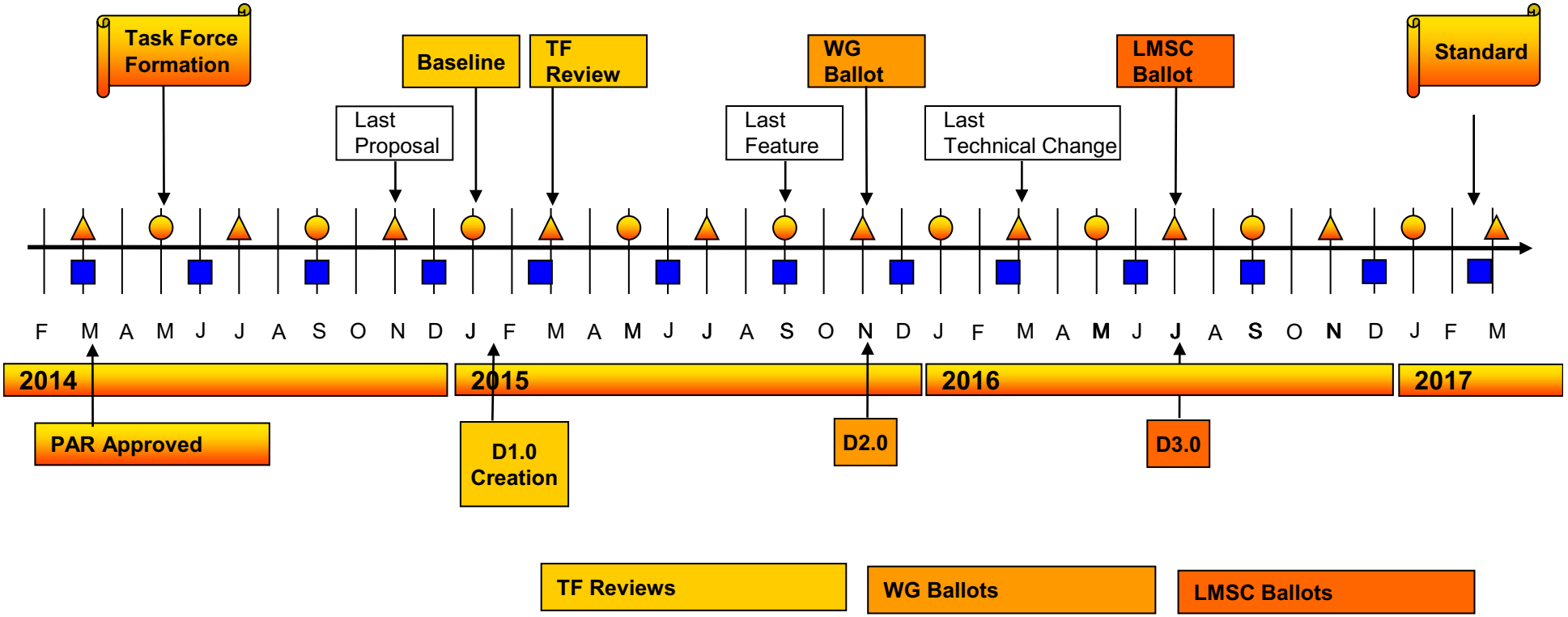
- **Maybe combined with full optical networks?**
  - Optical multiplexers, optical switches
  - But at the moment only tested in labs, expensive

- **100G-Ethernet**
  - Data rates from 40G to 100G
  - Variants for 100 m and 10 km with duplex communication

And what's next?

http://www.ieee802.org/3/bs/timeline_3bs_0514.pdf

IEEE P802.3bs 400GbE Adopted Timeline



Adopted by IEEE P802.3bs 400GbE Task Force, May 2014 Interim.

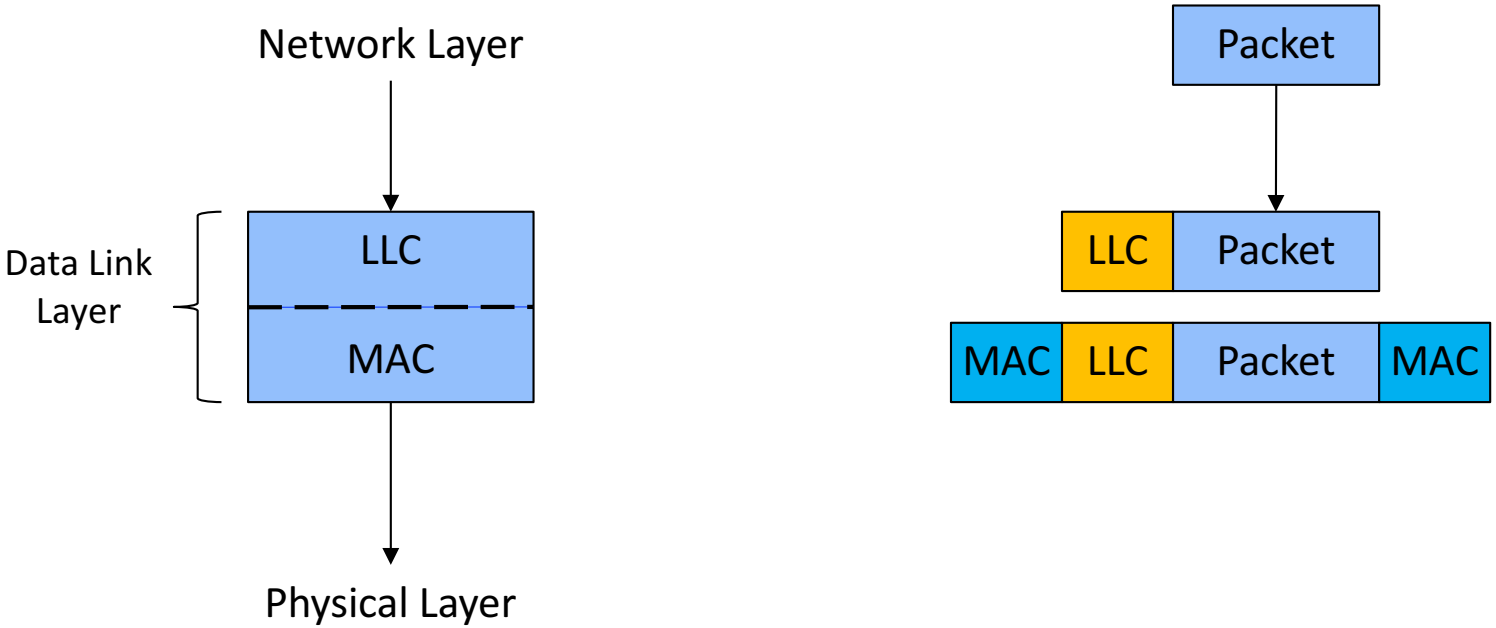
IEEE 802.2 – Logical Link Control

IEEE 802.2: Logical Link Control

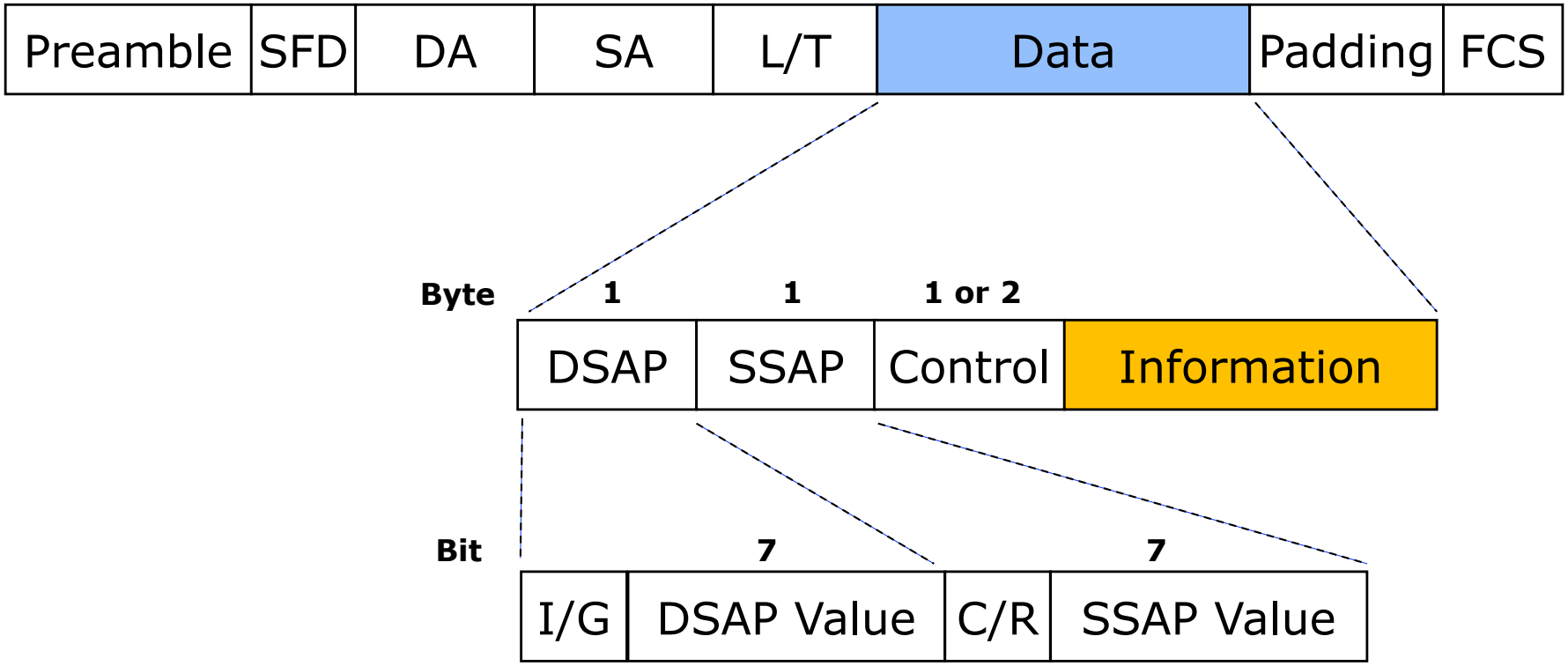
- **Ethernet and IEEE 802.3 protocols offer only best effort**
  - Unreliable datagram service (No acks)
  - What to do if error-control and flow-control is required?
- **Logical Link Control (LLC)**
  - Runs on top of Ethernet and other IEEE 802.3 protocols
  - Provides a single frame format and interface 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

