Høyskolen Kristiania

Høyskolen Kristiania

Digital Technology

TK1104

Guest lecturer: Peyman Teymoori

peymant@ifi.uio.no

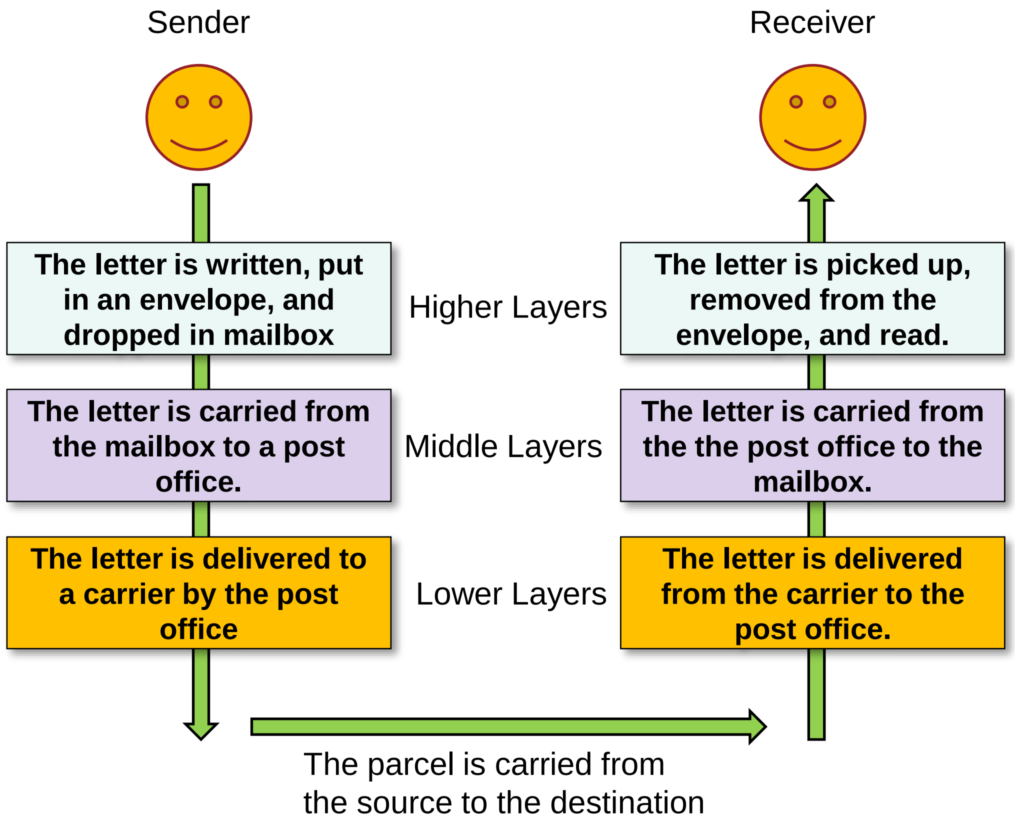
Lecturer: Toktam Ramezanifarkhani

Toktam.Ramezanifarkhani@kristiania.no

Toktamr@ifi.uio.no

Computer Networks – Link Layer

Analogy of Networking



Sender

Receiver

The letter is written, put in an envelope, and dropped in mailbox

Higher Layers

The letter is picked up, removed from the envelope, and read.

The letter is carried from the mailbox to a post office.

Middle Layers

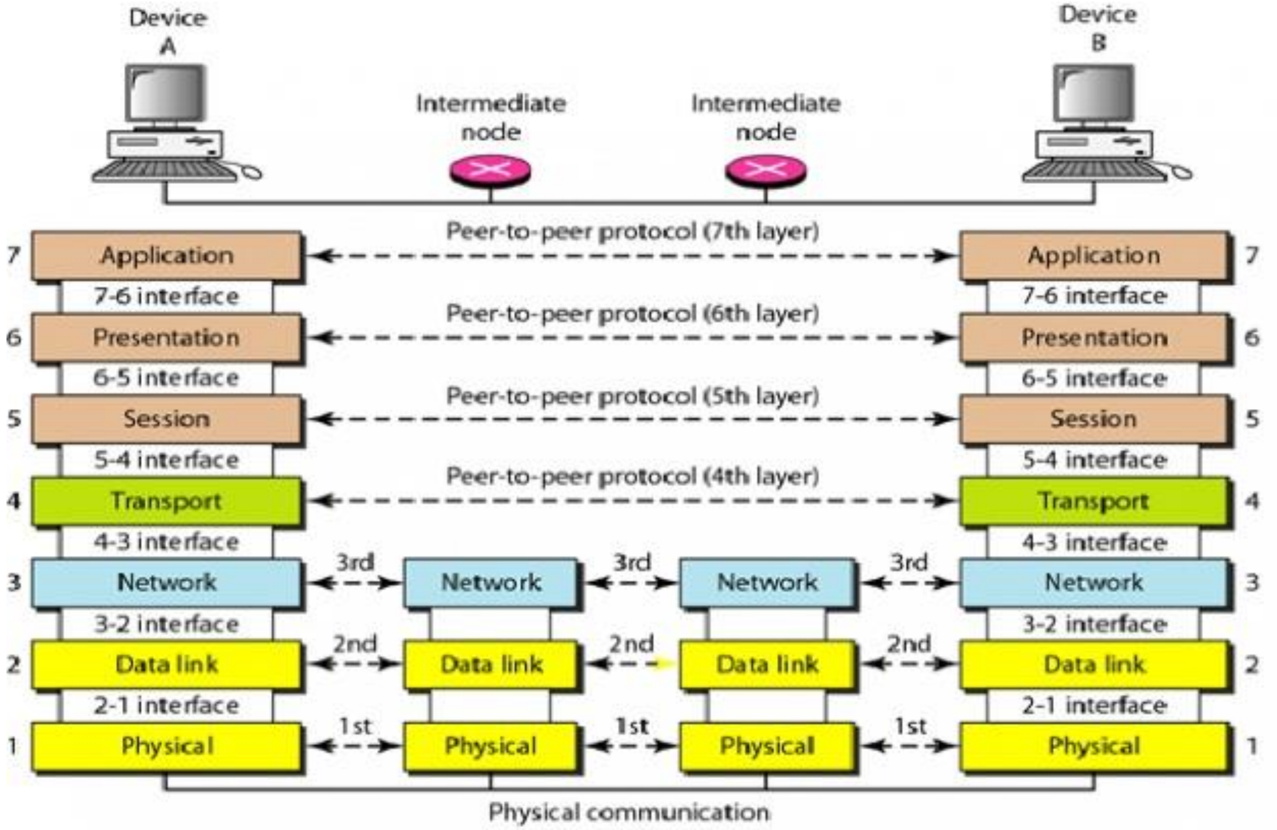
The letter is carried from the the post office to the mailbox.

The letter is delivered to a carrier by the post office

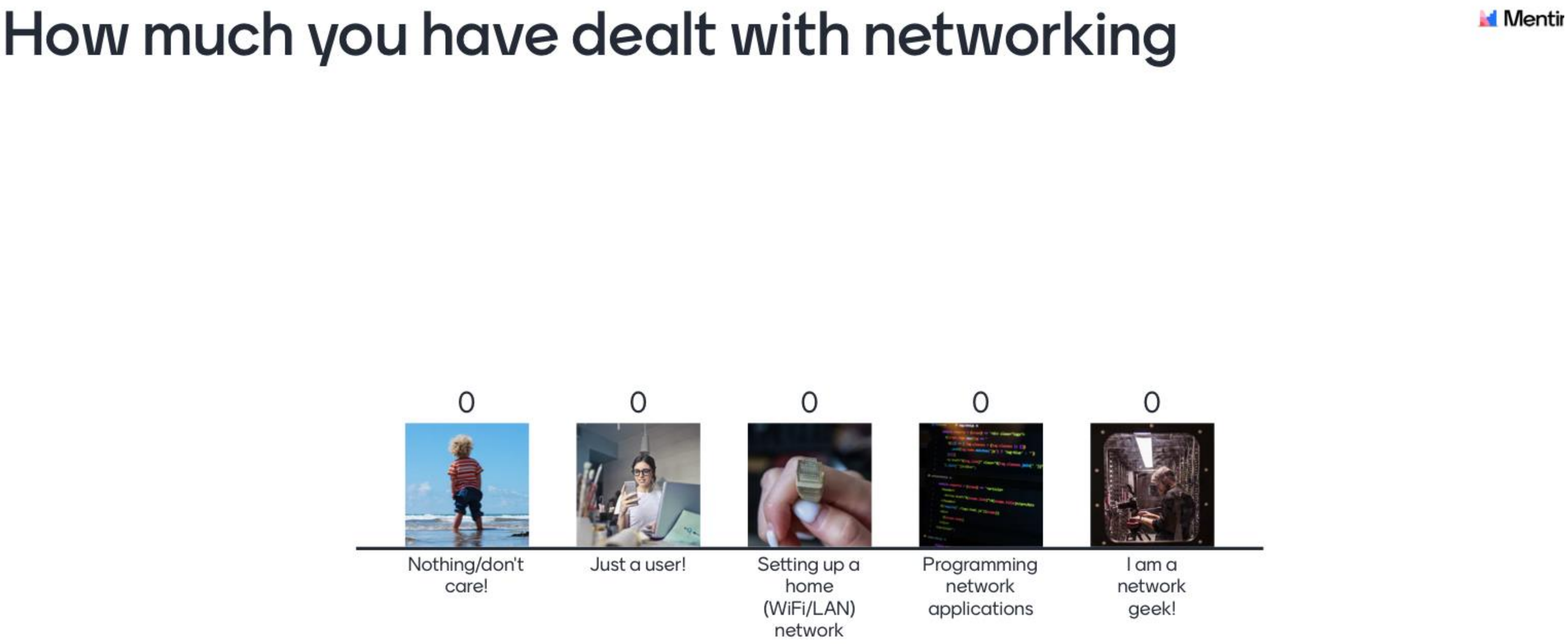
Lower Layers

The letter is delivered from the carrier to the post office.

The parcel is carried from the source to the destination



Go to menti.com and use code **3372 9155** 980

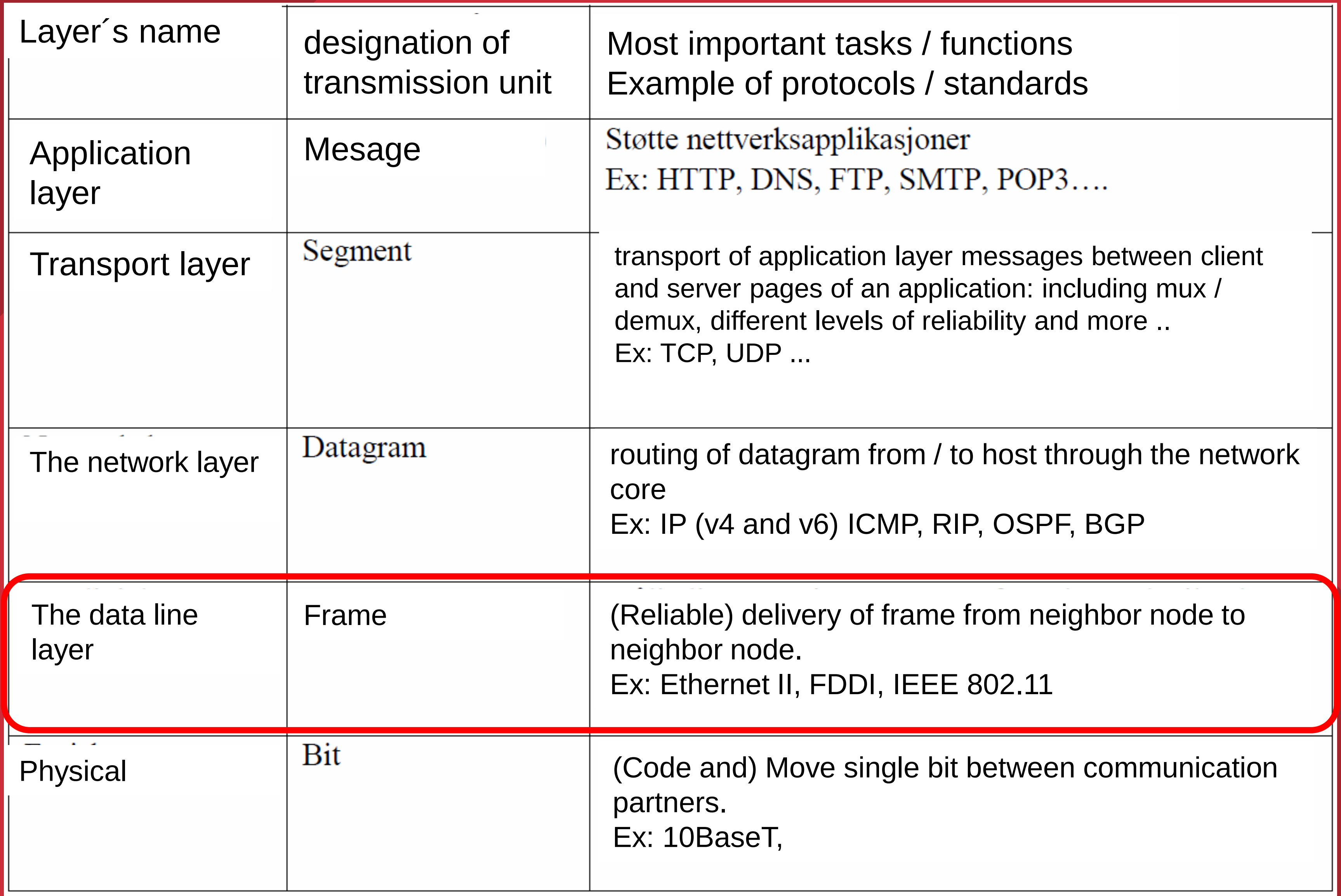


How much you have dealt with networking

Mentir
0
Nothing/don't care!
0
Just a user!
0
Setting up a home (WiFi/LAN) network
0
Programming network applications
0
I am a network geek!

Expectations:

- After the lectures, you will be able to
  - use the TCP/IP model to explain and analyze data communication through the Internet.
  - use the TCP/IP model and knowledge of protocols belonging to it to analyze the entire process of connecting to a LAN and downloading e.g., a web page.
  - use standard tools for debugging and correcting network connections.



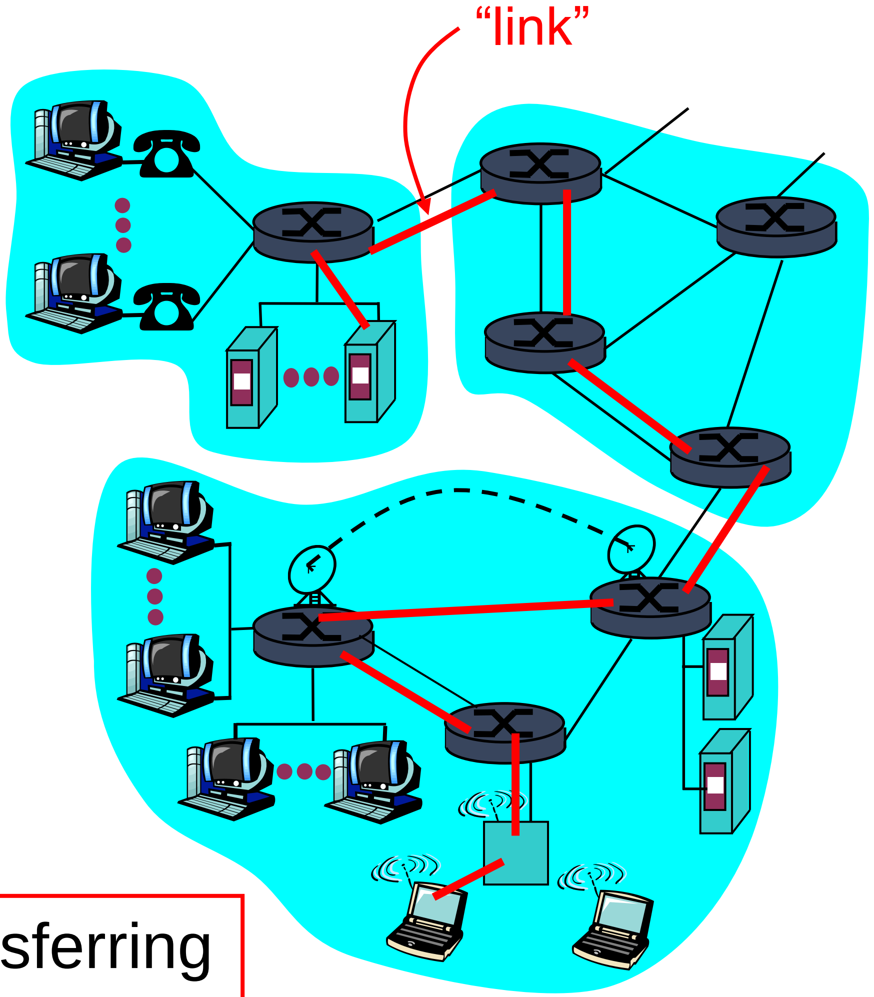
Layer´s name	designation of transmission unit	Most important tasks / functions Example of protocols / standards
Application layer	Mesage	Støtte nettverksapplikasjoner Ex: HTTP, DNS, FTP, SMTP, POP3….
Transport layer	Segment	transport of application layer messages between client and server pages of an application: including mux / demux, different levels of reliability and more .. Ex: TCP, UDP ...
The network layer	Datagram	routing of datagram from / to host through the network core Ex: IP (v4 and v6) ICMP, RIP, OSPF, BGP
The data line layer	Frame	(Reliable) delivery of frame from neighbor node to neighbor node. Ex: Ethernet II, FDDI, IEEE 802.11
Physical	Bit	(Code and) Move single bit between communication partners. Ex: 10BaseT,

Link layer / Data link layer / Data line layer

Link layer: Introduction

Some terminology:

- Machines, routers and switches are nodes
- Communication channels that connect neighboring nodes along the communication path are links.
  - wired (wired) links
  - wireless (radio) links
  - Local Area Network (LAN)
- A PDU is called a frame, encapsulating datagrams

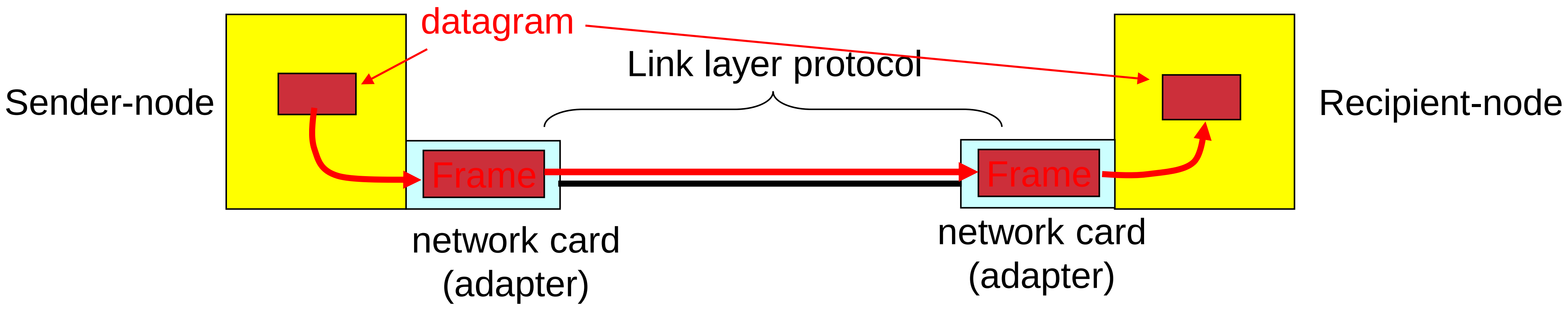


Link layer is responsible for transferring datagrams from one node to another **neighbor** node over a link

Link layer services

- Framing and link access
- Reliable delivery between neighboring nodes
- *Flow control*
- *Error detection*
- *Error recovery*
- *Half-duplex and full-duplex*

Network Interface Cards (NIC) communication



- Link layer implemented in network card (NIC)
  - Ethernet cards, 802.11 cards and so on
- Sender side:
  - encapsulation of datagram in a frame
  - adds bit for bit error detection, (sequence number, flow control etc.)

- Recipient side:
  - looks for bit errors, re-transmission, flow control etc.
  - extracts datagram, delivers this to recipient node
- NIC is partially autonomous
- Modern network adapters often also support transport and network layer functionality

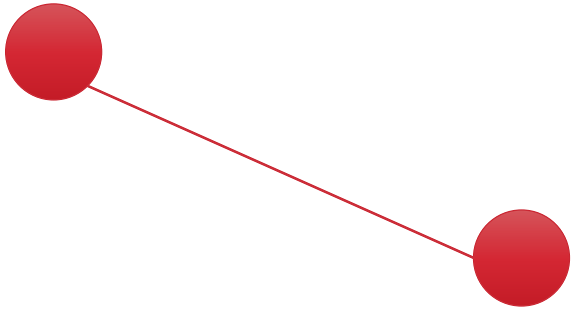
Go to menti.com and use code **3372 9155**

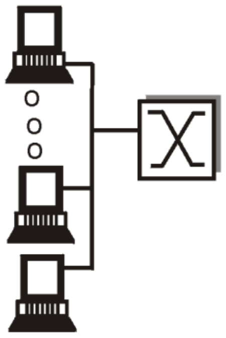
Medium Access Control

Links and protocols for multiple access

Two main types of "links":

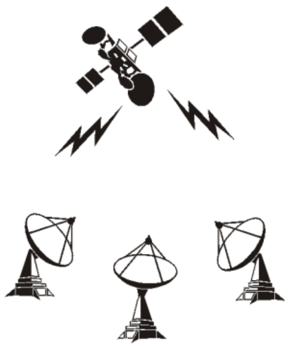
- Point to point
  - PPP for dial-up access
  - point-to-point link between two routers
- broadcast (shared medium).
  - traditional ethernet
  - 802.11 wireless local area network





shared wire
(e.g. Ethernet)

shared wireless
(e.g. Wavelan)



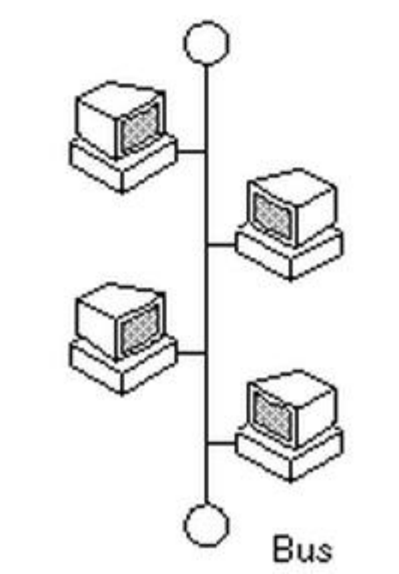
satellite

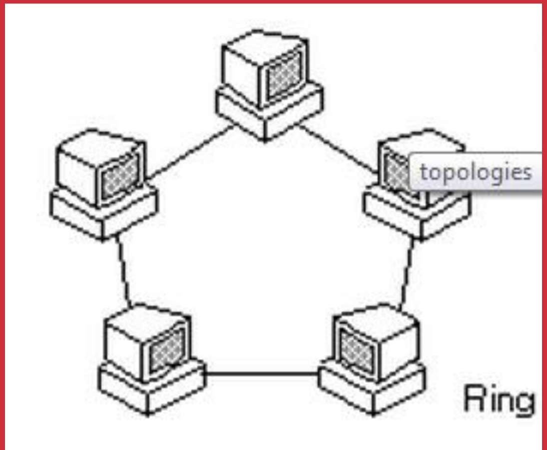
cocktail party

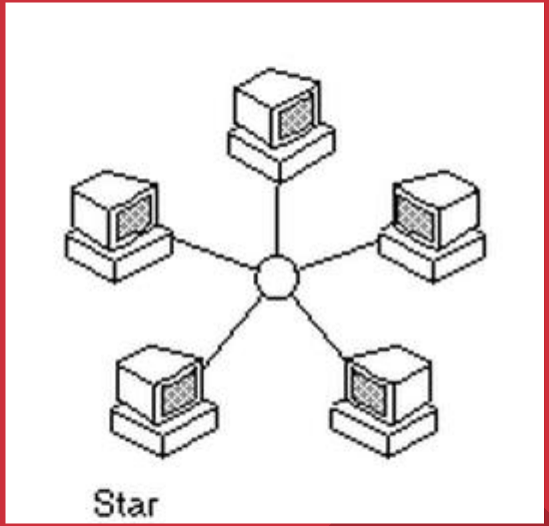
MAC protocols: taxonomy

Three different approaches to channel sharing:

- Channel partitioning
  - divides the channel into smaller pieces
    - Time slots
    - Frequencies
    - codes
  - assigns part of the channel exclusively to a node
- Random access
  - channel is not split, collisions can occur
  - have methods of handling collisions
  - Ethernet (IEEE 802.3)
- “In Order”
  - avoids collisions by only allowing one to send at a time
  - Token Ring (IEEE 802.5)
  - WiFi (IEEE 802.11 with Access Point)







Local Area Network

LAN technologies

Link layer to now:

- services, error detection / correction, multiple access

Next: LAN technologies

- addressing
- Ethernet
- hub, switch
- PPP

LAN addresses (= MAC addresses)

32-bit IP address:

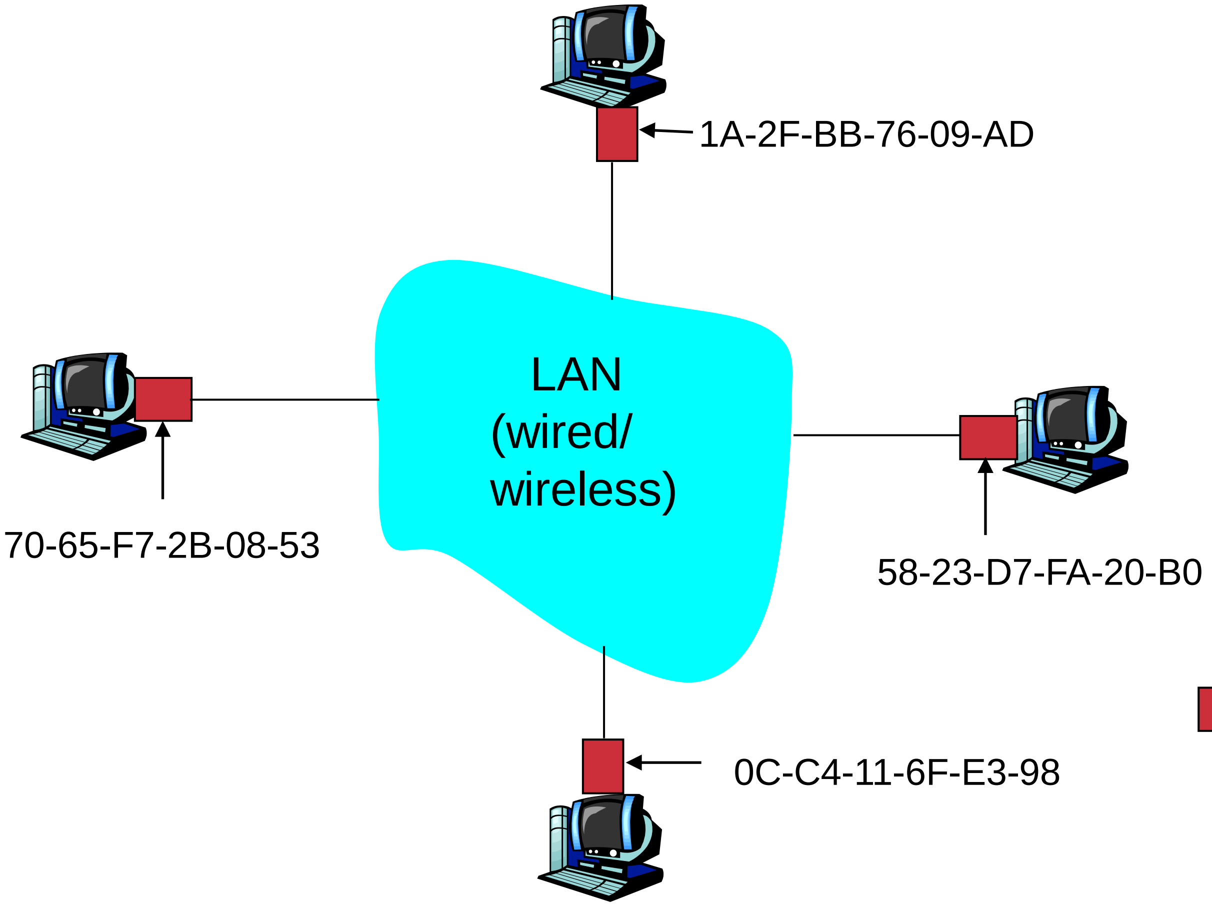
- *network layer address*
- *is used to get the datagram from your IP network to the recipient's IP network*

MAC (or “LAN” or “Physical” or “Ethernet”) address :

- is used to have a frame delivered from one interface to another interface on the same network.
- 48 bit MAC address (for most LANs) burned into the network card ROM

MAC addresses

Each network card has a "unique" MAC address



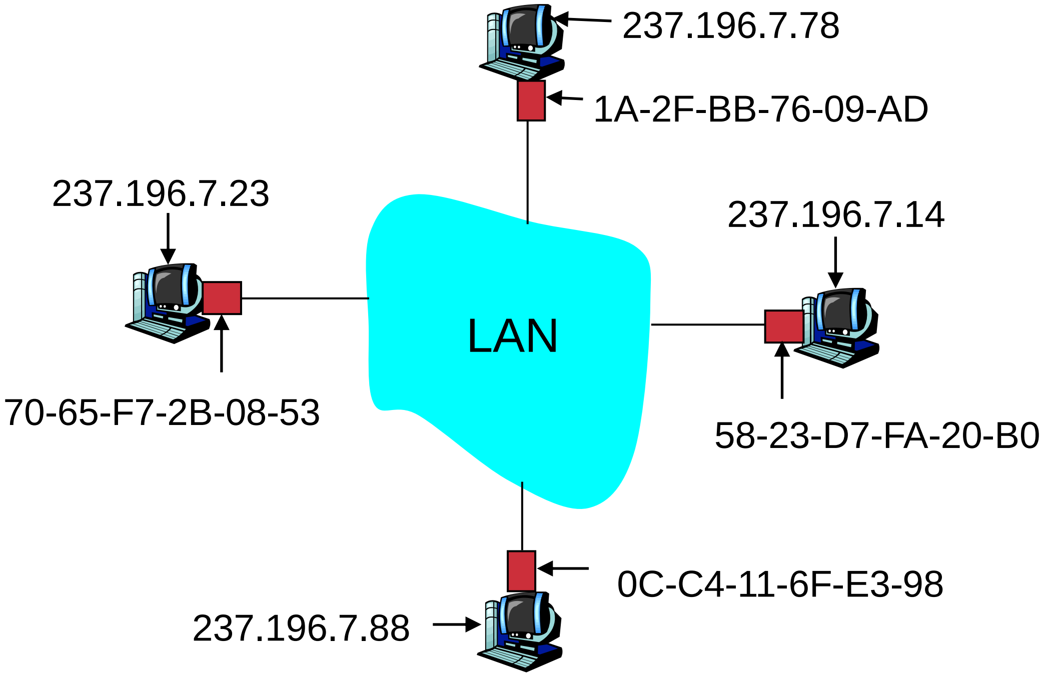
Broadcast address are FF-FF-FF-FF-FF-FF

Multicast MAC addresses start with 01-00-5E

🟥 = network card

ARP: Address Resolution Protocol

How to find MAC-
the address of a node that
you know its IP address?

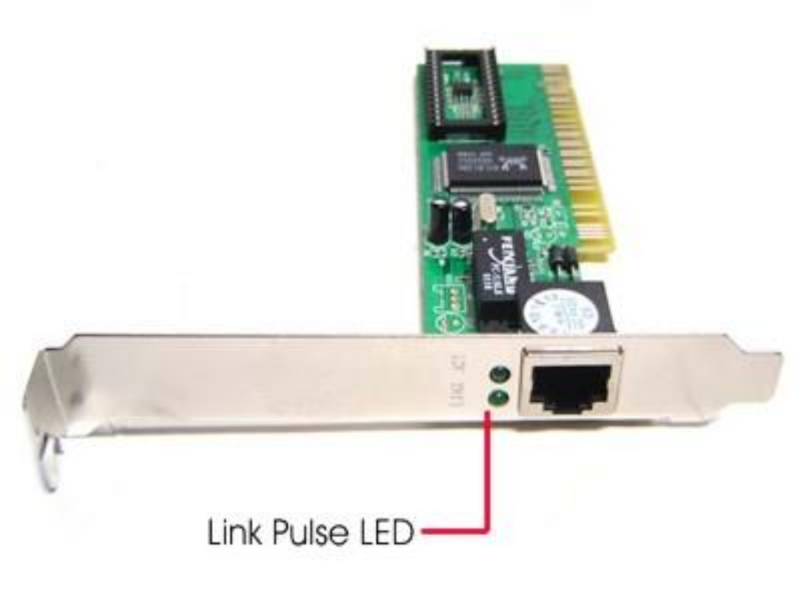


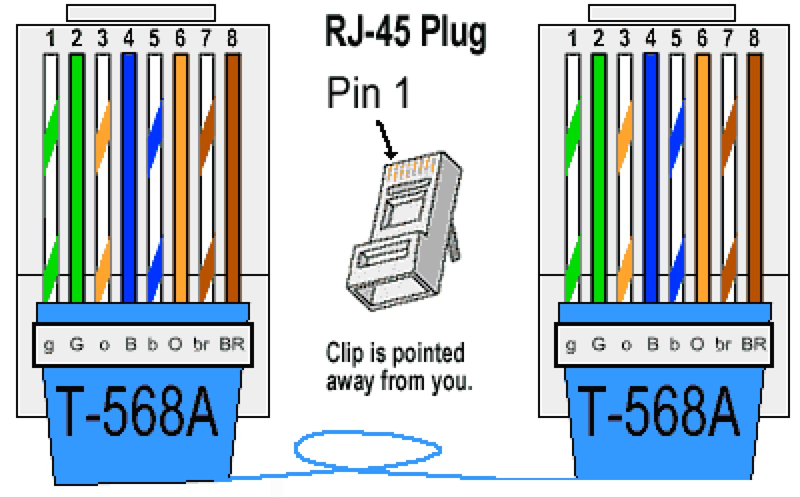
- Each IP node (machine and router) on a LAN has one ARP-table / cache
- ARP table: IP / MAC address mappings for some LAN nodes

  <<IP address; MAC address; TTL>

  TTL (Time To Live): the time the mapping should be in the ARP table (typically 20 min)

Go to menti.com and use code **3372 9155**


Link Pulse LED

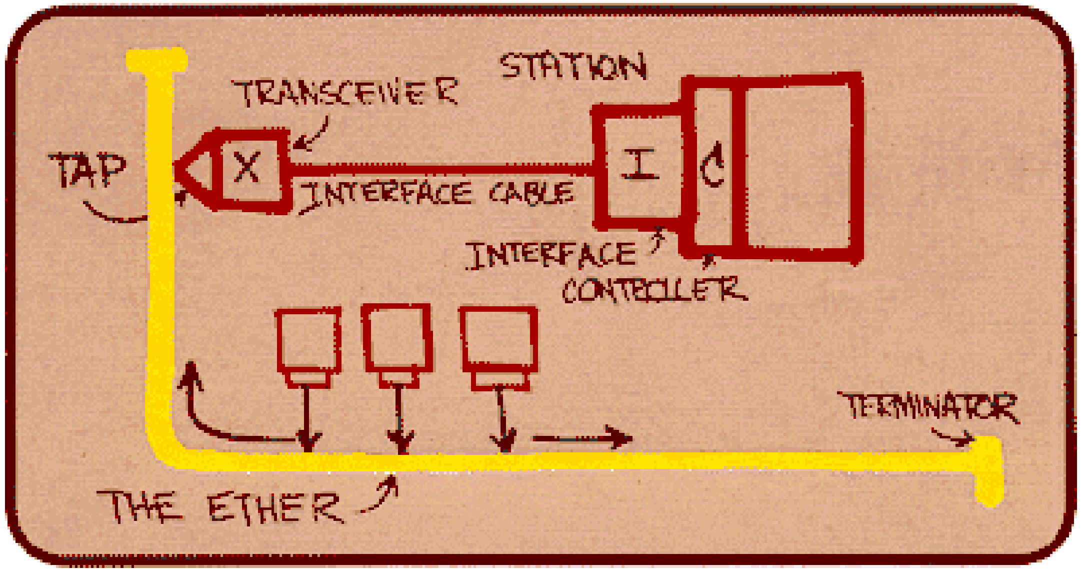

1 2 3 4 5 6 7 8
g G o B b O br BR
T-568A
RJ-45 Plug
Pin 1
Clip is pointed away from you.
1 2 3 4 5 6 7 8
g G o B b O br BR
T-568A

Ethernet

Ethernet

Dominant local network technology:

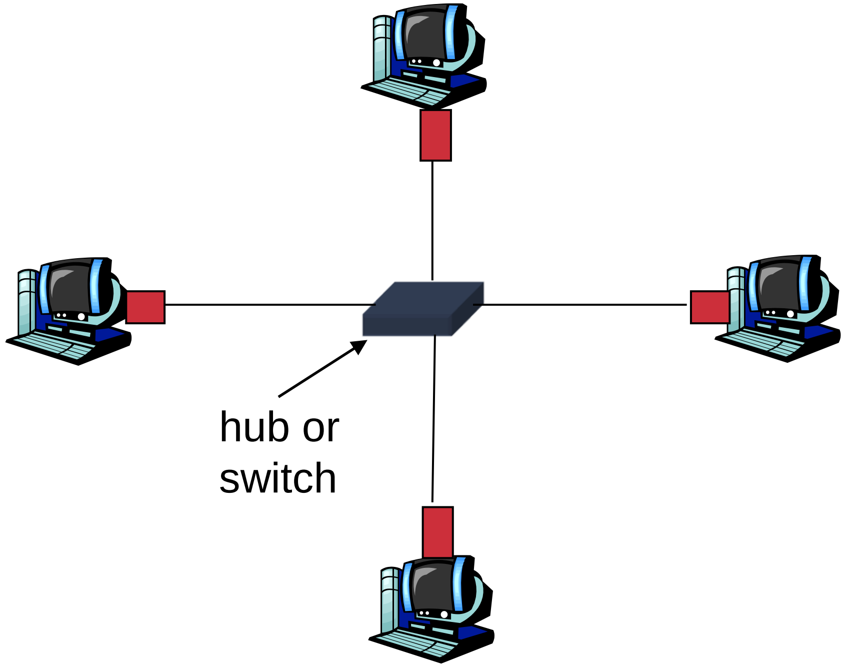
- Cheap
- First LAN technology in widespread use
- Easier and cheaper than token passing LAN
- Has kept pace in the speed race: 10, 100, 1000 Mb / s



Bob Metcalfe's
Ethernet Sketch

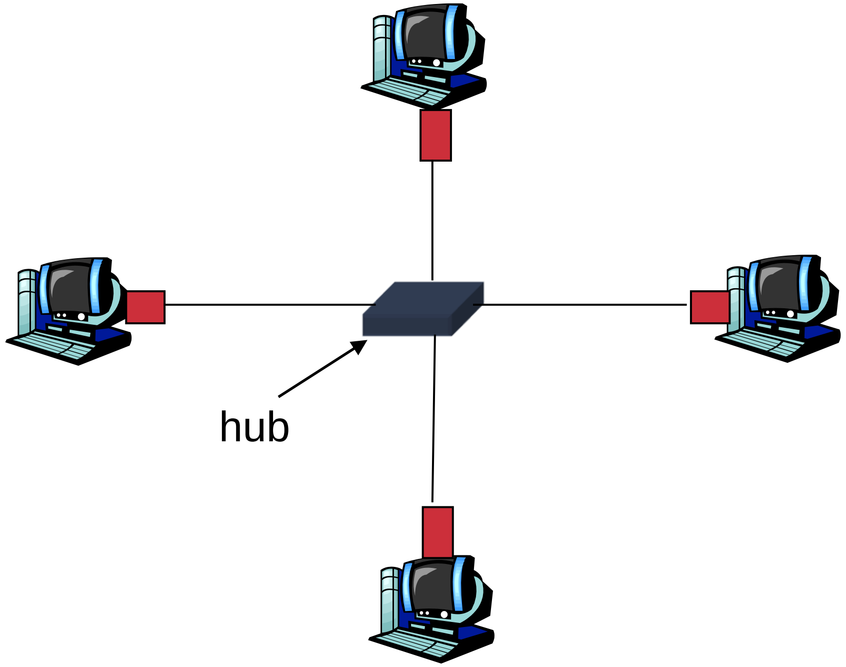
Star topology

- Bus topology was popular until the mid-90s
  - Ethernet is still defined with the assumption of bus topology and how to resolve collisions.
- Now it is the star topology that "goes and applies"
- Option: (hub or) switch (more later)



10BaseT and 100BaseT

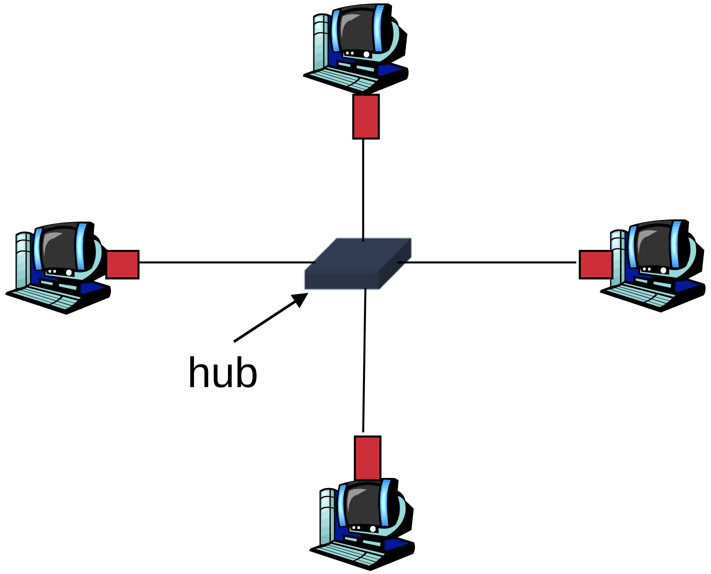
- 10/100 Mbps rate; the latter is called “fast ethernet”
- 1 GbE (1000BASE-T)
  - Uses all thread pairs, and complicated coding
- T stands for “twisted pair”
- Nodes associated with a hub: star topology; max distance from node to hub is about 100 m



Hub

Hubs are multiport repeaters (physical layer):

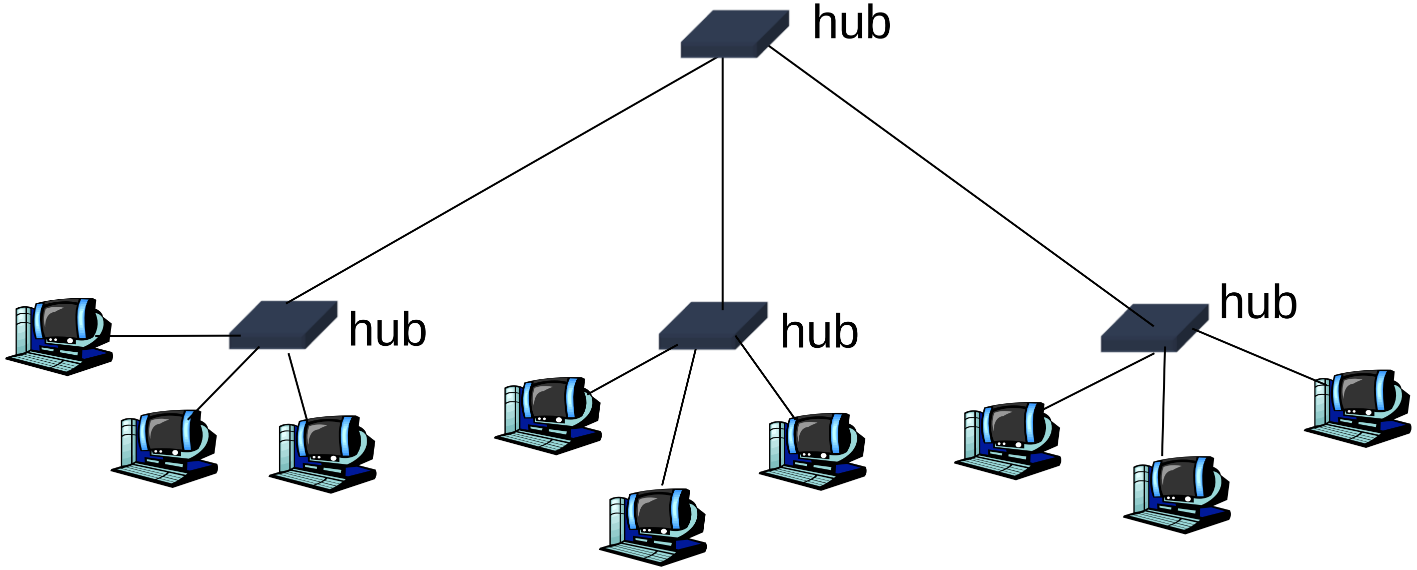
- bits that come in on a link are sent out on all other links
- no buffering of frames
- no collision detection in hub: NIC detects any collisions
- provides certain network management features



Switch

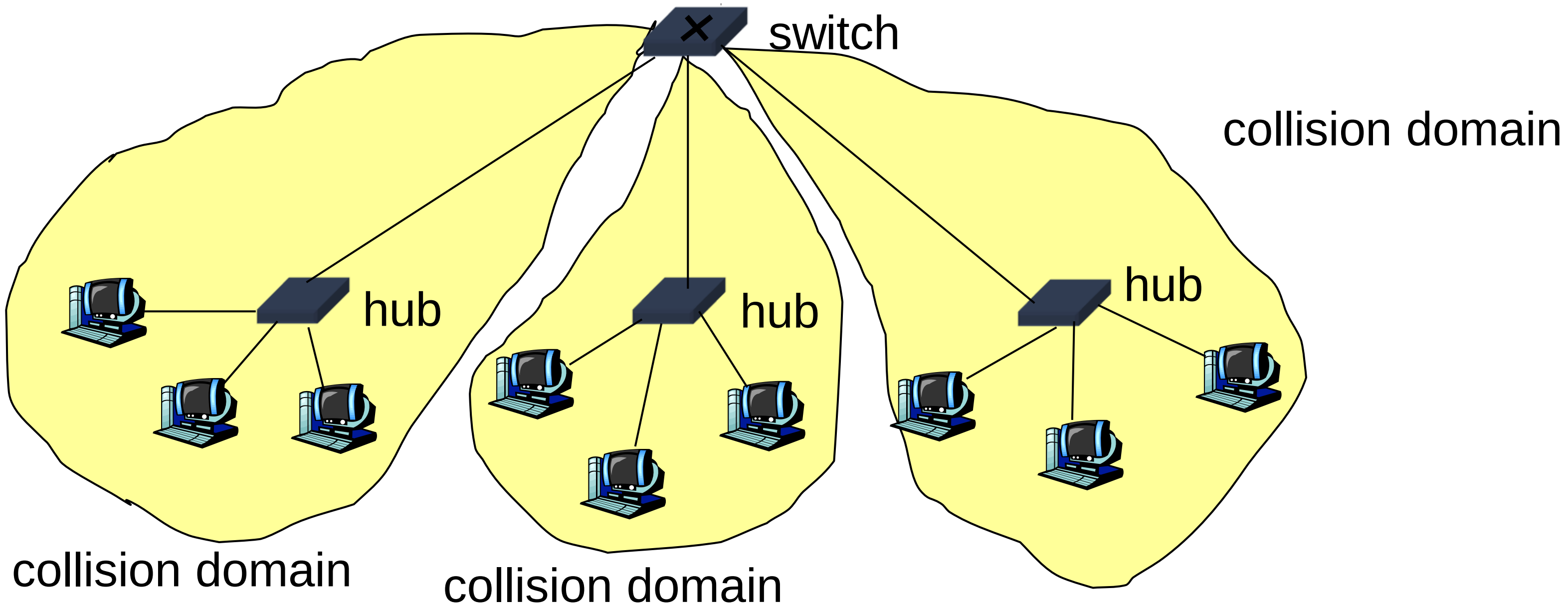
Coupling with hubs

- Spine hub interconnects LAN segments
- Extends the maximum distance between nodes
- Gives a big collision domain (disadvantage)
- Cannot connect 10BaseT and 100BaseT
  - To connect different physical and layer 2 technologies, you need one bridge



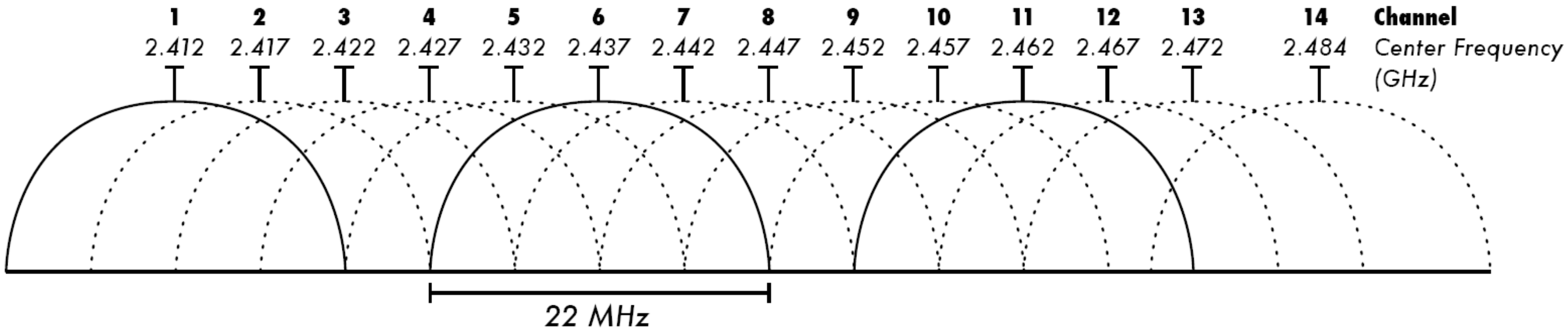
Switch: traffic isolation

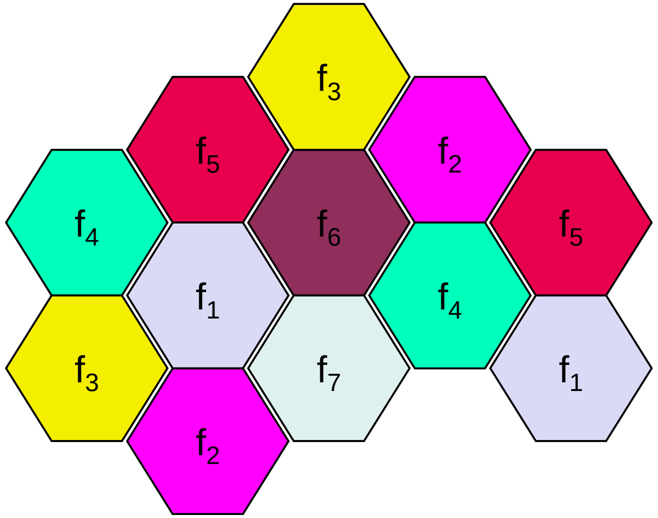
- installing a switch will divide the local network into segments
- Self-learning
- Uses Carrier Sense Multiple Access / Collision Detection (CSMA/CD)
- the switch filters frames:
  - frames going to machine on the same segment will not normally be sent to other segments
  - the segments become separate collision domains



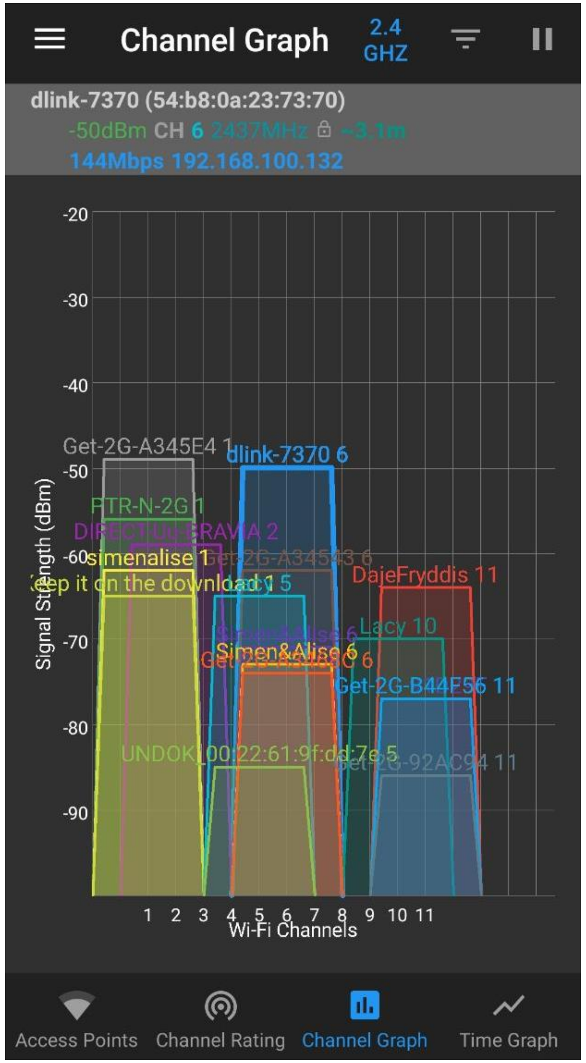
IEEE 802.11

Channels: 1-13, IEEE 802.11 b/g/n Standard





Install the WiFi Analyzer app to see the channels and select a less crowded one!



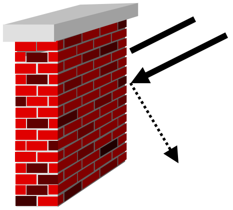
Signal propagation

Signal propagation in free space is the same as light (straight line)
Received effect proportional with $1/d^2$

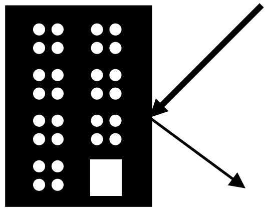
(d = distance between transmitter and receiver)

Received power / signal also affected by

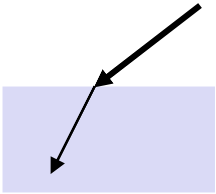
- damping (frequency dependent)
- obstacles
- reflection from major obstacles
- refraction depending on the density of the medium
- scattering from small obstacles
- diffraction on edges (bending of waves)



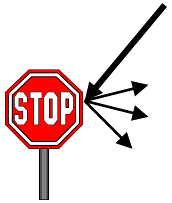
hinder



reflection



refraction

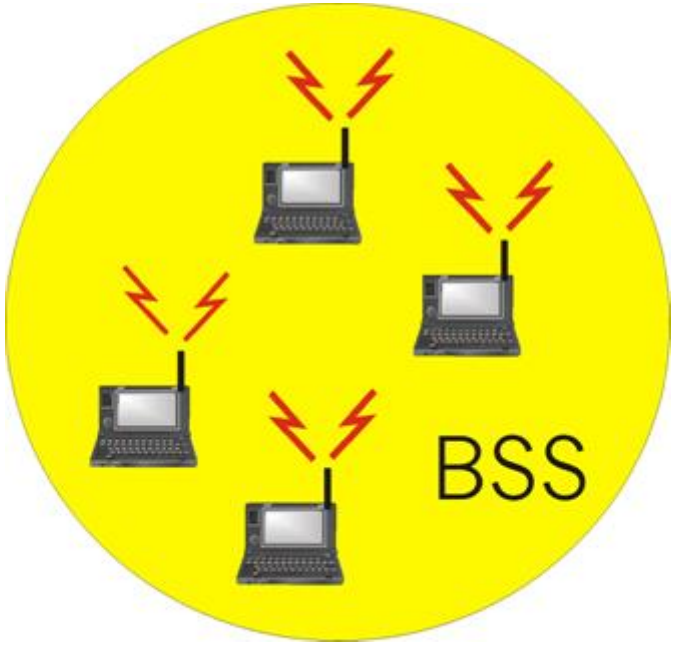


scattering

diffraction

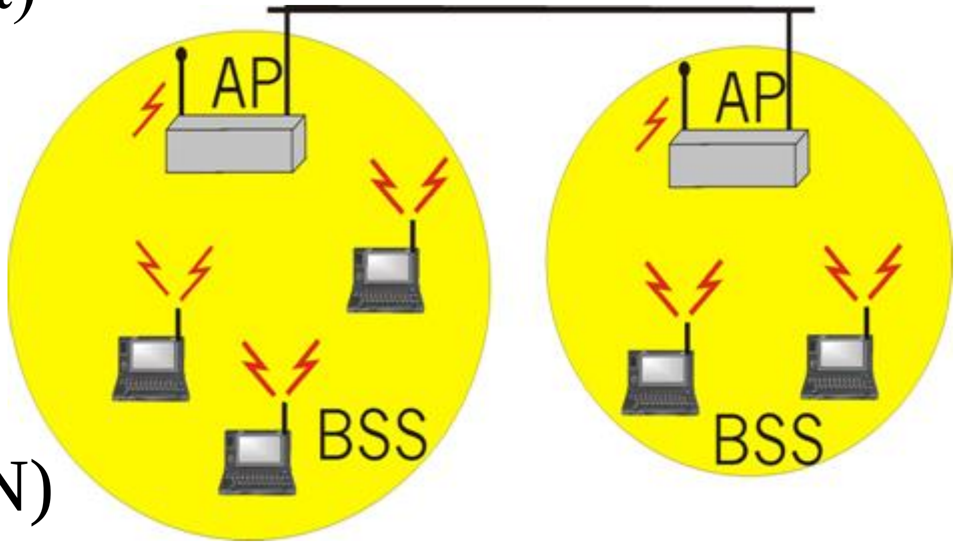
Ad Hoc Network

- No AP (i.e., no base station)
- Wireless host computers communicate directly and act as switches / routers for each other.
- Applications
  - "Laptop" meetings in the car, at the cabin or similar.
  - battlefield
- Uses Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA)



Network with AP

- The hosts communicate via a base station
  - base station = access point (AP)
- Basic Service Set (BSS) (corresponds to “cell” in the mobile phone context) consists of :
  - Wireless hosts
  - Access Point (AP)
- BSSs are combined into one Distribution System (DS) (WLAN)
- BSS has an SSID



Go Go to menti.com and use code **3372 9155**

END

What should we know?

- What tasks are solved on the link layer?
- What error detection mechanisms exist and are used?
  - Calculate parity bits and use 2D parity, calculate CRC
- What are the ways to share medium (MA)?
  - How to avoid or deal with collisions?
- MAC-addresses
  - Structure, multicast, broadcast
- IEEE 802.3 / Ethernet 2
  - Structure of the frame
  - Know the different types.

What should we know?

- Why **ARP** is needed and how it works.
  - Including use of the arp command
- Know the different LAN topologies
  - Bus, star, ring
- Know the difference hub,bridge,switch and router .
- Be able to explain how a switch works
  - How is the switch table built up?
- Be able to explain what new problems need to be solved in wireless networks (IEEE 802.11)
  - Explain the role of the AP, what is the SSID

About the exam (same we went through earlier)

About the exam

There is a 24-hour deadline for this home exam, but the expected workload is 4-6 hours, so it is not the intention to "work through the night". Please note that the exam MUST be submitted within the set deadline, and must be submitted via the exam platform WISEFLOW. It will not be possible to submit the assignment after the deadline - this means that you should submit in good time so that you can contact the exam office or user support if you have technical problems.

As this is a home exam, it is important to show a holistic understanding, and the assignments have a greater character of discussion. Comprehensive and explanatory answers to all assignments are therefore expected. You can choose to draw figures and sketches in the word processor, or by drawing on paper and uploading a picture - remember to insert the picture in the right place in the answer. (Pictures that are attached but not inserted in the answer are not considered part of the answer.)

About the exam

It is emphasized that the student must answer the exam independently and individually, cooperation between students and plagiarism is not allowed.

In arithmetic problems, it is essential that you emphasize how to arrive at the answer. Answers to arithmetic problems without showing procedures are to be regarded as unanswered problems.

NOTE: The answer should not be more than 15 A4 pages, with font size 12, normal margins and line spacing 1.0.

About the exam

Exercise 1: Theory questions (15%)

Exercise 2: Figures and binary data (35%)

Exercise 3: Practical exercises (30%)

The practical exercises will test your understanding of tools and of protocols, they will not be similar to the ones we have had in the exercises, but the exercises will be very relevant!

Exercise 4: “Heavier” theory and understanding (20%)

Today's rehearsal

- Exercises on Canvas

- Write down 3 topics that you feel you are struggling with, and that you need to work on more before the exam
- Remember the rehearsal lecture the day before the exam!

- Complete a previous exam
  - On Canvas under assignments, I have posted exams from 2020
  - In a home exam, there will be a little more focus on showing understanding, and a little less pure "cradle" assignments. This year, as you know, there will also be some practical tasks.
  - Figures and calculations can be drawn on paper, insert the picture in the answer :-)

Examples of practical tasks

- Use a standard network tool on the command line and copy the output from the tool in the answer; for example **traceroute**

- Advanced tools:

In this assignment you will demonstrate an understanding of the use of a raw-socket emulator tool such as ***PuTTY*** *(Windows) or* ***telnet*** *(Linux / OSX), a good understanding of the SMTP protocol is also required to complete this assignment.*

You must connect to SMTP on the standard port (Raw connection type), on host send.one.com. You must send an EMAIL from [candidate number] @ h-ck.me to besvarelse@h-ck.me, the email must be entitled «ASSIGNMENT 42» and body «OK».

What response do you get back from this server (provide full response from server)? Explain the procedure you used to solve the problem.

Høyskolen Kristiania

For optional self-study

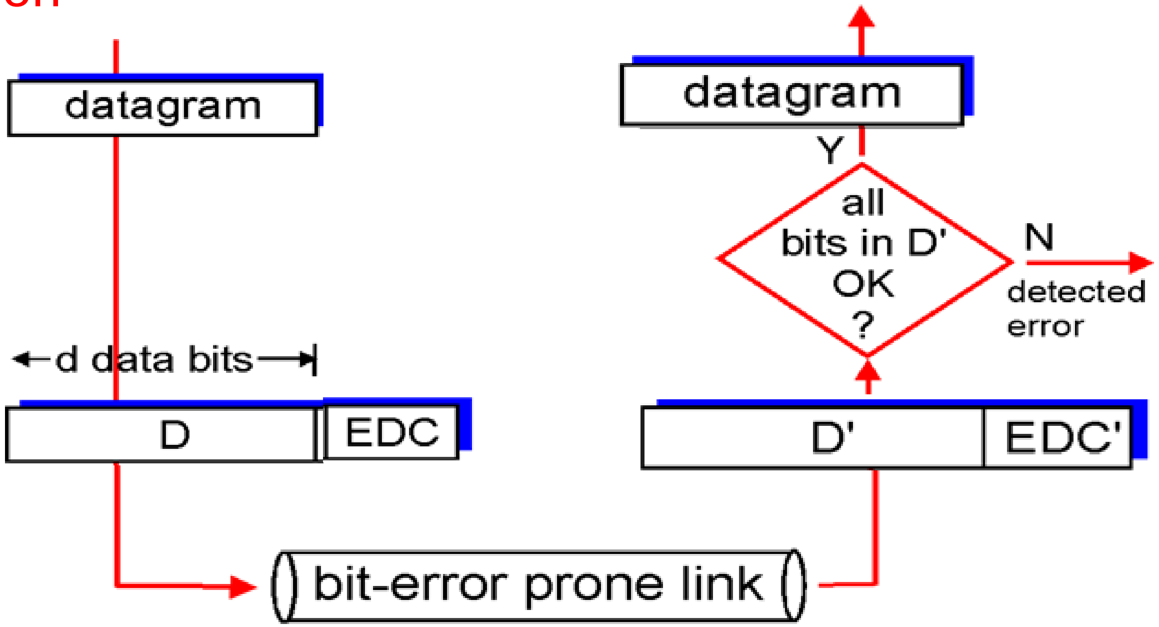
For those who want to learn some topics more in depth to understand it better, here are some extra topics related to today's teaching, it must be expected some personal work to understand these topics.

There will be no questions on the exam from these, and this is therefore not considered to be part of the syllabus.

Error detection

- D = Data protected by error checks may include header fields
- EDC = Error Detection and Correction bits (redundant bit)

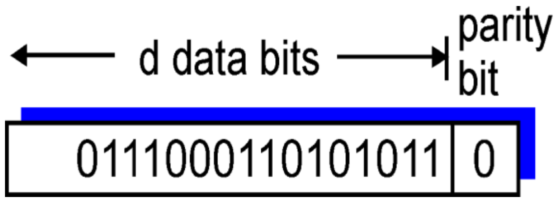
- Error detection is not 100% reliable
  - the protocol can overlook errors (although it is rare)
  - more error detection bits provide better detection and possibility of correction



Parity check

One-bit parity:

Can detect if one bit is wrong



Equal parity:

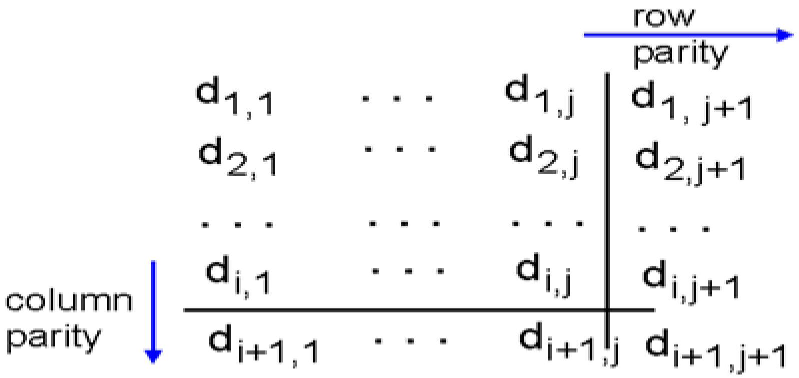
The total number of ones (incl. Parity bit) must be an even number

Odd parity:

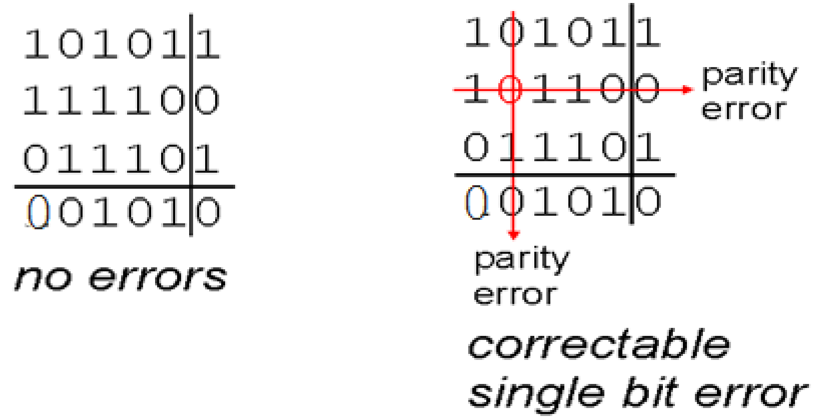
The total number of units (incl. Parity bit) must be an odd number

Two-dimensional parity bits:

Can detect and correct if one bit is wrong



$$\begin{array}{cccc|c} d_{1,1} & \cdots & d_{1,j} & & d_{1,\ j+1} \\ d_{2,1} & \cdots & d_{2,j} & & d_{2,j+1} \\ \cdots & \cdots & \cdots & & \cdots \\ d_{i,1} & \cdots & d_{i,j} & & d_{i,j+1} \\ \hline d_{i+1,1} & \cdots & d_{i+1,j} & & d_{i+1,j+1} \end{array}$$



$$\begin{array}{ccccc|c} 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ \hline 0 & 0 & 1 & 0 & 1 & 0 \end{array}$$

no errors

$$\begin{array}{ccccc|c} 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ \hline 0 & 0 & 1 & 0 & 1 & 0 \end{array}$$

correctable single bit error

Internet checksum (**repetition**)

Goal: detect bit errors in received segment

Sender:

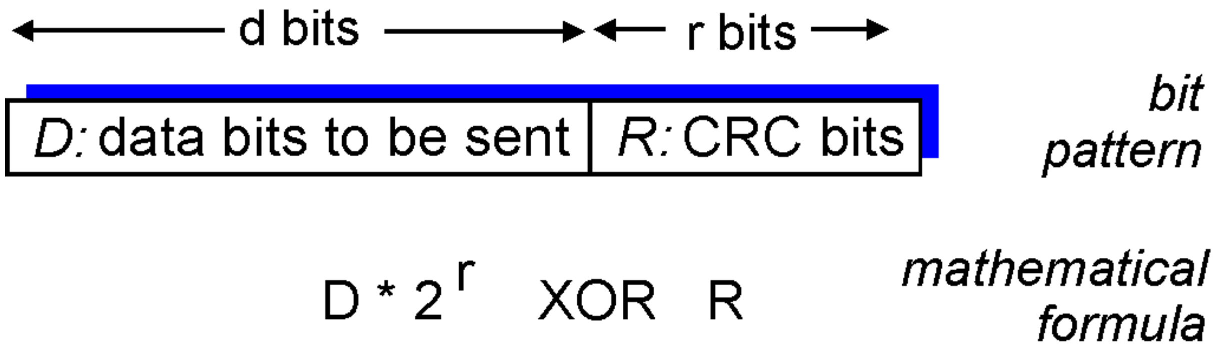
- treats the contents of the segment / datagram as a sequence of 16-bit numbers
- checksum: addition (one complement) of the contents of the segment
- sender enters checksum into UDP / TCP and IPv4 checksum fields

Recipient:

- calculates the checksum of the received segment
- see if the calculated checksum is correct:
  - No ➔ error detected
  - Yes ➔ no errors detected. But there can still be mistakes…

Cyclic redundancy check (CRC)

- ser databitene, D, as a binary number
- velger et bitmønster, r + 1 bit far ➔ generator, G
- goal: choose r CRC-bit, R, so that
  - DR is divisible by G (modulo 2)
  - recipient knows G and divides DR with G.
    If the division gives a residue, there is a bit error
  - discovers all skur-error less than r + 1 bit
- widely used in practice (ATM, HDCL, Ethernet, zip,…)



CRC example

Wants:

$$D \cdot 2^r \text{ XOR } R = nG$$

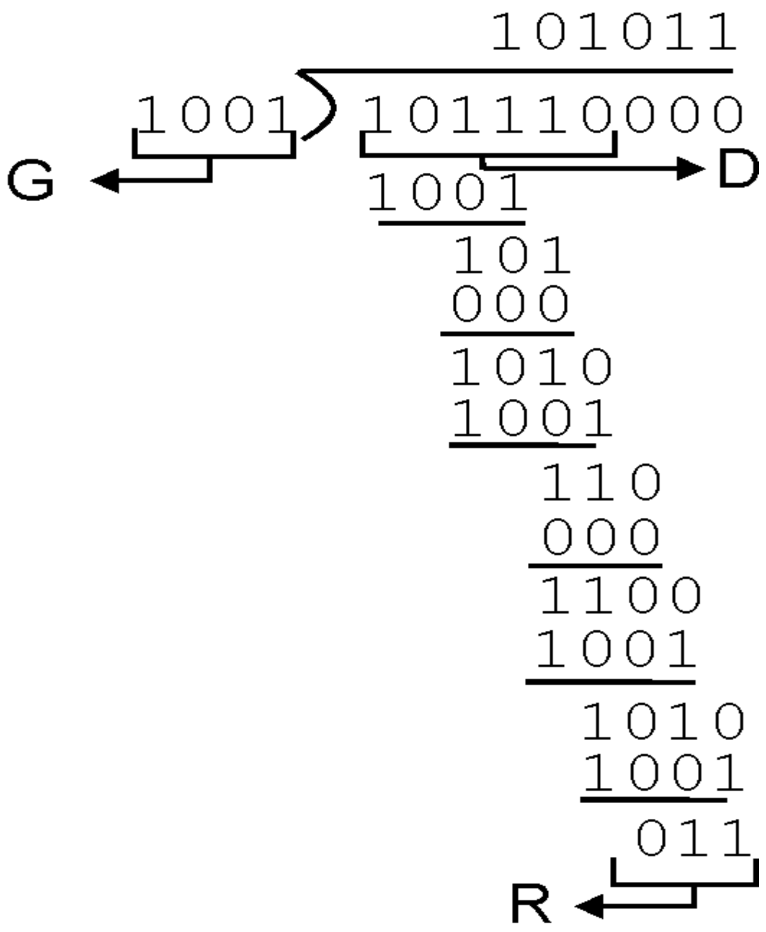
equivalent:

$$D \cdot 2^r = nG \text{ XOR } R$$

equivalent:

if we divide D. 2r with G is the rest, R, we apply

$$\boxed{R = \text{rest}[\frac{D \cdot 2^r}{G}]}$$



CRC-32

- Uses a few different keys
  - $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1$
- Easy to calculate in hardware
  - XOR ports and shift registers
- Detects all burst errors that are 32 bit or less
- Detects 1-2-32 = 99.9999999767% of all errors consisting of more than 32 bits
- Also used by ZIP, MPEG, PNG, etc.

Link layer: context

- Datagram is transmitted by **various link protocols** over various links:
  - e.g.
  - Ethernet on the first link
  - Frame Relay on the next link
  - FDDI (fiber) on the next link
  - …
  - 802.11 on the last link
- Each link layer protocol offers different services
  - eg: one protocol can be reliable, another unreliable

Transport analogy

- trip from Halden to Trondheim
  - train: Halden to Gardermoen
  - flight: Gardermoen to Værnes
  - bus: Værnes til Trondheim
- travelers = datagram
- transport stage = communication link.
- Transport type = link layer protocol
- travel agency = routing algorithm

“In turn” MAC protocols

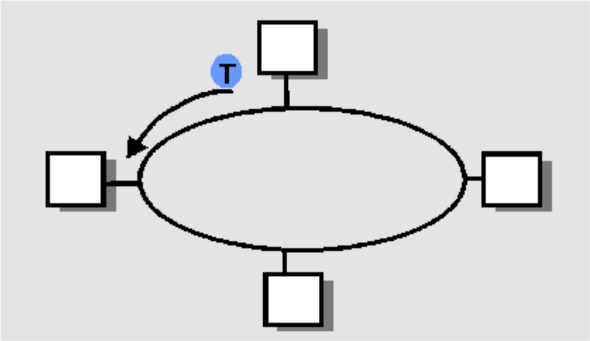
Alternative access options exist and are used in some places, e.g. IEEE 802.5

Polling:

- master node "invites" slave nodes to send - one at a time
- cons:
  - overhead due to polling
  - latency - have to wait for turn
  - single point of failure (master)

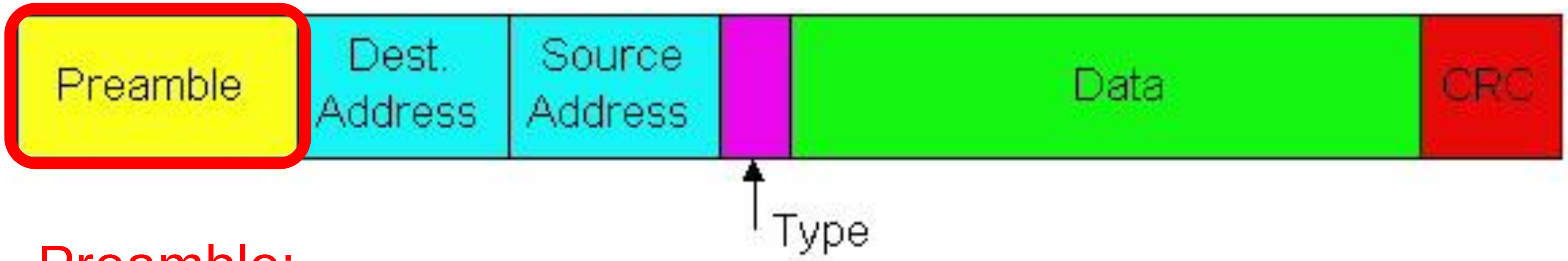
Token passing:

- ❒ a special frame - token (baton), sent from node to node
- ❒ token message
- ❒ cons:
  - ❍ token overhead
  - ❍ latency (delay)
  - ❍ single point of failure (token)



Ethernet frame structure

Network adapter (NIC, adapter) puts the IP datagram (or other layered PDU) into a Ethernet frame

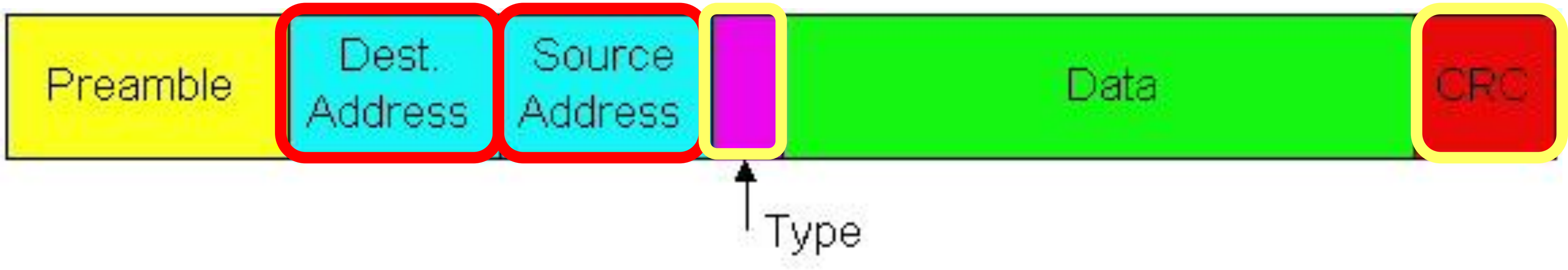


Preamble:

- 7 octets (7 bytes) with bit pattern 10101010 followed by one octet with bit pattern 10101011
- is used to synchronize the receiver's "clock" with the transmitter's

Ethernet frame structure (continued)

- Addresses: 6 octets (48 bit)
  - if the NIC receives a frame with its own address as the destination address or a broadcast frame (eg ARP packet), it delivers data in the frame to the network layer protocol
  - otherwise it throws the frame
- Type: indicates which web layer protocol the data belongs to (normally IP, but also other possibilities, eg Novell IPX or AppleTalk)
- CRC: cyclic redundancy check - if an error is detected, the frame is discarded



Ethernet CSMA/CD the algorithm

Web cards get datagrams from web layers and create a frame

2. Sender listens to the media to see if it is available. If no one else is listening, the network card will start sending. If the media is busy, it waits until it becomes available and then sends

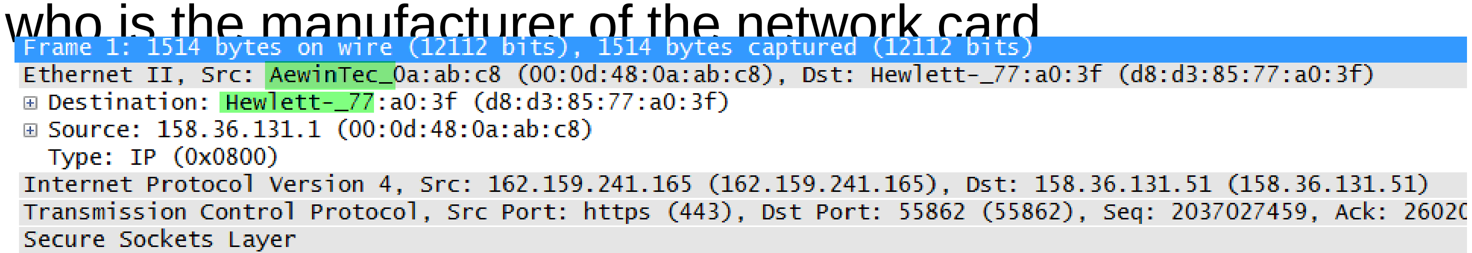
3. If the entire frame is sent without a collision, the network card is finished with the frame

4. If the transmitter detects another transmitter at the same time as it, it interrupts the transmission and sends a jam signal instead.

5. After the interruption, the transmitter will make an "exponential backoff": after collision no. M, the transmitter randomly selects a K from the set {0,1,2,…, 2m-1}. Then it waits K · 512 bit times and returns to step 2.

MAC addresses

- MAC address assignment is managed by the IEEE
- manufacturer buys part of the MAC address space
  - The first 24 bit tells who is the manufacturer of the network card



```
Frame 1: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: AewinTec_0a:ab:c8 (00:0d:48:0a:ab:c8), Dst: Hewlett-_77:a0:3f (d8:d3:85:77:a0:3f)
⊞ Destination: Hewlett-_77:a0:3f (d8:d3:85:77:a0:3f)
⊞ Source: 158.36.131.1 (00:0d:48:0a:ab:c8)
  Type: IP (0x0800)
Internet Protocol Version 4, Src: 162.159.241.165 (162.159.241.165), Dst: 158.36.131.51 (158.36.131.51)
Transmission Control Protocol, Src Port: https (443), Dst Port: 55862 (55862), Seq: 2037027459, Ack: 26020
Secure Sockets Layer
```

- Analogy:

(a) MAC-address: personal number

(b) IP-address: postal address

- MAC has a "flat" address structure ➔ portability
  - can easily move a network card from one local area network to another, provided that MAC address filtering is not set up in the AP or switch
- IP addresses are hierarchical and therefore not portable
  - The prefix part of the IP address indicates which network the computer is hanging on

Random access protocols

- When a node has packets to send
  - Transmitter with full channel rate, R
  - no a priori coordination between the nodes
- two or more transmitters simultaneously ➔ “collision”,
- random access MAC protocol specifies:
  - how collisions are detected
  - how to deal with collisions (e.g. using delayed retransmissions)
- Examples of random access MAC protocols:
  - slotted ALOHA
  - ALOHA
  - CSMA, CSMA / CD, CSMA / CA

ARP (Address Resolution Protocol)

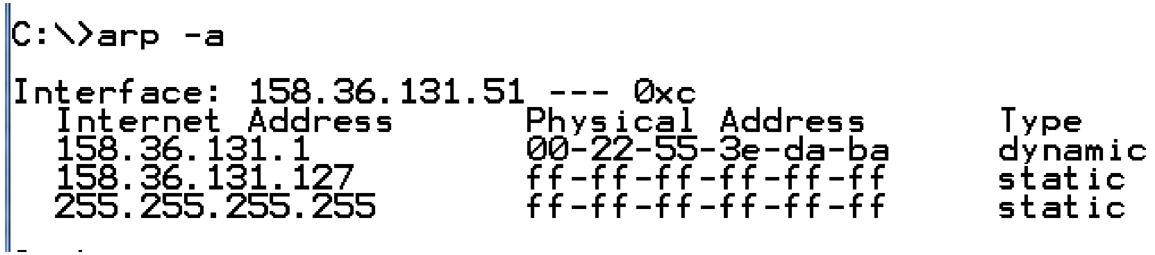
- A wants to send a datagram to B and knows B's IP address
  - Assume that B's MAC address is not in A's ARP table
- A broadcasts an ARP request that contains B's IP address
  - all machines on the LAN receive the ARP request
- B also receives the ARP packet and answers A with his MAC address
  - frame is sent directly to A's MAC address

- A caches the IP-to-MAC address pair in its ARP table until the information becomes obsolete
  - “Soft state": information that disappears if it is not refreshed.

- ARP is “plug-and-play”:
  - a node creates its ARP table without the help of anyone

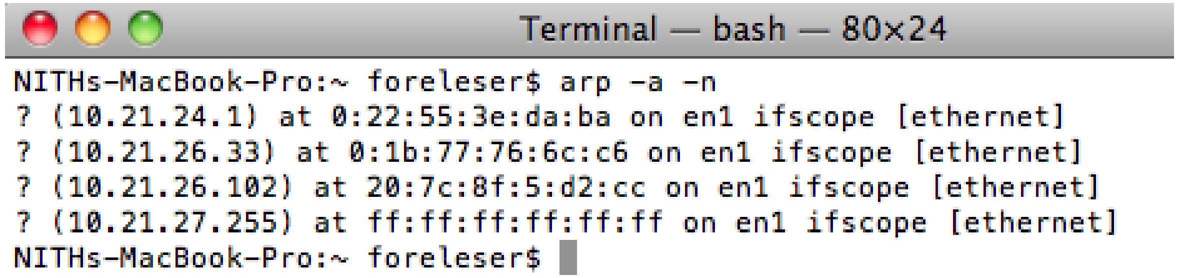
arp

- The arp-command can be used to
  - display ARP cache(-a)
  - clear ARP cache(-d)
  - Add fixed IP-MAC connections(-s)



```
C:\>arp -a

Interface: 158.36.131.51 --- 0xc
  Internet Address      Physical Address      Type
  158.36.131.1          00-22-55-3e-da-ba     dynamic
  158.36.131.127        ff-ff-ff-ff-ff-ff     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```



```
NITHs-MacBook-Pro:~ foreleser$ arp -a -n
? (10.21.24.1) at 0:22:55:3e:da:ba on en1 ifscope [ethernet]
? (10.21.26.33) at 0:1b:77:76:6c:c6 on en1 ifscope [ethernet]
? (10.21.26.102) at 20:7c:8f:5:d2:cc on en1 ifscope [ethernet]
? (10.21.27.255) at ff:ff:ff:ff:ff:ff on en1 ifscope [ethernet]
NITHs-MacBook-Pro:~ foreleser$ 
```

Unreliable, unconnected service

- Unconnected : No handshake between sender and receiver
  - On the other hand, the network cards negotiate which IEEE 802 version and bit rate they will use the first time they are connected.
- Unreliable: receiver does not send ACK or NAK back to the transmitter
  - the flow of datagrams delivered to the web layer may have gaps
  - if TCP is used, this will fill any gaps
  - otherwise the application will / must see the gaps in the data stream

Ethernet uses CSMA / CD

- No time slots
- network card listens online before sending (carrier sense)
  - does not send if someone else is already sending
- the transmitter continues to listen while transmitting and interrupts the transmission if it notices that another is also transmitting (collision detection)

- Before the transmitter attempts a retransmission, it waits a randomly selected time(random access)

Ethernet CSMA / CD (continued)

Jam signal: to make sure everyone is aware of the collision; 48 bit

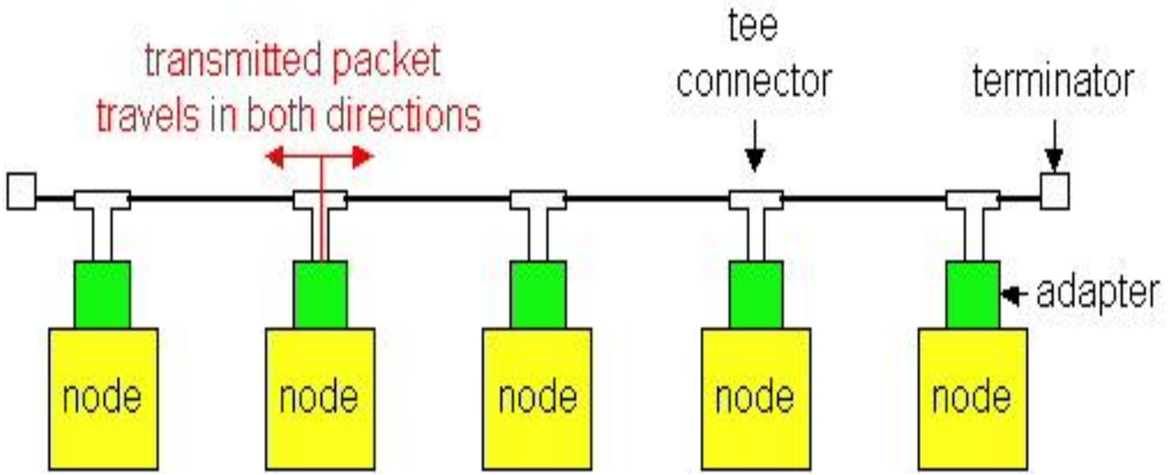
Bit time: 10 ns for 100 Mb / s Ethernet; for K = 1023, consequently, the waiting time will be about 5 ms

Exponential Backoff:

- *Goal*: adapts retransmission attempts to currently estimated load
  - heavy load: random waiting time often longer
- first collision: select K from {0, 1}; latency is K · 512 bit times
- after second collision: select K from {0,1,2,3}
- after ten collisions: select K from {0, 1, 2, 3, 4,…, 1023}
- If still no transmission time: Give up ..

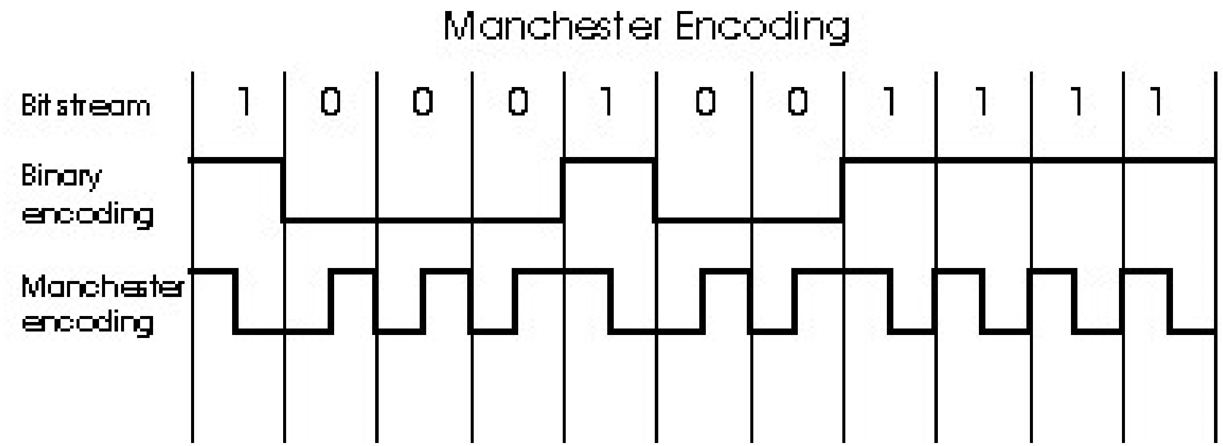
Ethernet technologies: 10Base2

- 10: 10 Mb/s; Base: baseband; 2: max 200 meters cable
- thin coaxial cable in a bus topology



- max 30 nodes per segment
- repeaters are used to connect several segments
- repeater repeats bit it hears on one interface on its other interface: operates on physical layer!

Manchester coding



- Used in 10BaseT and 10Base2
- Each bit has a transition (low-to-high or high-to-low)
- Enables synchronization of transmitter and receiver
- receiver must know where each bit starts
- no need for centralized, global clock
- (This belongs to the physical layer - not the link layer)

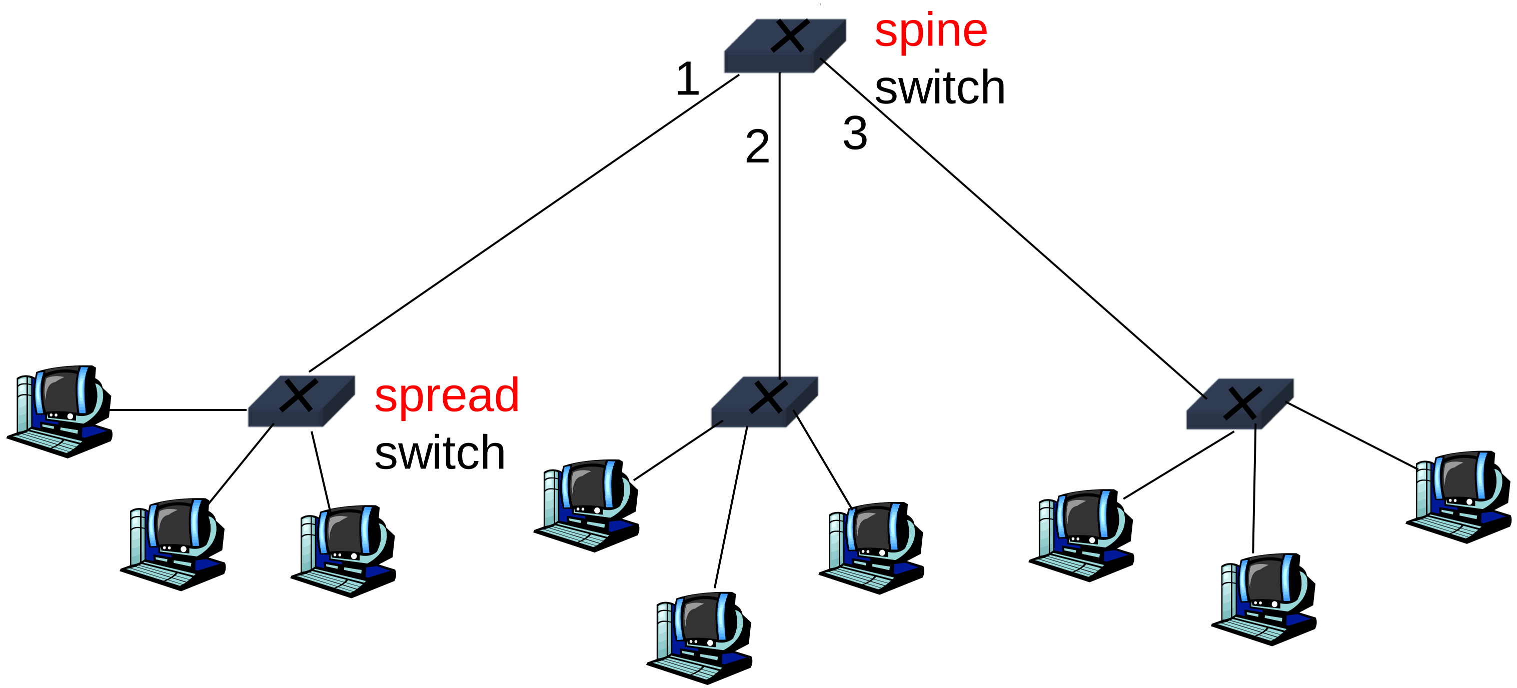
Gigabit Ethernet (1000Base-T)

- uses standard ethernet frame format
- Uses all four wire pairs in the UTP cable
- for shared channels, CSMA / CD is used; should have short distances between nodes for peak performance, but can be used up to 100 m
- Uses several advanced coding techniques: 5 level pulse amplitude modulation etc.
- Full-duplex at 1 Gb / s for point-to-point links
- Also available for fiber etc.
- 10 Gbps exists and is constantly gaining ground
- Many different physical standards (PHY)
- 10GBASE-T for Cat 6, 6A or 7 UTP with RJ45

Switch

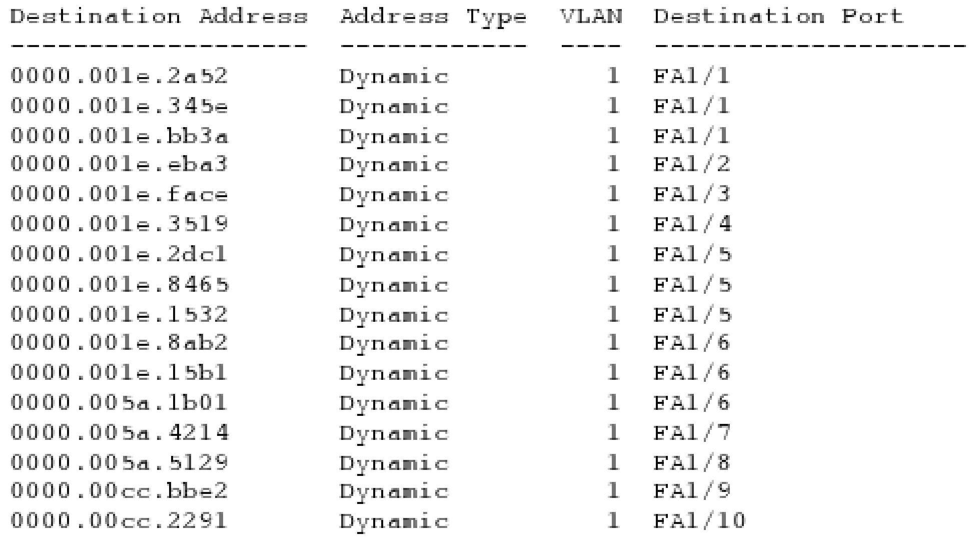
- Link layer box
  - caches and forwards Ethernet frames
  - checks frameheads and forwards when needed– based on the recipient's MAC address
  - when the frame is to be forwarded on a segment, CSMA / CD is used
- transparent
  - machines are unaware of the presence of the switch
- plug-and-play, self-learning
  - switches do not need to be configured

Forwarding



- How to decide which LAN segment the frame should be sent to?
- Looks like a routing issue ..

Self-learning



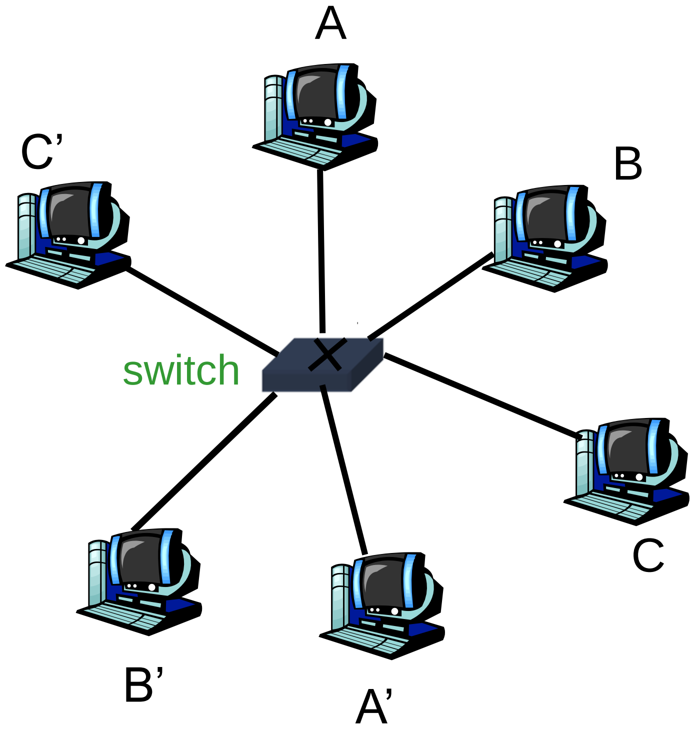
```
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
0000.001e.2a52       Dynamic          1  FA1/1
0000.001e.345e       Dynamic          1  FA1/1
0000.001e.bb3a       Dynamic          1  FA1/1
0000.001e.eba3       Dynamic          1  FA1/2
0000.001e.face       Dynamic          1  FA1/3
0000.001e.3519       Dynamic          1  FA1/4
0000.001e.2dc1       Dynamic          1  FA1/5
0000.001e.8465       Dynamic          1  FA1/5
0000.001e.1532       Dynamic          1  FA1/5
0000.001e.8ab2       Dynamic          1  FA1/6
0000.001e.15b1       Dynamic          1  FA1/6
0000.005a.1b01       Dynamic          1  FA1/6
0000.005a.4214       Dynamic          1  FA1/7
0000.005a.5129       Dynamic          1  FA1/8
0000.00cc.bbe2       Dynamic          1  FA1/9
0000.00cc.2291       Dynamic          1  FA1/10
```

- A switch has a switch-table
- rows in the switch table :
  - (MAC address, interface, timestamp)
  - obsolete elements in the table are deleted (TTL can be 60 min)
- The switch *learns* which machines can be accessed on the various interfaces
  - when it receives a frame, the switch will "remember" which segment the frame came from combined with the sender's MAC address
  - saves this in its switch table

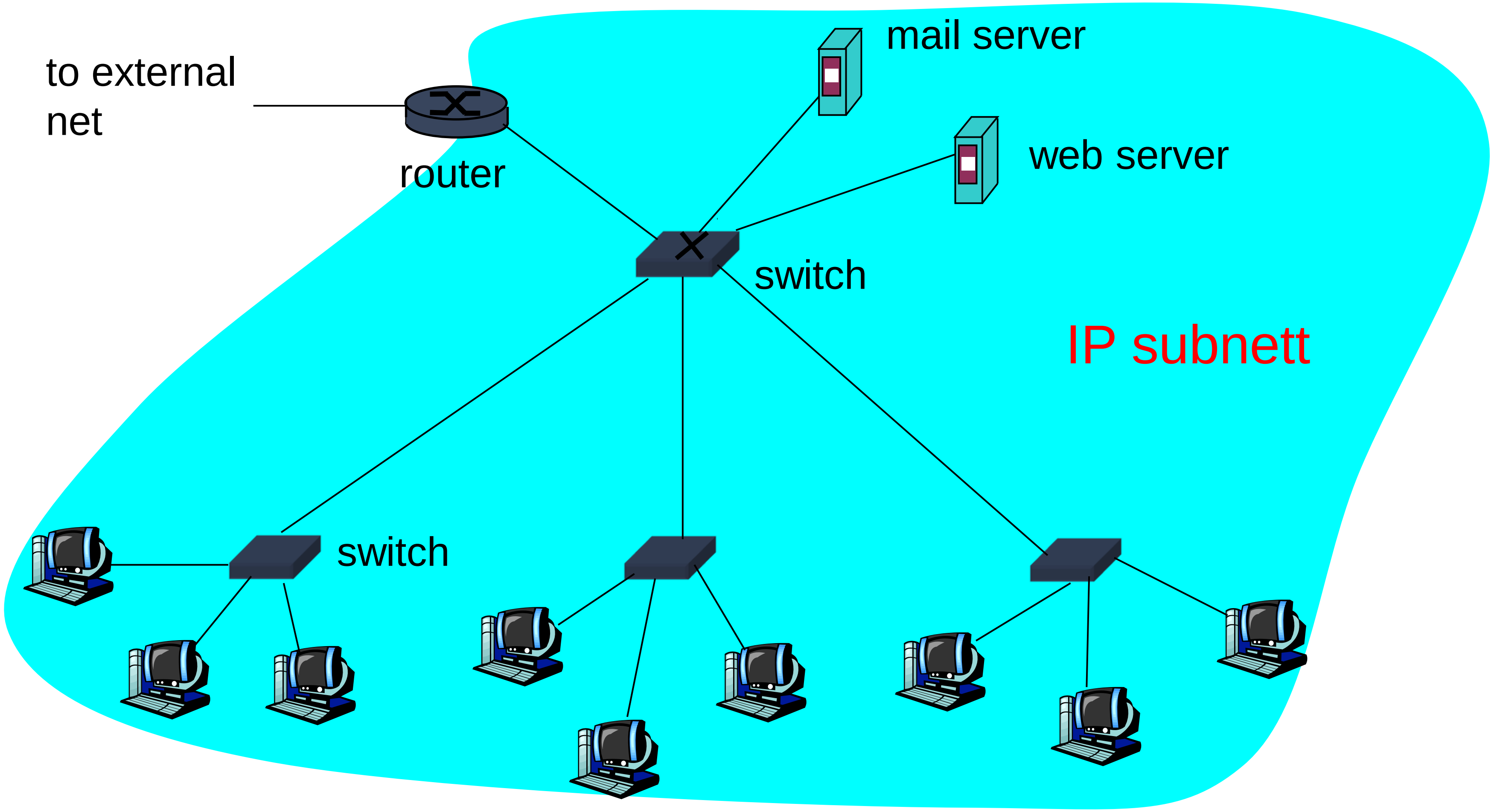
Switches: dedicated access

- Switch with many interfaces
- Machines have a direct connection to the switch
- No collisions, full duplex

Switching : A-to-A 'and B-to-B' at the same time, no collisions

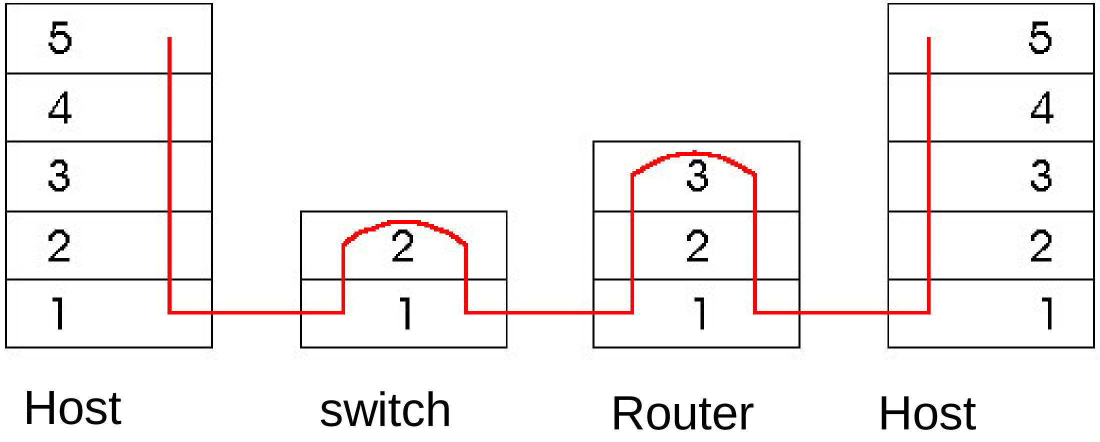


Network for an institution



Switches vs. routers

- both are "store-and-forward" devices
  - routers: layer layer devices (looks at layer layer headers)
  - switches are link layer devices
- routers use routing tables and implement routing algorithms
- switches use switch tables, do filtering, and have self-learning

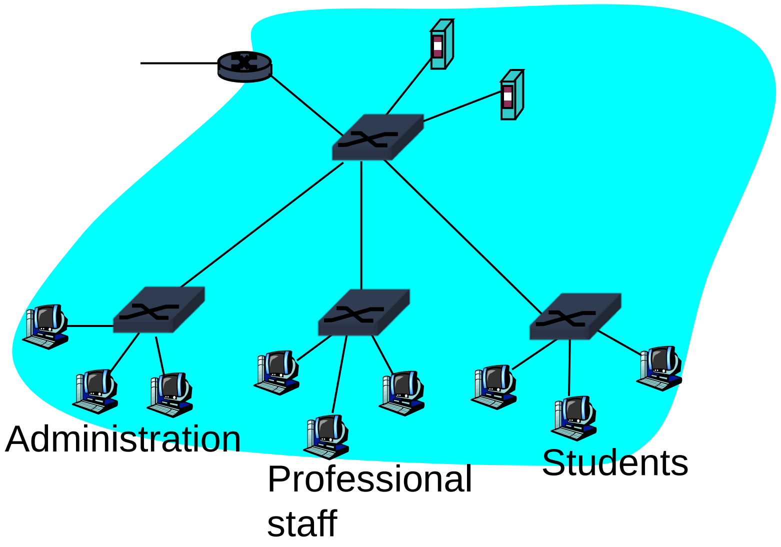


Comparison - summary

	hub	router	switch
Traffic - isolation	no	yes	yes
plug & play	yes	no	yes
optimal routing	no	yes	no
cut through	yes	no	yes

VLAN: motivation

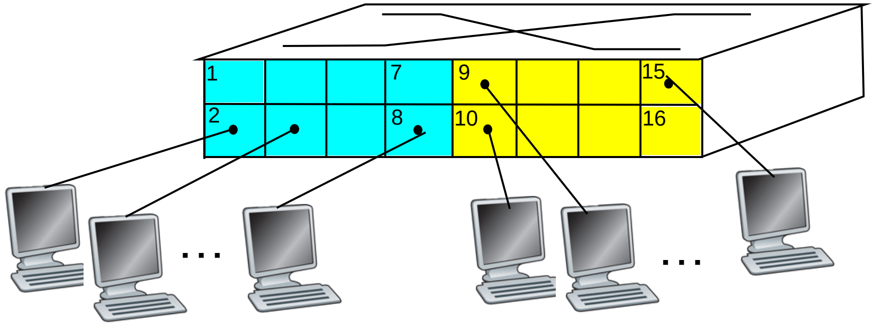
What's wrong with this LAN?



- What happens if: Adm user changes office to Fagstab corridor, but will continue to hang on Adm switch?
- A single broadcast domain:
  - all layer-2 broadcast traffic (ARP, DHCP) is sent to the entire LAN (security / privacy, inefficient
- The spreading switches use only a few of their ports.

Virtual LAN

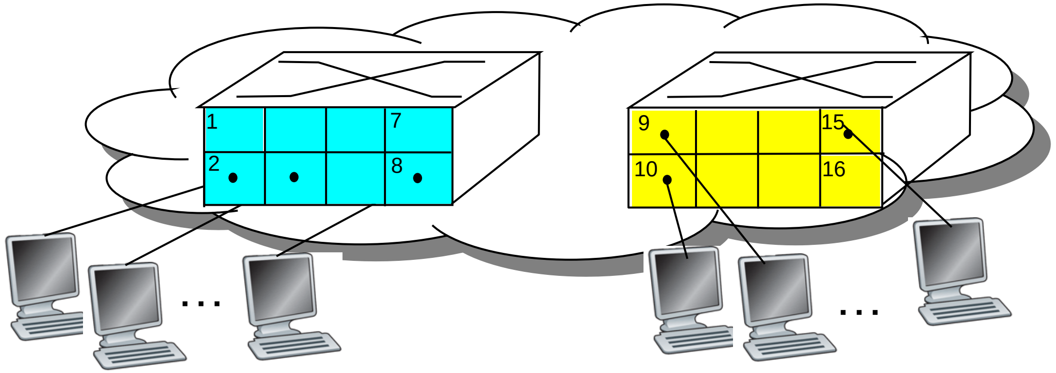
Port-based VLAN: switch ports are grouped (with switch management software) such a *single* physical switch ……



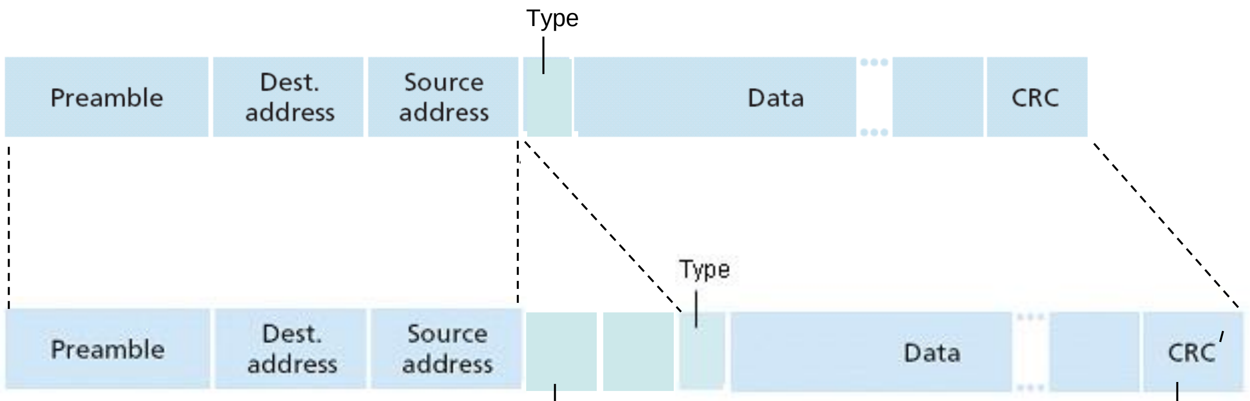
Virtual Local Area Network

Switch (s) that support VLAN can be configured to define more **virtual** LAN in a simple physical LAN.

… Acts as multiple virtual switches



802.1Q VLAN frame format



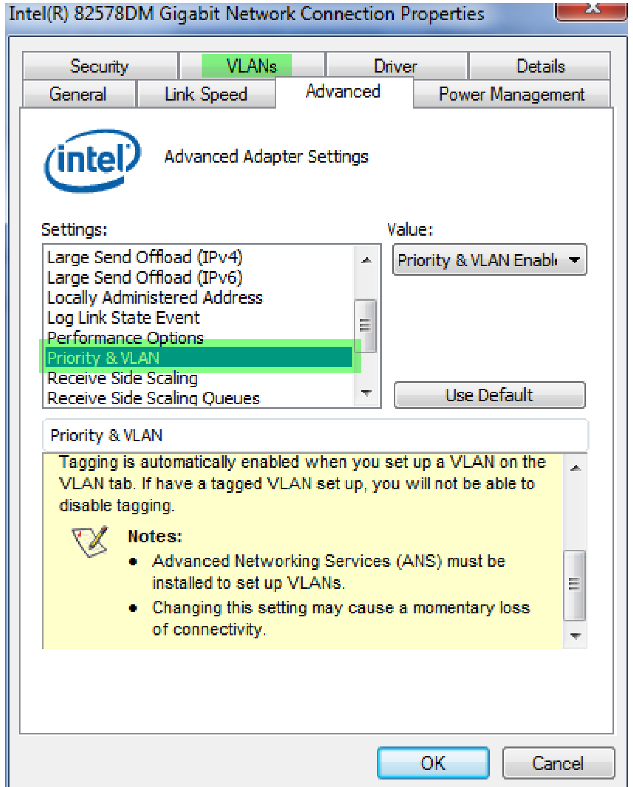
802.3 frame

802.1Q frame

2-byte Tag Protocol ID (value: 81-00)

Converted CRC

Tag Control Information (12 bit VLAN ID field, 3 bit priority field, cf. IP TOS)



Advanced Adapter Settings

Settings:
- Large Send Offload (IPv4)
- Large Send Offload (IPv6)
- Locally Administered Address
- Log Link State Event
- Performance Options
- Priority & VLAN
- Receive Side Scaling
- Receive Side Scaling Queues

Value: Priority & VLAN Enabl

Priority & VLAN

Tagging is automatically enabled when you set up a VLAN on the VLAN tab. If have a tagged VLAN set up, you will not be able to disable tagging.

Notes:
- Advanced Networking Services (ANS) must be installed to set up VLANs.
- Changing this setting may cause a momentary loss of connectivity.

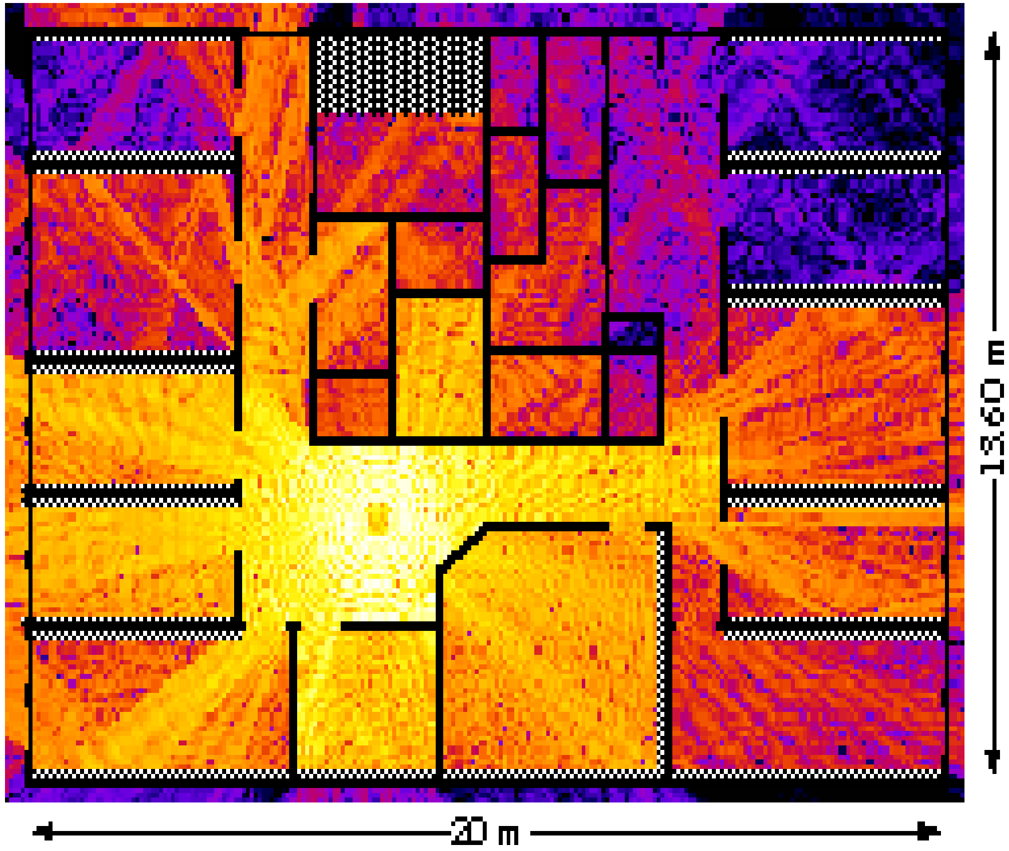
IEEE 802.11 Wireless LAN (Wi-Fi)

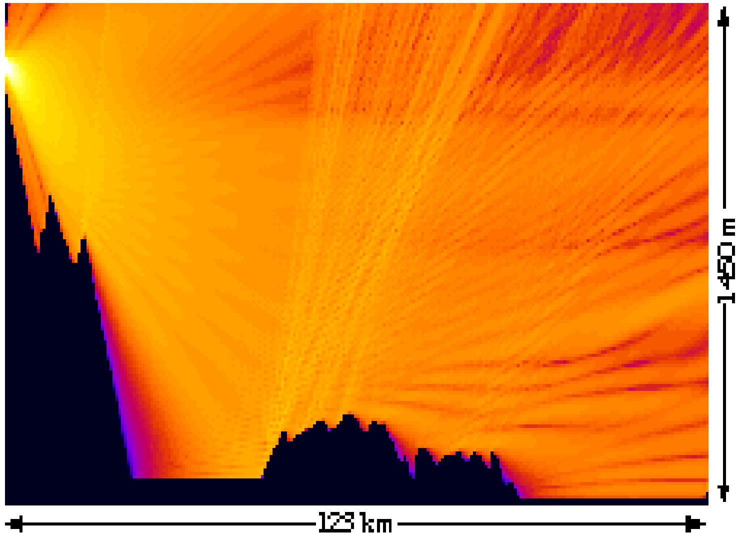
- Everyone uses CSMA/**CA** for access
- All offer both base station (AP) and ad-hoc network versions

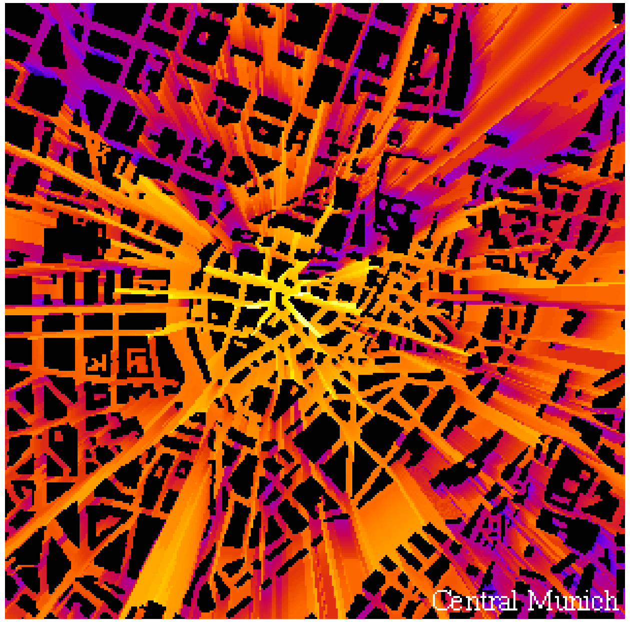
- 802.11b
  - 2.4 GHz license-free radio waveband
  - up to 11 Mbps
  - direct sequence spread spectrum (DSSS) in physical layer
  - Similar to CDMA, but all hosts use the same "chipping code"
  - Range 38/140 m
  - Begins to be phased out in favor of g and n; but most wireless cards still support it.

- 802.11a
  - 5-6 GHz
  - up to 54 Mbps
  - OFDN
- 802.11g
  - 2.4 GHz range
  - Up to 54 Mbps
- 802.11n
  - 2.4 and / or the 5 GHz range
  - Up to 150 Mbps
  - Range 70/250 m
  - Multiple (4) antennas (MIMO)
  - Forward Error Correction

Example: radio radiation / intensity







IEEE 802.11 MAC Protocol: CSMA/CA

802.11 CSMA: transmitter

- if sense channel available for **DISF** seconds.

then transmit entire frame (no collision detection)

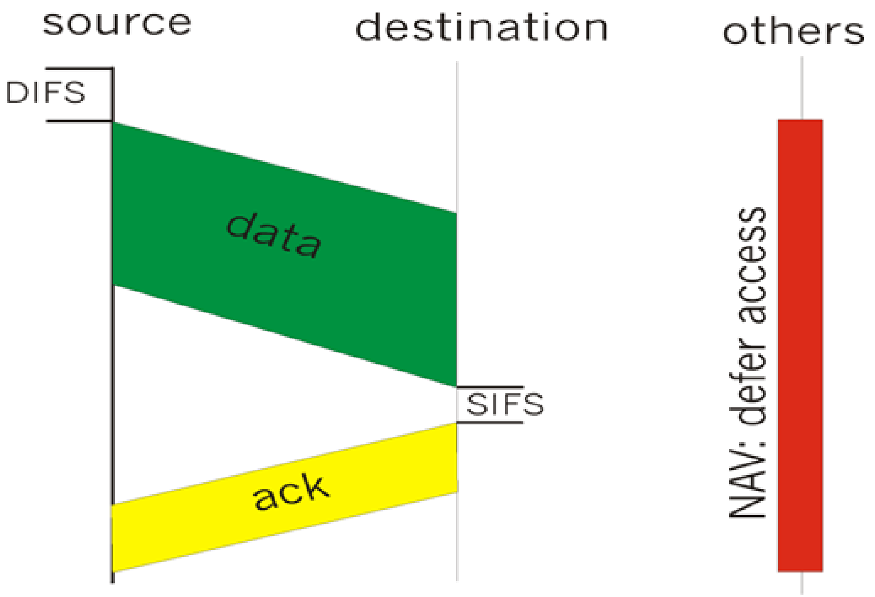
-if sense channel busy then binary backoff

802.11 CSMA receiver

- if received OK

send ACK after SIFS

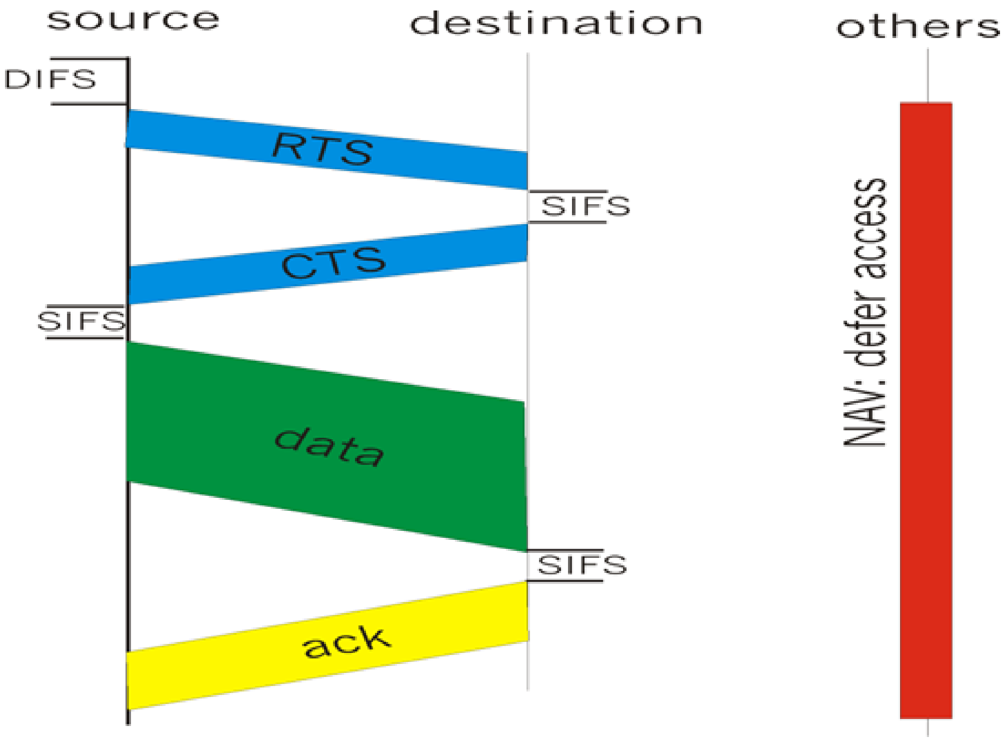
(ACK required due to "hidden nodes issue")



DIFS = Distributed Inter Frame Spacing
SIFS = Short Inter Frame Spacing

RTS-CTS exchange

- Sender transmits card RTS (request to send) packet: indicates the duration of the transmission
- Recipient responds with short CTS (clear to send) package
  - alerts (possibly hidden) other nodes
- Hidden nodes then refrain from sending in the reserved time: NAV

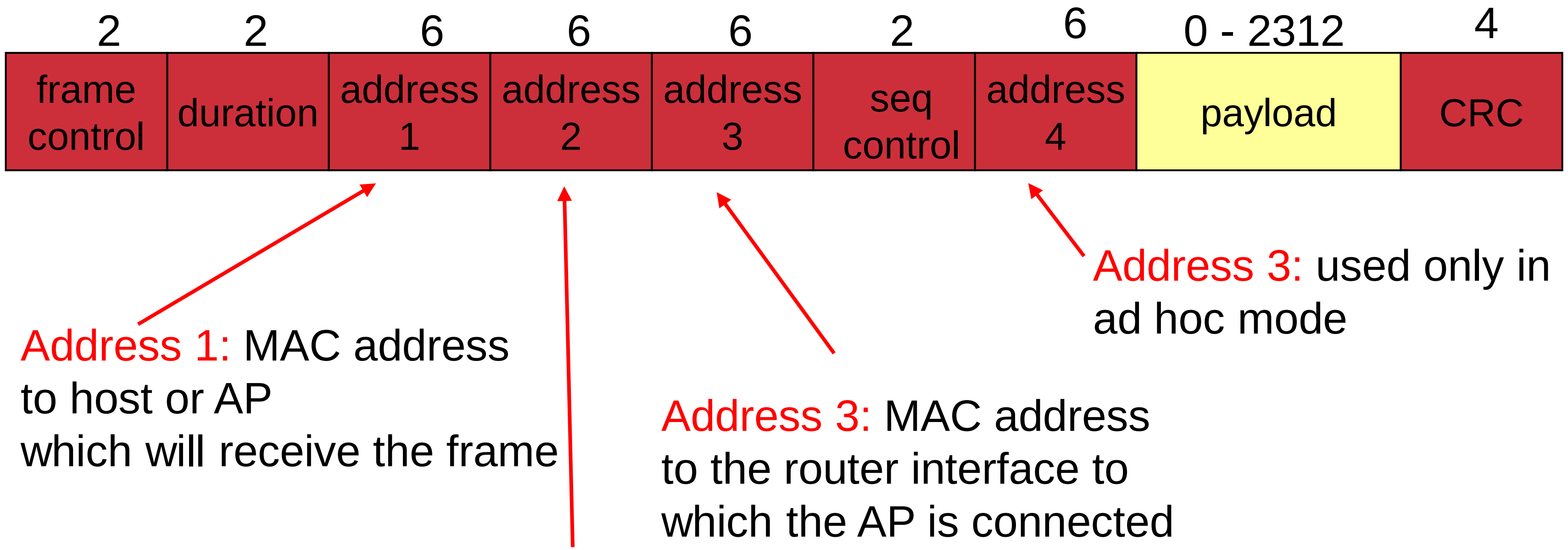


Different CAs

- IEEE 802.11 thus allows:
  - "Pure" CSMA
  - CSMA / CA
  - Reservations

  - Polling from AP
    - AP assigns time to each node on loop (RR)

802.11 frame: addressing



2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

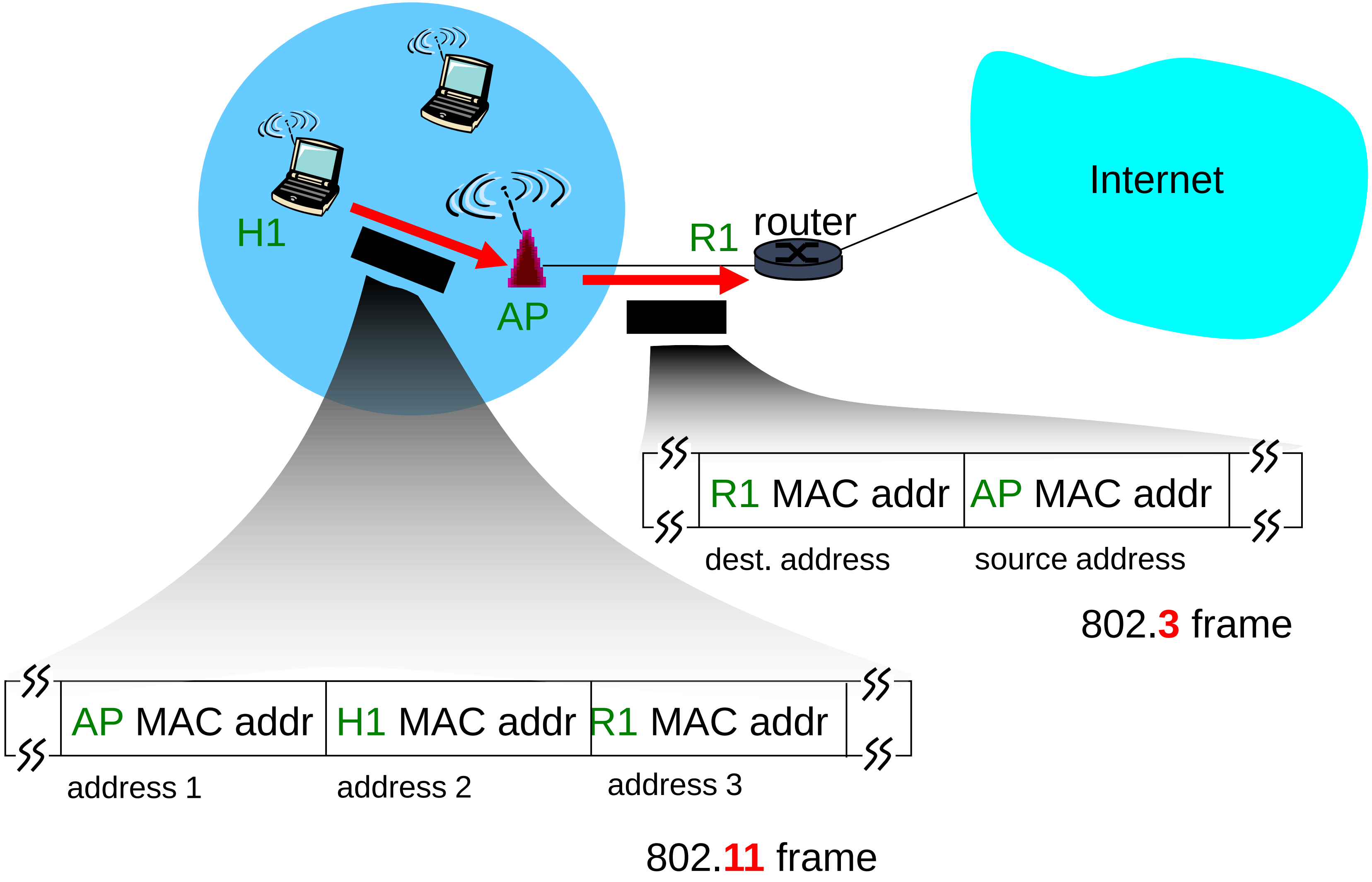
Address 3: used only in ad hoc mode

Address 1: MAC address to host or AP which will receive the frame

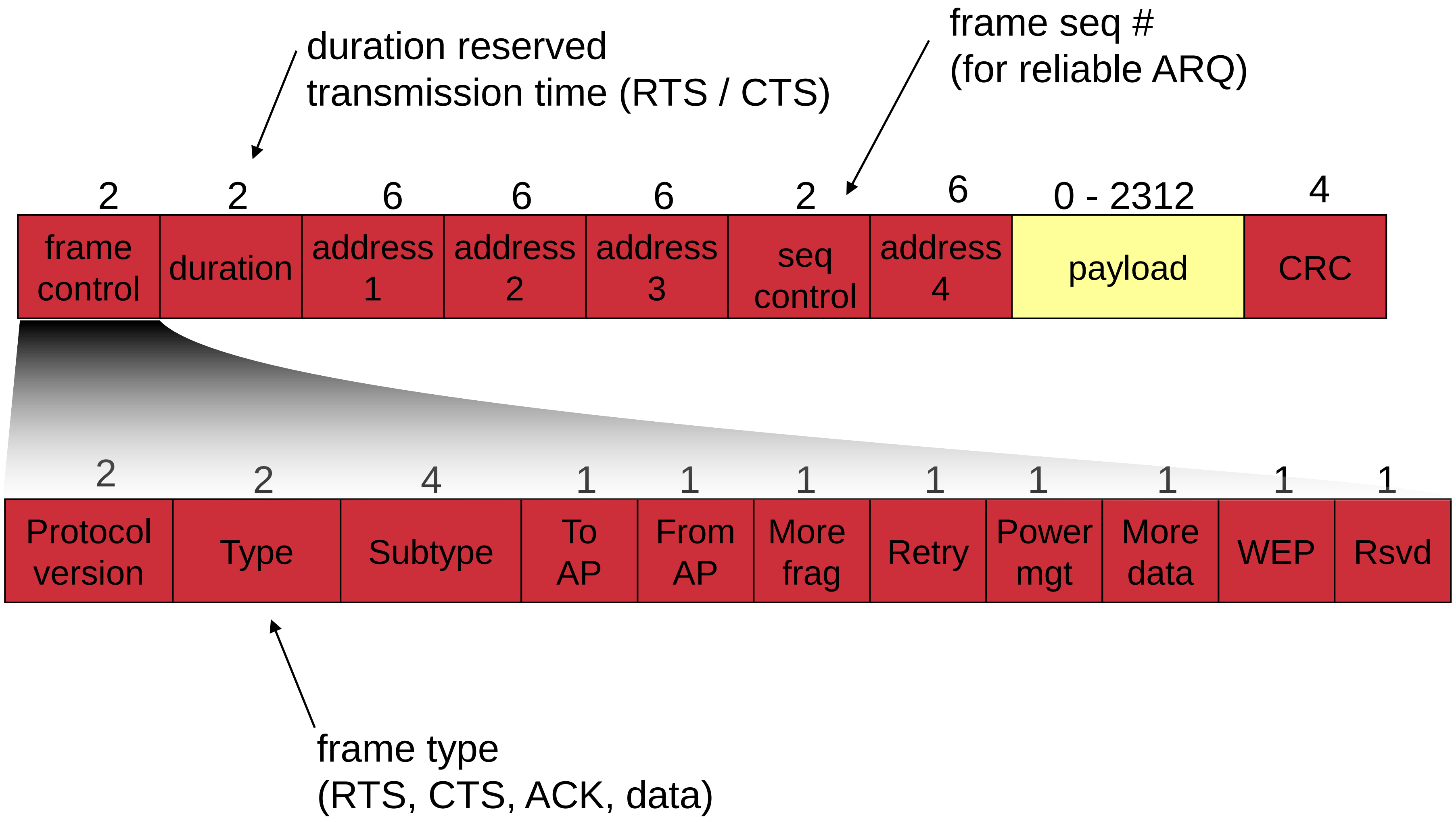
Address 3: MAC address to the router interface to which the AP is connected

Address 2: MAC address to host or AP which sends the frame

802.11 frame: addressing



802.11 frame: more



duration reserved transmission time (RTS / CTS)

frame seq # (for reliable ARQ)

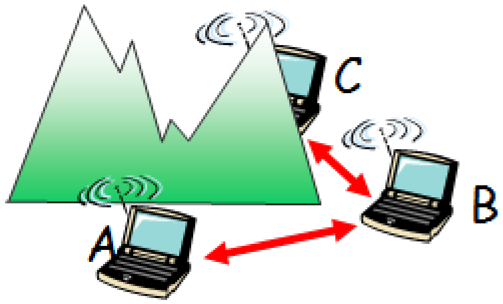
2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

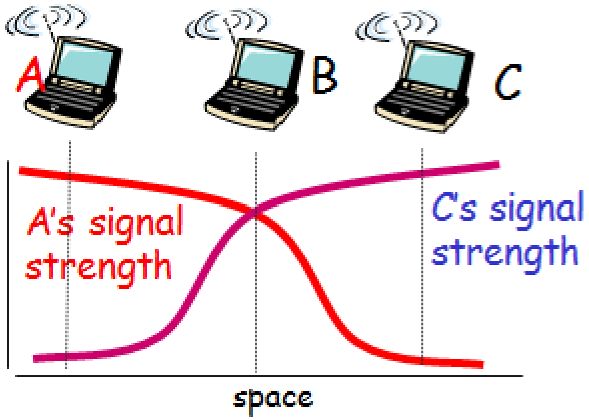
2	2	4	1	1	1	1	1	1	1	1
Protocol version	Type	Subtype	To AP	From AP	More frag	Retry	Power mgt	More data	WEP	Rsvd

frame type (RTS, CTS, ACK, data)

Wireless LAN: Problem -> CA.

- If two terminals are "hidden" from each other, collisions can occur





- Collision Detection is thus not sufficient
- Uses CSMA/CA (Collision Avoidance)
- Can use Request-To-Send and Clear-To-Send signals to reserve connection

Collision Avoidance

- Problem:
  - