CONTENT of this CHAPTER

- Framing
- Error Detection & Correction
- Flow control
- Multiple Access Control

- Protocols
  - PPP
  - Ethernet
  - Wifi
  - ATM
  - SDH

- Infrastructure
  - Physical elements
  - Virtual LANs

Standard Link Layer Protocols

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

- Metropolitan Area Network (MAN): 10 - 100 km, city range
  - Historical
    - DQDB
    - FDDI II
    - Resilient Packet Ring
  - today: Gigabit **Ethernet**, **SDH**

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

CONTENT of this CHAPTER

- Framing
- Error Detection & Correction
- Flow control
- Multiple Access Control

- Protocols
  - PPP
  - Ethernet
  - Wifi
  - ATM
  - SDH

- Infrastructure
  - Physical elements
  - Virtual LANs

Point-to-Point Protocol (PPP)

- PPP establishes a direct connection between two nodes
  - e.g. a connection between two NICs
  - supports synchronous and asynchronous connections

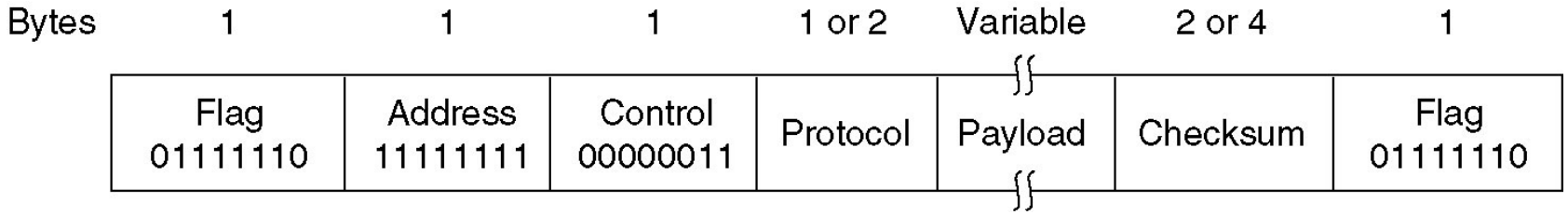
- Specified frame format, with error detection
- PPP uses a **sliding window** approach for flow control
- PPP doesn't use medium access control (no need to on point-to-point links)
- Specified connection establishment / tear down processes

PPP: Connection Establishment Process

- Connection in 3 steps
  - Step 1: PPP establishes a basic connection (tests that the Physical Layer is ready)
  - Step 2: the Link Control Protocol (LCP) configures NICs on each end of the link
    - Maximum frame size (MTU)
    - Escape characters
    - Magic numbers (identifying an end, used to detect looped links)
    - Authentication method, e.g. Extensible Authentication Protocol (EAP)
    - Also manages graceful termination of link layer connection
  - Step 3: Internet Protocol Control Protocol (IPCP) configures IPv4 network layer options
    - configures settings such as IPv4 network address or compression options
    - Manages tear down of the network layer connection (free up IP address)
    - there are other Network Control Protocols (NCP), defined for IPv6 or AppleTalk for instance

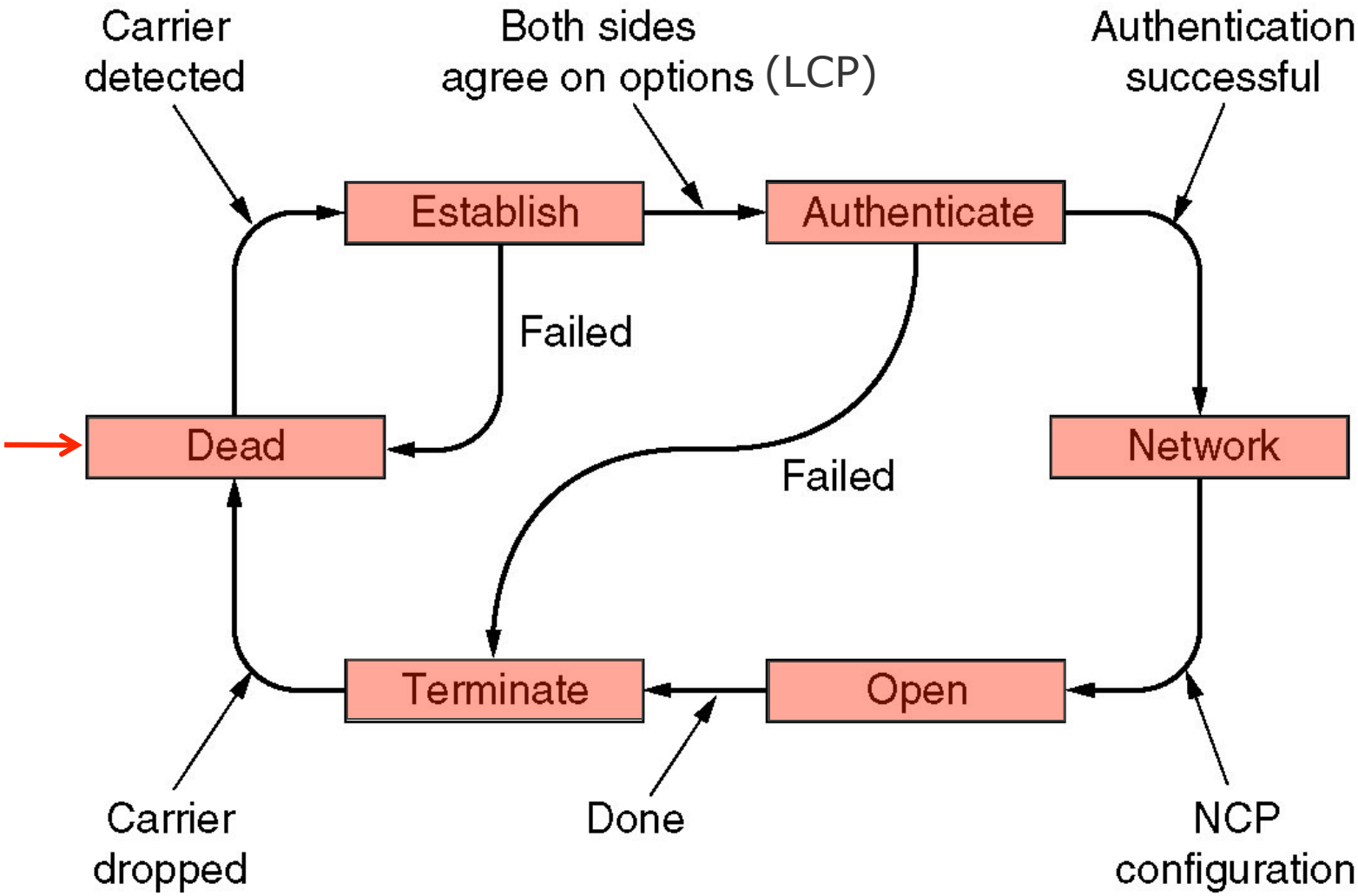
Point-to-Point Protocol (PPP)

- PPP is **character oriented** (= byte-oriented) and uses **byte-stuffing**
- PPP frame format reuses the format of another protocol (HDLC)



- Flag: start of frame with special byte 01111110
- Address field: useless here ("inherited" from HDLC). Set to 11111111
- Control field: set to 00000011 (unnumbered mode). This means without sequence numbers and acknowledgments.
- Protocol field: specifies to which network layer protocol the payload should be delivered. If set to 00000110, the indicated network layer protocol is IP.
- Checksum: default is 16 bits CRC with generator polynomial $x^{16} + x^{12} + x^5 + 1$ computed over the Address, Control, Protocol, Payload (and Padding) fields
  - Just detection, no correction

PPP: Finite State Machine



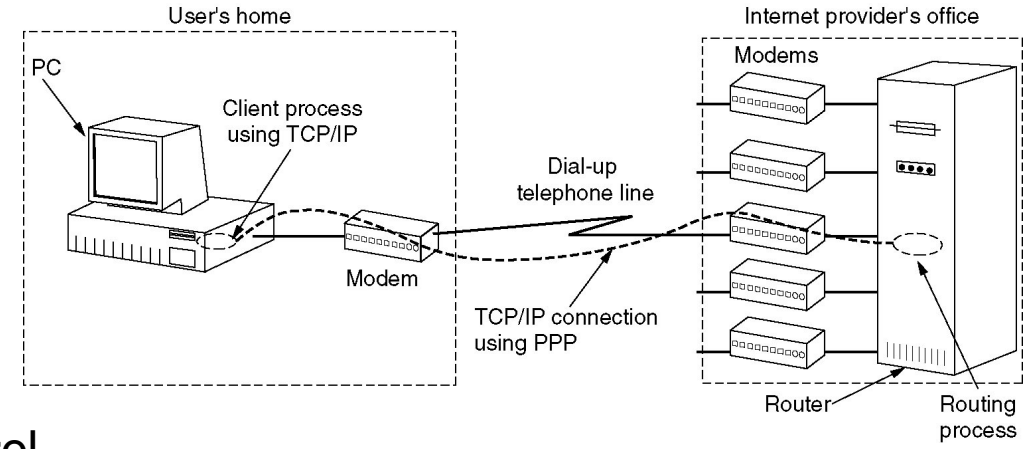
PPP: The Link Control Protocol

- The Link Control Protocol (LCP) frame types defined in RFC 1661
  - I = Initiator proposes option values
  - R = Responder accepts or rejects proposed options

Name	Direction	Description
Configure-request	I→R	List of proposed options and values
Configure-ack	I←R	All options are accepted
Configure-nak	I←R	Some options are not accepted
Configure-reject	I←R	Some options are not negotiable
Terminate-request	I→R	Request to shut the line down
Terminate-ack	I←R	OK, line shut down
Code-reject	I←R	Unknown request received
Protocol-reject	I←R	Unknown protocol requested
Echo-request	I→R	Please send this frame back
Echo-reply	I←R	Here is the frame back
Discard-request	I→R	Just discard this frame (for testing)

PPP Standards

- PPP used to be the default link layer protocol for dial-up Internet access
  - Specified inRFC 1661, RFC 1662, RFC 1663



- PPP is still used as a link layer protocol on point to point optical links and for the last mile with DSL / cable modem
  - PPPoE (PPP over Ethernet, RFC 2516)
    - Encapsulation of PPP frames inside Ethernet frames
  - PPPoA (PPP over ATM, RFC 2364: PPP over AAL5)
    - Encapsulation of PPP frames in AAL5

CONTENT of this CHAPTER

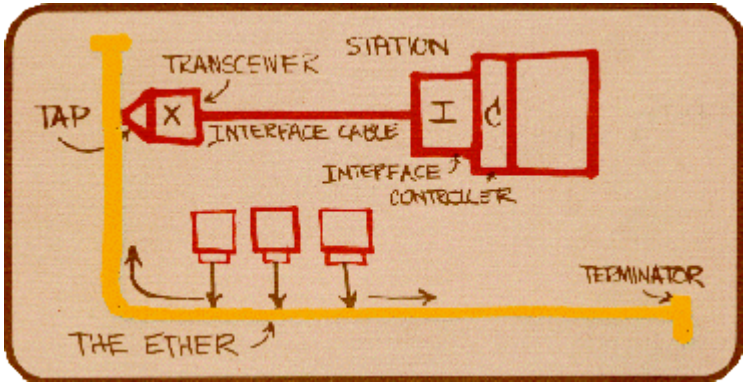
- Framing
- Error Detection & Correction
- Flow control
- Multiple Access Control

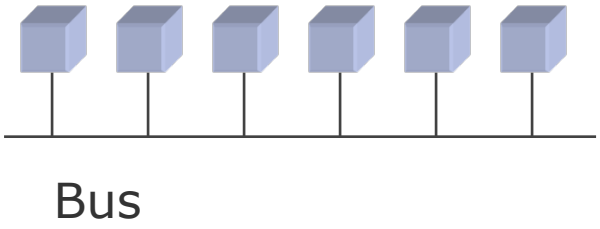
- Protocols
  - PPP
  - Ethernet
  - Wifi
  - ATM
  - SDH

- Infrastructure
  - Physical elements
  - Virtual LANs

Ethernet: Random Multiple Access on Wire

- Origin of Ethernet:
  - 1970's: ALOHA pioneers random multiple access (on wireless)
  - 1970's: Xerox experimental network on coaxial cables, data rate of 3 Mbps.
    - targeting LANs with sporadic but bursty traffic.
  - 1976: Ethernet by **Robert Metcalf** at Xerox Parc
    - Ether: matter through which electromagnetic radiation was thought to propagate
    - Improvements to ALOHA: listen to the medium before transmitting (CSMA/CD)
    - Bus topology (+ repeaters to connect several segments)

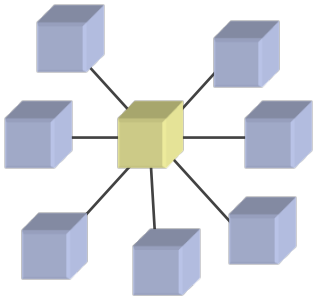




  - 1978-1983: development and standardization of 10 Mb Ethernet (**IEEE 802.3**)
    - Robert Metcalf founded 3Com and sold many, many million Ethernet adapters

Ethernet: Evolution

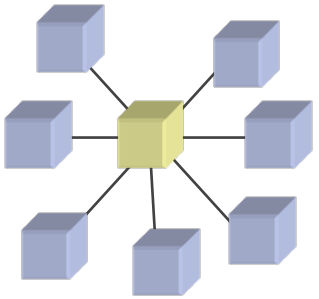
- Issues with bus topology
  - uneasy to maintain and debug
  - if the cable gets damaged (cut or bent), difficult to detect *where* it is damaged
- Solution: use star topology
  - the cable goes through a central point
  - easier to maintain and to diagnostic



- At first, central point was a only a hub
  - Just a repeater => broadcast on twisted pair (copper cables)
  - Still need medium access control (CSMA/CD)
- But now in some cases the central point is a switch
  - One NIC per switch interface => back to point-to-point links
  - No need for for mediul access control anymore! (i.e. no CSMA/CD)
  - More and more fibers replace copper to link to the Ethernet switch!

Ethernet: Evolution

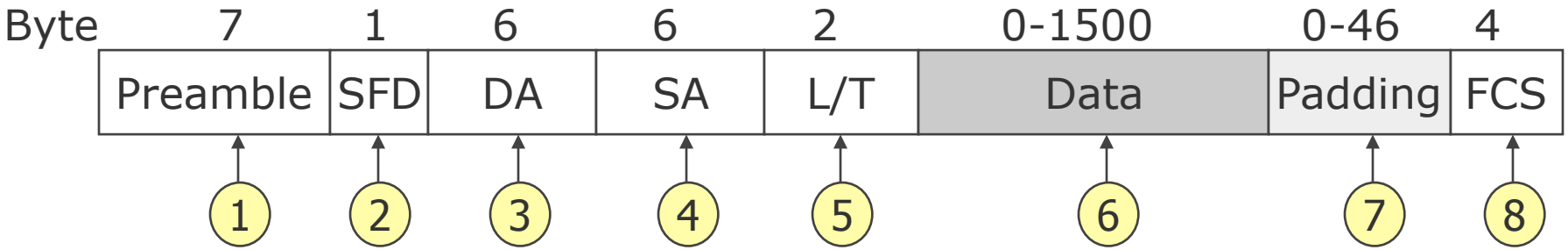
- Issues with bus topology
  - uneasy to maintain and debug
  - if the cable gets damaged (cut or bent), difficult to detect *where* it is damaged
- Solution: use star topology
  - the cable goes through a central point
  - easier to maintain and to diagnostic



- At first, the central point was only a hub
- But now in some cases the central point is a switch

- Typical Ethernet deployment at home:
  Ethernet hub, star topology, achieving 100 Mbit/s to 1 Gbit/s
- Typical Ethernet deployment in a data center:
  Ethernet switch, star topology, achieving 10 Gbit/s to 40 Gbit/s

Ethernet: The Ethernet Frame Format



1: 7 bytes flag for synchronization
Each byte of the flag is 10101010

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

3: 6 byte destination address
MAC address of receiver

4: 6 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

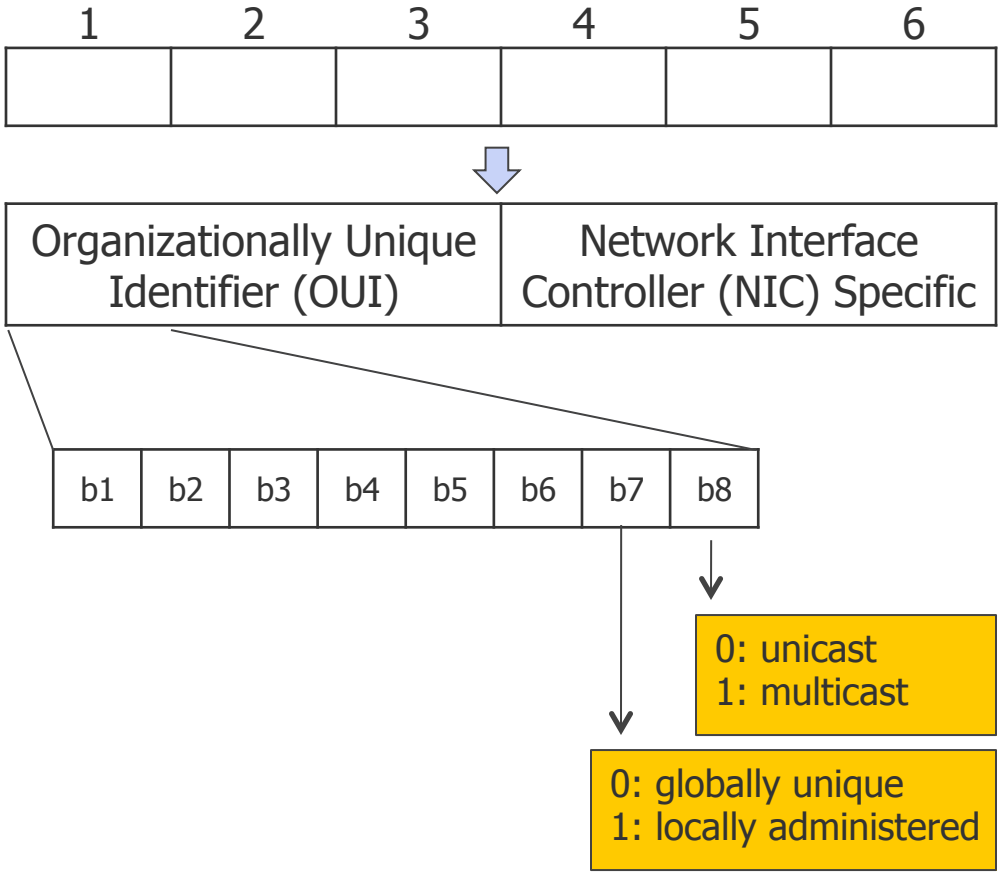
7: (0 – 46) byte padding

- 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: use of a 32 bit CRC computed over DA, SA, length/type, data/padding fields

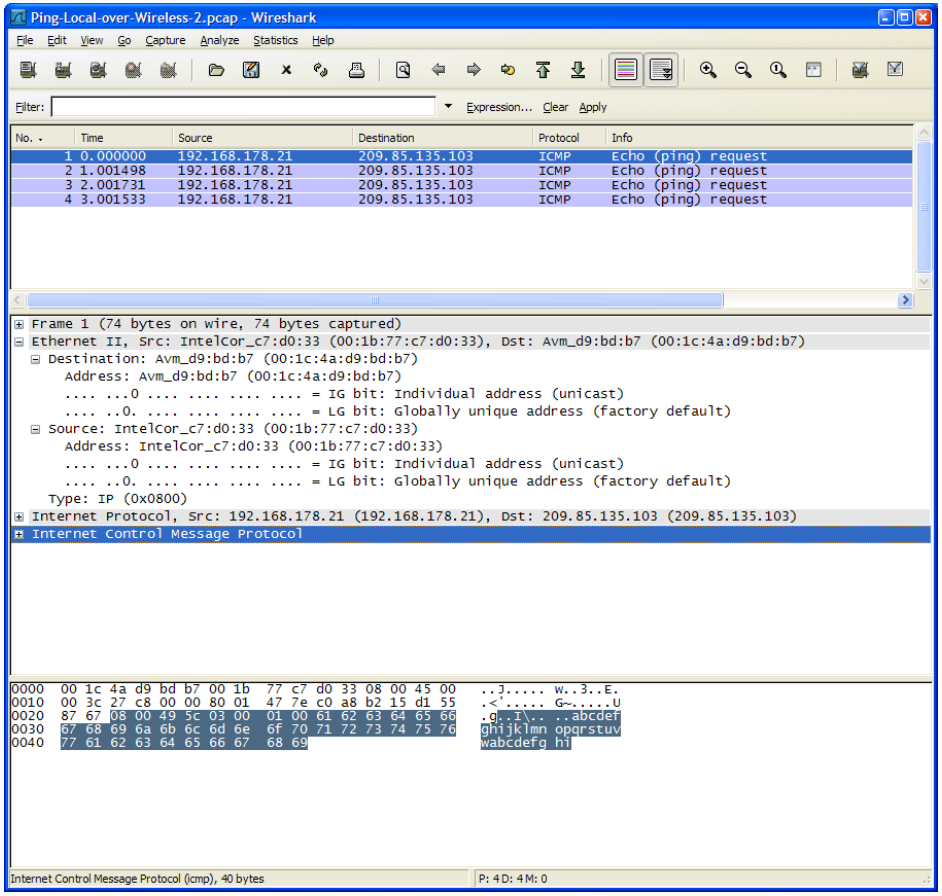
The Ethernet Frame: Addresses

- MAC address: 6 bytes long
  - Unicast (starts with 0)
  - Multicast (starts with 1)
  - Broadcast (111…1)
- Administrative aspect:
  - Globally unique, assigned by IEEE
  - Locally administered
- MAC address representation
  - Typically in hexadecimal notation
    - Example 01:23:45:67:89:ab
- Useful tools:
  - Linux / OS X: `ifconfig, cat /proc/net/arp`
  - Windows: `getmac, ipconfig /all, arp -a`
  - http://www.heise.de/netze/tools/mac-adressen



The Ethernet Frame: Network Analyzer

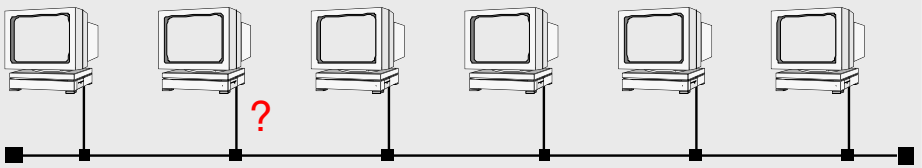
- Network packet analyzer: Wireshark
  - http://www.wireshark.org/



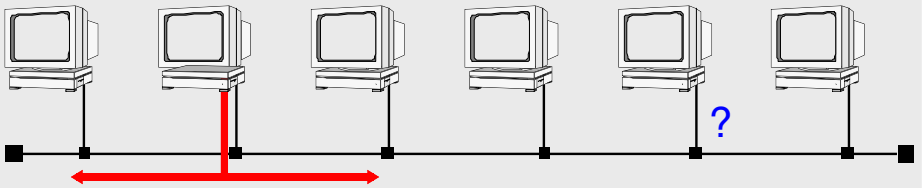
Ethernet – Random Multiple Access Control

- Ethernet's collision resolution mechanism is based on CSMA/CD
  - Carrier Sense Multiple Access/Collision Detection (IEEE 802.3)
  - Listen before send, stop as soon as simultaneous transmissions are detected

1. Is the medium available? (Carrier Sense)

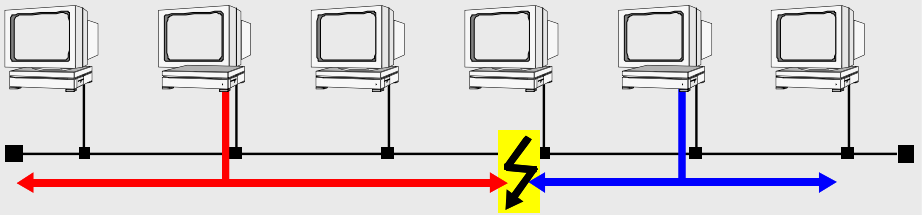


2. Data transmission



3. Check for collisions (Collision Detection)

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



- Advantages: simple, does not rely on centralized coordination
- Drawbacks: no guaranteed access, a large delay before sending is possible

Ethernet: Binary Exponential Backoff

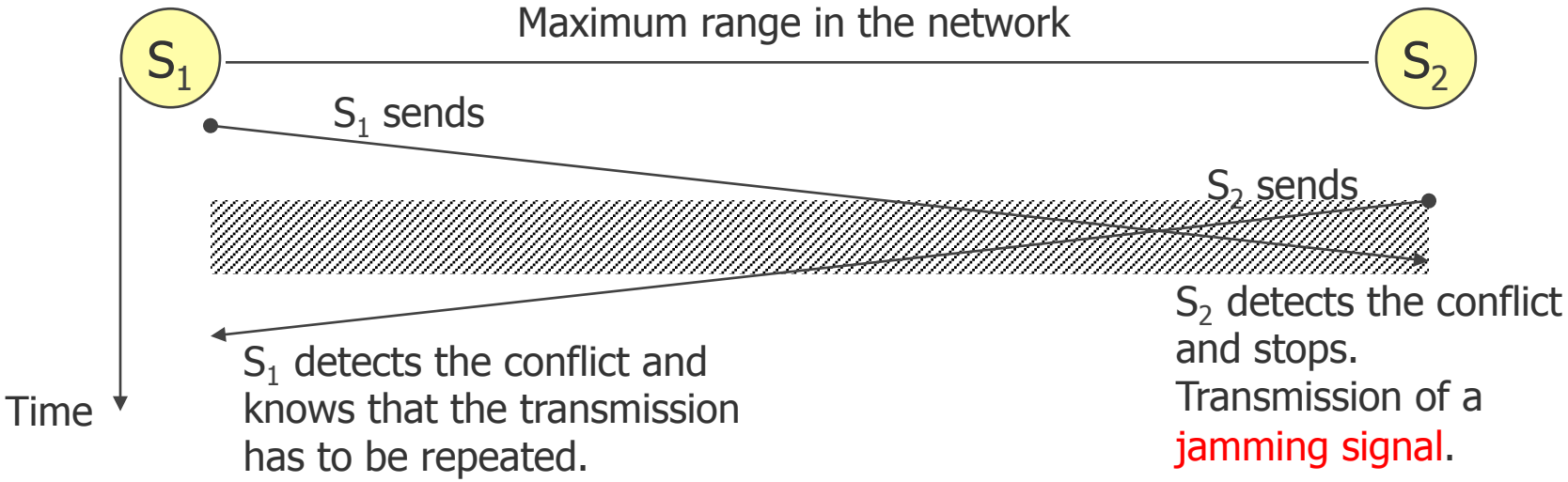
- In addition to CSMA/CD, Ethernet uses Binary Exponential Backoff (BEB)
  - Goal: **avoid repetition** of simultaneous transmissions **after a collision**
  - Problem analysis: a random **waiting period** is drawn from a given interval.
    - The interval is kept small, in order to avoid long waiting periods up to the repetition.
    - Thus, the risk of a subsequent conflict is high.
  - Solution: the random waiting period is drawn from an **increasing interval**
  - After i-th collision, a node draws a random number x from the interval $[0, 2^i-1]$
  - After 10-th collision, the interval remains fixed with $[0, 2^{10}-1]$
  - After the 16-th collision a node gives up
- When the channel is free again after the collision, the sender waits for x time slots, and then tries to transmit according to CSMA/CD.
  - 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

Ethernet: Binary Exponential Backoff

- Advantage of BEB:
  - Adaptive to a large range of traffic loads
    - Short waiting periods (by small interval) if not much traffic is present
    - Distribution of repetitions (by large interval) if much traffic is present
- Drawbacks of BEB:
  - Potentially unfair
    - BEB tends to prefer last contention winner and new contending nodes over other nodes when allocating channel access

Ethernet: Detection of Collisions

- Problem: finite propagation speed. Collision detection isn't instantaneous!
  - e.g. a node thinks the channel is free while another node just started transmitting
  - While sending, when to stop listening? What is the maximum conflict period?

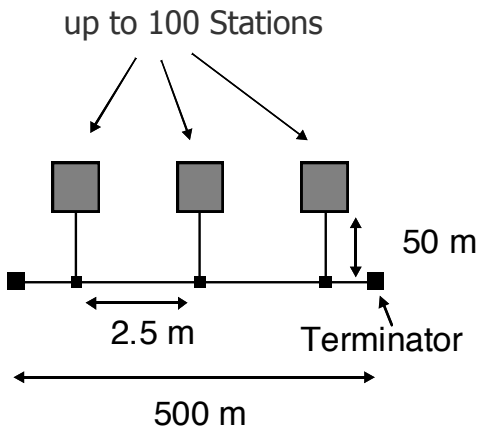


- Solution: adjust minimum packet length & maximum travelled distance
  - A sender should be sure that the beginning of its message reached the receiver before it assumes there was no collision and stops listening while sending.

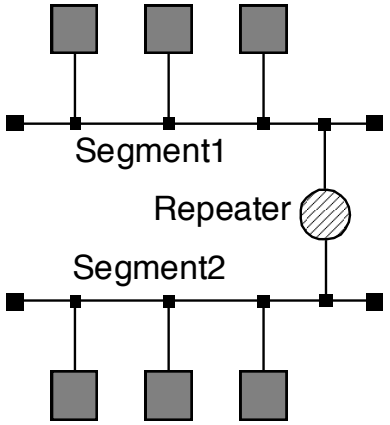
⇒ specified minimum payload is 46 bytes => 50 µs per frame at 10Mbit/s

⇒ in practice maximum distance is around 2500m for basic Ethernet

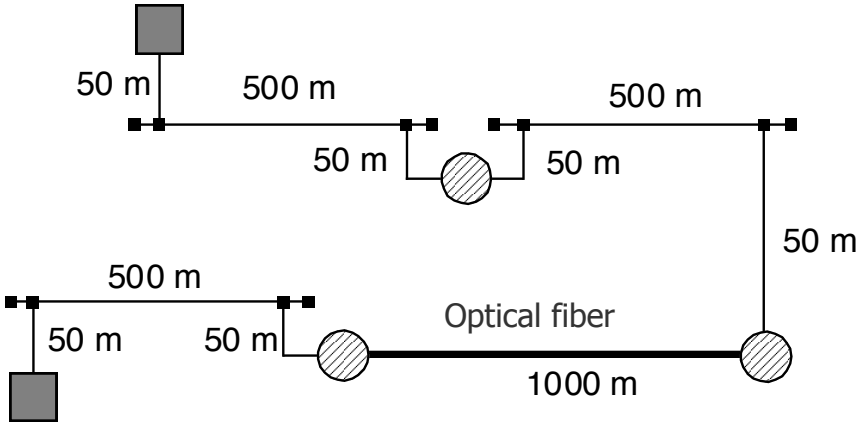
Ethernet: Segments, Repeaters, Maximum Range



Basic configuration: segment



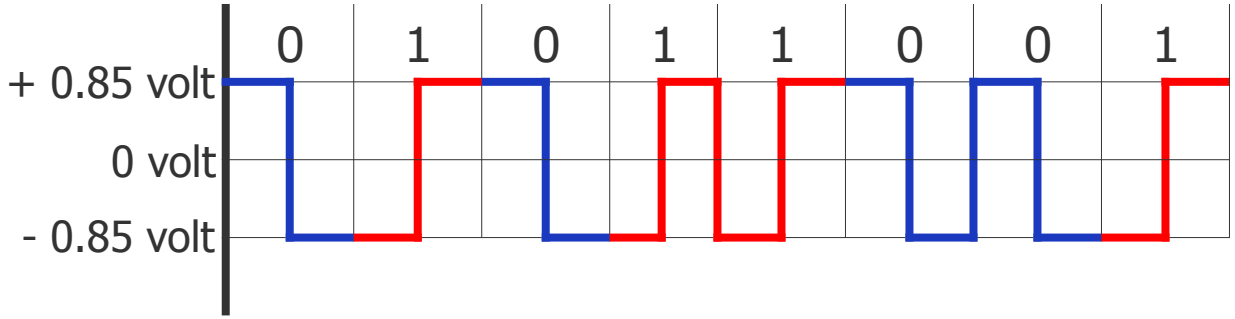
Connection of segments through a repeater



Ethernet with maximum range

Ethernet: on the Physical Layer

- The physical layer used with basic Ethernet is **baseband**
- Encoding used is **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



- Advantages:
  - Clock synchronization with each bit
  - no direct current

- Drawbacks:
  - Half the bandwidth is "wasted", i.e., to send 10Mbit/s, 20MHz is required

Ethernet Standards

Based on IEEE 802.3 "CSMA/CD"

6 classes of Ethernet variants:

- Basic Ethernet ➡ 10 Mbps
- Fast Ethernet ➡ 100 Mbps
- Gigabit Ethernet ➡ 1,000 Mbps
- 10Gigabit Ethernet ➡ 10,000 Mbps
- 40Gigabit Ethernet ➡ 40,000 Mbps
- 100Gigabit Ethernet ➡ 100,000 Mbps

http://www.ethernetalliance.org

Examples of specific name variants:

- 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

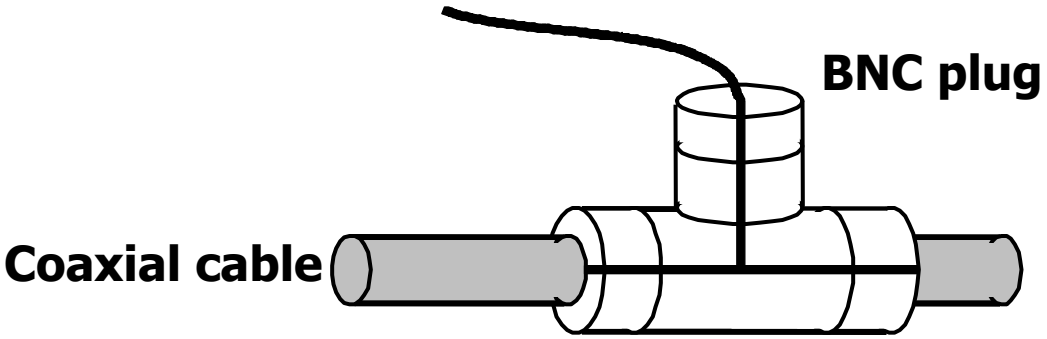
Ethernet Standards: Typical Parameter Values

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

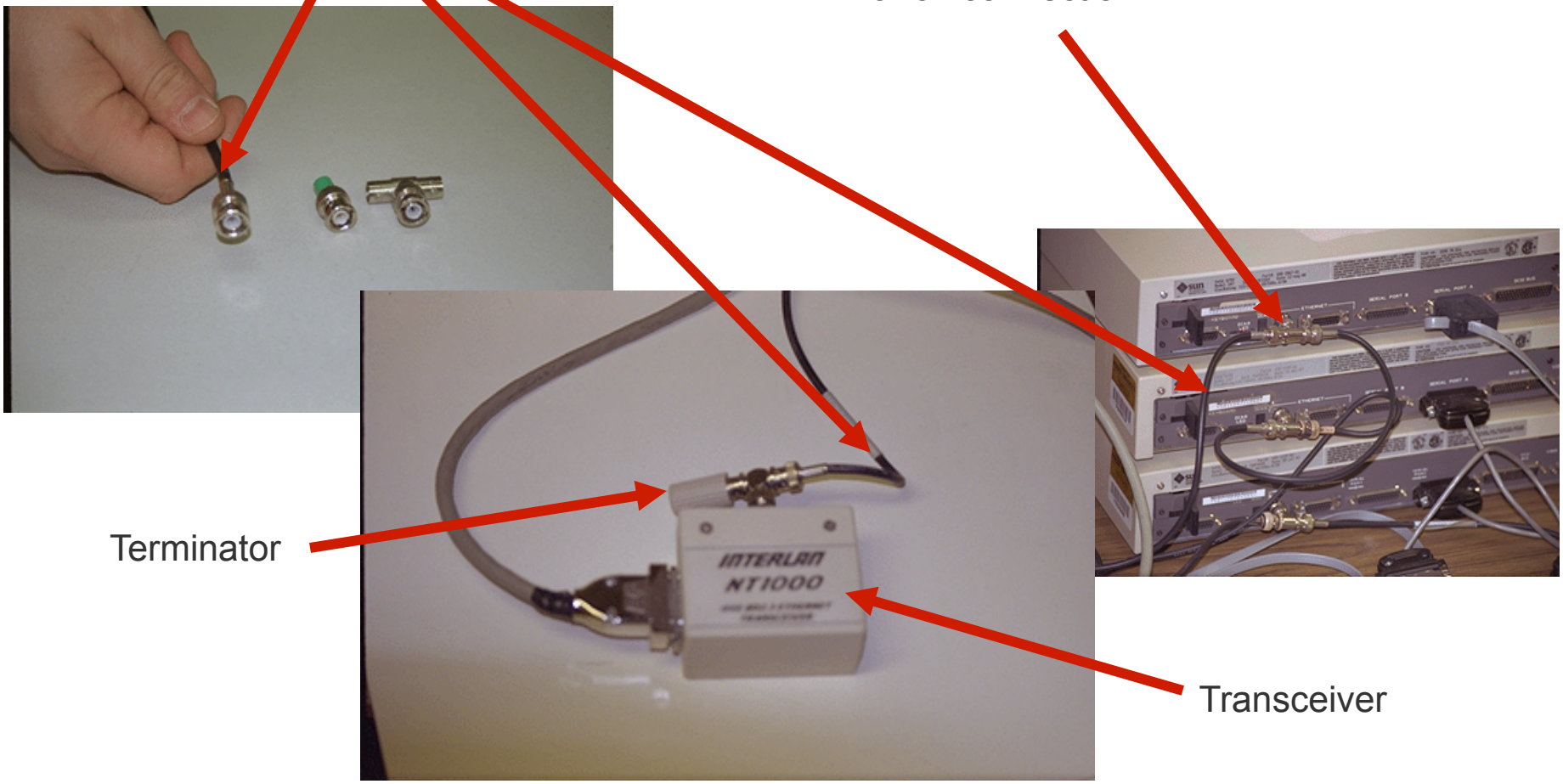
Remark: some parameters depend on the variant, e.g., the minimum frame length, due to different signal propagation delay on different mediums (e.g. fiber *vs* copper)

Ethernet Standards: 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

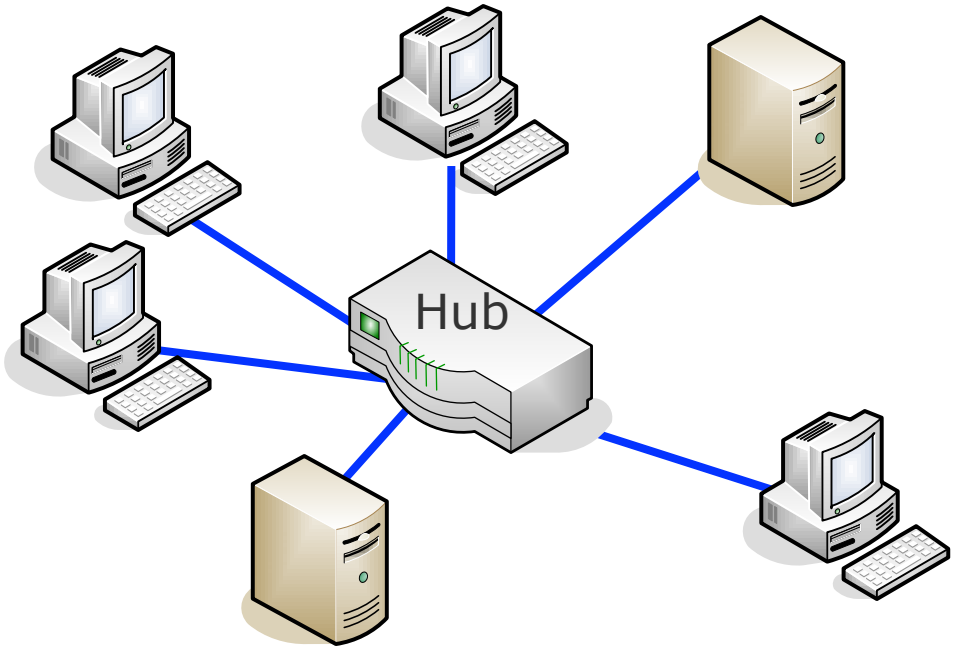


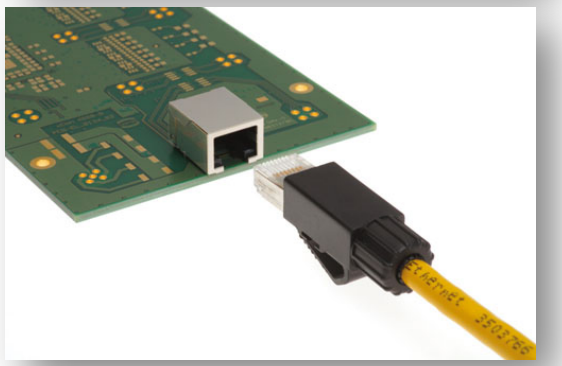
Ethernet Standards: 10Base-2 (Cheapernet)



Ethernet Standards: 10Base-T (Twisted Pair)

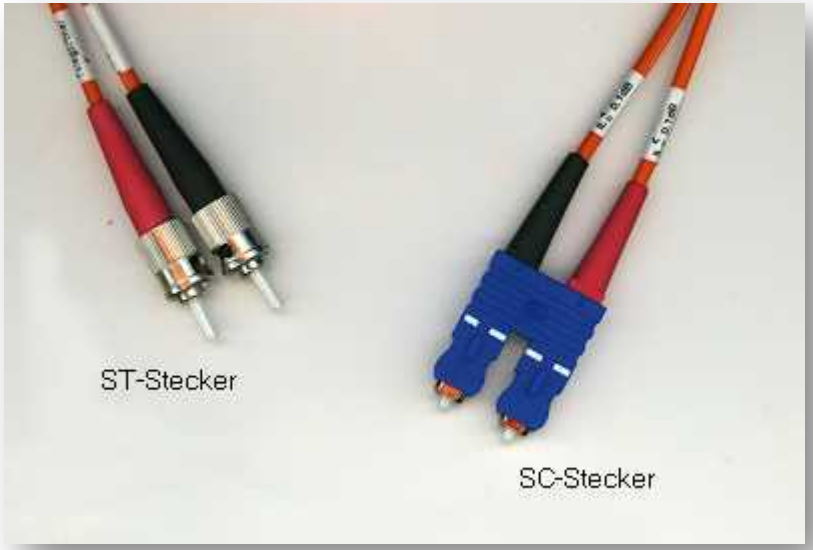
- Star topology using twisted pair: several devices are connected by a hub
- Devices are attached by a RJ-45 plug (Western plug), however only 2 of the 4 pairs of the cables are used
- Cable length to the hub max. 100 m
- Total extension thereby max. 200 m
- Long time the most commonly used variant

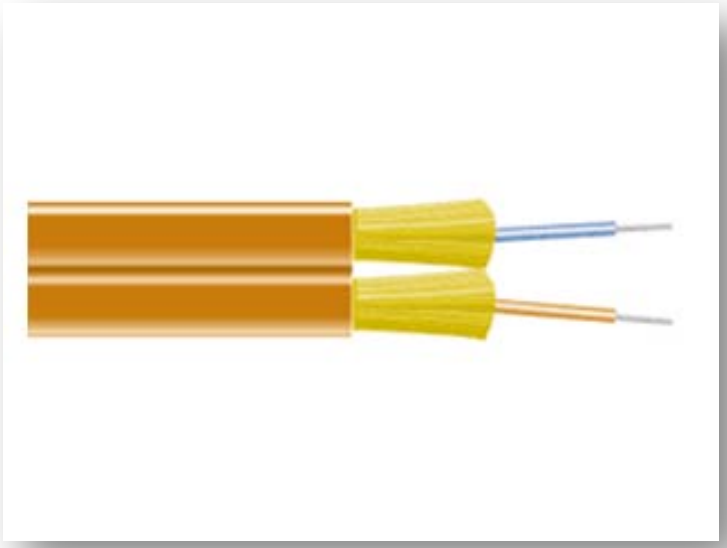




Ethernet Standards: 10Base-F

- 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 Standards: Fast Ethernet

- Principle: still use the Ethernet basics, but make it faster
  - Compatibility with existing Ethernet networks
  - Its concept is based on **10Base-T** with a central **hub** or **switch**.
  - 100 Mbps as data transmission rate, achieved by better technology, more efficient codes, utilization of several pairs of cables…
  - 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 around 200 meters …
- Auto configuration of NICs
  - Negotiation of speed
  - Negotiation on communication mode (half-duplex, full-duplex)

Ethernet Standards: 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 Mbit/s 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 Standards: Gigabit Ethernet

- 1998: the IEEE standardized **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"
- Solution: a new **minimum frame length of 512 byte** was specified
  - Extension of the standard frame by a 'nodata' field (after the FCS, because of compatibility to Ethernet). This procedure is called **Carrier Extension**.
  - nodata is added by the hardware, the software part is kept unaware
  - When a frame is passed on from a Gigabit Ethernet to a Fast Ethernet, the 'nodata' part is simply removed

Ethernet Standards: Gigabit Ethernet

- Auto configuration of NICs as in Fast Ethernet
  - data, half-duplex, duplex, …
- 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.

- Usually, with Gigabit Ethernet, switches are used instead of hubs
  - No collisions ➡ **maximum cable length** only determined by signal absorption.
  - Appropriate for backbone connections in a MAN

Ethernet Standards: 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
- Appropriate for MANs!

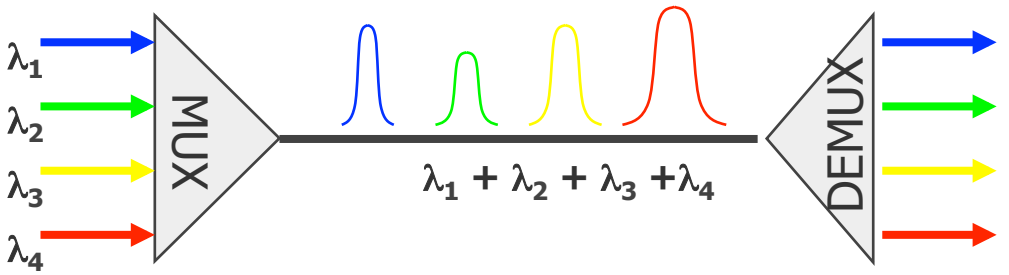
Ethernet Standards: 10-Gigabit Ethernet

- 10-Gigabit Ethernet, **IEEE 802.3ae**
  - Star topology using a switch and optical fibers
  - 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)

Ethernet Standards: 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

serial: only one transmission at a time
WWDM: wavelength division multiplexing => several transmissions in parallel
S: short
L: long
E: extended

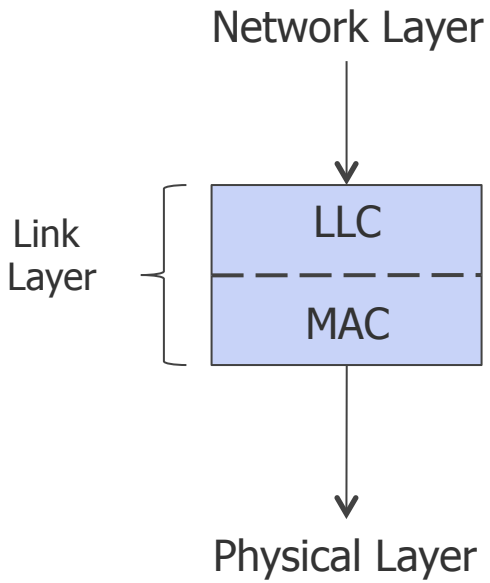


Ethernet Standards: Other High End Variants

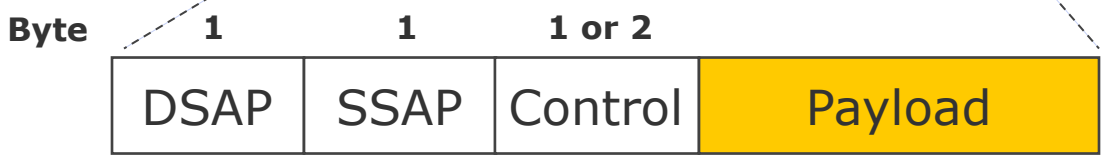
- 10G variants on copper (impossible only a few years ago!)
  - **IEEE 802.3ak**: 10GBASE-CX4 (Coax)
    - Four pairs of cable for each direction
    - Cable length of up to 15 meters …
  - **IEEE 802.3an**: 10GBASE-T (Cat. 6/7 TP)
    - Cat6 (50 meters) or Cat7 (100 meters) cabling
    - Use of all 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 …
- 40G and 100G variants specified recently in IEEE Std 802.3ba-2010
  - **40GBASE-T:** 4 twisted pairs at 10G each
  - **100GBASE-CR4:** 4 twisted pairs at 25G each

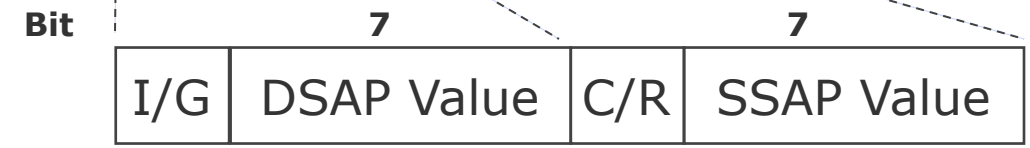
Ethernet Standards: Logical Link Control (IEEE 802.2)

- Ethernet and IEEE 802.3 MAC protocols offer only best effort
  - Unreliable datagram service (no acknowledgements)
- Logical Link Control (LLC) interfaces with network layer to provide:
  - Unreliable datagram service
  - Acknowledged datagram service
  - Reliable connection oriented service
- LLC standardized as IEEE 802.2
- LLC header contains
  - Destination access point ➡ Which process to deliver?
  - Source access point
  - Control field ➡ Seq- and ack-numbers

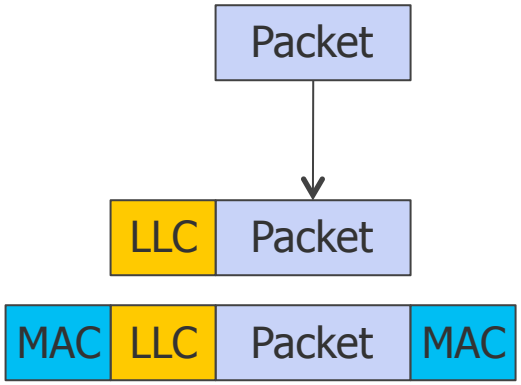


Ethernet Standards: IEEE 802.2 Header





LLC Encapsulation



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

CONTENT of this CHAPTER

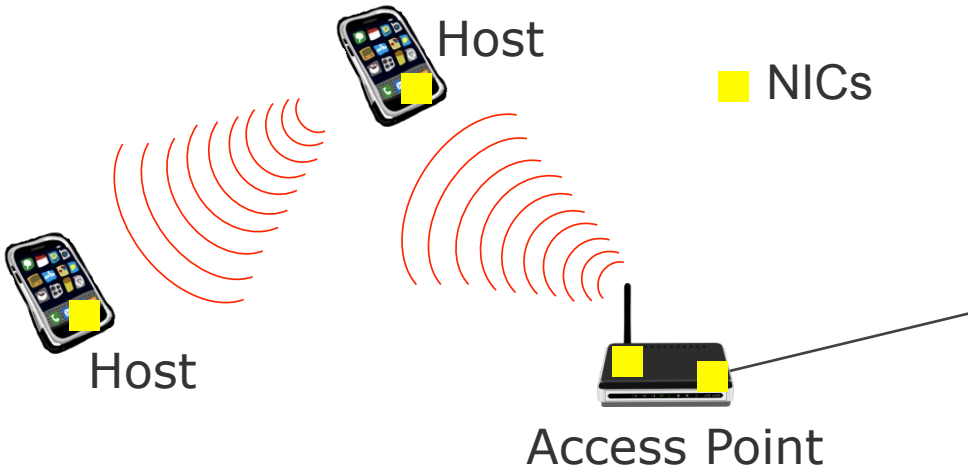
- Framing
- Error Detection & Correction
- Flow control
- Multiple Access Control

- Protocols
  - PPP
  - Ethernet
  - Wifi
  - ATM
  - SDH

- Infrastructure
  - Physical elements
  - Virtual LANs

WiFi: Components

- Two types of components that communicate
  - Access Point (AP)
    - e.g. DSL box at home
  - Wireless NIC on hosts
    - e.g. smartphone, tablet, laptop

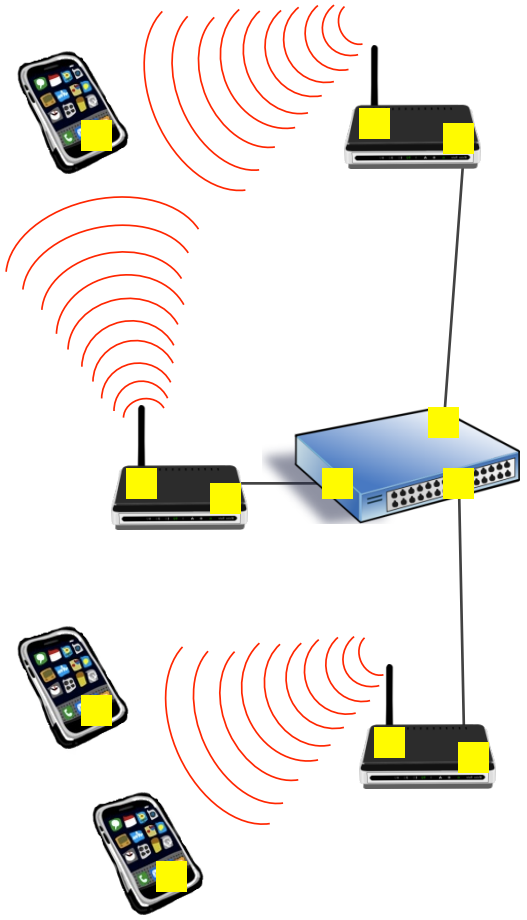


- Two modes of operation:
  - infrastructure mode
    - hosts to/from AP
  - ad hoc mode
    - host to host, without AP involved
    - Specified but not systematically implemented/tested (typically there are issues)

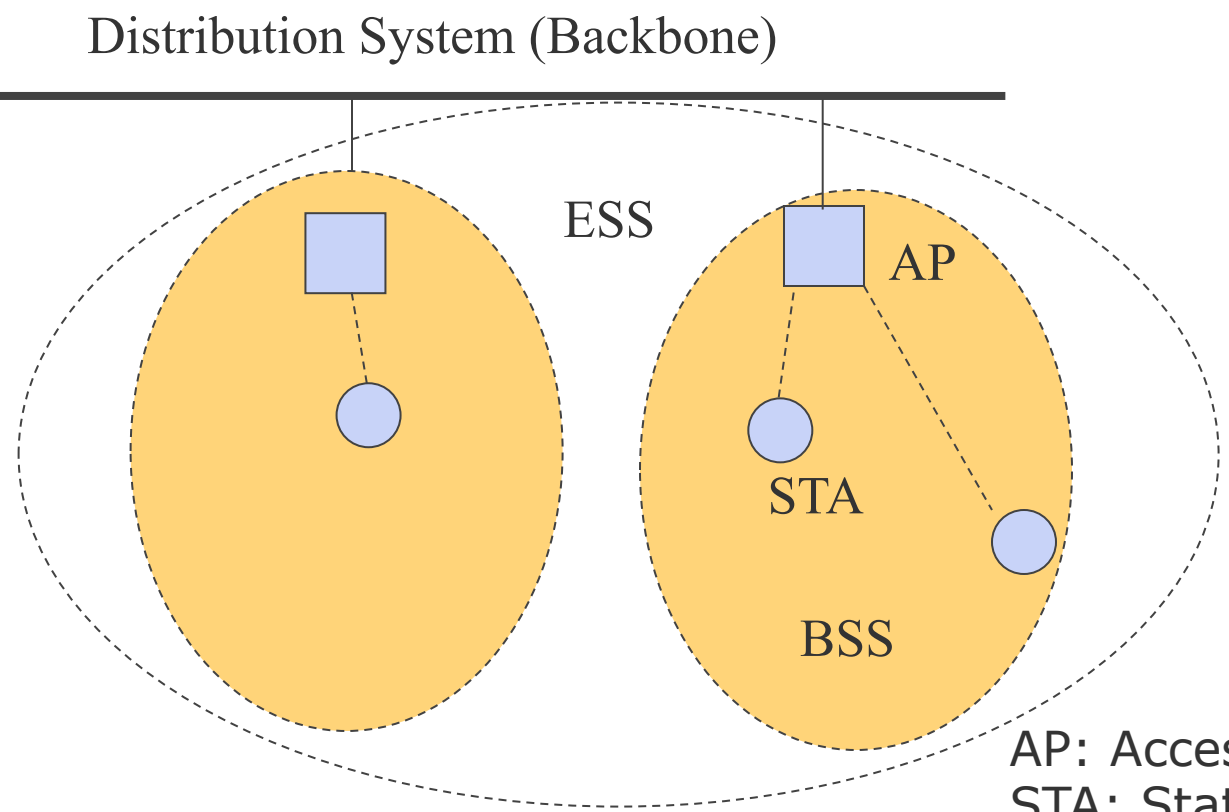
- WiFi infrastructure mode made to look as much as possible as Ethernet
  - Similarity to Ethernet star topology with a central repeater (hub)
  - Use of MAC addresses of 6 bytes like in Ethernet.

WiFi: Roaming & Wireless Mesh Networks

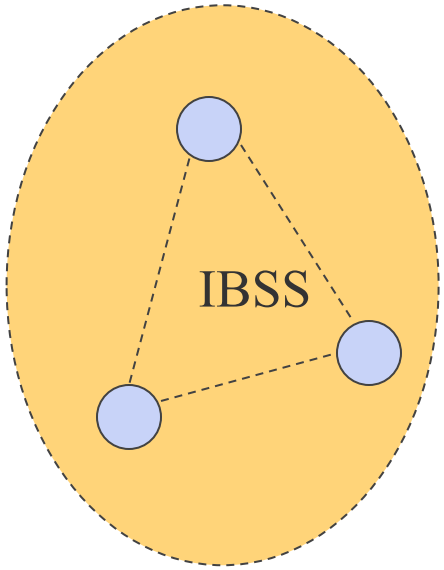
- Campus roaming configuration with a backbone of APs wired together via a switch
  - Users can move about within reachability of the AP backbone
  - Users can start a session on one AP and continue it on an other AP without interruption
  - e.g. of deployment: eduroam
- Wireless mesh network: wireless connectivity in the backbone of APs
  - Community mesh networks such as Freifunk have been deployed successfully
  - Other deployments (municipal efforts like Google Wifi coverage project in Mountain view) have not been so successful



WiFi: Terminology



infrastructure mode



ad hoc mode

AP: Access Point
STA: Station (=host)
BSS: Basic Set Service
ESS: Extended Set Service
IBSS: Independent Basic Set Service

WiFi: Wireless Channel

- 12 radio channels around 2.4GHz
  - in some countries 13 or 14
- Maximum 3 non-overlapping channels
  - if 14 channels then 4 are possible

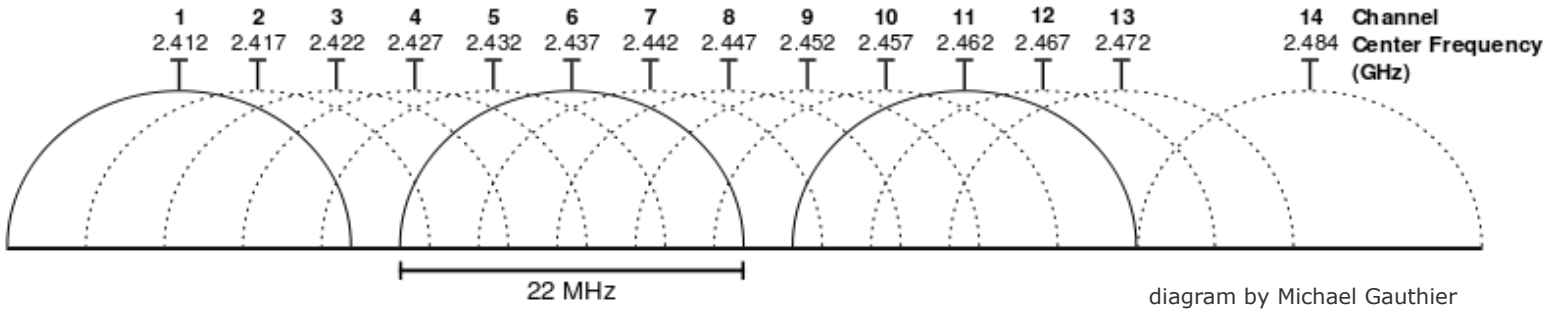
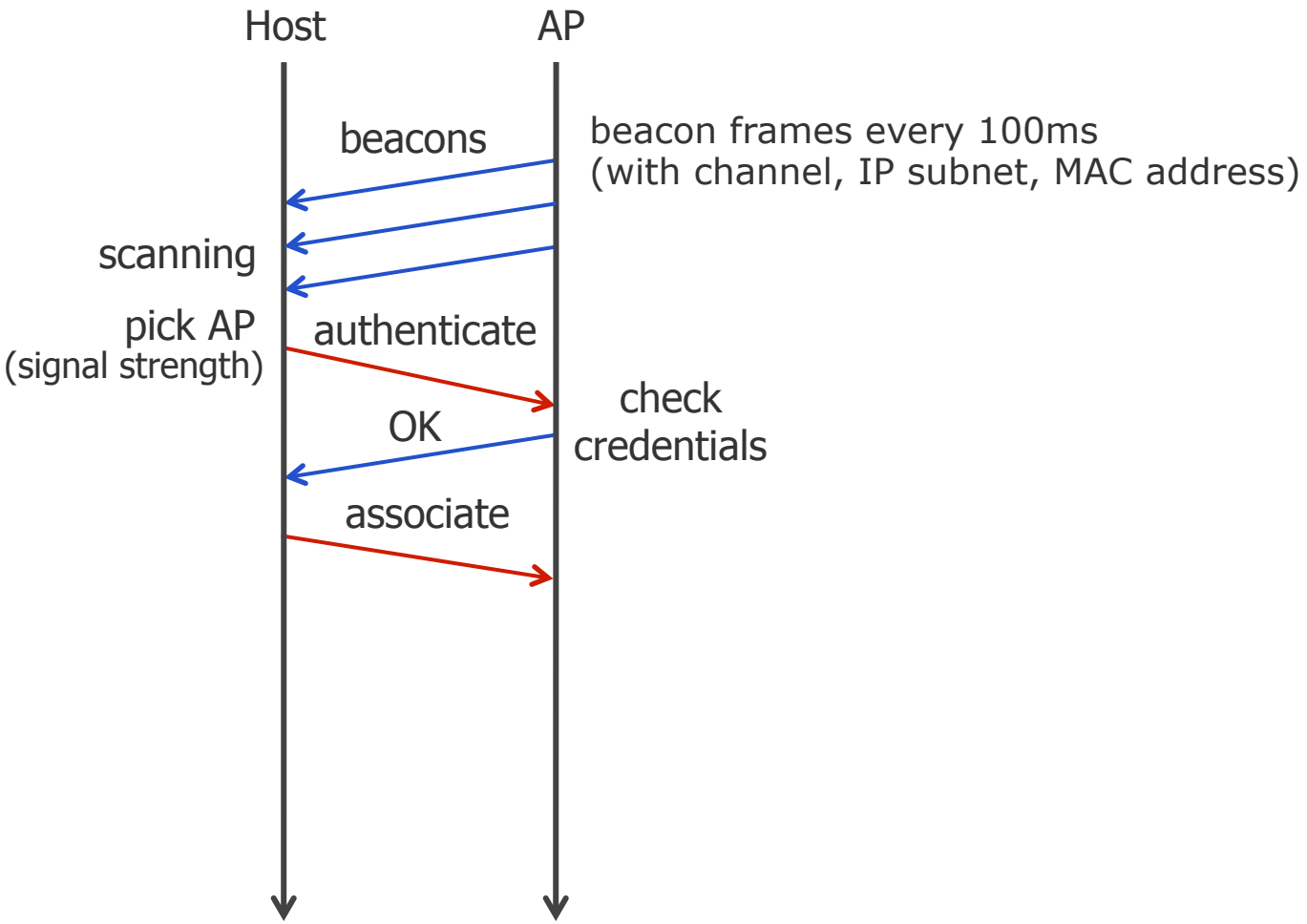


diagram by Michael Gauthier

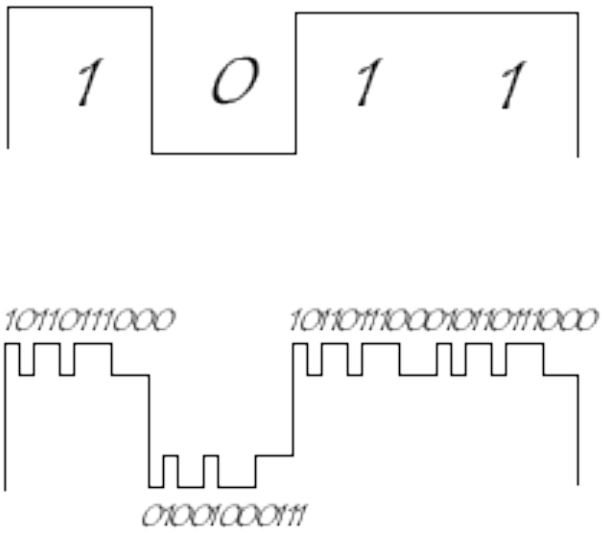
- A wireless link is very different from a wired link
  - very noisy, orders of magnitude more than wire
    - losses as high as 90-100% are not rare
  - overlapping channels = collisions
    - interference happens at the receiver (hidden terminal problem)
    - sender may not realize there is a collision

WiFi: Host – Access Point Association Process



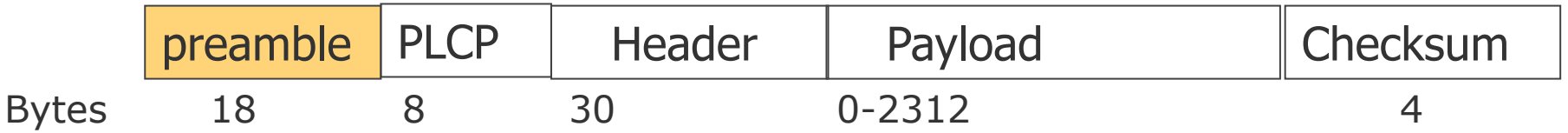
WiFi: Some Coding Techniques used in WiFi

- Encoding: spread spectrum code
  - Each data bit encoded by a 11 bits Barker pseudo–random sequence (10110111000)



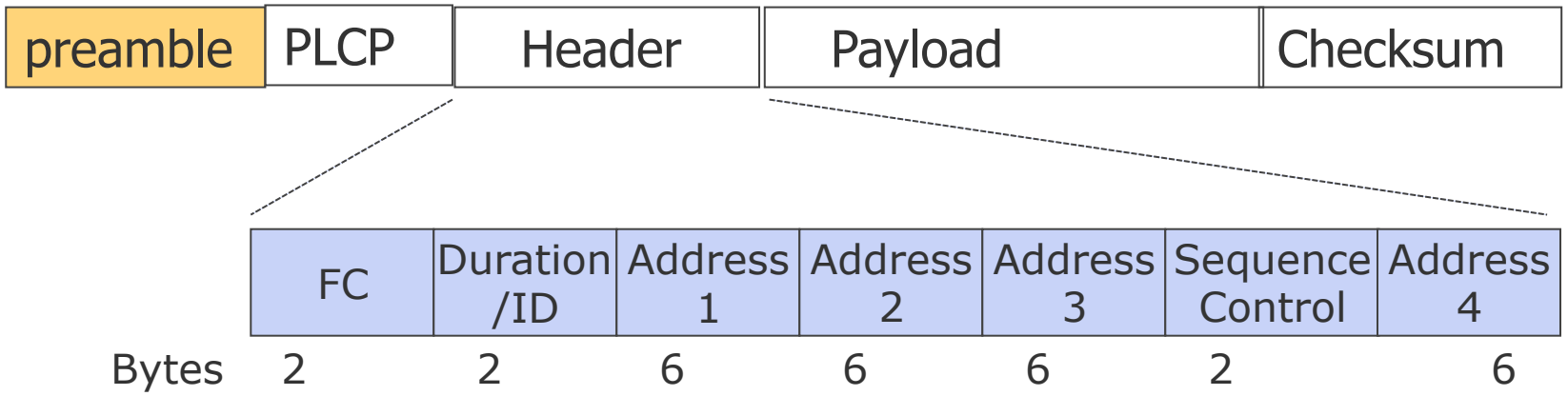
- Modulation using phase shifting
  - Differential PSK, Differential QPSK… depending on mode

WiFi: Frame Format



- **Preamble** (18 bytes): shorter version of 9 bytes is also specified
- **PCLP** (8 bytes): Physical Layer Convergence Procedure. Indicates modulation scheme
- **Header** (30 bytes): indicates source and destination addresses etc.
- **Payload** (max 2312 bytes): can be zero with control/management frames
- **Checksum** (4 bytes): a 32 bit CRC

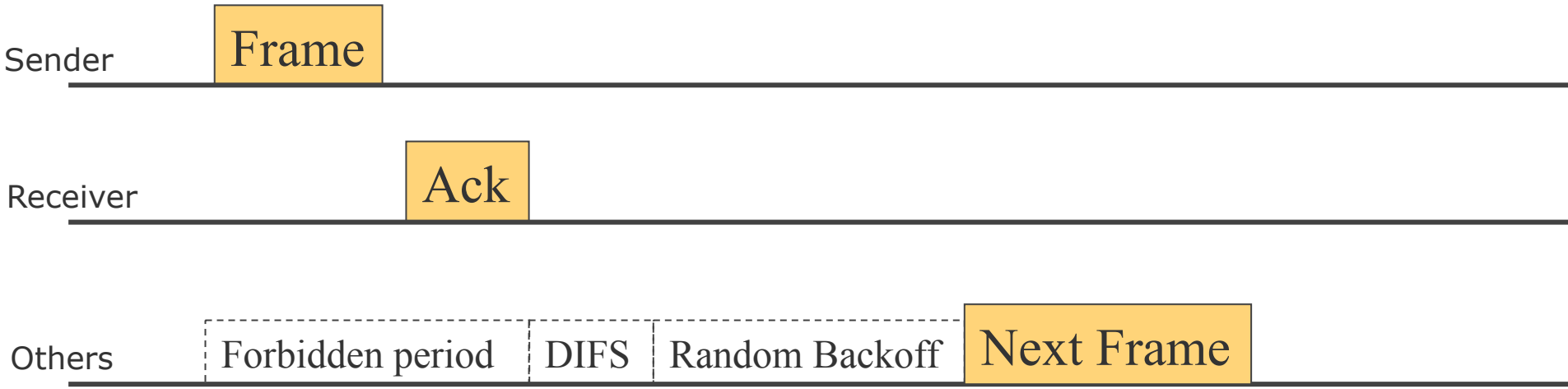
WiFi: Frame Format



- **FC** (2 bytes): Frame Control. Indicates protocol version, frame type (various types of control frames, management frames, data frames)
- **Duration/ID** (2 bytes): indicates the number of microseconds expected to transmit the frame
- **Addresses** (6 bytes each): (1) receiver, (2) transmitter (physical), (3) and (4) are situation-dependent, can be BSS identifier, original sender, final destination, or can even be elided.
- **Sequence Control** (2 bytes): sequence number and fragment number

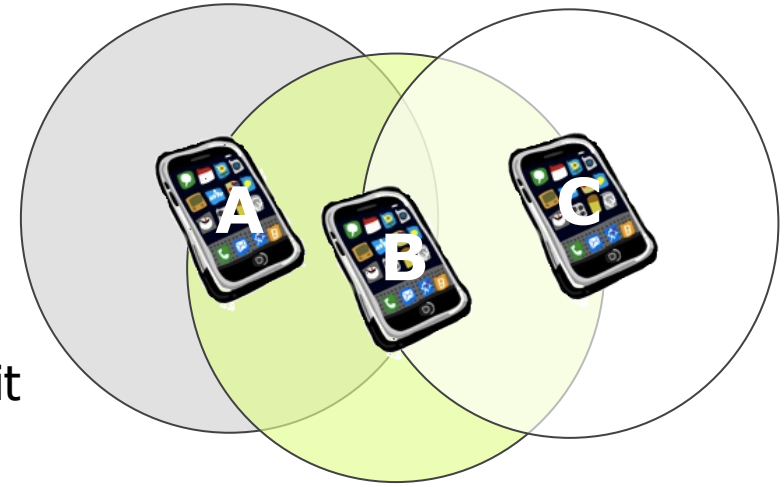
WiFi: Multiple Access Mechanism

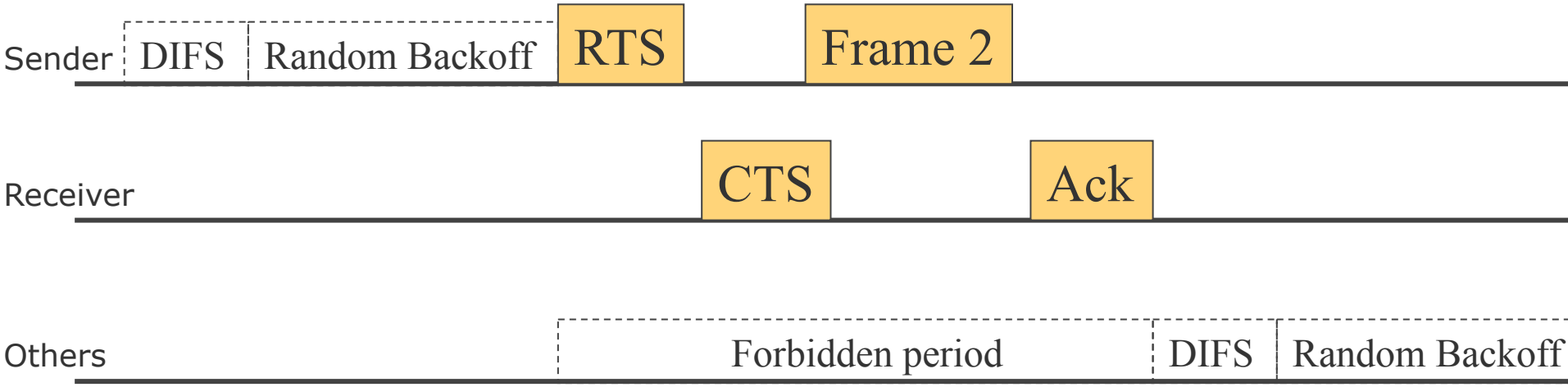
- Receiver acknowledges correctly received frames
  - On wireless, only the receiver can detect collisions
  - If a wireless host transmits its transmission will dwarf any attempt to listen
- Multiple access based on CSMA/CA
  - Step 1: medium busy detected by other potential senders
  - When the medium is free again, hosts that want to send wait for:
    - A deterministic period DIFS (Interframe Space) configured on each host
    - Then a random backoff, (re)drawn for each (re)transmission
    - The first host that has its backoff that fires transmits.
    - Others hear the transmission and go back to step 1



WiFi: Optional Channel Reservation Step

- Problem: potential senders may not hear each other
  - Hidden node problem e.g. A and C want to send to B
- Solution: channel reservation
  - Sender first asks for permission to send
    - RTS (Request to Send)
  - Receiver grants permission to send
    - CTS (Clear to Send)
  - Other hosts wanting to send refrain to transmit





WiFi: Access Priorities, Exponential Backoff

- Priorities
  - By configuring shorter and longer DIFS on different hosts, different priority
    - Longer DIFS => lower priority
  - When a hosts is waiting for its backoff timer to fire and hears another host starting to transmit, it freezes its timer until the next DIFS is over
    - New contenders for the channel have lower priority
- Binary Exponential Backoff (BEB)
  - Backoff is a random number of mini-slots between 0 and C_{max}-1
    - 1 mini-slot < DIFS
  - Double C_{max} upon detecting a collision (= lack of ACK or lack of CTS)
  - Limited number of attempts for retransmissions
    - Configurable max_retry (7-16)

WiFi Standards: From Previous Millenium

- IEEE 802.11 b
  - Standard published in 1999
  - Max 11 MBit/s (unidirectional communication, not counting headers, interferences, obstacles)
  - In practice, 5 Mbit/s in the best case
  - 3 non-overlapping channels at 2.4GHz
  - Approx. 90 meters range
  - Older devices use still use this standard

- IEEE 802.11 a
  - Standard published in 1999
  - Max 54 Mbit/s
  - 8 non-overlapping channels in the 5GHz band
  - Higher frequency => shorter wavelength => smaller range: approx. 30 meters
    - less easy to go through walls & around corners (physics)
  - 802.11 a was not very successful and soon replaced by newer 802.11 standards

WiFi Standards: Why 2,4GHz and 5GHz bands?

- 2,4GHz and 5GHz bands do not have the best properties
  - Not very effective through walls, obstacles, vegetation
  - Absorbed by water: human bodies, animals, rain affect connectivity/throughput
  - Noisy (microwave ovens, baby monitors and cordless telephones use these bands)
- Better frequency bands are reserved/licensed
  - e.g. 700MHz band used by analog TV broadcast
  - Given away for free a century ago. Worth trillions of euros nowadays!
- Unlicenced frequency bands for industrial, scientific and medical (ISM band)
  - These bands were initially considered as being « junk spectrum »
  - But: triumph of technology, trillion industry! Millions of NICs sold *each day*.
- Plan was to transition from analog TV broadcast to digital TV broadcast
  - Digital uses less spectrum than analog
  - Freed-up spectrum for data communication, extending IMS? 4G? 5G?

WiFi Standards: Current Standards

- IEEE 802.11 g
  - Standard published in 2003
  - Max 54 MBit/s
  - 3 non-overlapping channels at 2.4GHz (using OFDM)
  - Approx. 90 meters range
  - Easy transition with backward compatibility, multimode a/b/g access points
  - Most devices use this standard nowadays

- IEEE 802.11 n
  - Standard published in 2009
  - Max 108 MBit/s, enough for HDTV wireless streaming (single user, at home)
  - 1 channel at 2,4GHz (channel binding, MIMO, 64-QAM modulation)
  - Approx. 90 meters range
  - Easy transition with multimode a/b/g/n access points
  - Newer devices use this standard

WiFi Standards: Other Standards

- IEEE 802.11 ac
  - Expected in 2014
  - Around 1GBit/s
  - 1 channel at 5GHz (channel binding, MIMO, 256-QAM modulation)

- IEEE 802.11r
  - Published in 2008
  - Standard specifying roaming for AP backbone
  - Fast transitions between access points by redefining the security key negotiation protocol, allowing both the negotiation and requests for wireless resources (similar to RSVP but defined in 802.11e) to occur in parallel.

WiFi: Wireless Security & Privacy

- Requirements: authentication and over-the-air privacy
- Solution: WEP (Wired-Equivalent Privacy)
  - Authentification and encryption based on secret symmetric key K
    - e.g. shared WiFi password configured at home on a DSL box
  - When a host requires authentification the AP sends a challenge (128 random bits)
    - The terminal returns the 128 bits xored with the key K
    - The access point checks the challenge response and confirms authentification
  - In larger entreprise deployments (e.g. eduroam) the AP can be configured to check authentication via a remote server (to which it is connected via a switch)
- Problem: WEP is easily breakable with a man-in-the-middle attack
  - Eavesdropping can provide the key K via simple comparison between challenge and terminal reply!
  - Breakable in less than 30 seconds with state of the art harware/software
- Improvement: WPA (WiFi Protected Access), and WPA2
  - Uses a per-packet key

CONTENT of this CHAPTER

- Framing
- Error Detection & Correction
- Flow control
- Multiple Access Control

- Protocols
  - PPP
  - Ethernet
  - Wifi
  - ATM
  - SDH

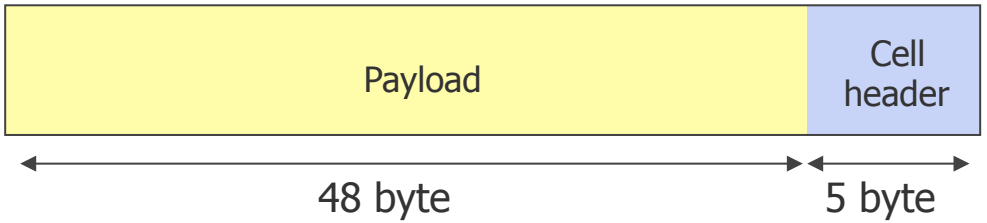
- Infrastructure
  - Physical elements
  - Virtual LANs

ATM: Characteristics

- Characteristics of ATM
  - The telco's response to the rise of data networks and the Internet in the 1990s
  - ITU-T standard (resp. ATM forum) for simultaneous data, speech, and video transmissions. Data rates: 34, 155, or 622 Mbit/s (on optical fiber)
  - Cell-based multiplexing & switching technology combines advantages of
    - Circuit Switching (granted capacity and constant delay)
    - Packet Switching (flexible and efficient transmission)
  - Connection-oriented communication: virtual circuits are established
    - Supports PVCs, SVCs, and connection-less transmission
  - Guarantee of quality criteria for the desired connection (bandwidth, delay, …)
    - For doing so, resources are being reserved in the switches.
    - No flow control or error handling

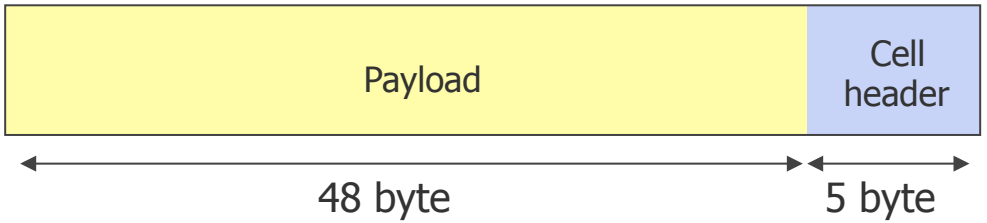
ATM: Cells & Asynchronous TDMA

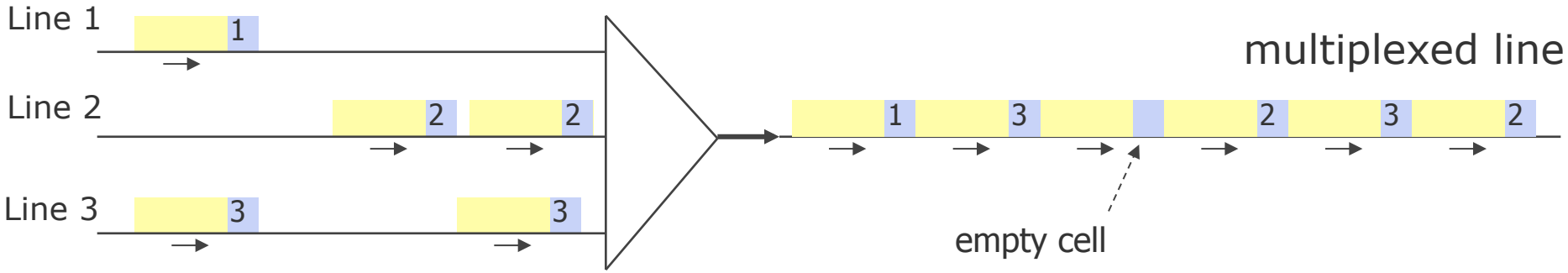
- **Cell switching**
  - Similar to packet switching, but fixed cell size: 53 byte
  - Similar to time division multiplexing, but without reserved time slots



ATM: Cells & Asynchronous TDMA

- **Cell switching**
  - Similar to packet switching, but fixed cell size: 53 byte
  - Similar to time division multiplexing, but without reserved time slots





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

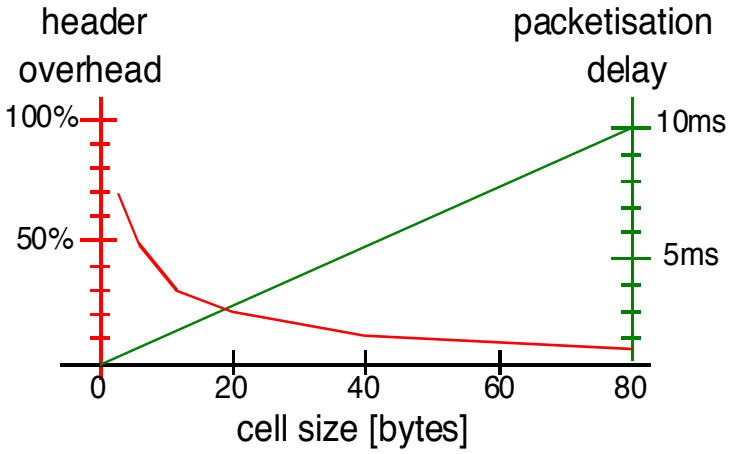
ATM: Why fixed 48 bytes payload?

Problem: big packets can cause large jitter to other streams like voice on low/medium bandwidth links

Principle: jitter is reduced if every packet has same (small) size. But what size?

- Larger cells cause unacceptable latency for voice transmission (wait to piggyback more voice samples)
- Smaller cells produce too much overhead for other types of data (relationship Header/Payload)

Solution: fixed 48 byte payload, causing 48x125µs=6ms latency, acceptable for voice transmission.

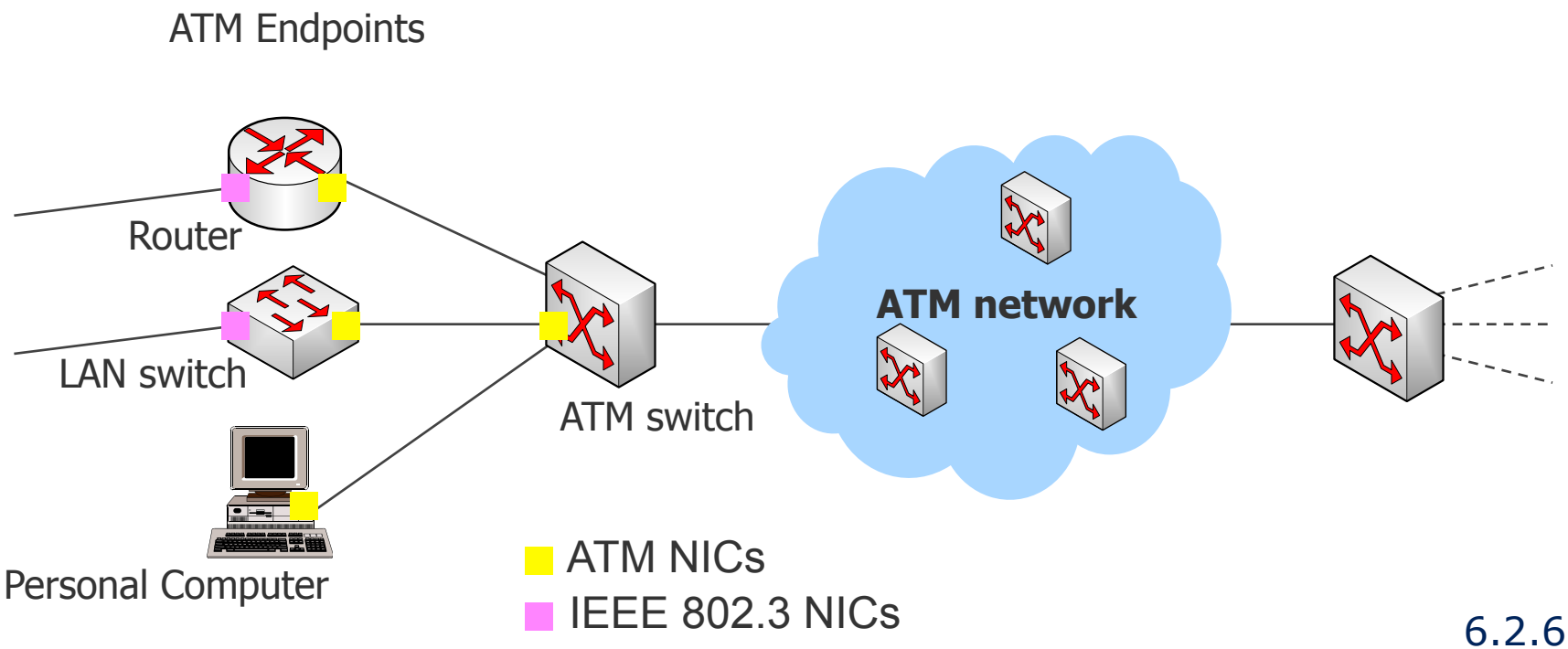


- **Nyquist sampling theorem:**
  Sampling rate > 2×cutoff frequency of the original signal
  Cutoff frequency of a phone line: 3.4 kHz
  ➡ scanning rate of 8000 Hz i.e. one sample every 125µs
- Standard acceptable quantization error for voice: discrete levels with 8 bits
- Standard voice data stream therefore has a data rate of: 8 bits × 8000 1/s = 64 kbps

With higher throughput links (1-10 Gbit/s) and typical 1500 bytes MTU data packets, jitter is not a problem for voice
➡ A technical reason explaining the few ATM deployments

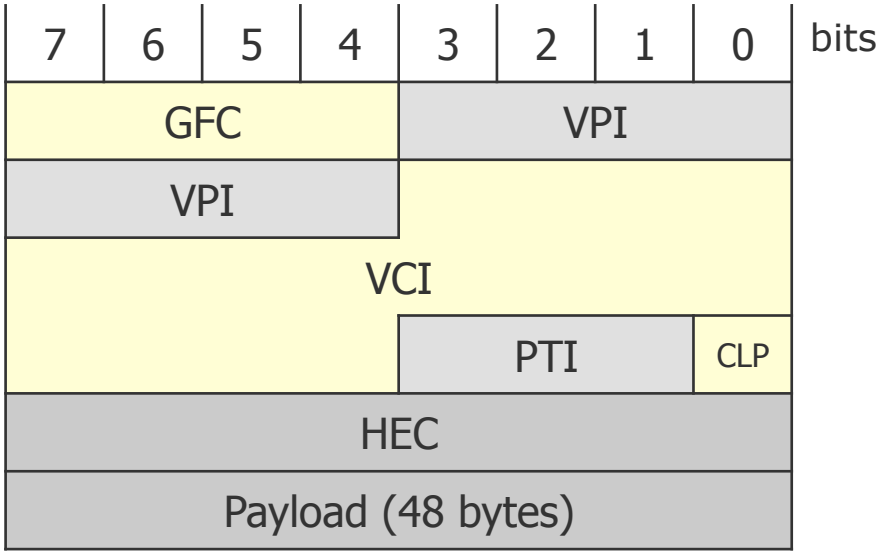
ATM: Network Elements

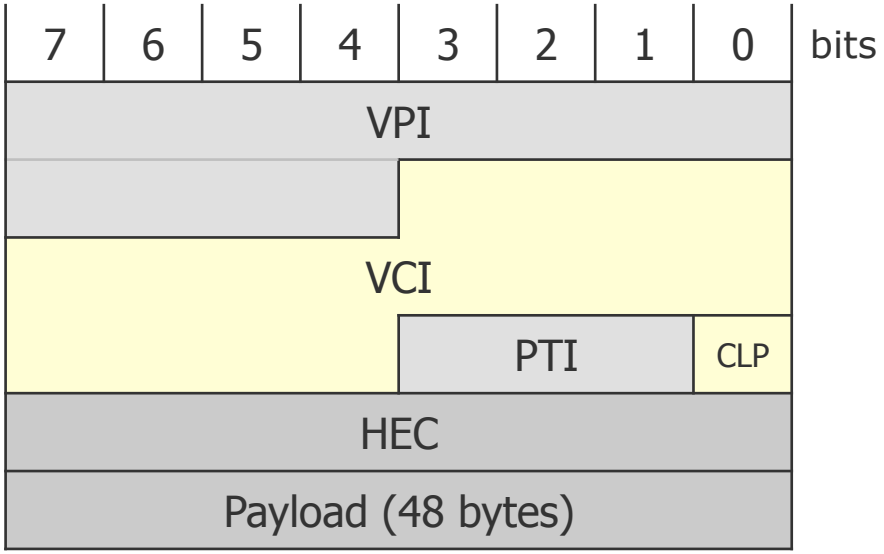
- Two types of components:
  - ATM Switch
    - Dispatching of cells through the network by switches. The cell headers of incoming cells are read and information is updated. Afterwards, the cells are switched to the destination.
  - ATM Endpoint
    - Has an ATM network interface adapter to connect different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



ATM: Frame Format

- UNI header (host to router)
  - Generic Flow Control (GFC)
    - 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)
    - Special 8 bit CRC on the first 4 bytes; single bit errors can be corrected.
- NNI header (router to router)



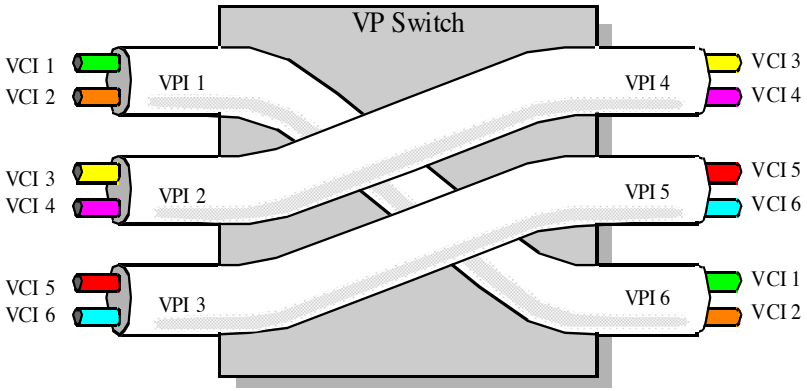


ATM: Virtual Circuits

- Physical connections "contain" **Virtual Paths** (VPs, logical pipe)
- VPs "contain" **Virtual Channels** (VCs, logical channels inside a logical pipe)
- VP, VC identifiers only have local significance (only within a given switch).
- Distinction between VPI and VCI introduces a hierarchy on the path identifiers. Advantage: Reduction of the size of the switching tables.

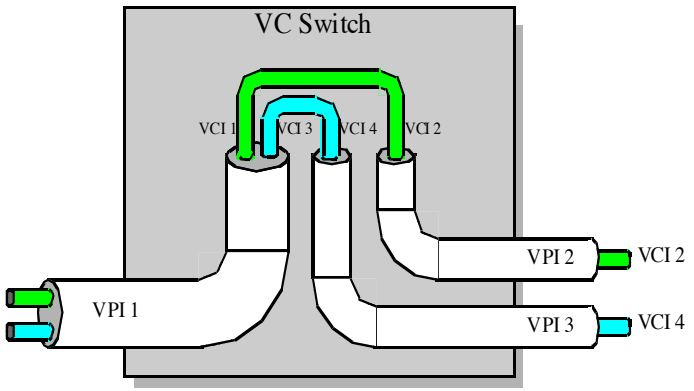
There are 2 types of switches in the ATM network:

Virtual Path Switching



VP-SWITCH

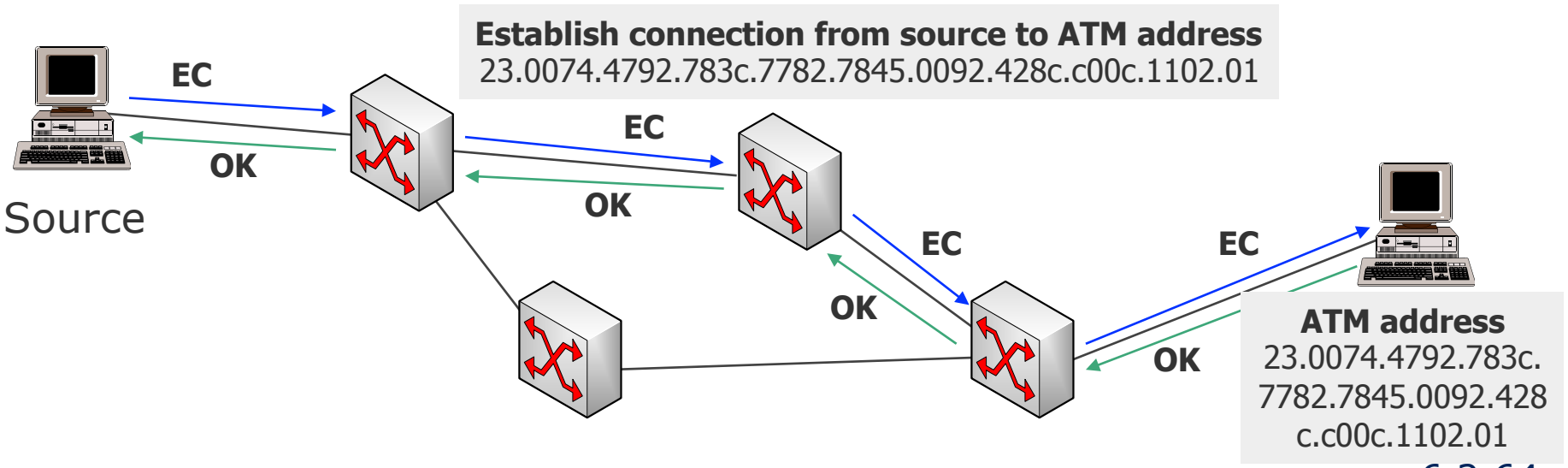
Virtual Channel Switching



VP/VC-SWITCH

ATM: Virtual Circuits

- 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: Quality of Service Classes

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:

- Moving pictures
- Telephony
- Video conferences

- Data communication
- File transfer
- Mail

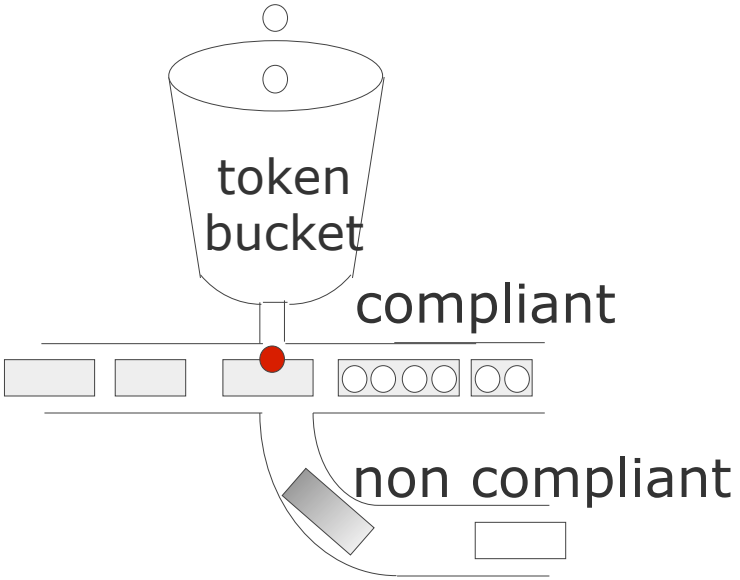
Adaptation Layers (AAL)
an AAL is the interface between ATM and applications

AAL 1	AAL 2	AAL 3	AAL 4
Constant bitrate	Variable bitrate	AAL 5 (available/unspecified birate)	

IP over ATM

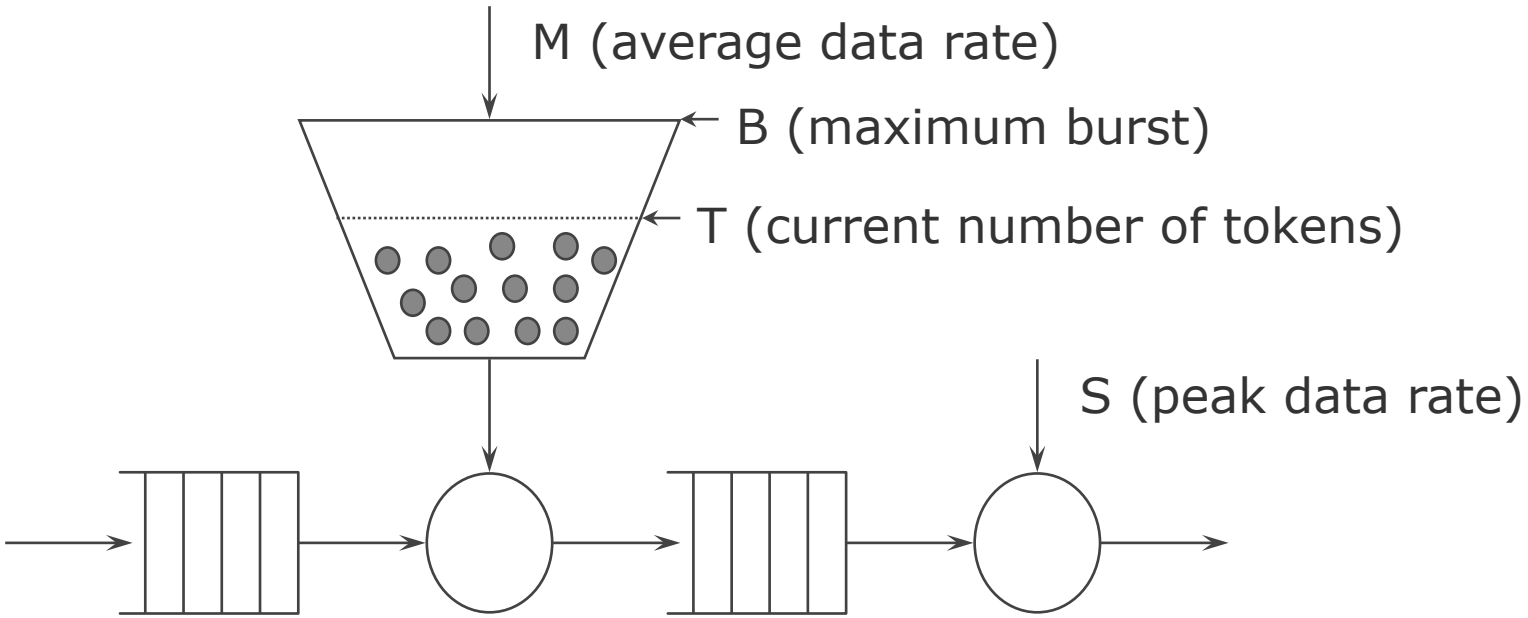
Burst Control with Token Bucket

- Goal: enforce QoS limits
- Principle: a "leak" in a bucket which is full of tokens
  - Bucket with max. B tokens
  - Tokens „refill" the bucket with rate R into the bucket
  - **Monitors average rate R (bit/s) with a tolerance (burst) B**
  - Packets marked as non compliant if too few tokens available
  - Only metering, no traffic shaping
    - Bursts conserved if shorter than B
  - Compliant traffic is processed as premium traffic (according to QoS)
  - Non-compliant traffic is processed as best-effort (might even be dropped)
  - This technique is used by ATM



ATM: Burst Control with Dual Token Bucket

- Traffic Shaping with Token-Bucket:
  - The **first bucket** is of size B bytes, bucket fill rate equals **average data rate** M byte/s in tokens
    - Packet of length L can only be sent if at least L tokens are available in the bucket, thus T ≥ L
    - Max. B bytes can pass the first bucket as a burst (plus some bytes depending on the refilling of the bucket)
  - The **second bucket** with size 1 and fill rate S defines the **peak data rate**: send a byte only if a token is available



ATM: Advantages & Drawbacks

- Advantages
  - shorter entries and simpler, faster lookup in switching table (compared to datagrams, routing table and longest prefix match)
  - More deterministic latency due to fixed cell size (compared to variable sized datagrams)
  - QoS guarantees can be established per virtual circuit / virtual channel (an be monetized)
    - Other tries at QoS in the Internet (IntServ, DifServ) failed
- Drawbacks
  - Too few applications built directly on ATM
  - TCP/IP was already in place and applications were built on top of the IP stack
  - Thus: IP over ATM (RFC 1577), LAN emulation (LANE, ATM forum)
- Today: ATM was aiming for "everything" but mostly failed to be adopted
  - SDH is nowadays dominant in WANs
  - Ethernet is nowadays dominant in LANs and MANs
  - Not much left… ATM is mostly used for DSL and for MPLS

CONTENT of this CHAPTER

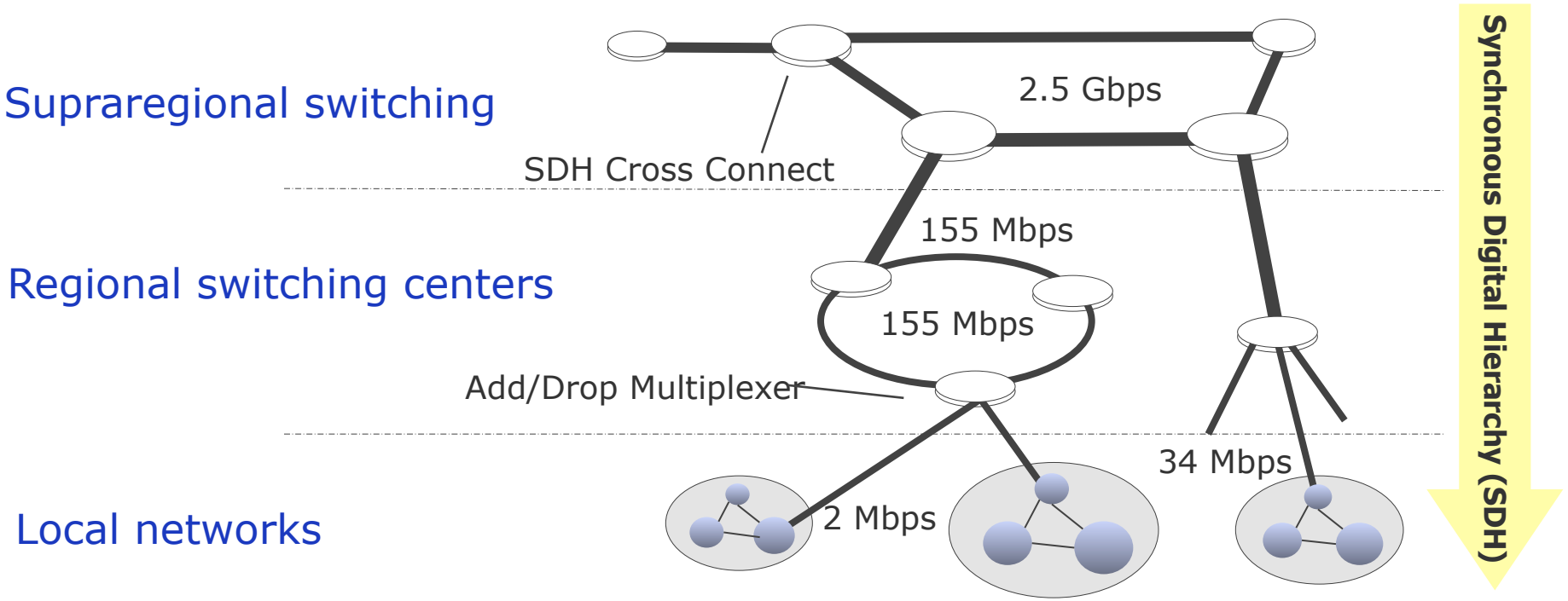
- Framing
- Error Detection & Correction
- Flow control
- Multiple Access Control

- Protocols
  - PPP
  - Ethernet
  - Wifi
  - ATM
  - SDH

- Infrastructure
  - Physical elements
  - Virtual LANs

SDH: Goals & Structure

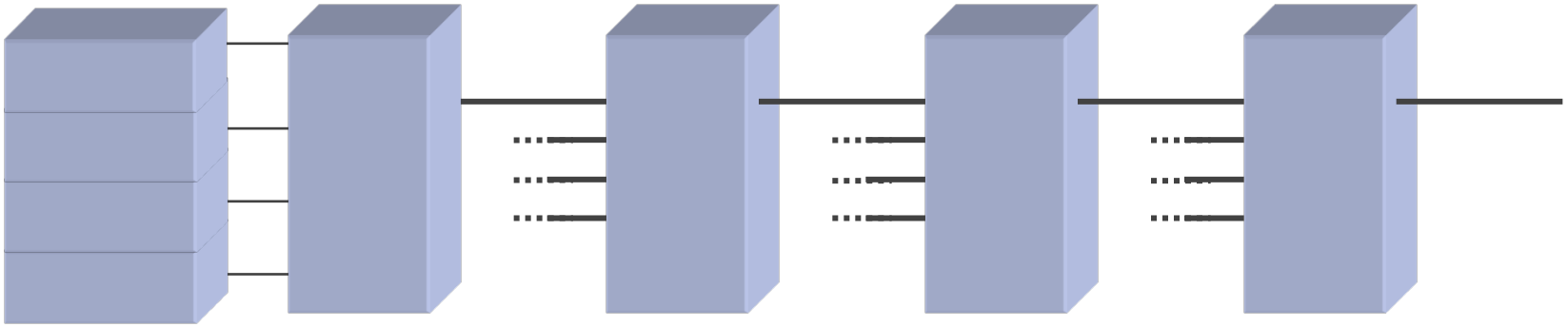
- Synchronous Digital Hierarchy (SDH)
  - Aims at flexible capacity utilization and high reliability
  - Much higher data rates than ATM (currently 40Gbit/s, and several Tbit/s are in sight)
  - Most WAN deployments now use SDH
  - Similar and interoperable US standard: SONET (SDH is the european standard)
- SDH manages arbitrary topologies with a hierarchical structure



SDH: Characteristics

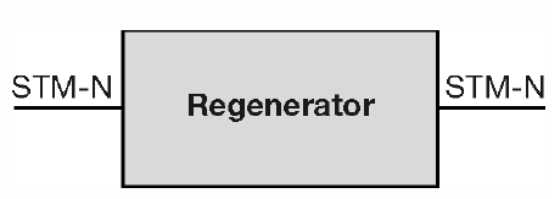
- Problem: at ultra-high data rates, no time to "synchronize" with a preamble sequence as done with PPP/Ethernet/Wifi etc.

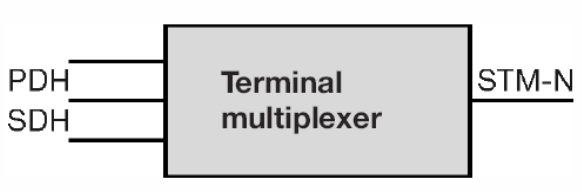
- Solution: synchronized, centrally clocked network (picosecond precision needed!)
  - Enable byte-by-byte multiplexing of high throughput data streams
  - Use **standard bit rates** on each level of the hierarchical structure
  - **Simplified multiplexing**, such that the data can experience a **constant delay** (suitable for voice transmission)
    - Direct access to signals by cross connects without repeated demultiplexing
    - Shorter delays in inserting and extracting signals (possible with standard bit rates)

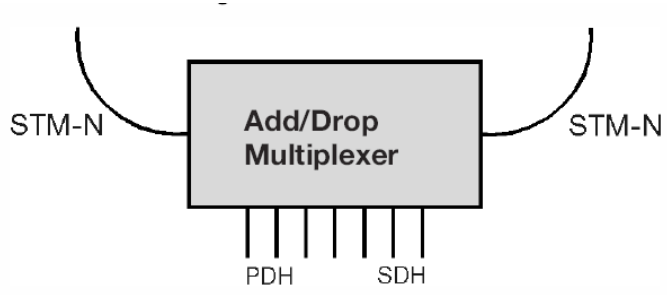


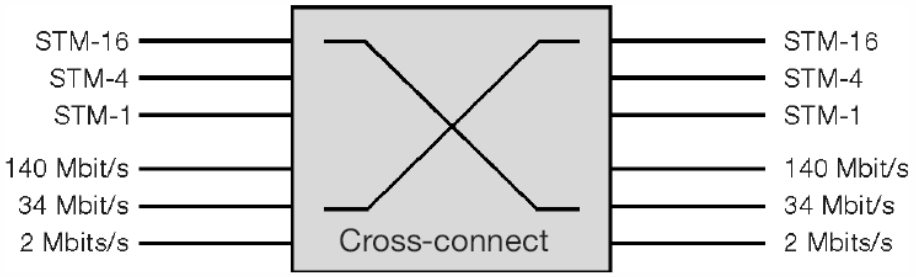
SDH: Terminology & Components

- PDH: Plesiochronous Digital Hierarchy
  - Non-synchronous input (IP, ATM…)
- Network elements
  - **Regenerator**
    - 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-Connect**
    - Mapping of PDH tributary signals into virtual containers
    - Switching of various containers

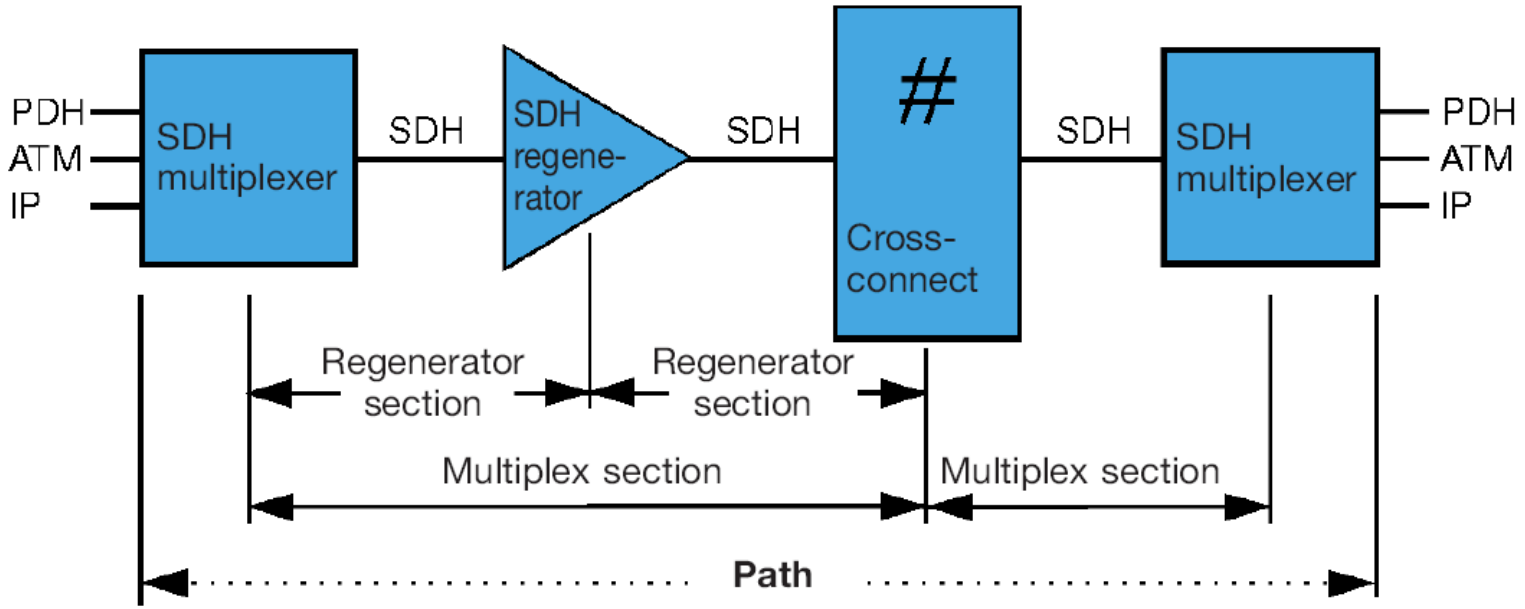






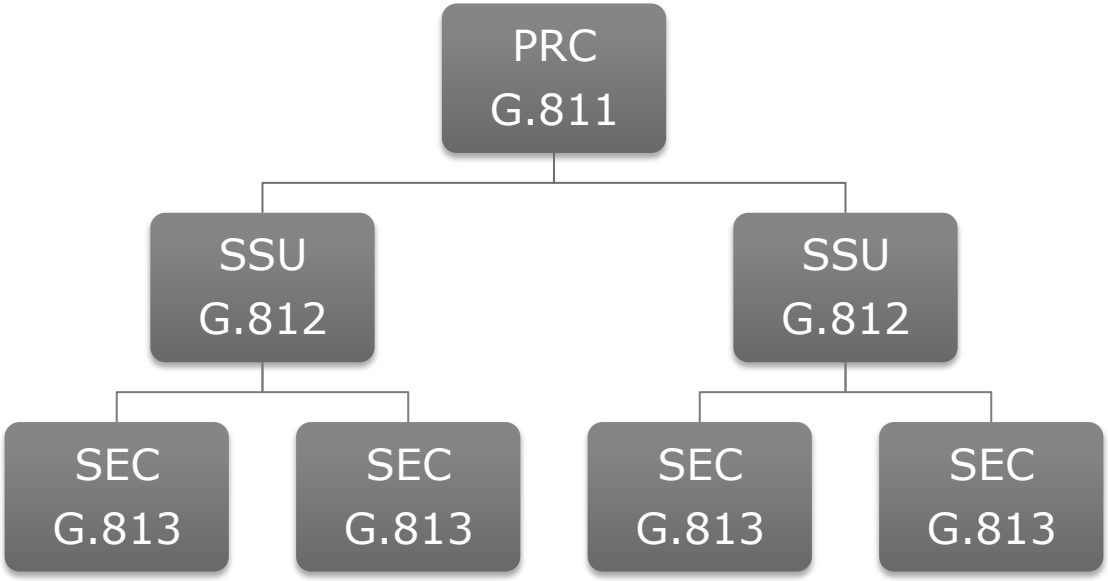


SDH: A Typical Path



SDH: Synchronization

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



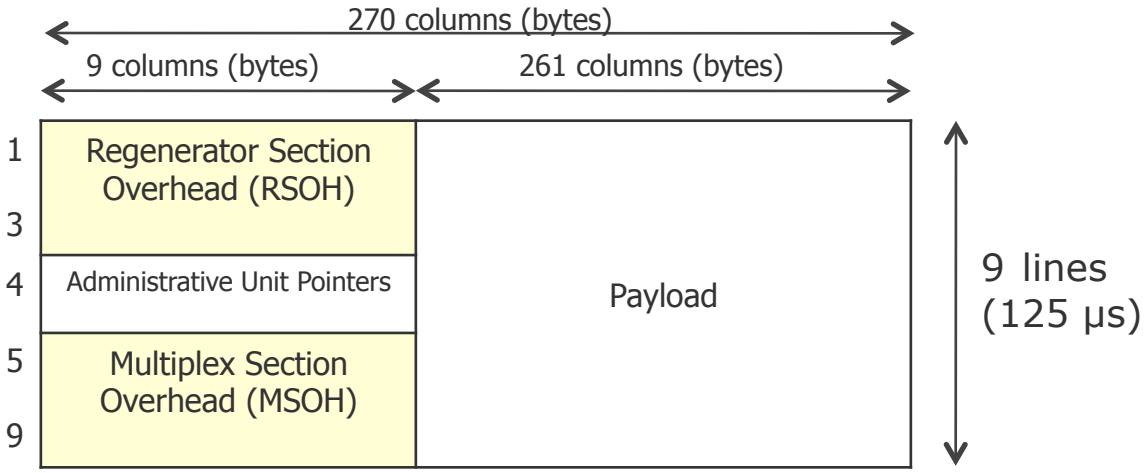
SDH: Frame Format

Synchronous Transport Module (STM)

- 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
- Basic data rate of 155 Mbps
  9x270x8x8000 bps = 155.52 Mbps



Administrative Unit Pointers

- Permit the direct access to components of the Payload

Regenerator Section Overhead Header

- Contains information concerning the route between two repeaters or a repeater and a multiplexer

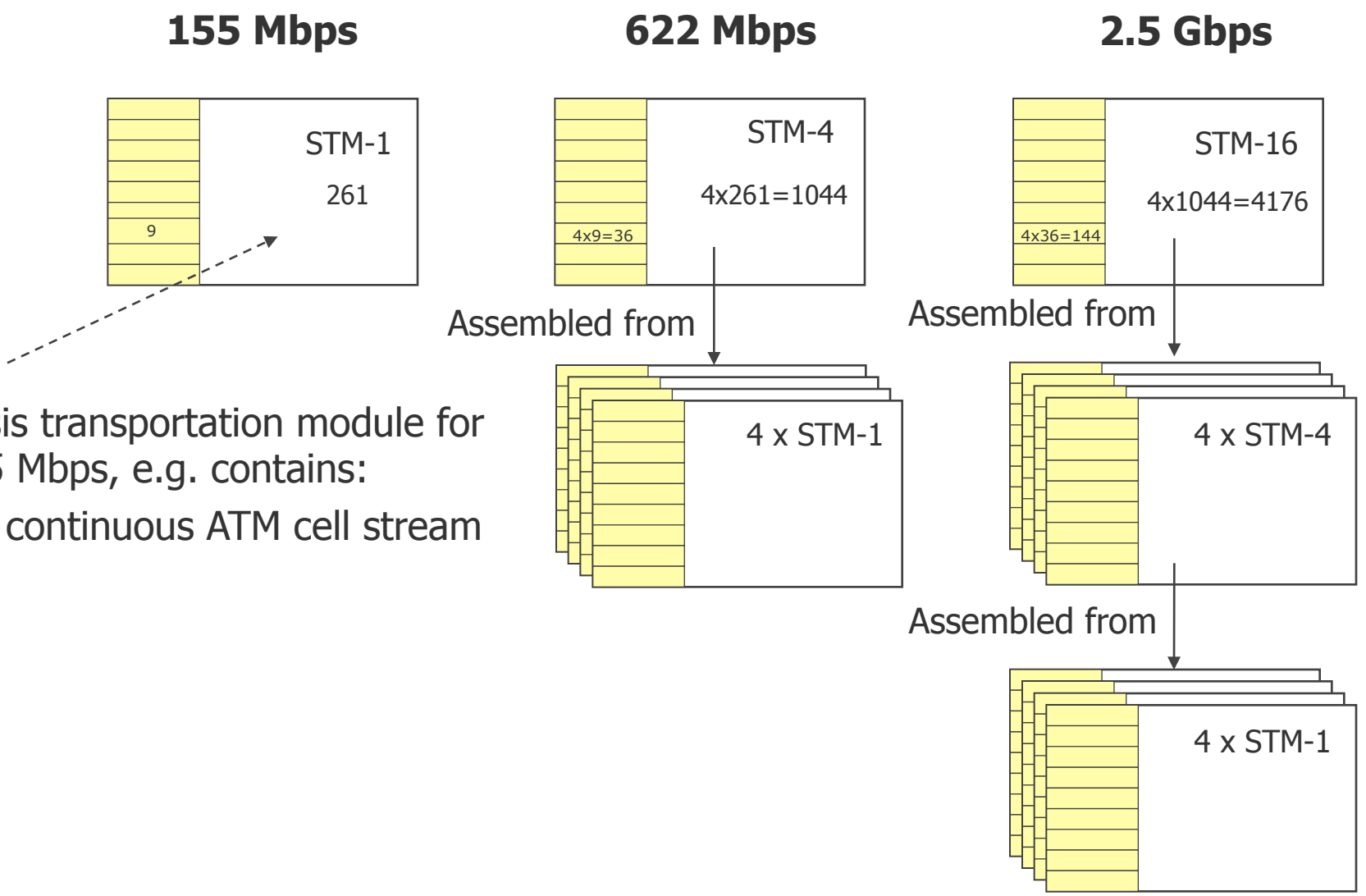
Regenerator Section Overhead Header

- 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

SDH: Simpler Multiplexing using a Hierarchy

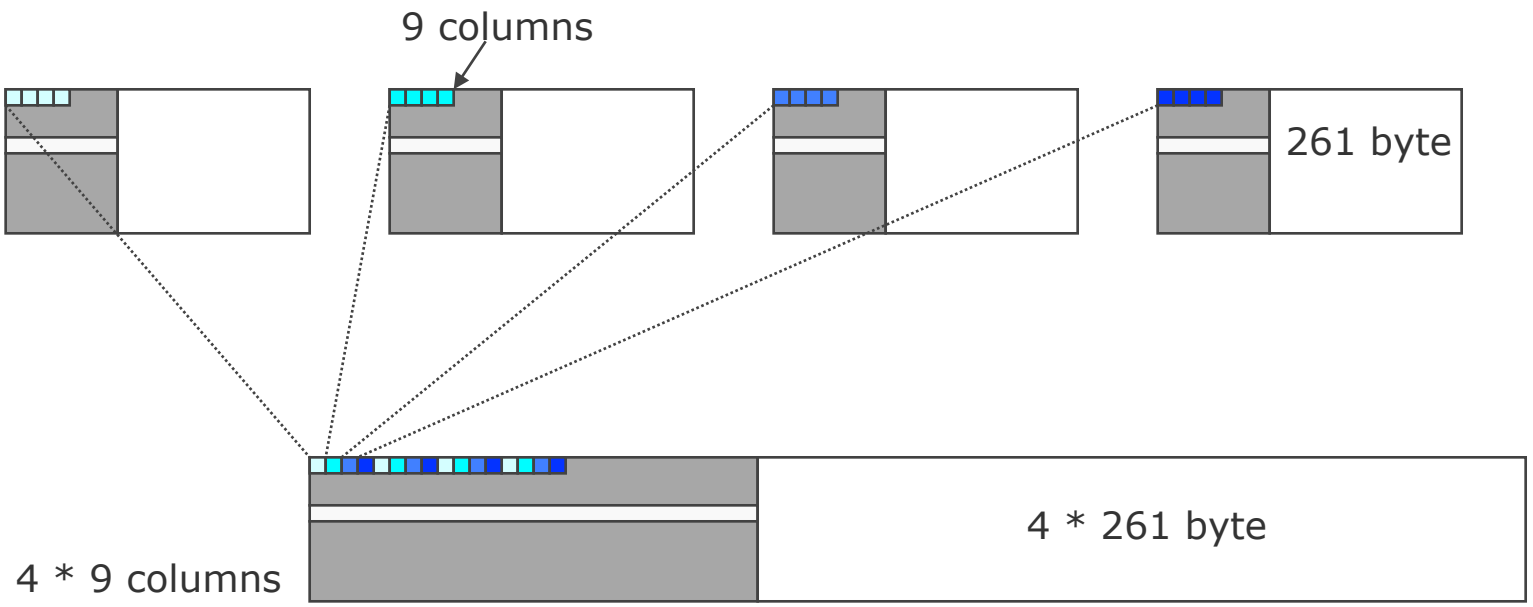


Basis transportation module for 155 Mbps, e.g. contains:

- a continuous ATM cell stream

SDH: Simpler Multiplexing using a Hierarchy

- Higher hierarchy levels assemble several STM-1 modules
- Higher data rates assembled by multiplexing the contained signals byte-by-byte
- Each byte stream has a data rate of 64 kbps (suitable for voice telephony)
- Recursively higher hierarchy levels assemble several STM-4 modules etc.



SDH: Data Rates

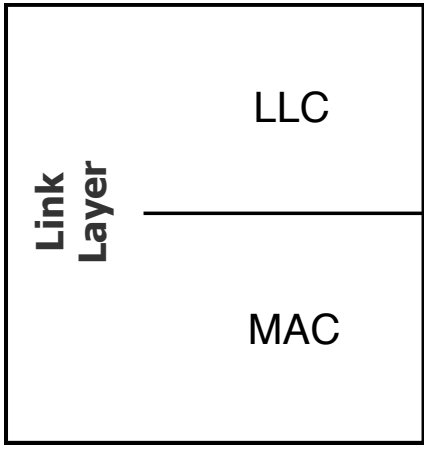
SONET		SDH	Data rate (Mbps)	
Electrical	Optical	Optical	Gross	Net
STS-1	OC-1	STM-0	51.84	50.112
STS-3	OC-3	STM-1	155.51	150.336
STS-9	OC-9	(STM-3)	466.56	451.008
STS-12	OC-12	STM-4	622.08	601.344
STS-18	OC-18	(STM-6)	933.12	902.016
STS-24	OC-24	(STM-8)	1,244.16	1,202.688
STS-36	OC-36	(STM-12)	1,866.24	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

With Dense WDM SDH can do way more (e.g. with 4096 channels: 164Tbit/s)

Link Layer Protocols: Summary

- Example of protocol used on Point-to-Point NICs: **PPP**
- Example of protocol used on wired LANs and MANs: **Ethernet**
- Example of protocol used on wireless LANs: **Wifi**
- Example of protocol used on WANs: **ATM**, **SDH**

- Typical architecture
  - **LLC** sublayer: IEEE 802.2 Logical Link Control provides a uniform interface and frame format to the network layer, independent of the MAC technology
  - **MAC** sublayer: defines medium access technology (WiFi, Ethernet, ATM…)



IEEE 802.2 Logical Link Control (LLC)			
802.11 WiFi	802.3 Ethernet	802.5 Token Ring	ATM ATM LAN Emulation

CONTENT of this CHAPTER

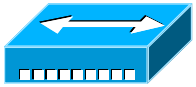
- Framing
- Error Detection & Correction
- Flow control
- Multiple Access Control

- Protocols
  - PPP
  - Ethernet
  - Wifi
  - ATM
  - SDH

- Infrastructure
  - Physical elements
  - Virtual LANs

Network Infrastructure

- To build a modern computer network, several categories of 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)

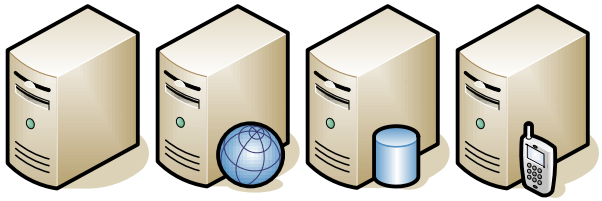


  - Bridge
    - Connects several local area networks (possibly of different types) to a large LAN

  - Switch
    - Like a hub, but without broadcast

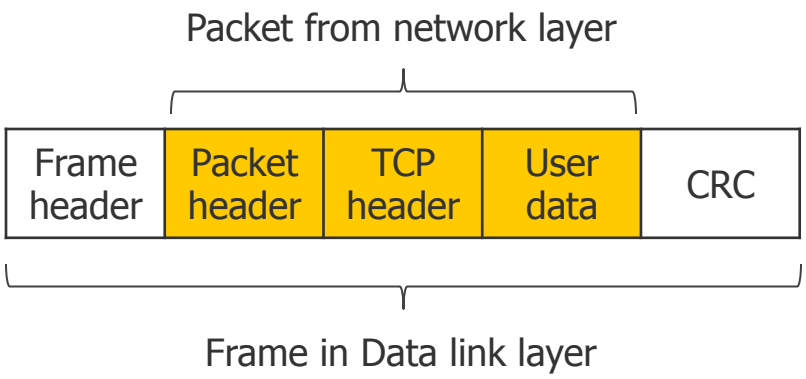
  - Router
    - Connects several LANs with the same network protocol over large distances

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

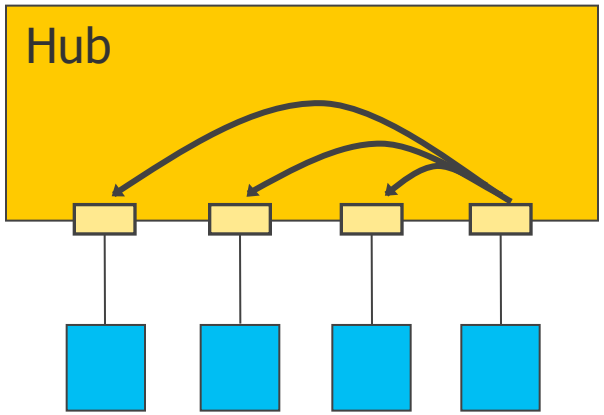


Network Infrastructure

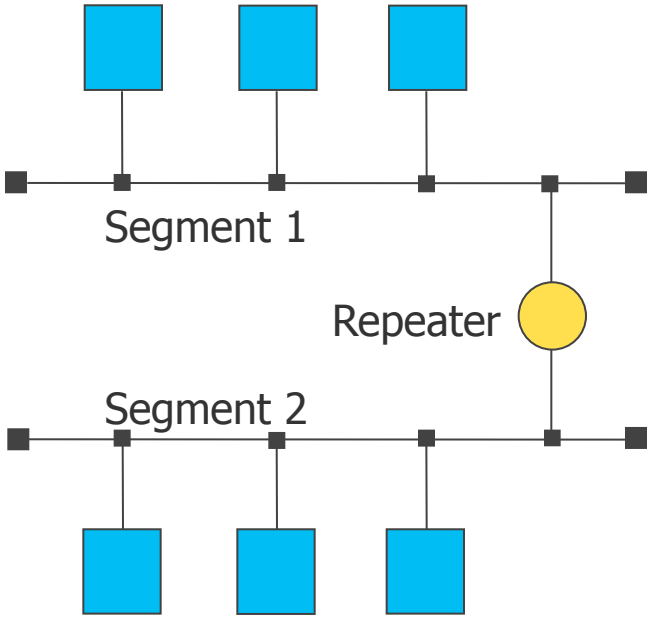
Application layer	Application gateway
Transport layer	Transport gateway
Network layer	Router
Data link layer	Bridge, Switch
Physical layer	Repeater, Hub



Hubs & Repeaters



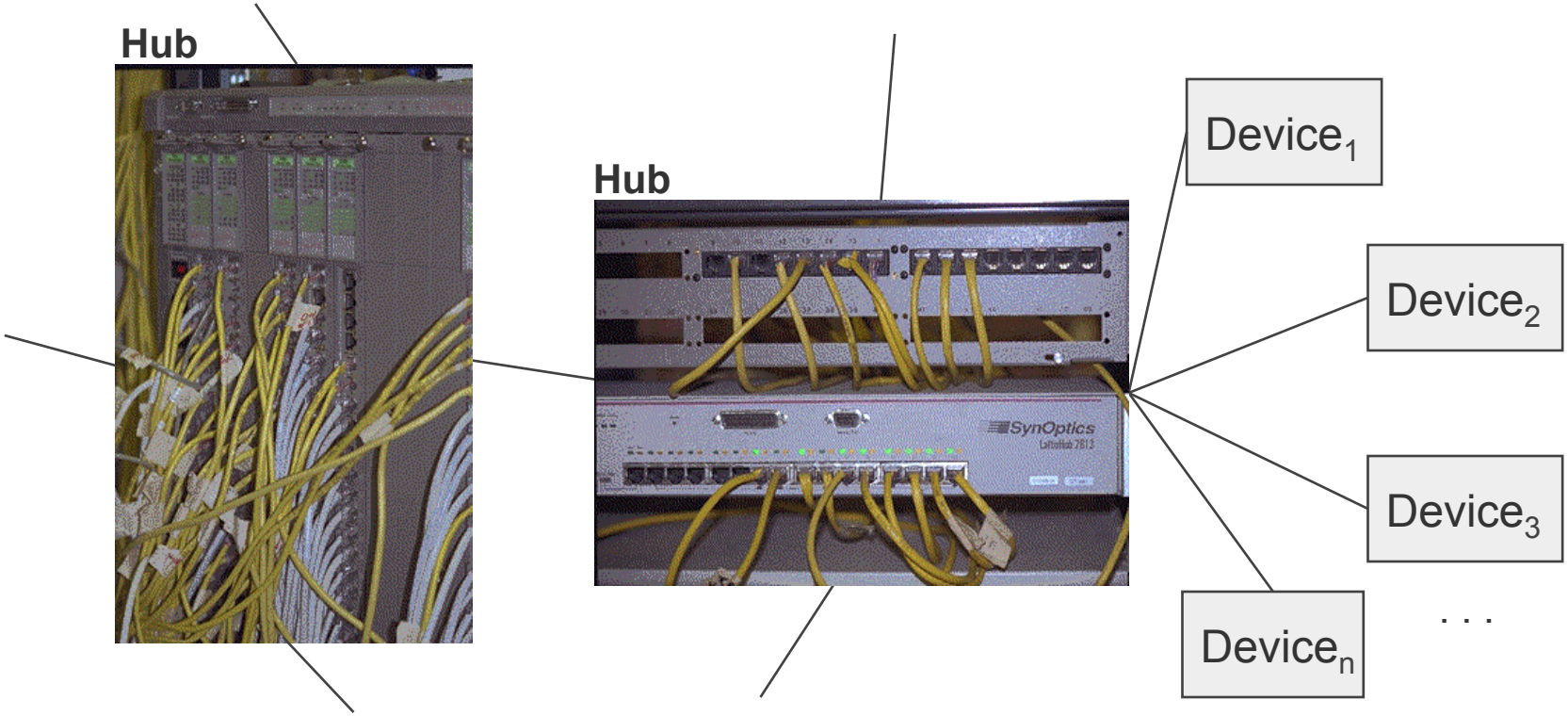
Hub: "one to all"



Repeater: Linking of 2 networks

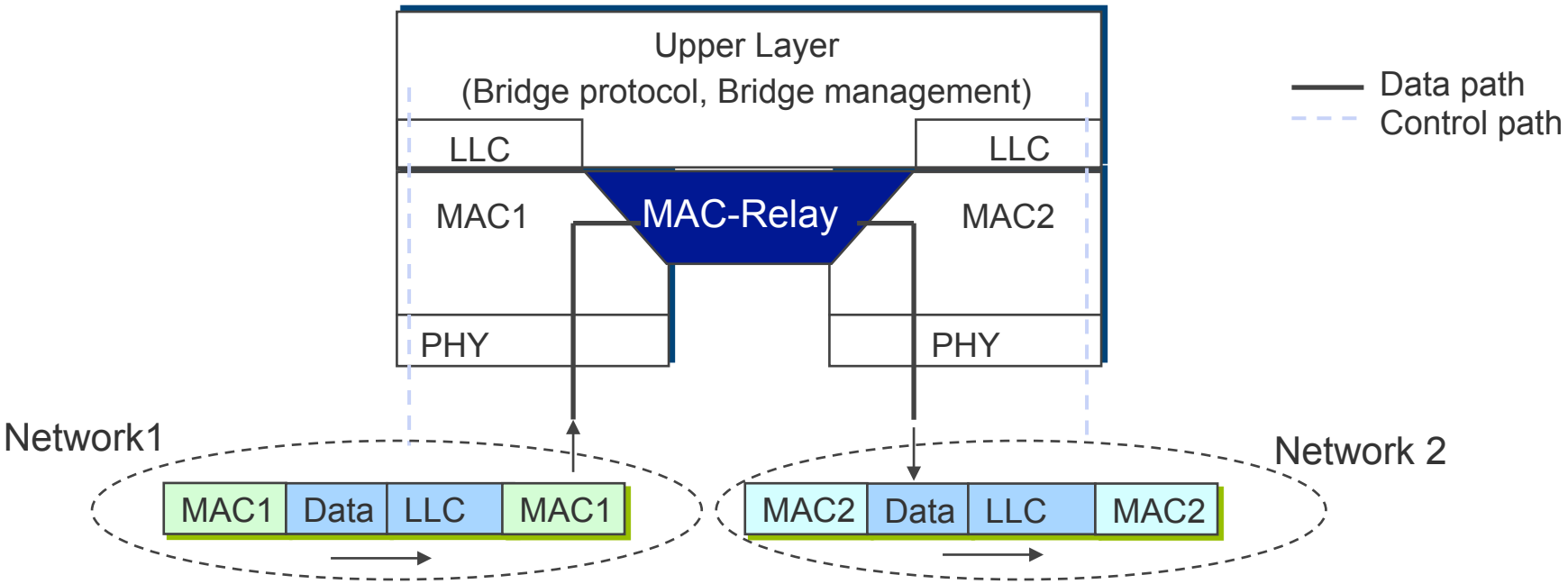
- Receives and refreshes the signal received at the **Physical Layer**
  - Signal received on one port is reproduced on the other port(s)
  - Increases the network range
- Does not understand frames, packets, or headers
- Offers only one channel shared by all connected nodes
- Low cost
- Low security (any nodes can monitor all the traffic)

Hubs & Repeaters: Examples



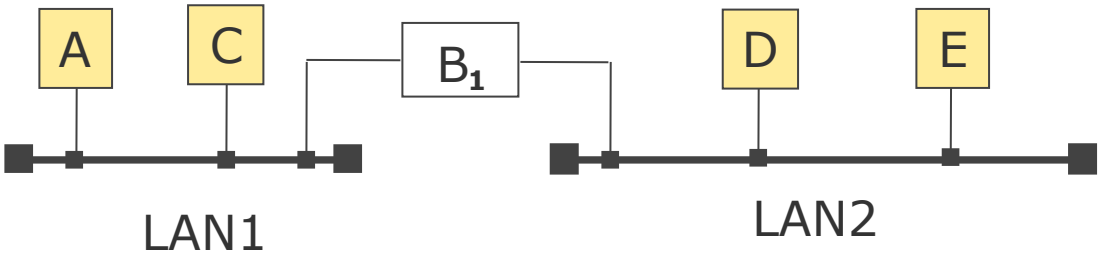
Bridges

- A bridge relays frames between 2 or more LANs
  - Operates at **the Link Layer**
  - Processes frame addresses
  - Can support different network type



Bridges: Reasons for Bridging

- Problem: what to do if many LANs exist?
  - e.g. because several buildings each have a LAN
  - e.g. because a single LAN is not long enough (Ethernet supports only up to 2.5 km)
  - e.g. because of load management (it can "isolate" part of the data traffic)
  - e.g. security/reliability reasons

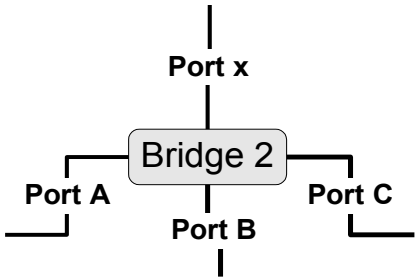


- Solution: connect them with bridges
  - A bridge examines the data link layer address for appropriate relaying

- Requirements:
  - Bridging should be transparent. Typical problems when relaying frames between LANs:
    - Different frame formats
    - Different data rates
    - Different max. frame length
    - Security: Some support encryption others do not
    - Quality of Service
  - Bridging should be flexible. Moving of machines from one segment to another should not require the change of software or hardware.

Bridges: Relaying Procedures

- 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?

Found and = x?

Not found ?

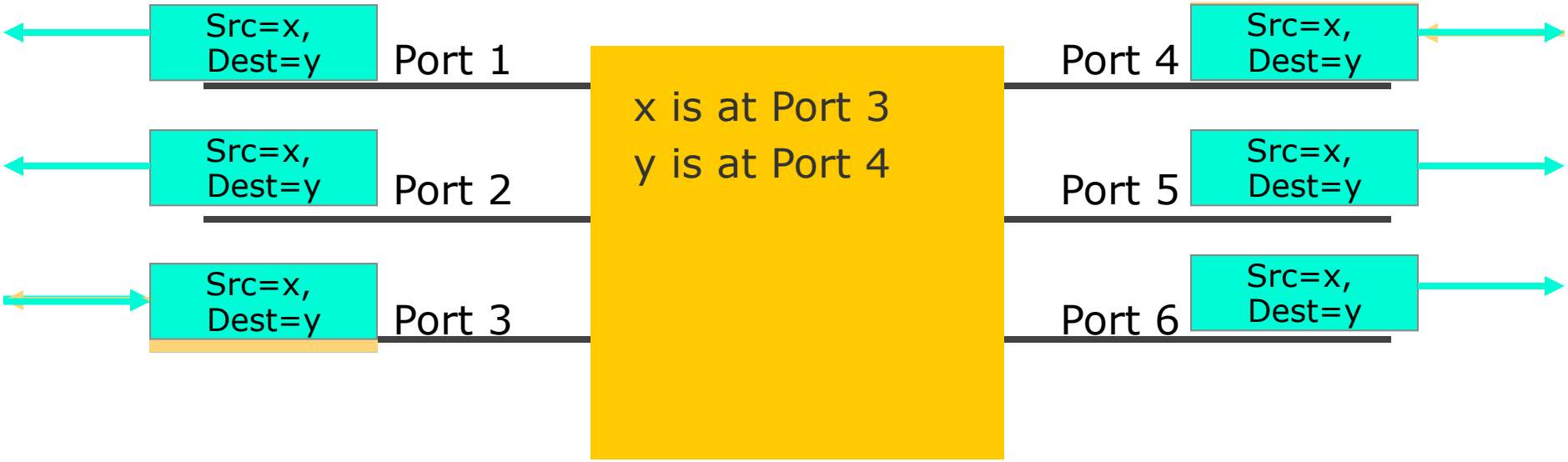
Broadcast the frame on the appropriate port

Ignore frame

Flood, i.e., broadcast the frame on all port except port x.

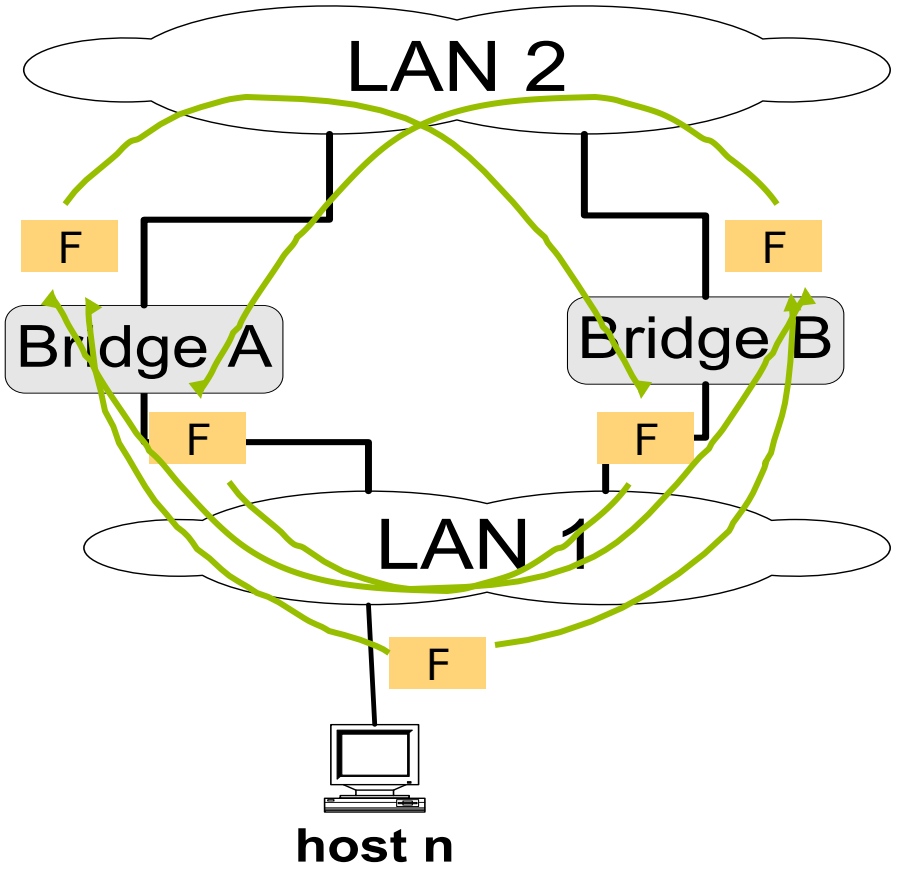
Bridges: Automatic Address Learning

- 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 bridge 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).



Bridges: Loops

- Problem: complex bridging architecture can lead to 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 on and on…

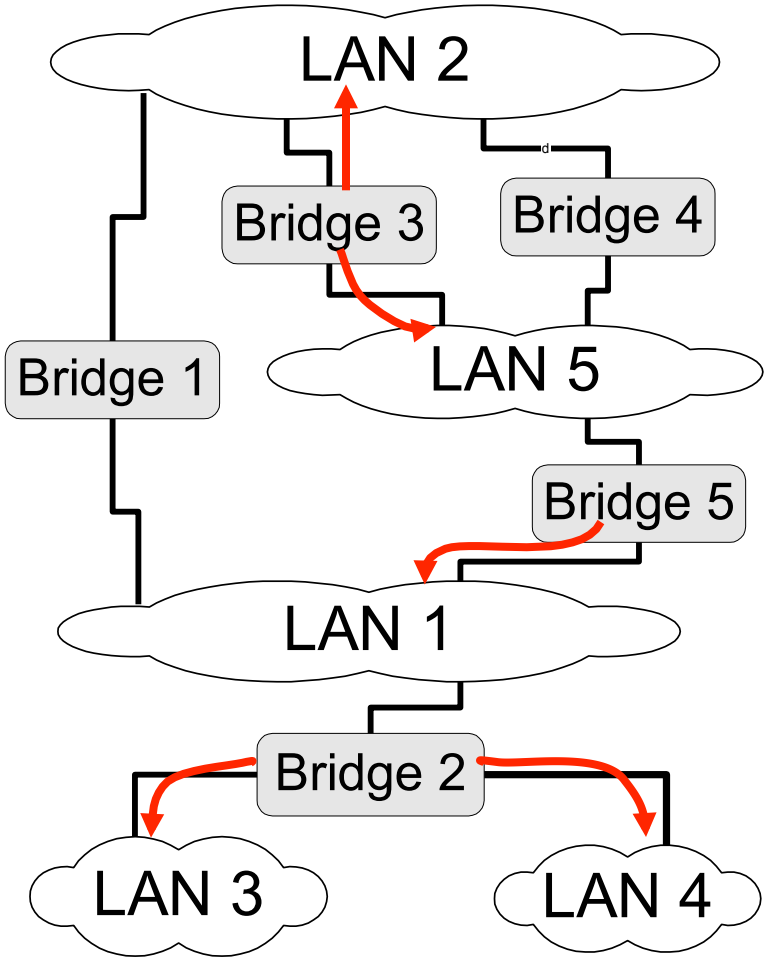


- Solution: The Spanning Tree Algorithm

Bridges: Preventing Loops with a Spanning Tree

- Principle: relay only along edges of a loop-less tree structure, connecting all bridges

- Spanning Tree Algorithm:
  - Step 1: Determine a single root bridge
    - The bridge with the smallest ID
  - Step 2: Determine a designated bridge for each LAN
    - The bridge which is nearest to the root bridge
  - Step 3: Determine root ports
    - Port for the best path to root bridge considering costs for using a path, e.g., the number of hops.



Bridges: The Spanning Tree Algorithm

- At the beginning, each bridge assume to be root and floods a packet containing its ID, current cost (initialized with zero) over all of its ports

root ID	cost	bridge ID	port ID

e.g. for station B on port P_1:

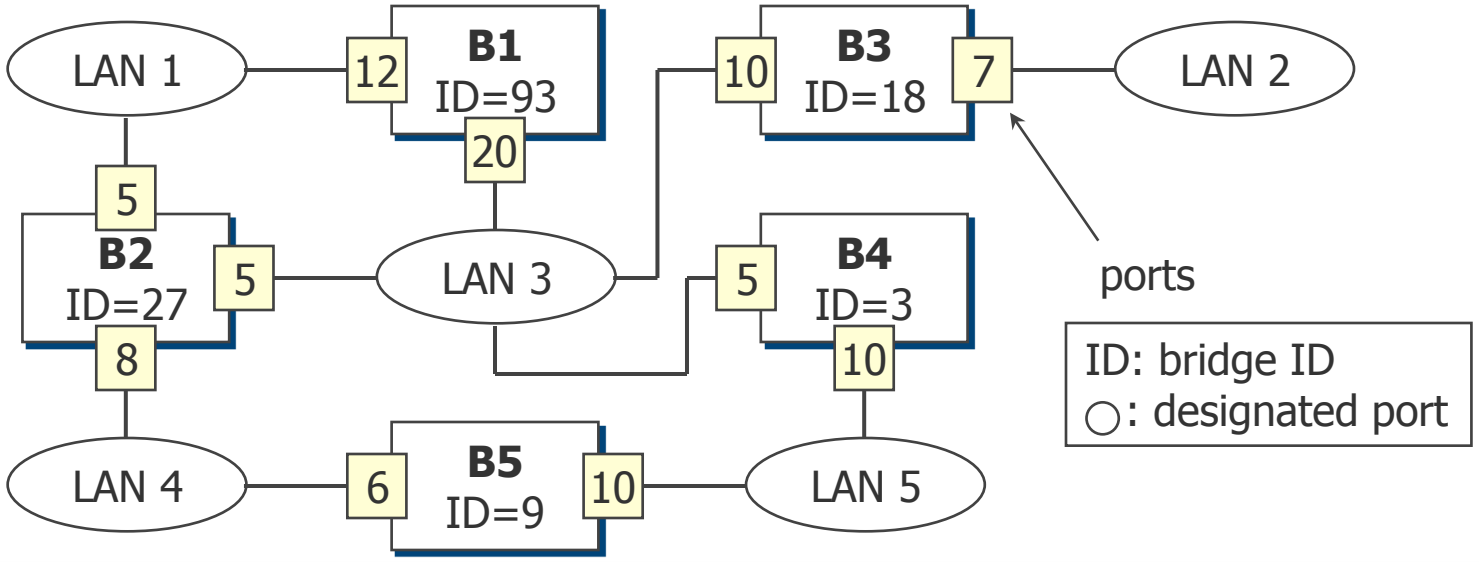
B	0	B	P_1

- A bridge receiving such a packet checks the root ID and compares it with its own. 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 its own cost for the bridge from which the packet was received to the current cost value.

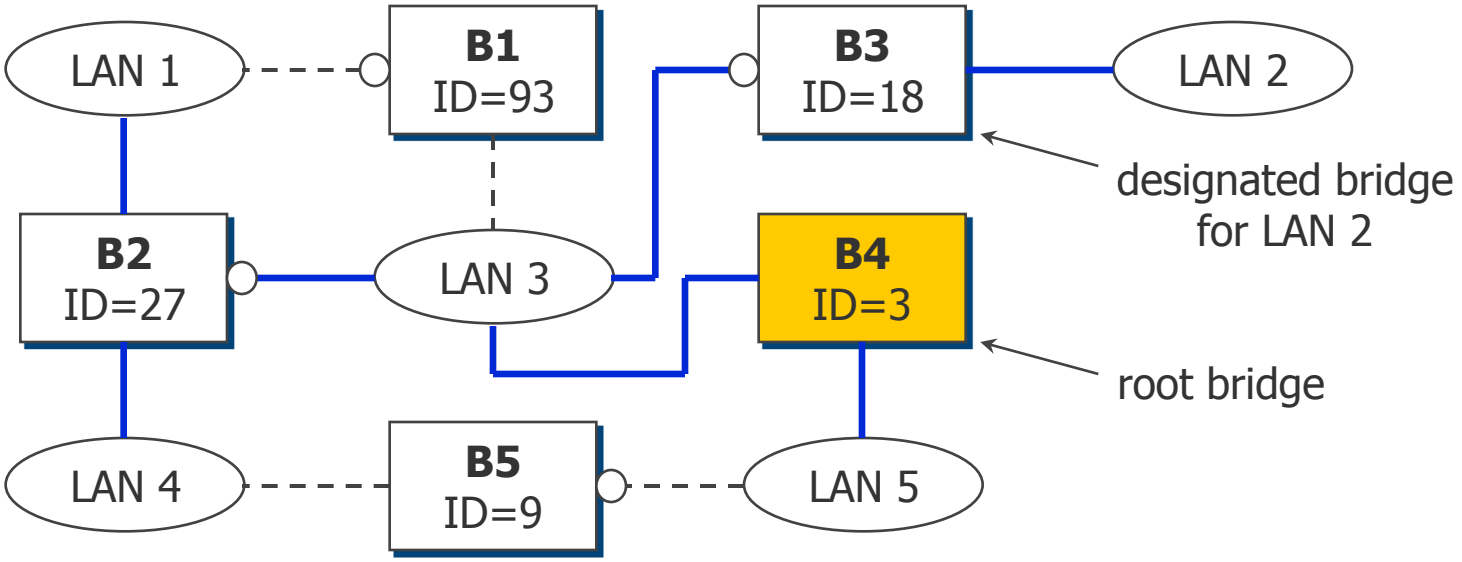
- When the (updated) packets of all bridges have passed all other bridges, all bridges have agreed on the root bridge. The received packets containing the smallest costs value to the root bridge determine the designated bridge for a LAN and designated ports for the bridges to send out data.

Bridges: Spanning Tree Algorithm Example

Network:



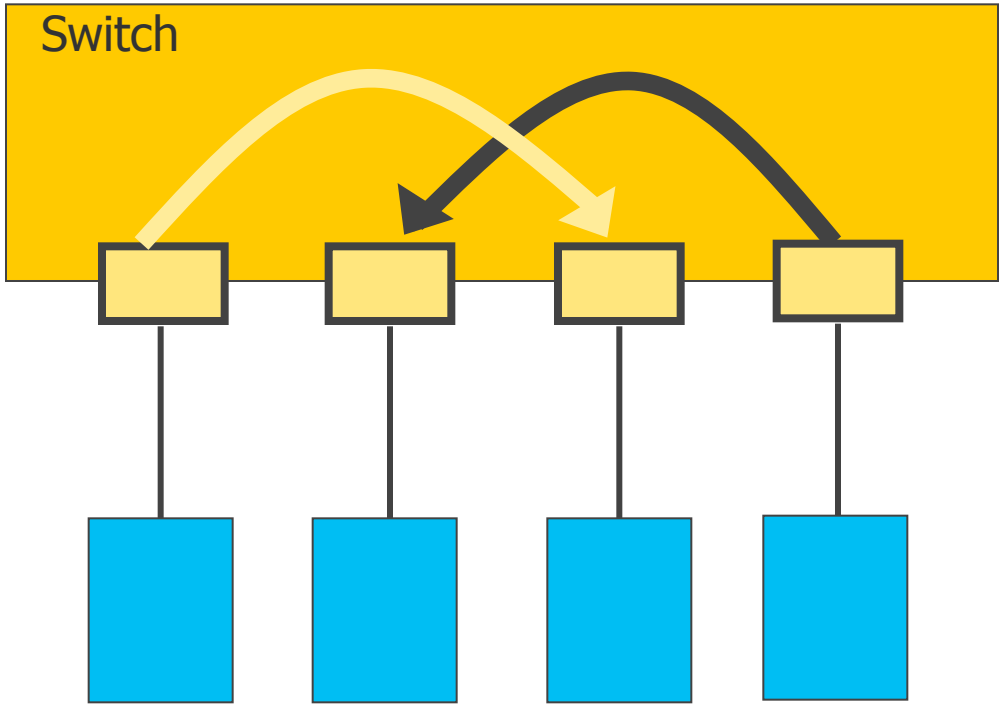
Spanning Tree:



Switches

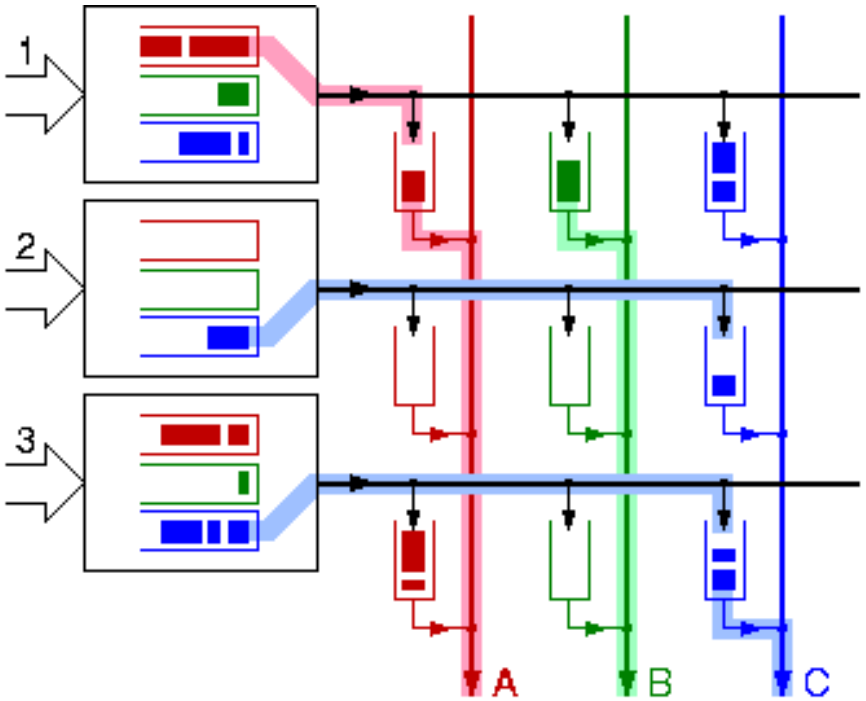
- Similar to a bridge, except point-to-point NIC on each port
  - (Instead of broadcast for a bridge)
  - Buffer for each individual station/each port
  - Connected nodes can send and receive at the same time
  - More expensive

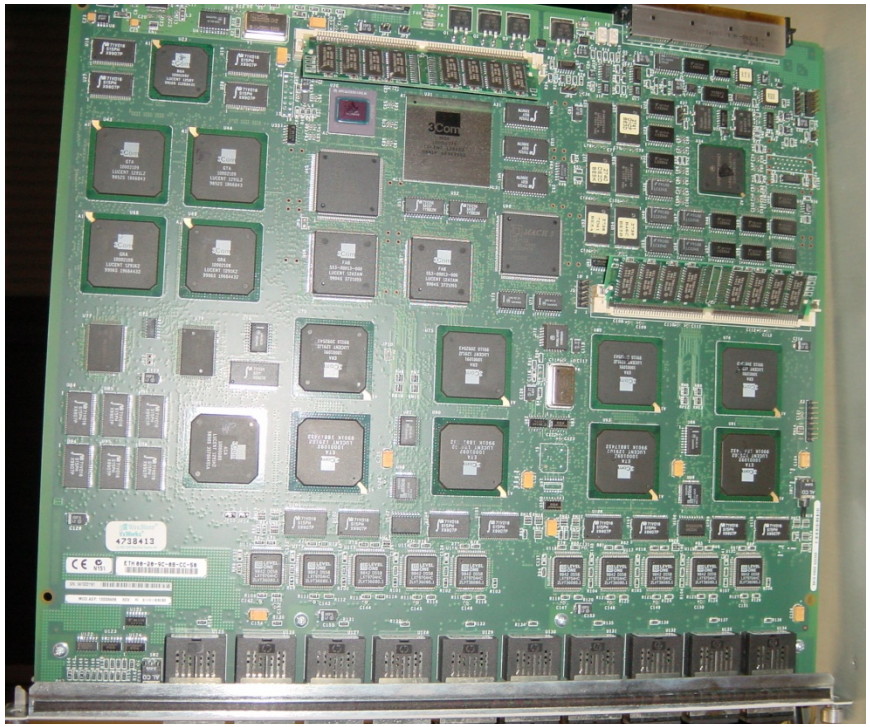
- "Layer 3-Switch": also has functionalities of level 3, i.e., it can e.g. take over the routing.
- "Layer 4-Switch": looks up additionally in the TCP-header, can therefore be used e.g. for load balancing.



Switches: Hardware Implementation

- Most often 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, collisions are quasi-impossible!

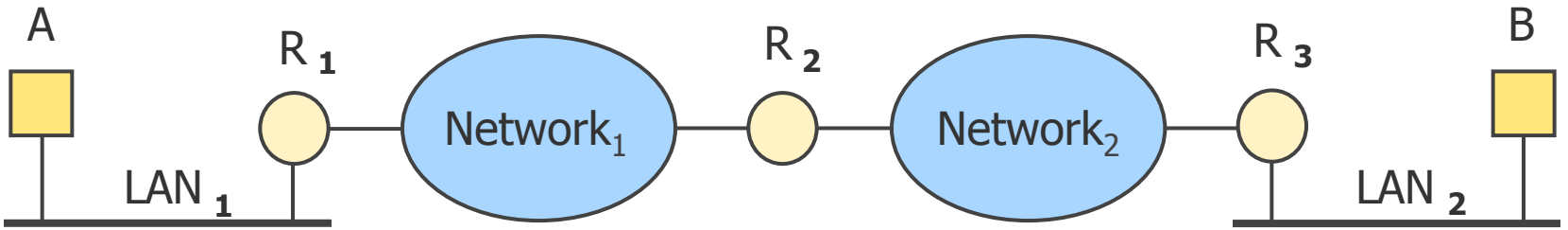




Routers

- There are limits to what can be achieved with bridges and basic switches
  - Bridges can support only up to a few thousand computers in the network, because addresses used are not scalable (i.e. do not have any geographical reference).
  - 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.

➡ **Routers** operate at the Network Layer and overcome these weaknesses
  - Packets forwarded towards destination on the basis of a global address
  - No restriction concerning the number of hosts (hierarchical addressing, local admin.)
  - Broadcasts are not let through by the routers, Multicast depending on the router
  - Communication between host and router improves performance

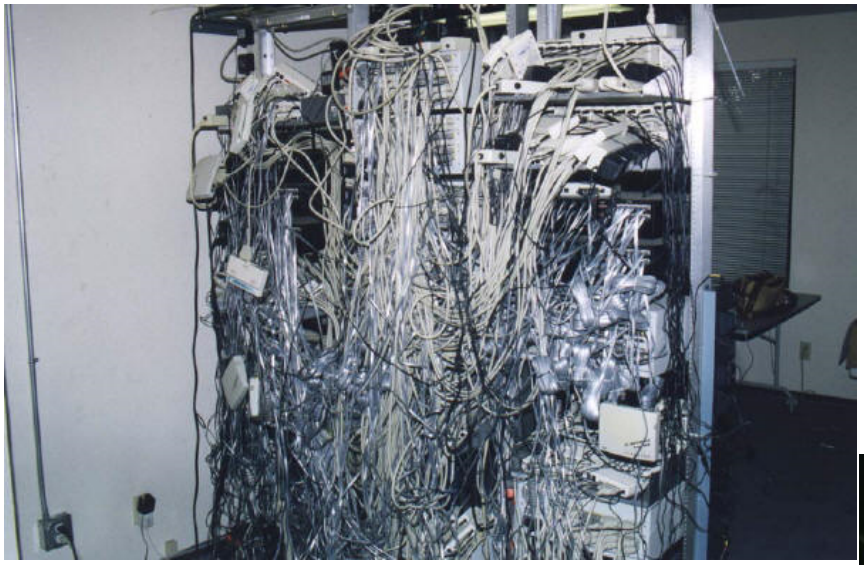


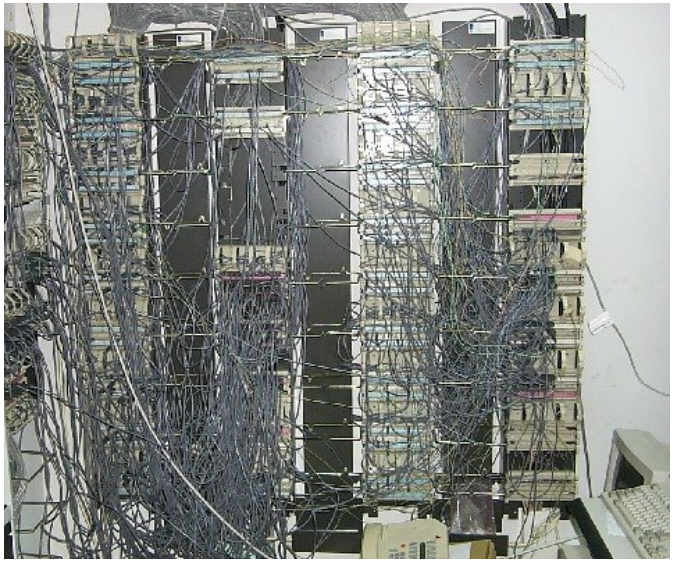
Gateways

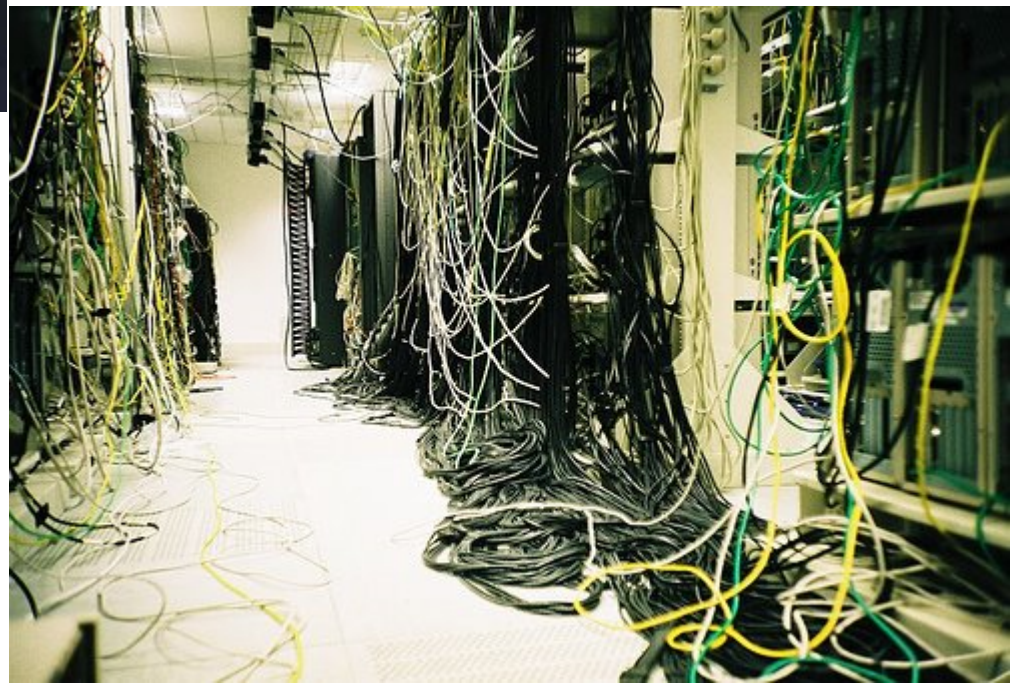
- Transport Layer Gateways
  - Connection of computers using different transport protocols, e.g., a computer using TCP/IP and one using ATM transport protocol
  - Copies packets from one connection to another

- 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

Cabling: Examples to Avoid

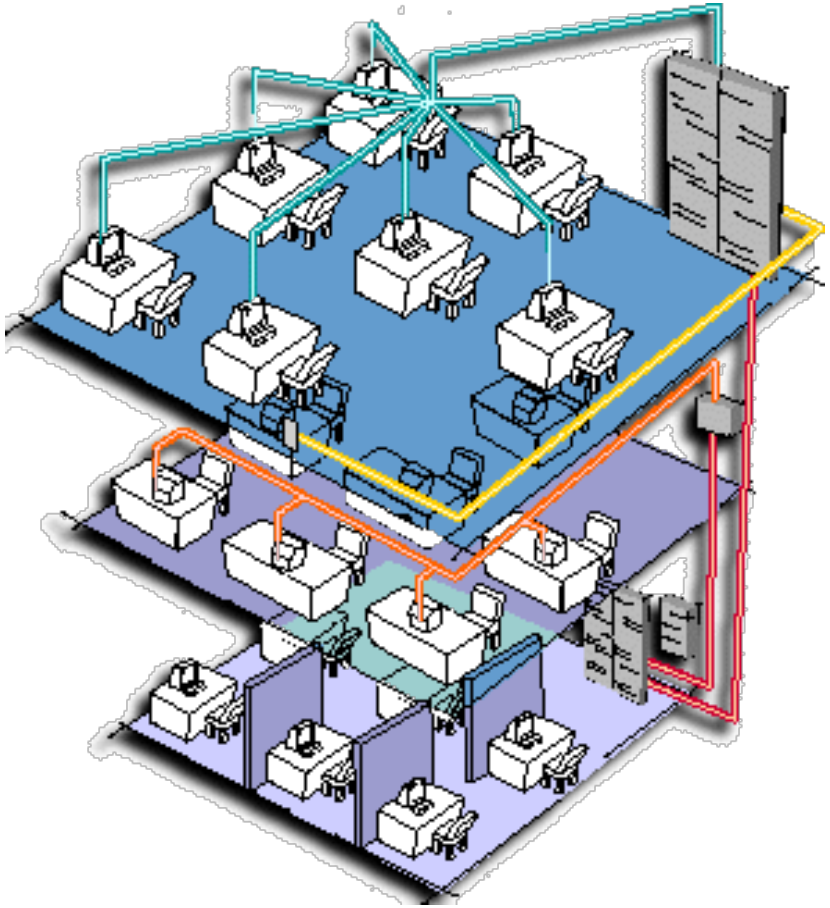






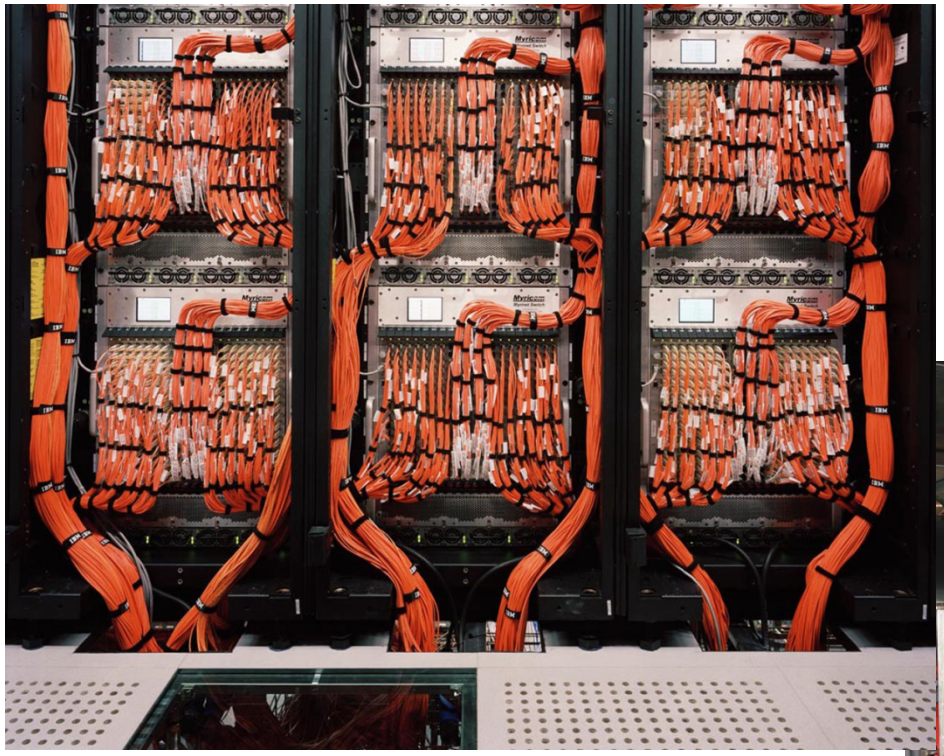
Structured Cabling: Concept

- 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: Examples to Imitate

Structured Cabling: Examples to Imitate



Structured Cabling: Advantages

- 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 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

CONTENT of this CHAPTER

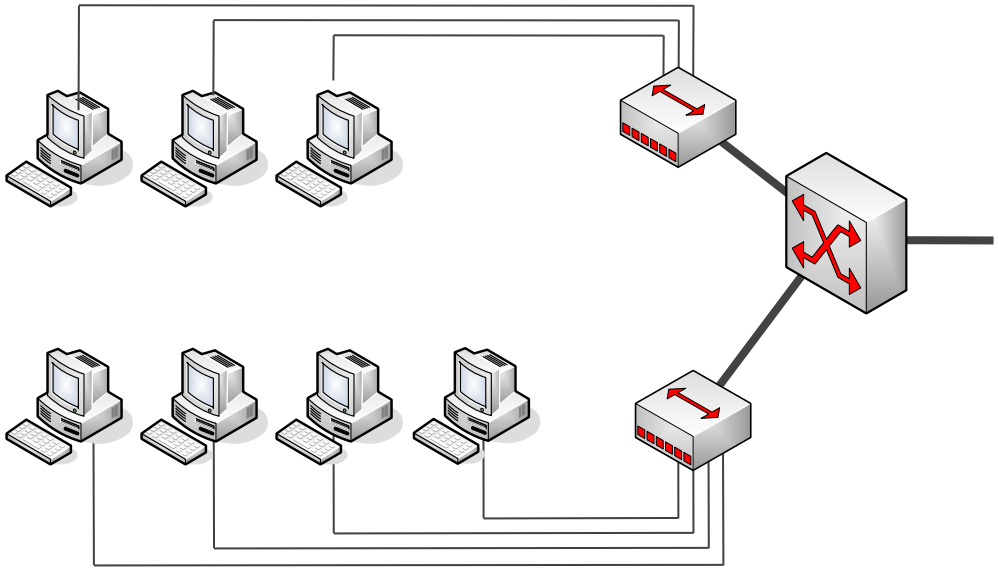
- Framing
- Error Detection & Correction
- Flow control
- Multiple Access Control

- Protocols
  - PPP
  - Ethernet
  - Wifi
  - ATM
  - SDH

- Infrastructure
  - Physical elements
  - Virtual LANs

Virtual LANs

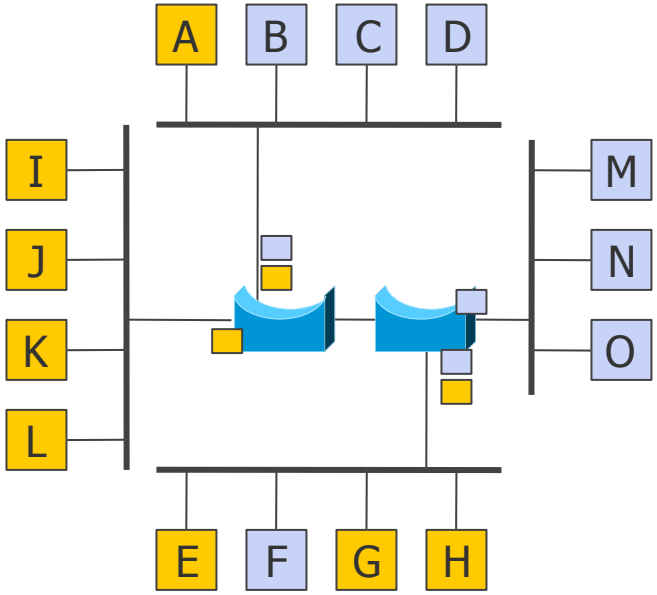
- Initially, computers of an entreprise network were typically on a single LAN
- Nowadays, there are usually several LANs
  - Over time new cabling was deployed, using newer Ethernet technologies
  - Different departments wanted different LANs (better security, load management)
  - What happens if users move from one department to another? No rewiring please!

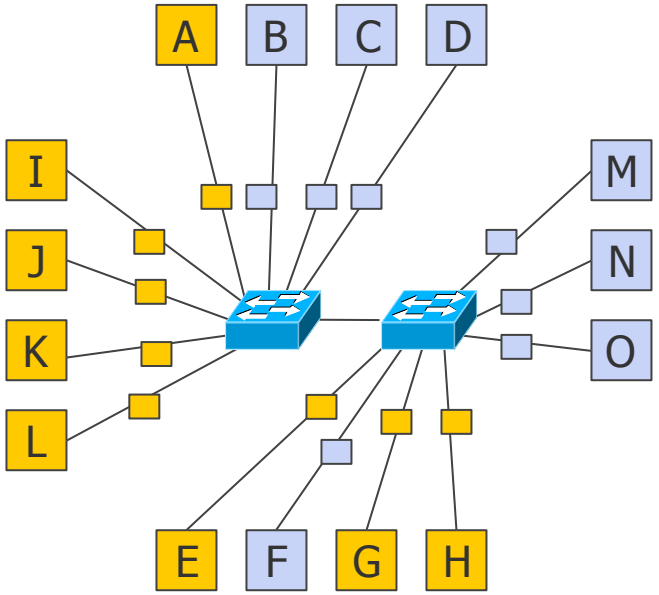


- Virtual LANs allow the configuration of LANs logically, rather than physically
  - Requirement: decoupling of the **logical topology** from the **physical topology**

Virtual LANs

- Virtual LANs require VLAN-aware switches
  - VLANs are often named by colors (VLAN ID)
  - Allows diagrams which show logical and physical topology at the same time





- VLAN-aware devices are needed
  - e.g. a switch has a table which tells which VLAN is accessible via which port
  - In this case, a port may have access to multiple VLANs

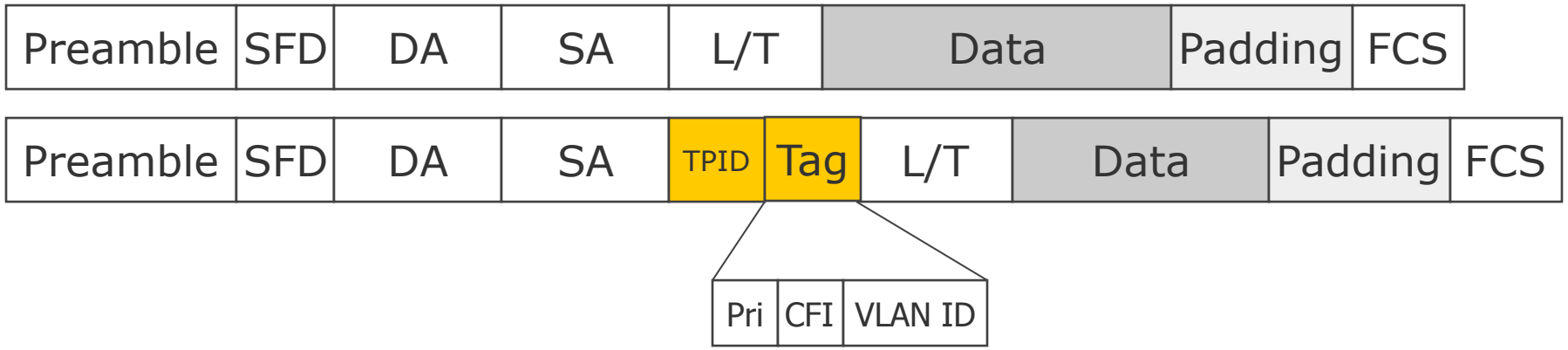
Virtual LANs: VLAN-aware Switches

- How does a switch know the VLANs?
  - Solution 1: Assign each port of the device to a VLAN ID
    - Only machines belonging to the same VLAN can attach
  - Solution 2: Each MAC address is assigned to a VLAN
    - Device needs tables of the 48-bit MAC addresses assigned to VLANs
  - Solution 3: Each Layer 3 protocol (IP address) is assigned to a VLAN
    - Violates the independency of layers

- IEEE 802.1Q specifies a field in frame header telling the VLAN assignment
  - Problems:
    - What happens with legacy Ethernet cards?
    - Who generates the new field?
    - What happens with max. length frames?
  - Solution:
    - The first VLAN-aware device adds VLAN-tag (decides which based on port MAC address)
    - The last VLAN-aware device removes VLAN-tag
    - New cards (Gigabit Ethernet) support 802.1Q

Virtual LANs: Frame Format Modification

- IEEE 802.1Q Frame Format
  - Additional 4 bytes inserted between SA field and L/T field



  - TPID (2 bytes): Tag Protocol Identifier (0x8100)
    - serves as flag to differentiate with beginning of L/T field in a non-VLAN, classical frame
  - Tag (2 bytes) comprises of three fields
    - **VLAN ID: 12-bit VLAN identifier**
      - The only relevant field
    - 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 (Token Ring). Mostly historical.

The Link Layer: Summary

- The physical layer enables bit per bit transmissions from A to B, through one physical medium (wire/fiber/radio).
- The link layer enables transmission of flows of coherent, error-controlled structures of bits (frames) from A to B, if A and B are **directly connected**
  - Refinement 1: instead of B, it may be several receivers in case of multiple access
  - Refinement 2: more than one segment can be locally stitched via a relaying device (switch, hub, bridge, repeater)
  - e.g. **Ethernet** (in LAN/MAN), **WiFi** (in LAN), **PPP**, **ATM**, **SDH**/SONET (in WANs)
- Problem: relaying frames at the link layer is not manageable at global scale
  - Need efficient framework across different link-layer technologies
  - Need scalable addressing scheme
  - Need specific mechanisms to build end-to-end paths
- Solution: the network layer provides these functionalities, our focus now.