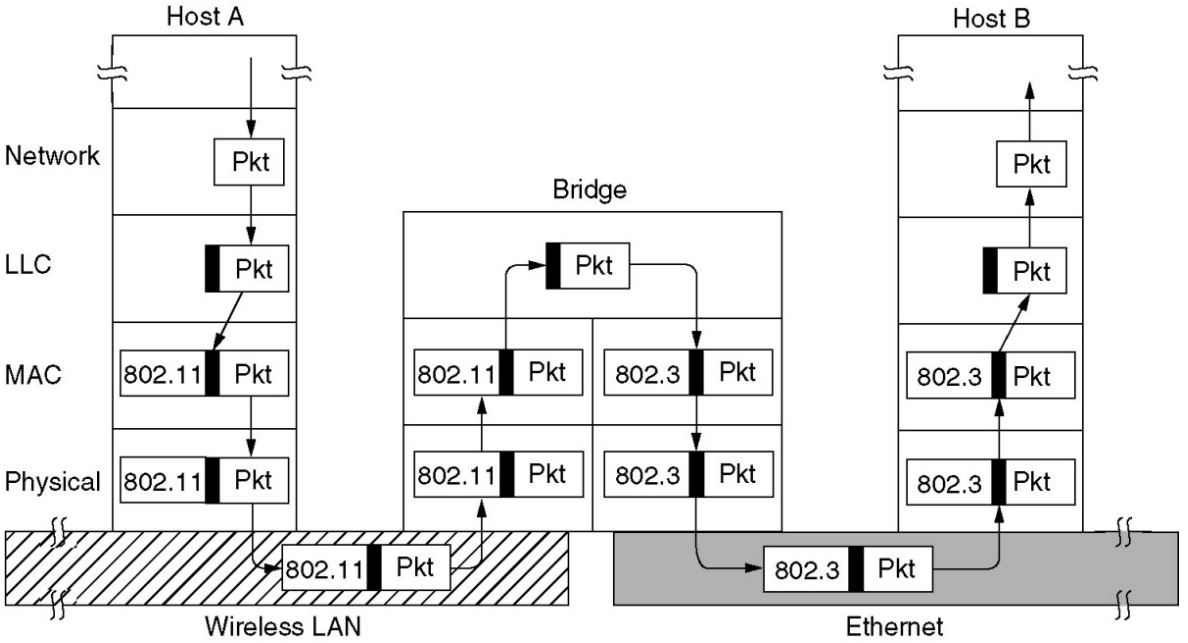
Network Infrastructure

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

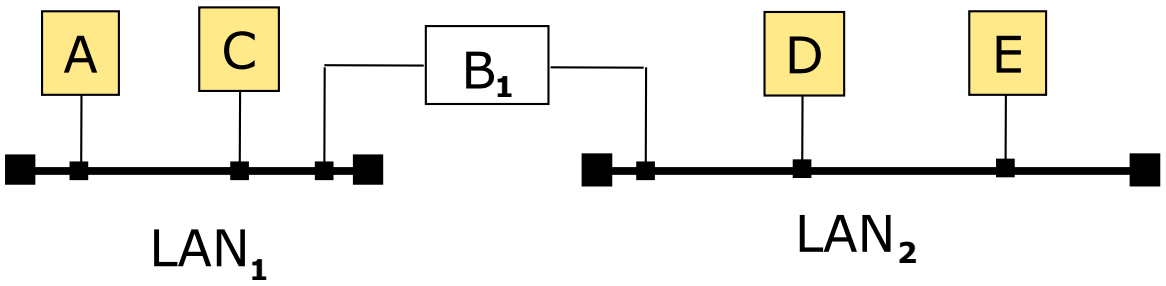
- **Bridges from 802.x to 802.y**



- **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

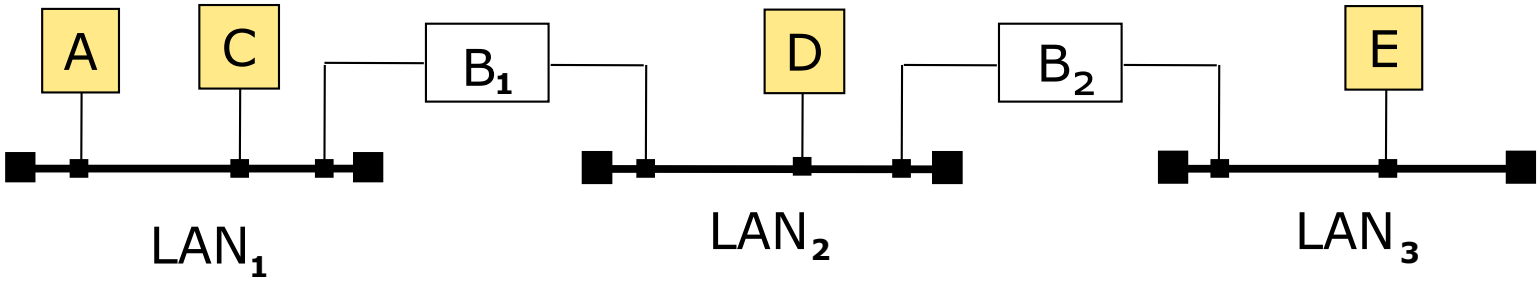
Infrastructure Components: Bridges

- **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

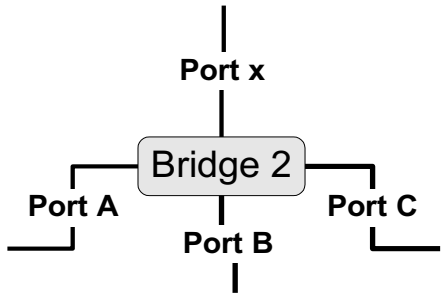
- **Transparent bridges (e.g. for CSMA and Token Bus networks)**



- **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

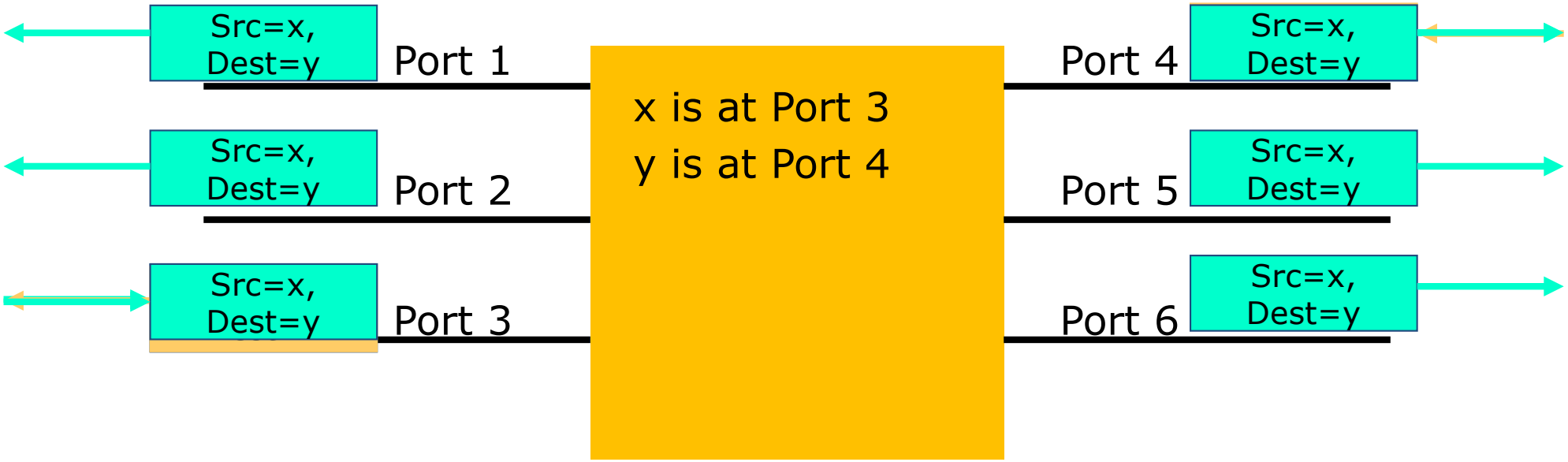
Transparent Bridges

- To realize transparency, bridges have to learn the location of hosts
- 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:



Transparent Bridges: Address Learning

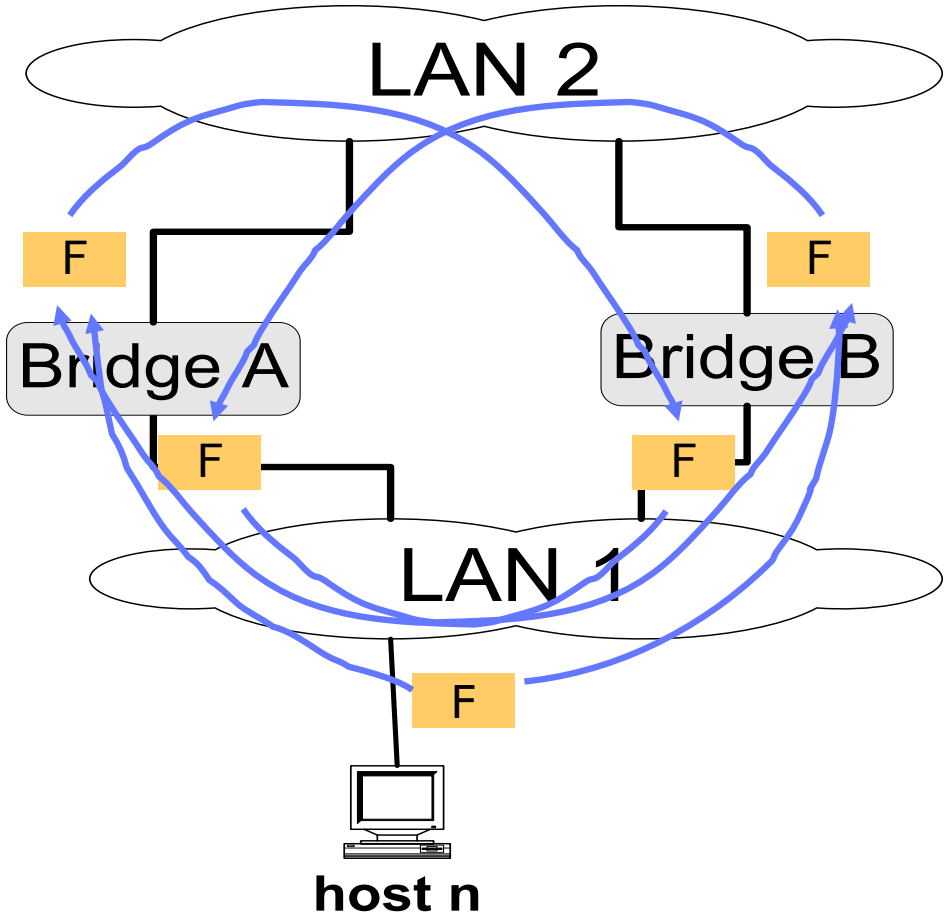
- **Database entries are set automatically with a simple heuristic**
  - the source field of a frame that arrives on a port tells which hosts are reachable from this port.
- **Algorithm:**
  - For each frame received, the source stores the source field in the forwarding database together with the port 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

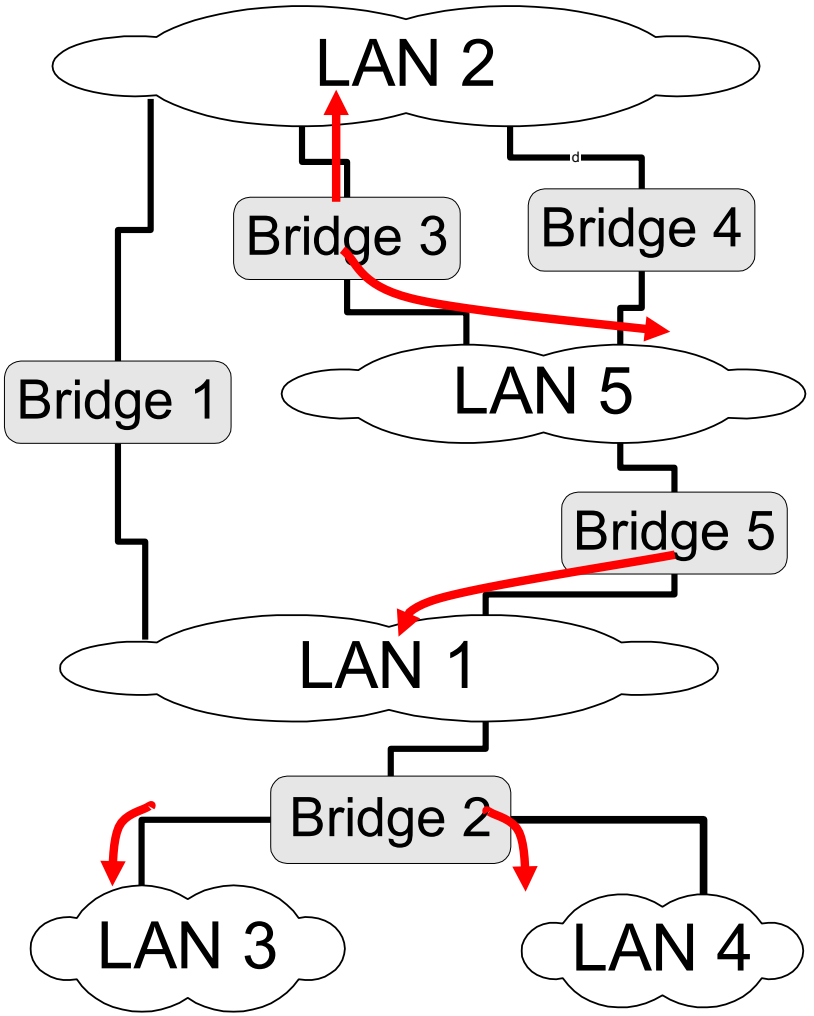
➢ Solution: Spanning Tree Algorithm



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:**

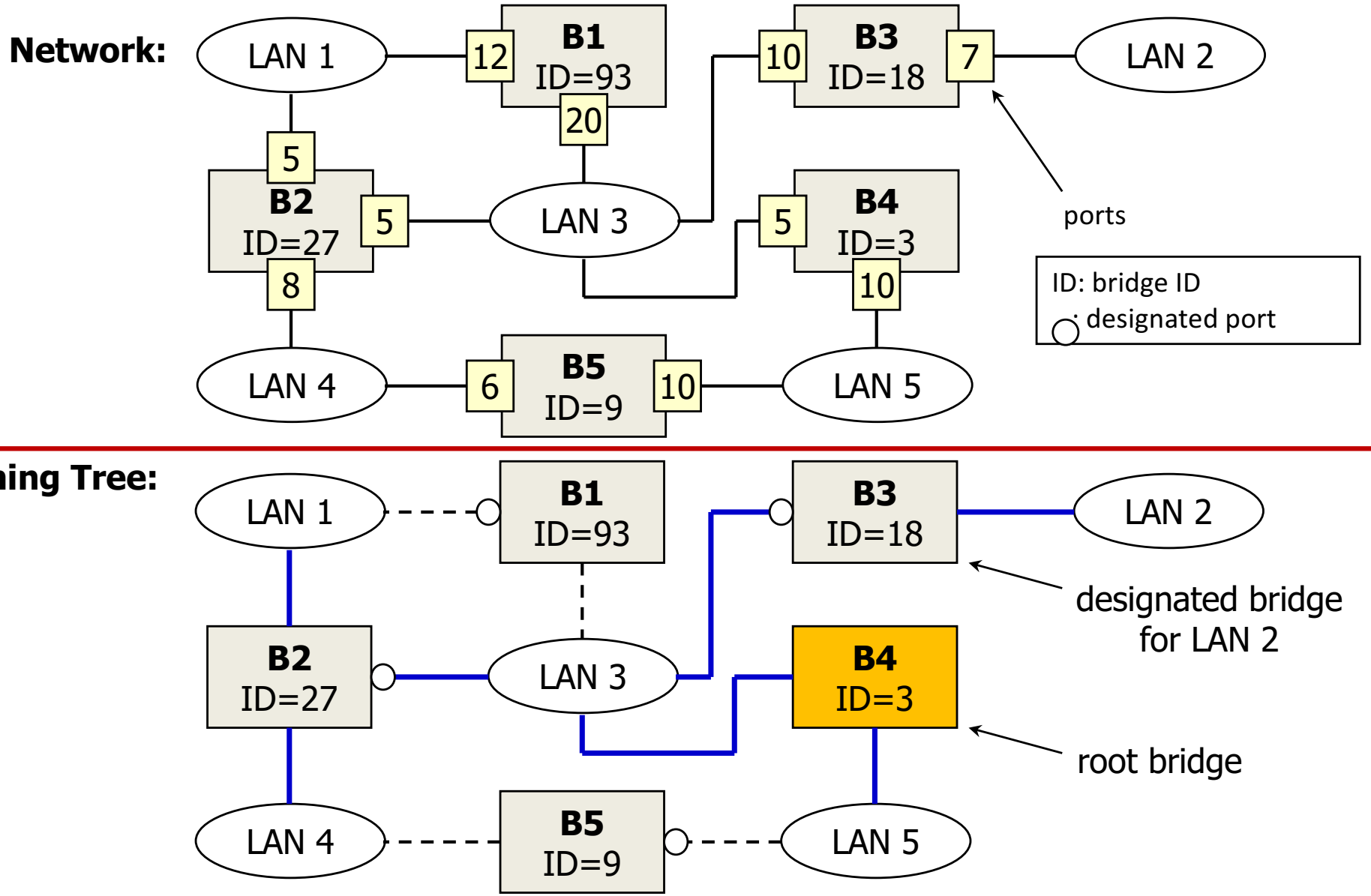
root ID	costs	bridge ID	port ID

e.g. for station B on port P_1:

B	0	B	P_1

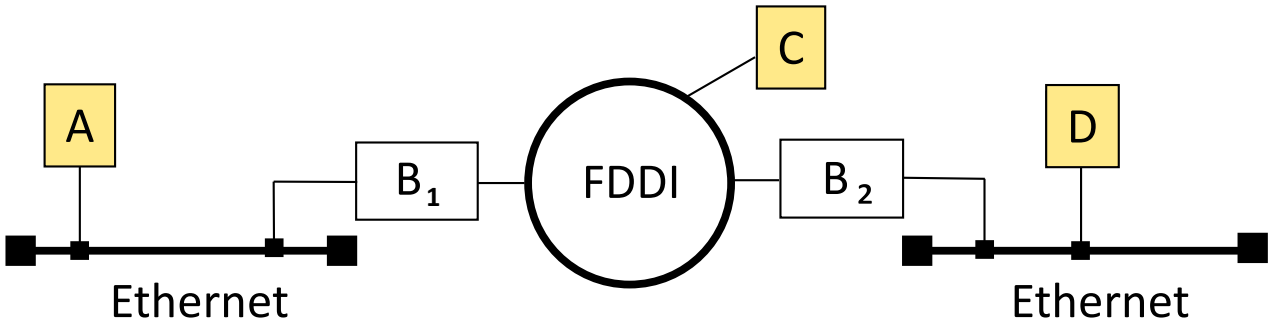
  - A bridge receiving such a packet checks the root ID and compares it with its own one. Root ID and costs are updated for received packets with smaller ID in the root bridge field and forwarded. Updating the costs is made by adding the own costs for the station from which the packet was received to the 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



Infrastructure Components: Bridges

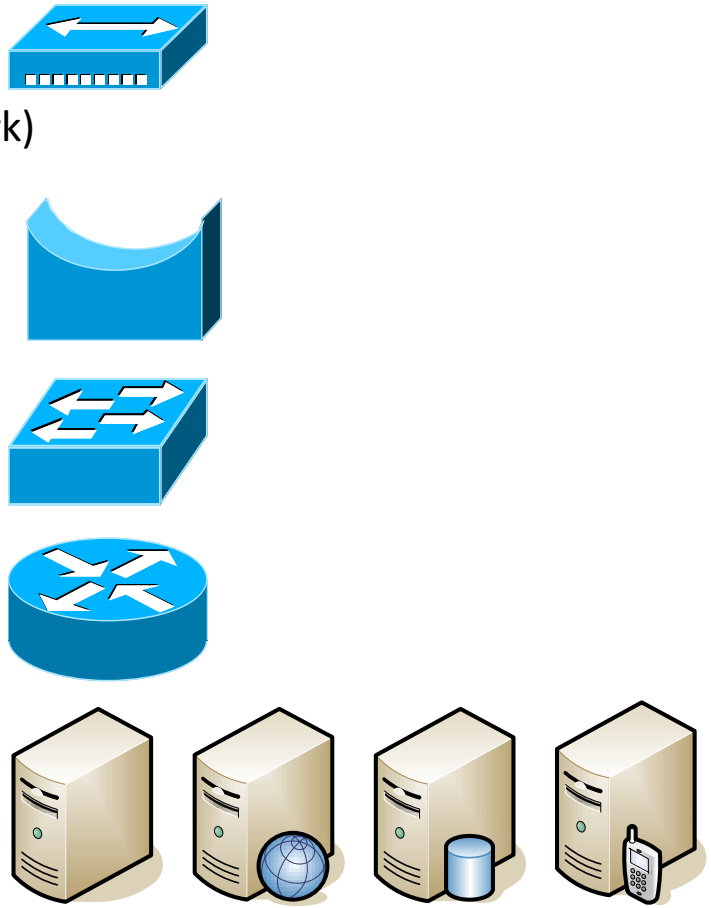
- **Source Routing Bridges (e.g. for ring networks)**



- **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

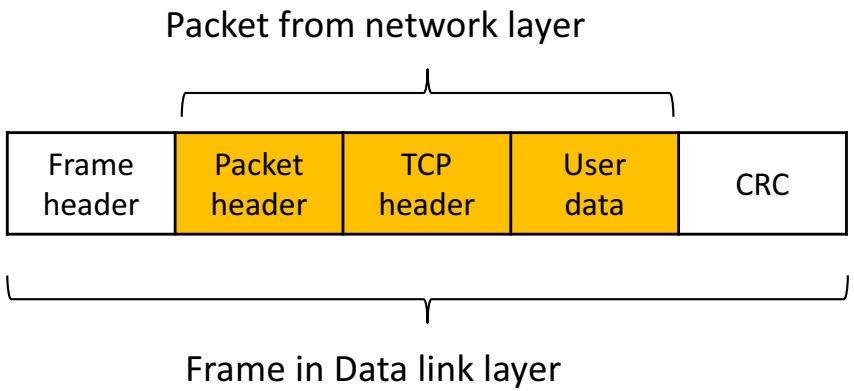
Network Infrastructure

- **For building computer networks network devices 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
    - Understand two different technologies and can convert the contents from one to the other and vice versa



Network Infrastructure

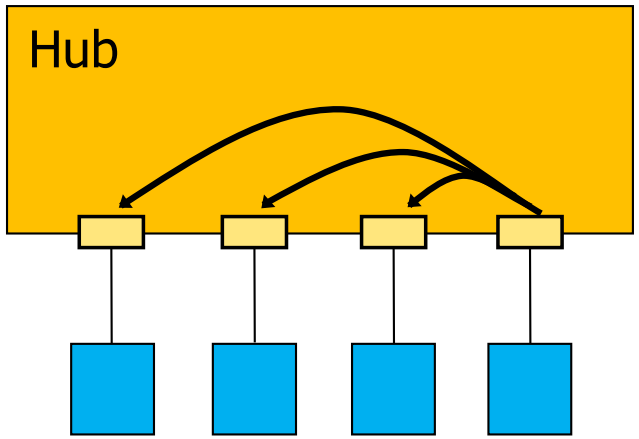
Application layer	Application gateway
Transport layer	Transport gateway
Network layer	Router
Data link layer	Bridge, Switch
Physical layer	Repeater, Hub



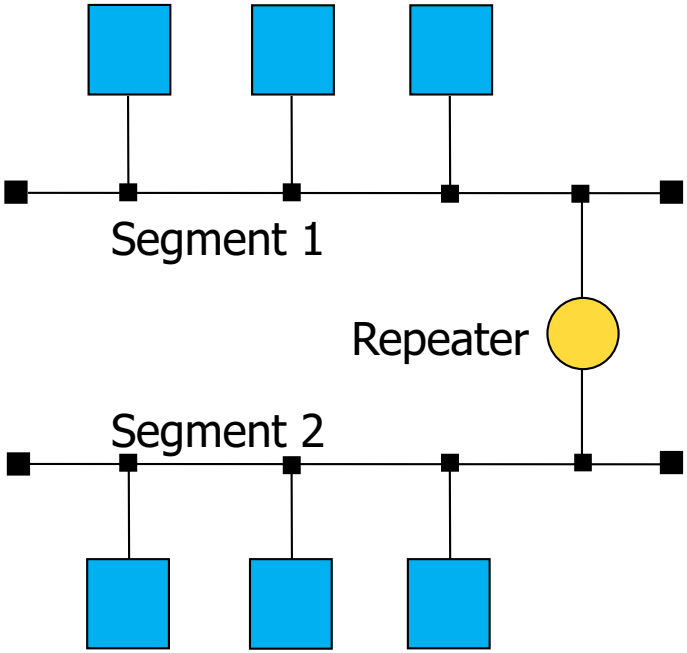
Infrastructure Components: Hub & Repeater

Layer 1

- **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**

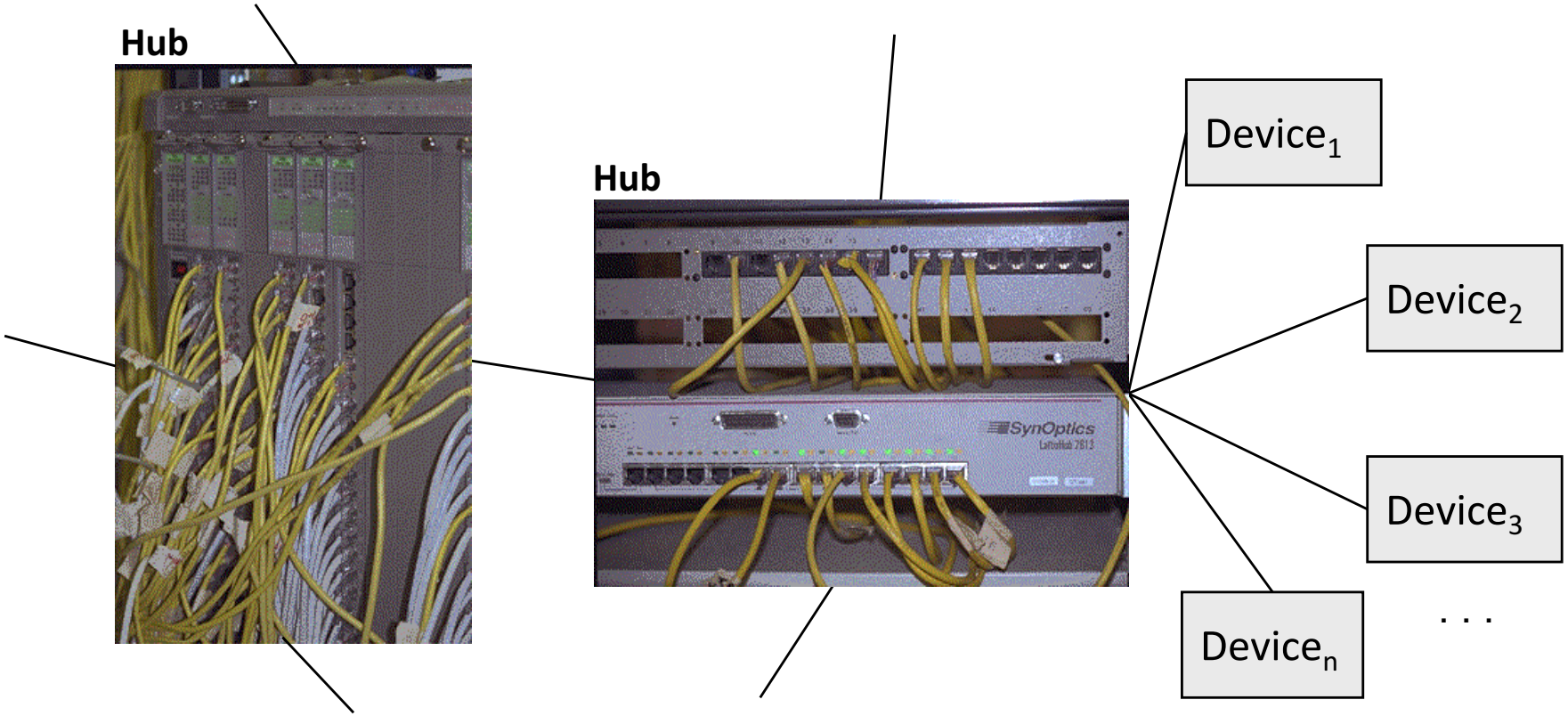


Hub: "one to all"



Repeater: Linking of 2 networks

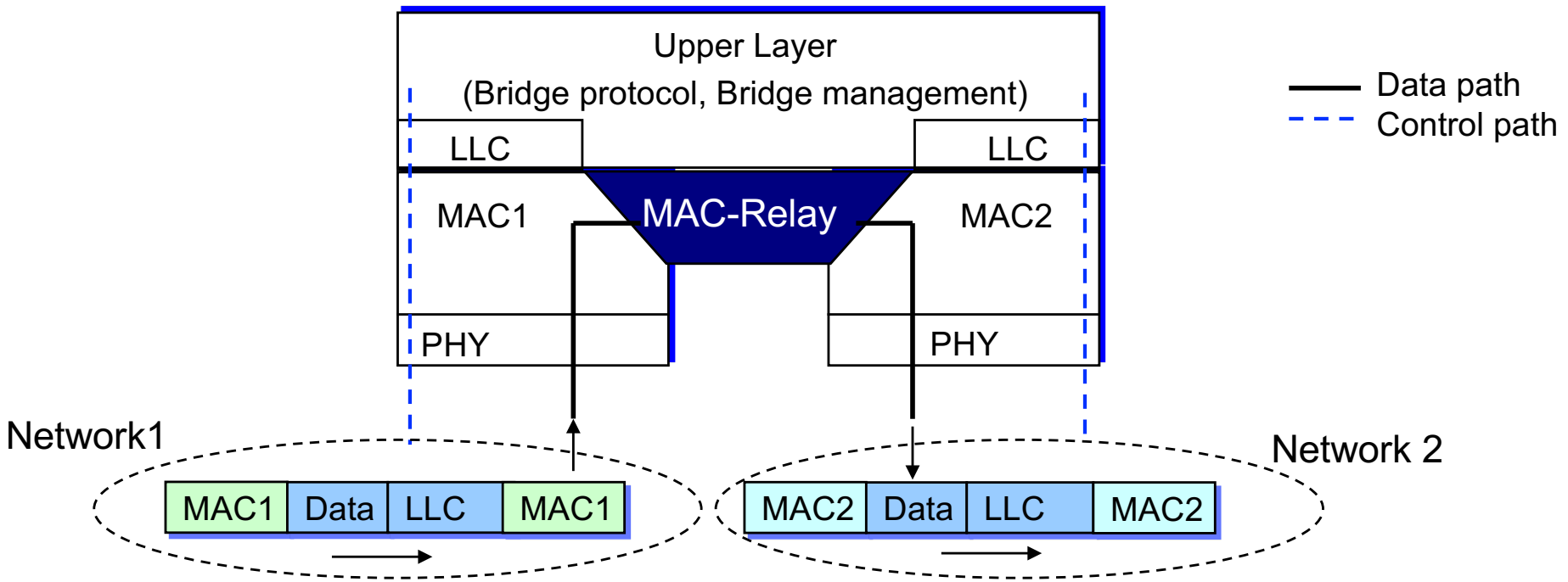
Infrastructure Components: Hub & Repeater



Infrastructure Components: Bridge

Layer 2

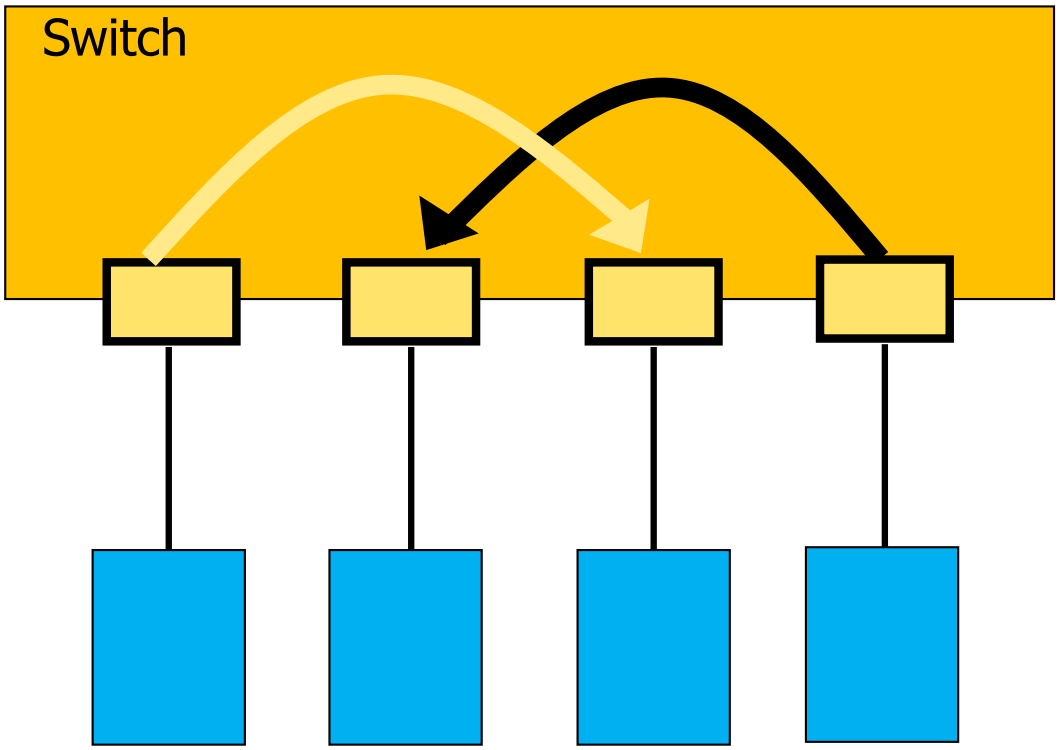
- **Bridge**
  - Bridge connects 2 or more LANs
  - Operates on frame addresses
  - Can support different network type



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

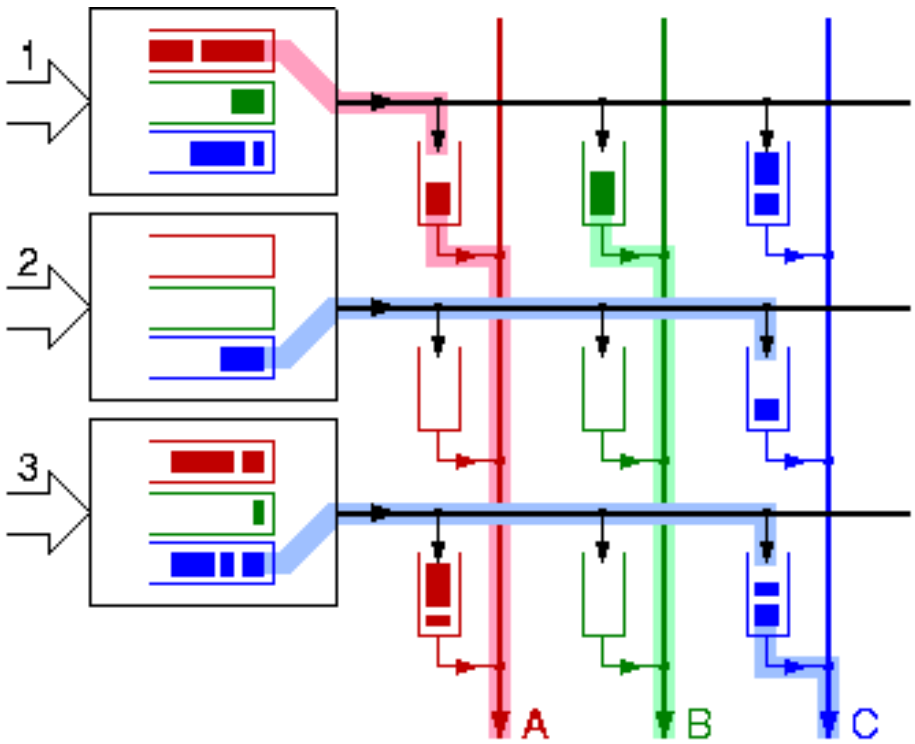


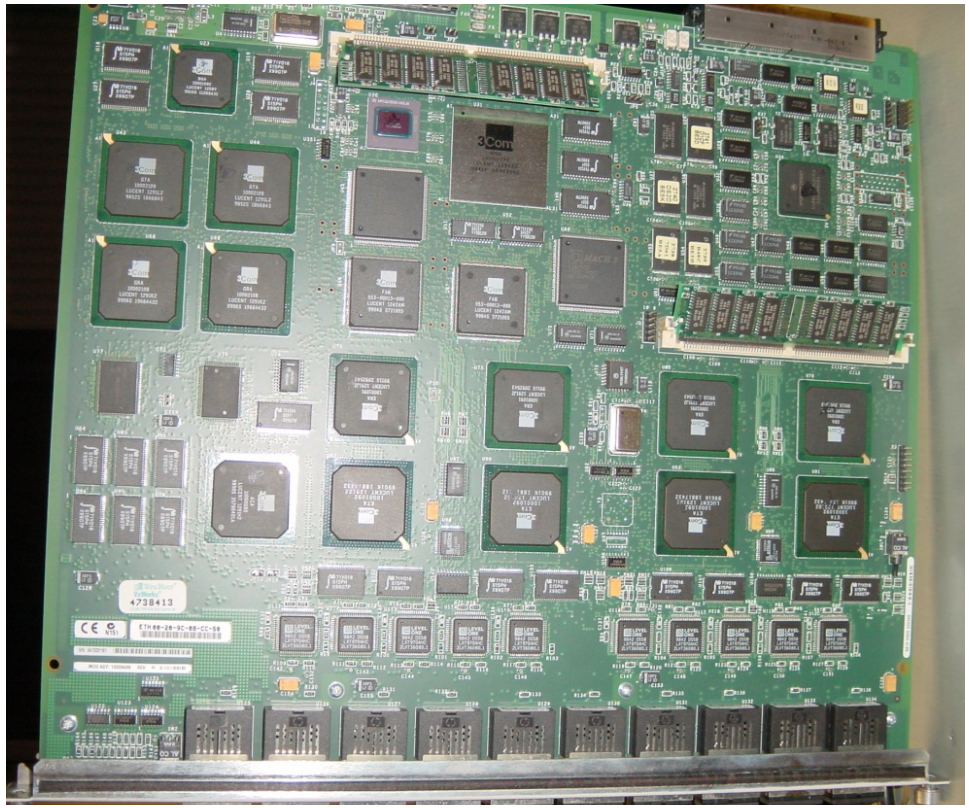
- "Layer 3-Switch": also has functionalities of level 3, i.e., it can e.g. take over the routing.
- "Layer 4-Switch": looks up additionally in the TCP-header, can therefore be used e.g. for load balancing.

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

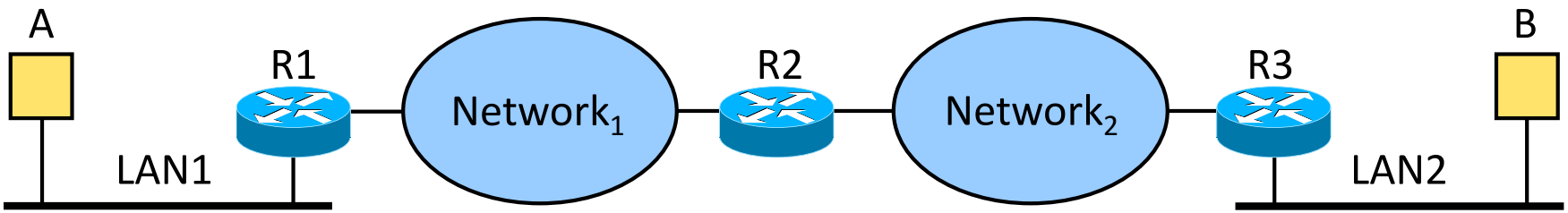
- **What are the limitations of bridges?**
  - Even though bridges are suitable to connect computers in several networks, there are also some disadvantages, e.g.:
    - Bridges can support only some thousand stations, which especially has the reason that addresses are used which do not have any geographical 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

Layer 3

- **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



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

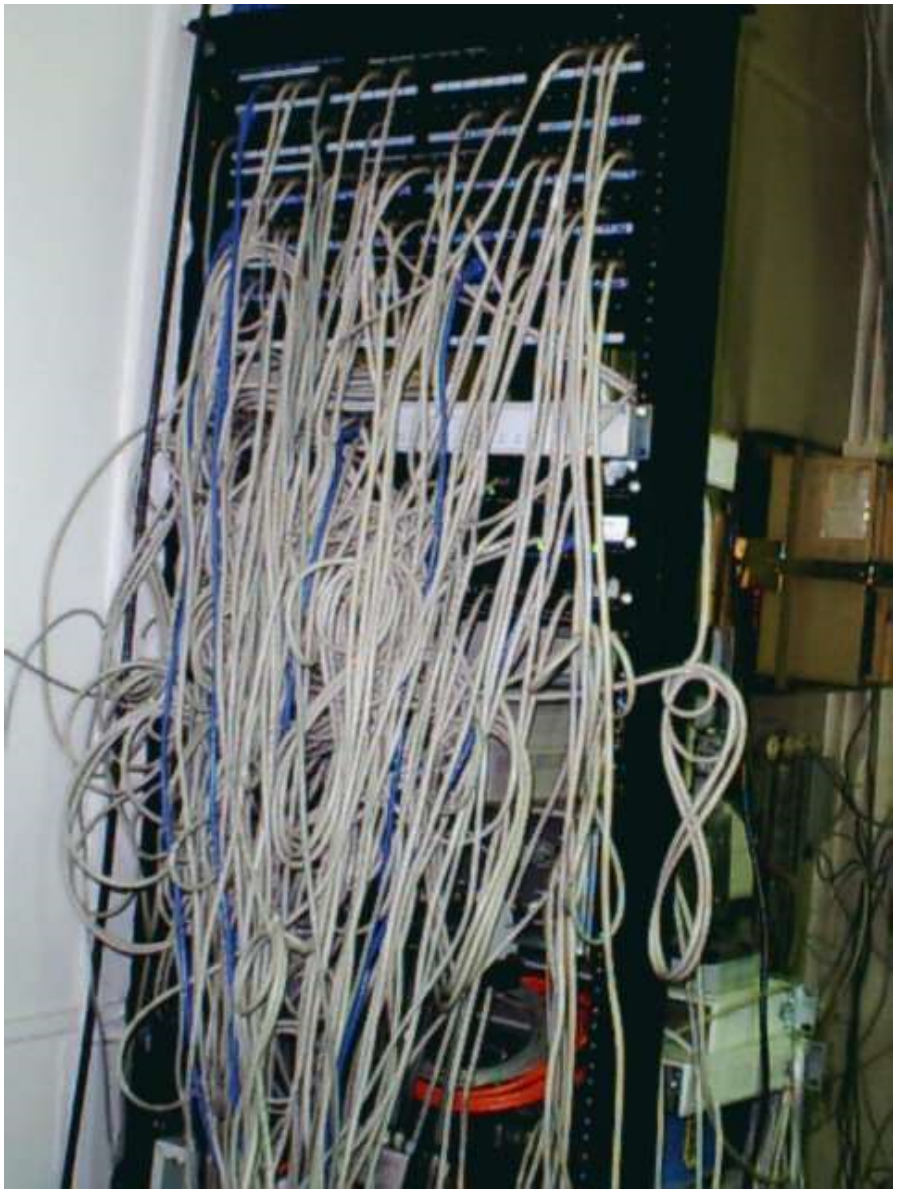
- **Application Layer Gateways**
  - Understand the format and contents of the data and translate messages from one format to another format, e.g., email to SMS

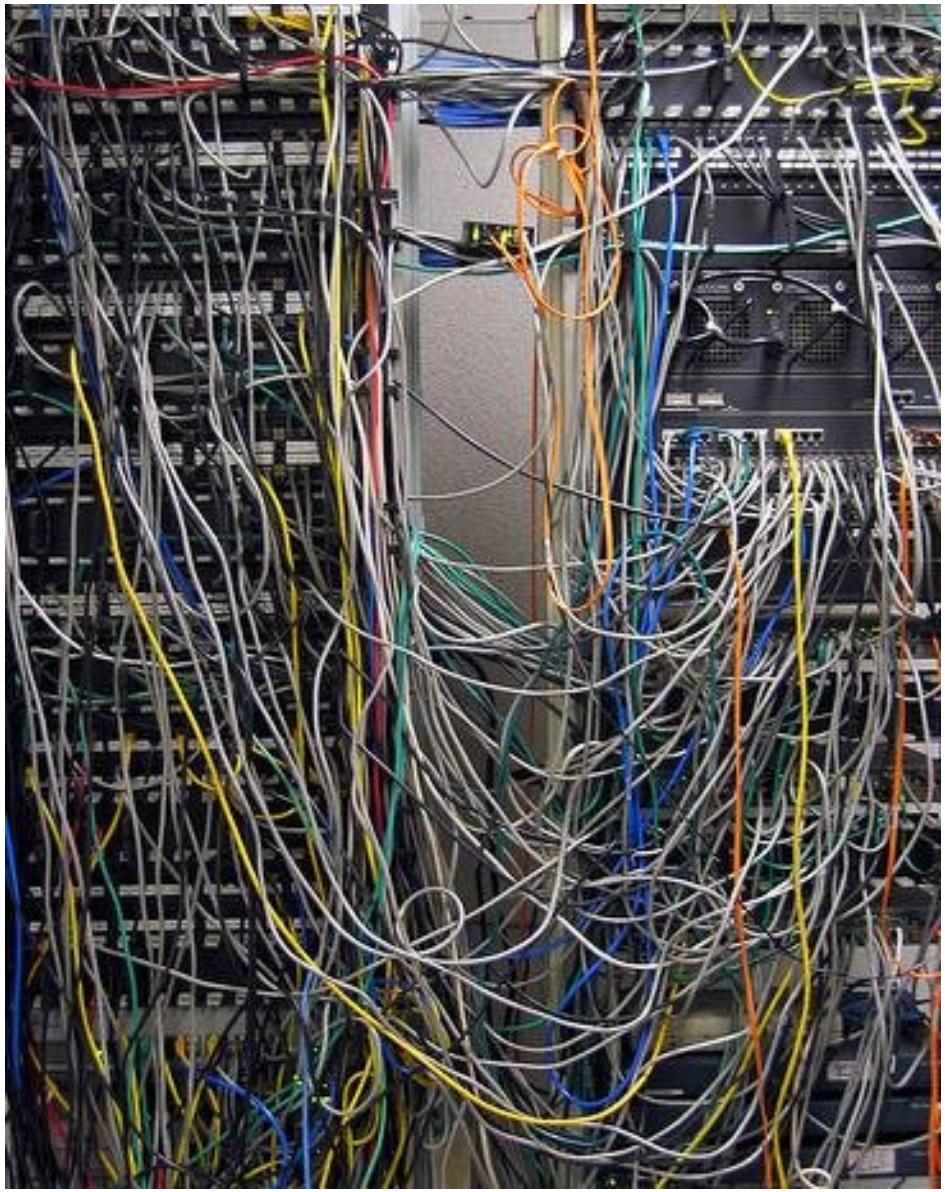
Structured Cabling

Structured Cabling

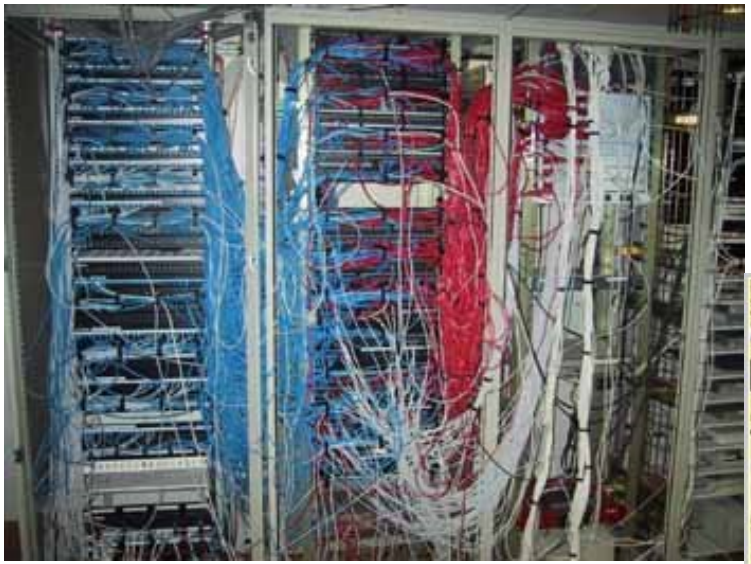
- **Why we need a structured cabling?**

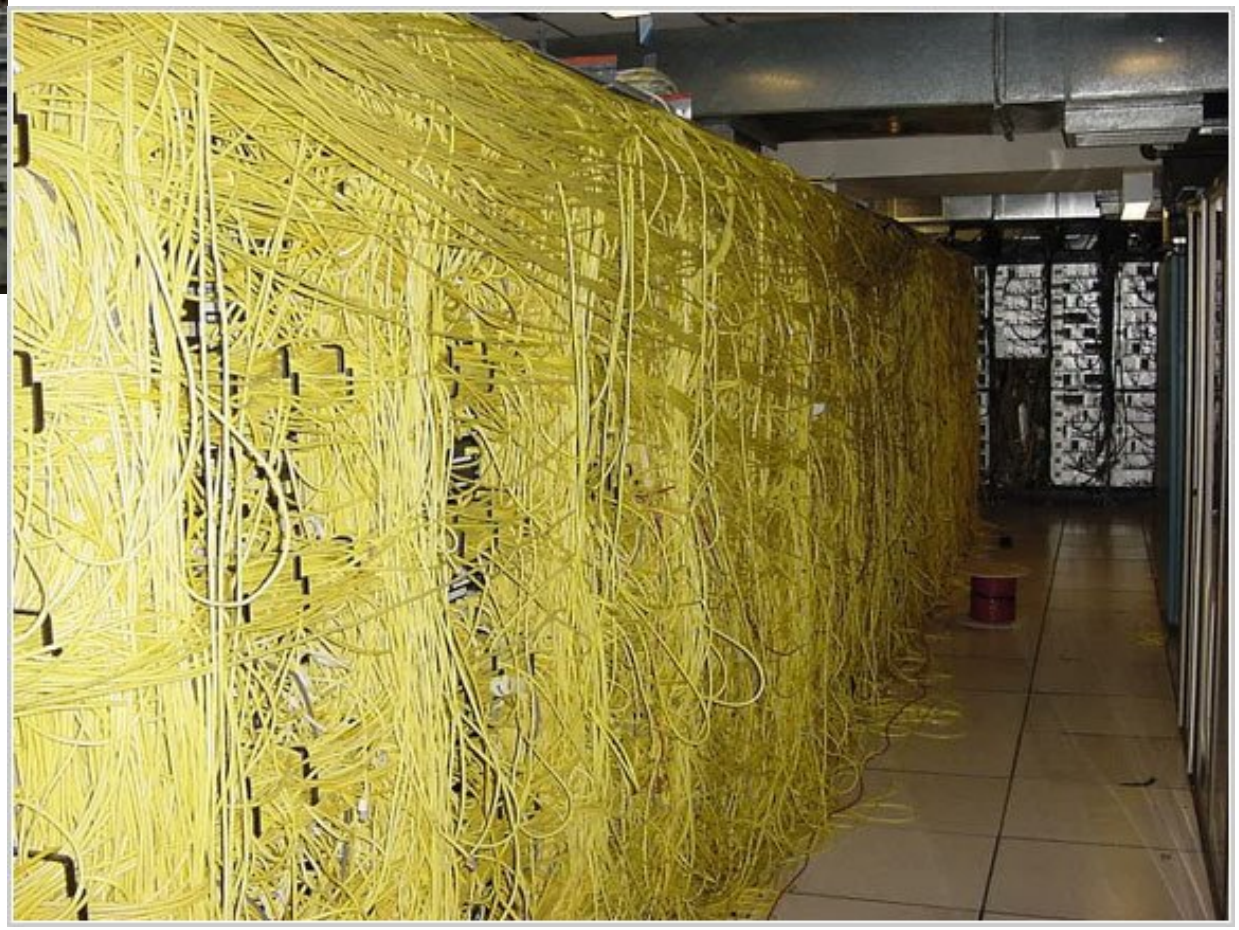
Structured Cabling



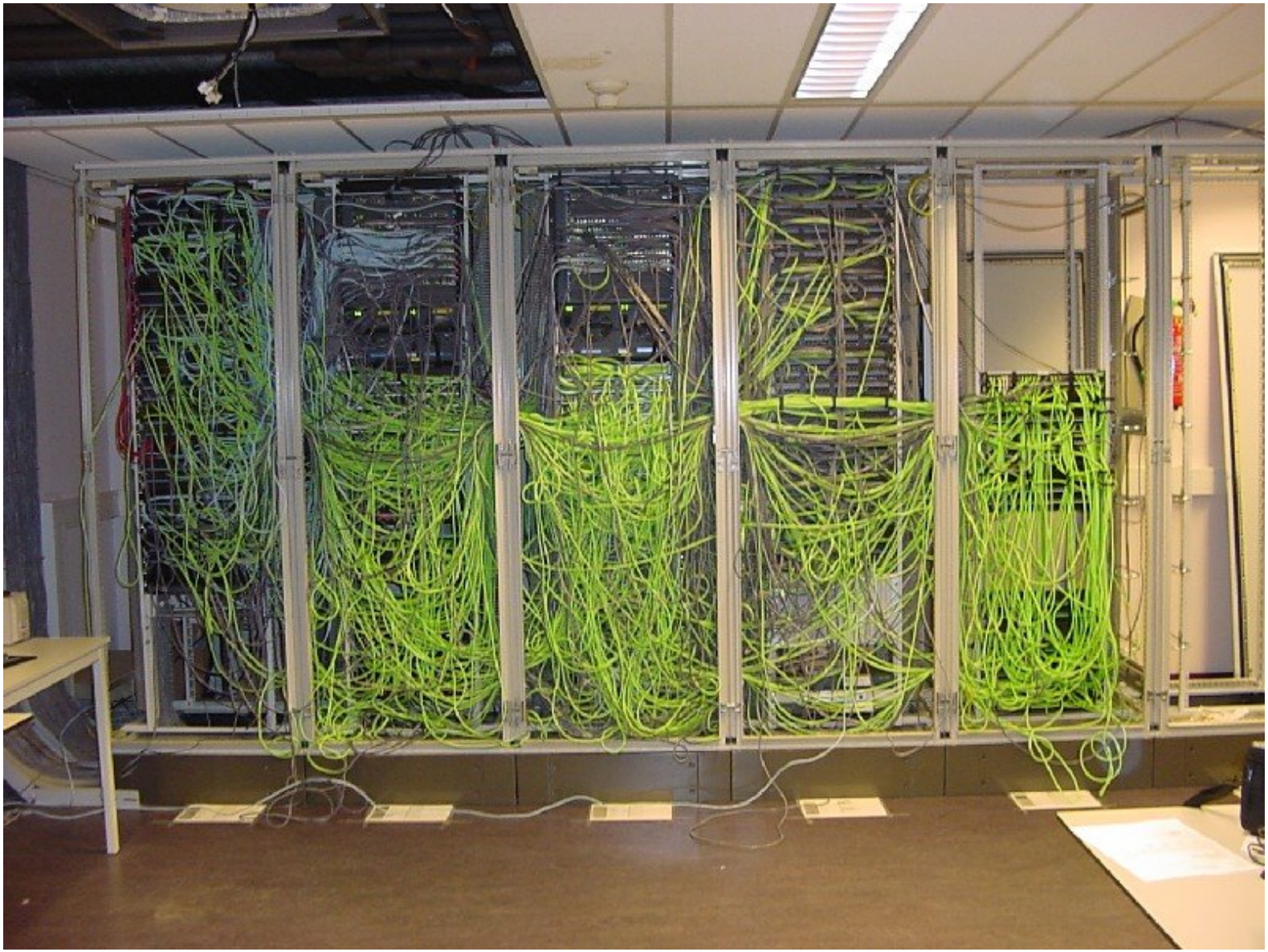


Structured Cabling

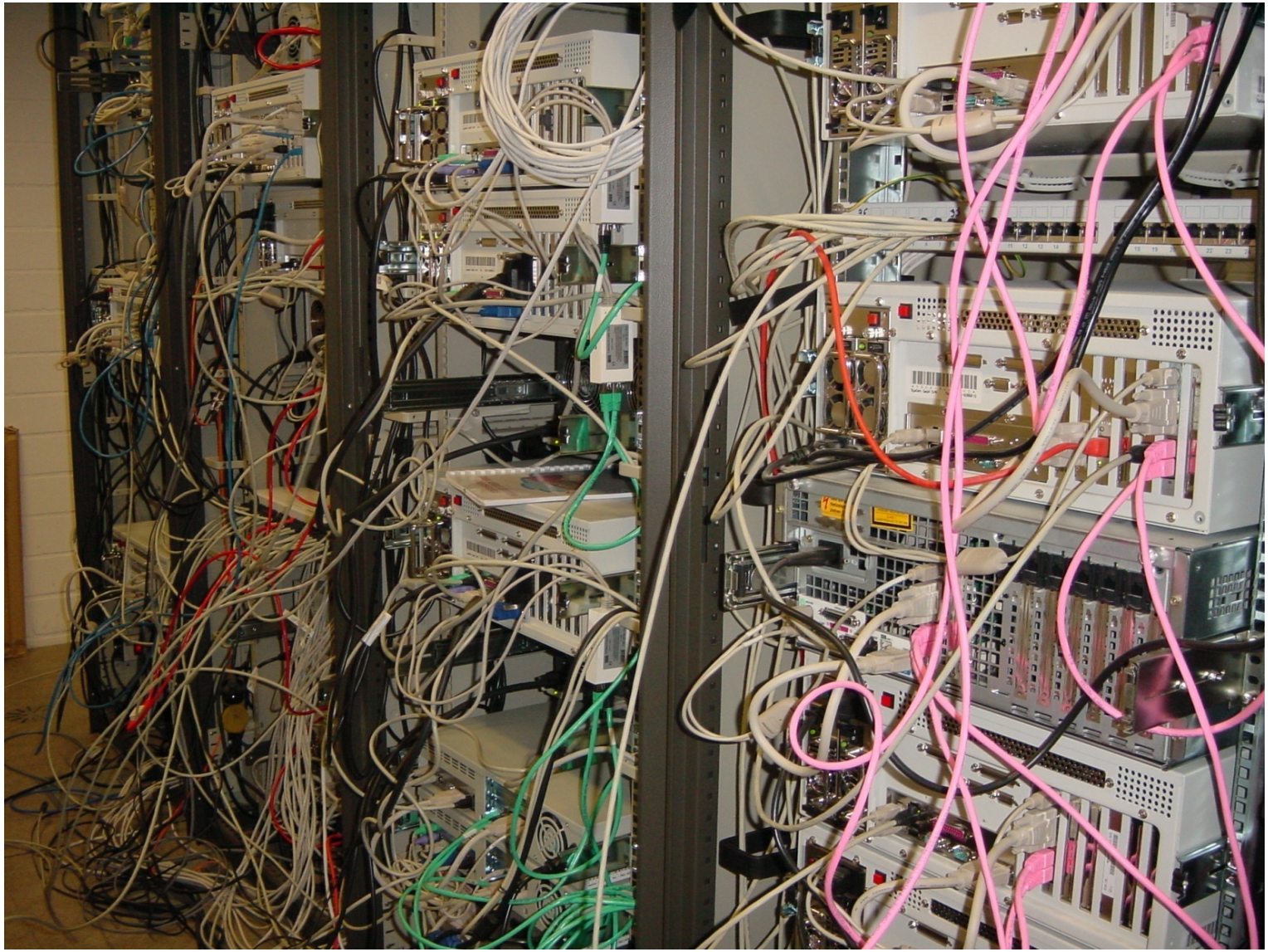




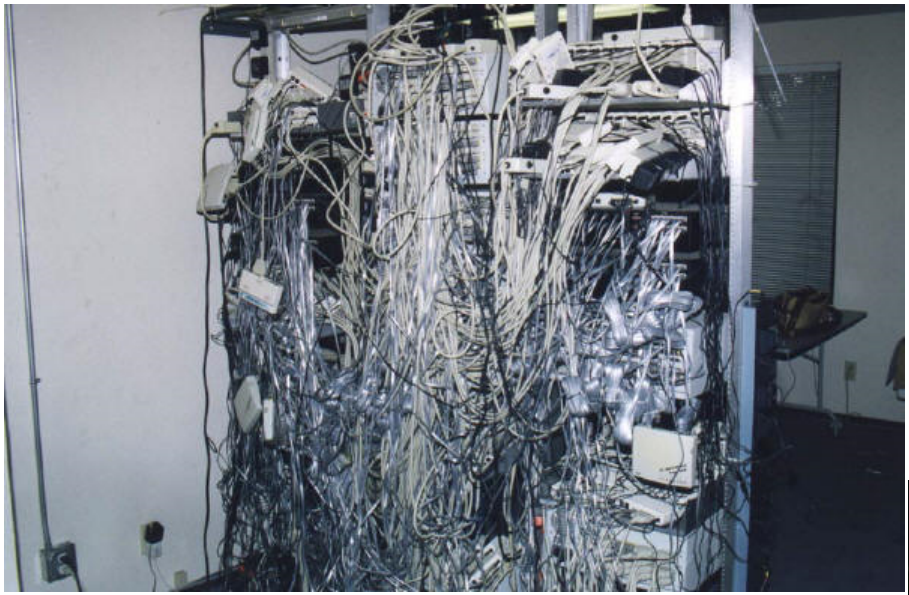
Structured Cabling

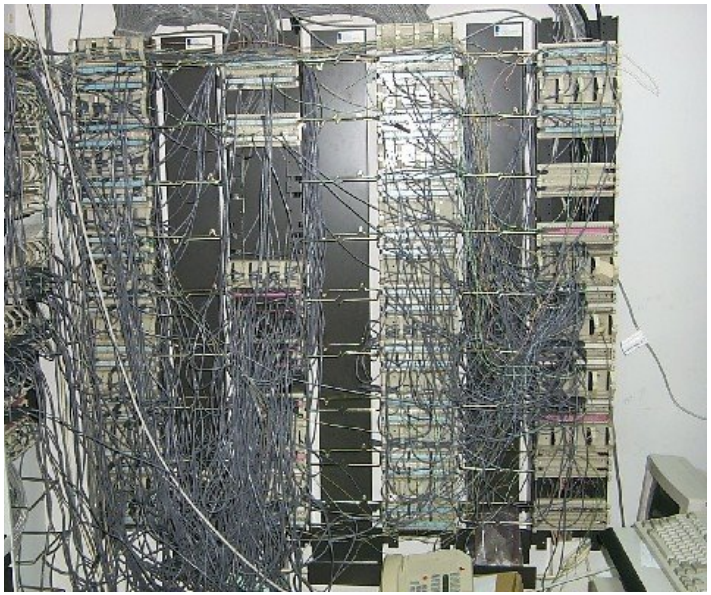


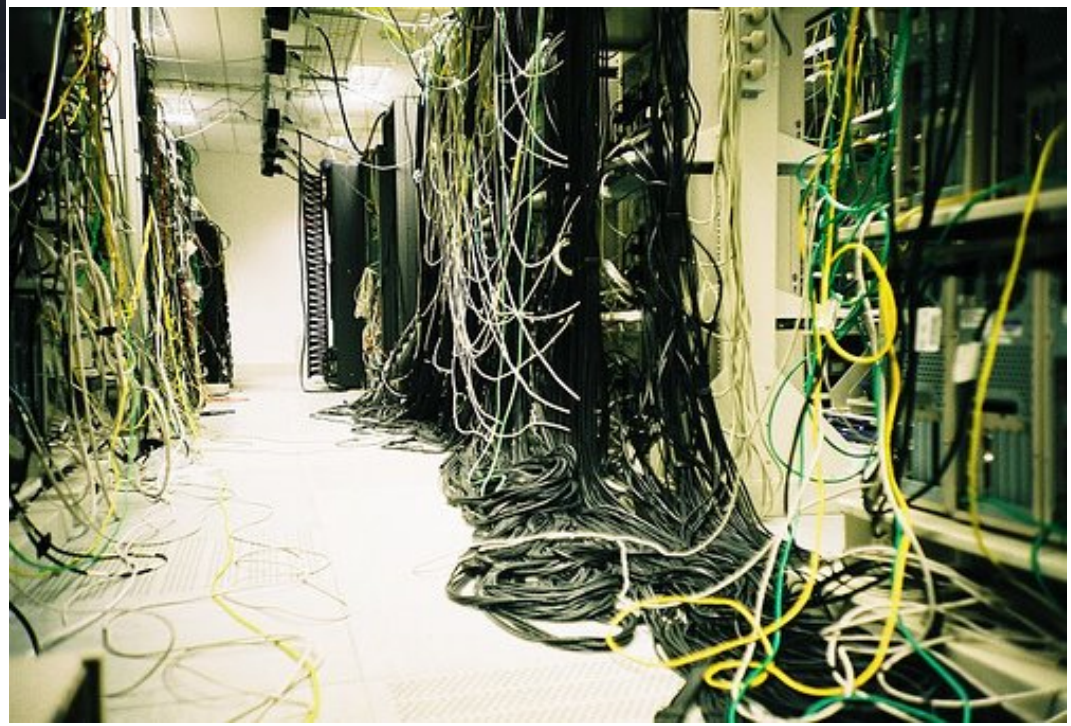
Structured Cabling



Structured Cabling

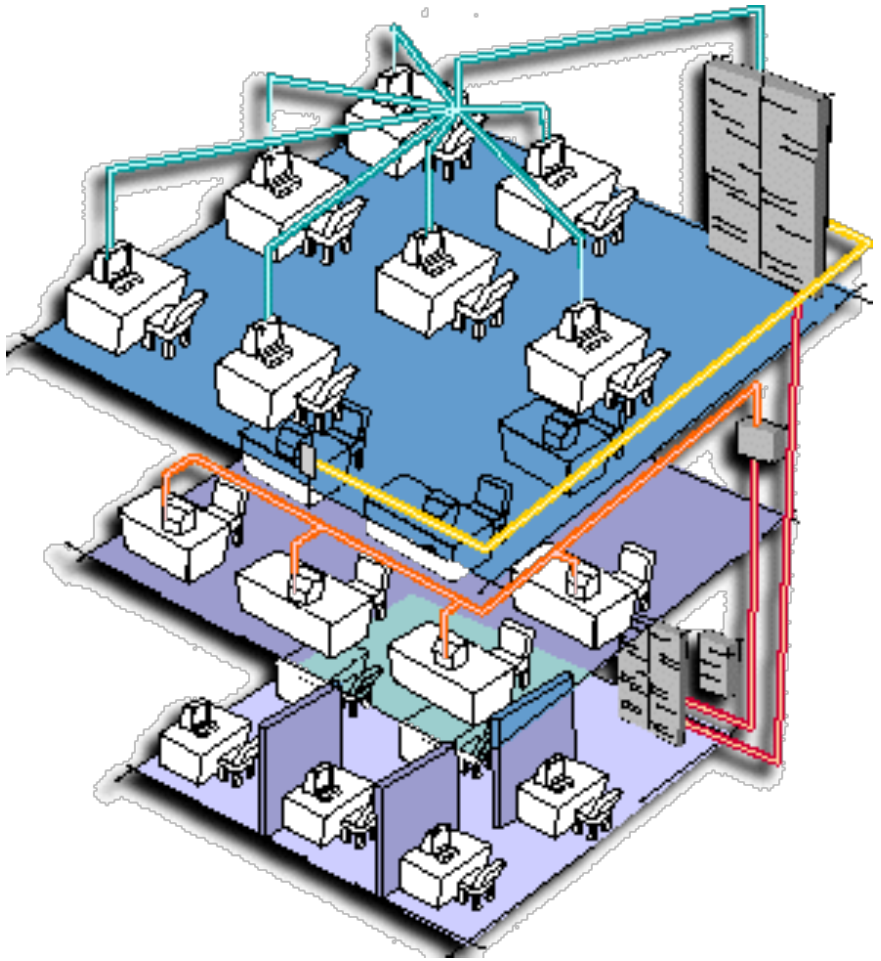






Structured Cabling

- **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



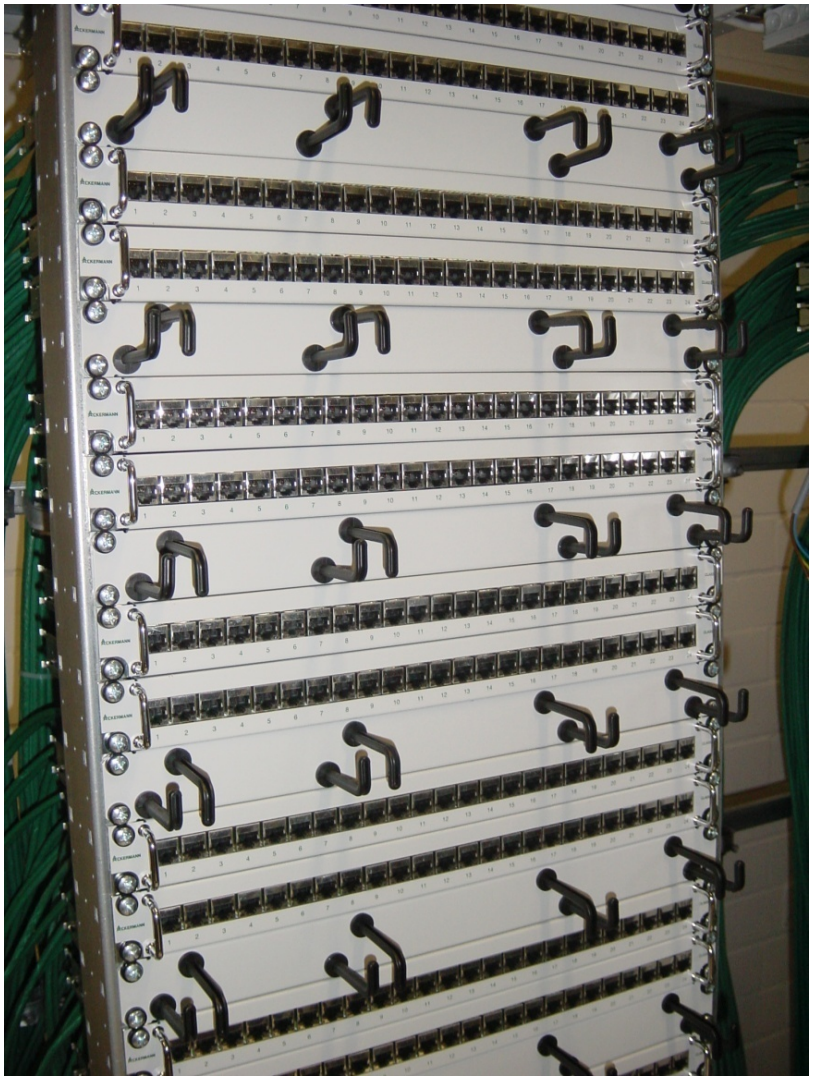
Structured Cabling

- **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

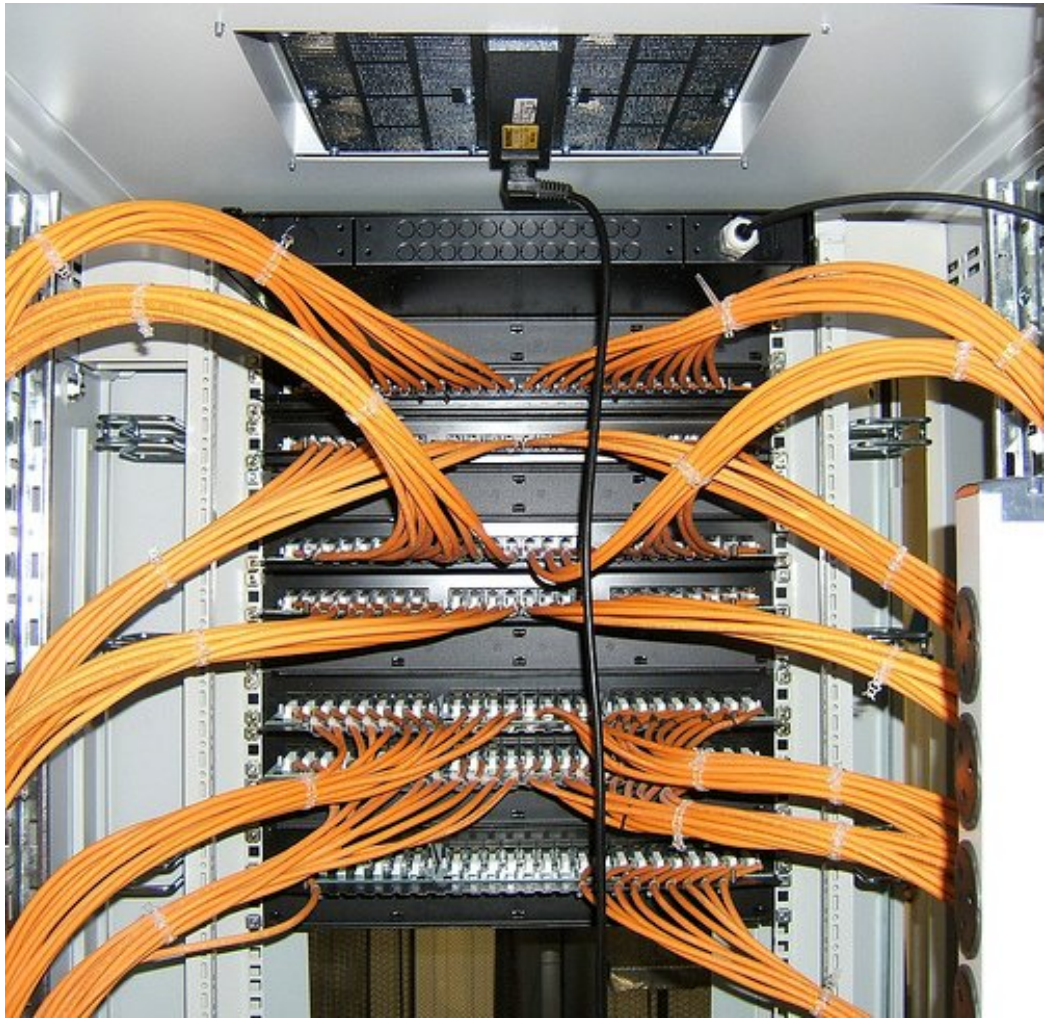
Structured Cabling

Structured Cabling

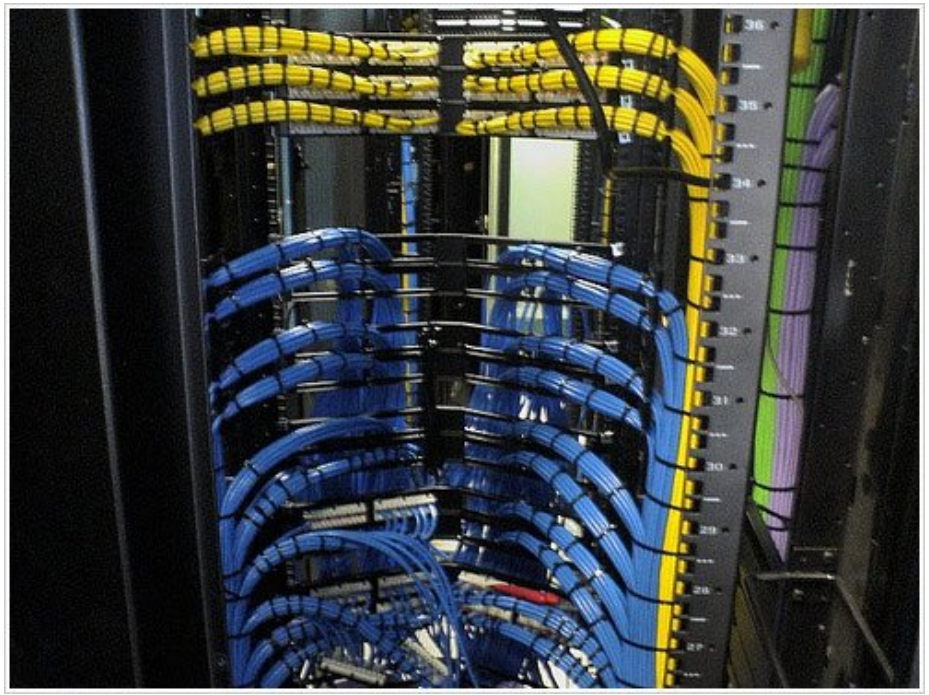
Structured Cabling

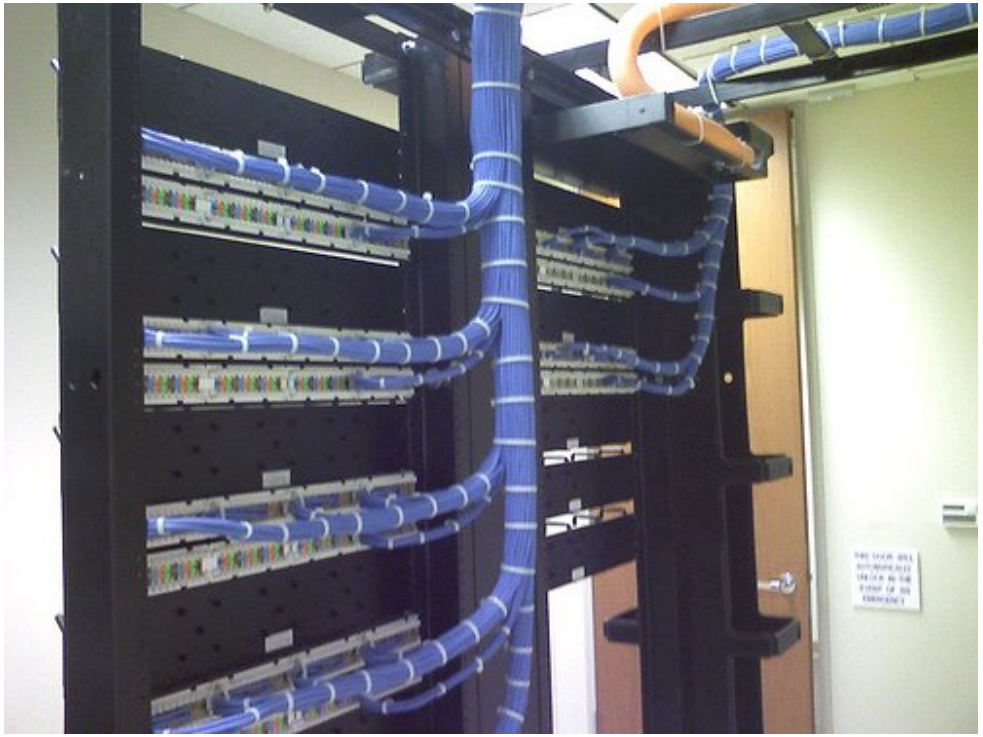


Structured Cabling

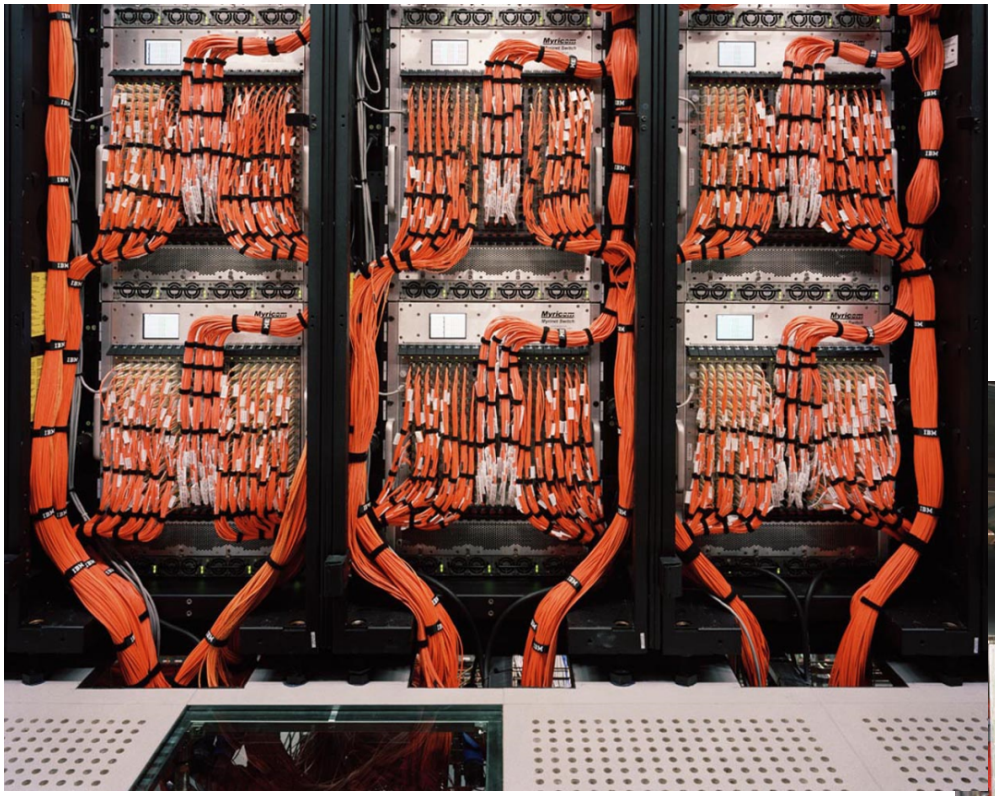


Structured Cabling





Structured Cabling

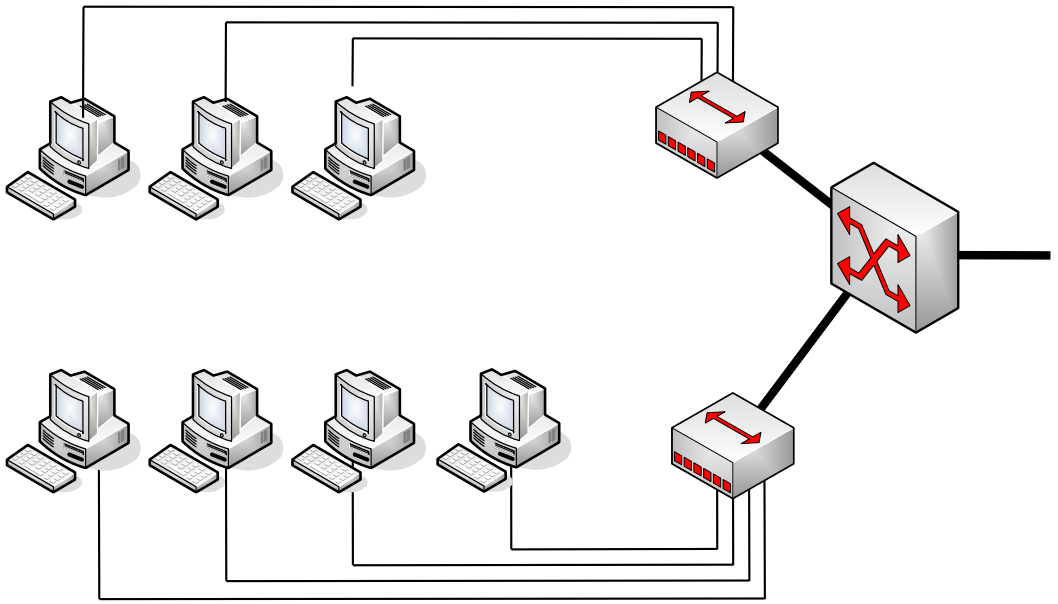


Structured Cabling

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**

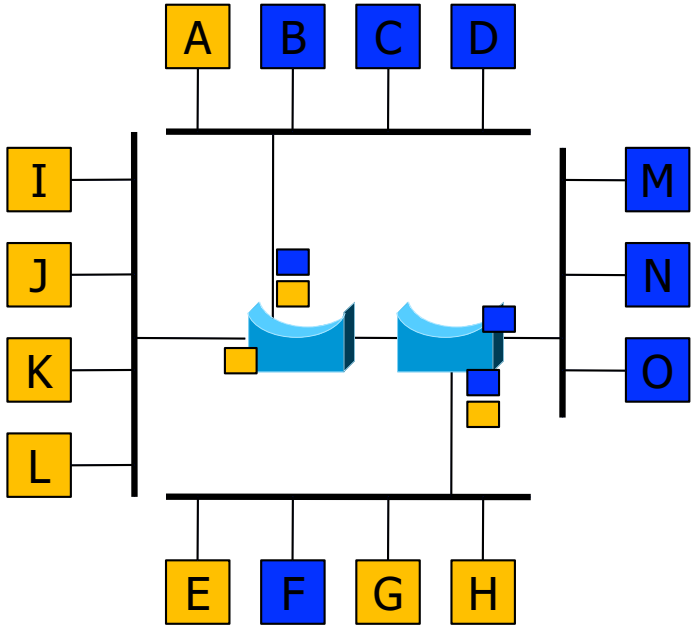


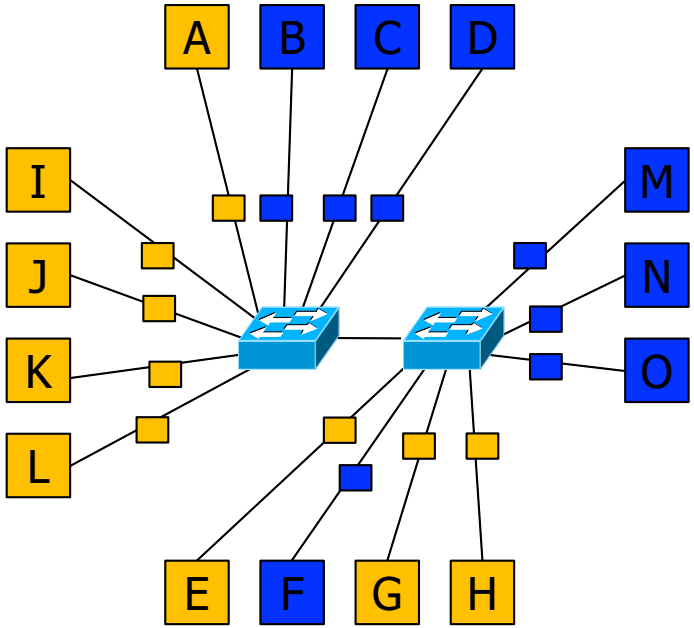
Virtual LANs

- **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

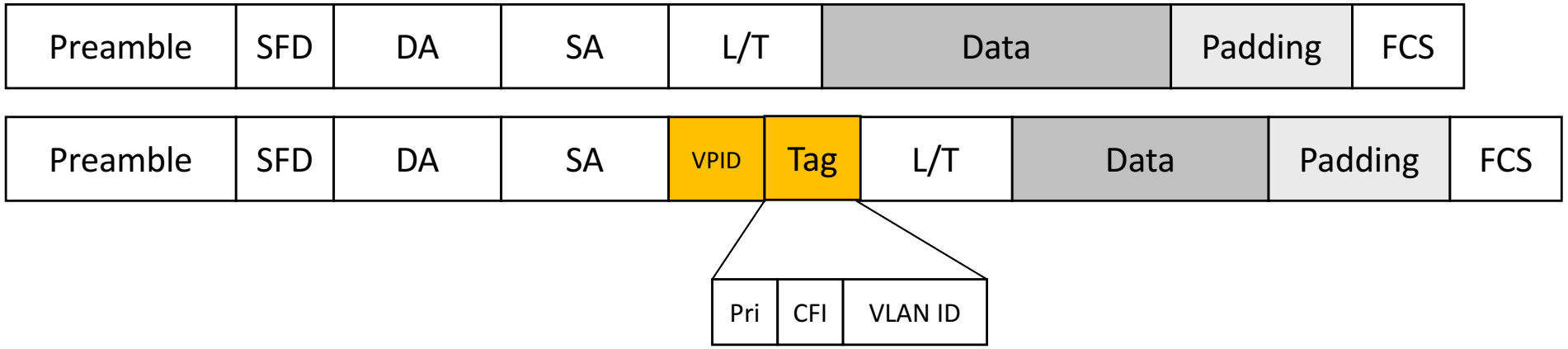
- **Virtual LANs require VLAN-aware switches**
  - VLANs are often named by colors (VLAN ID)
  - Allows colored diagrams which show logical and physical topology at the same time
- **VLAN-aware devices have to know about the VLANs**
  - Switch has a table which tells which VLAN is accessible via which 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
  - VPID: VLAN Protocol ID (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:**
  - Layer 1 defines
    - transmission medium and bit representation on this medium
    - transmission mode, data rate, pin usage of connectors, …
  - Layer 2 protects
    - against transmissions 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, thus 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?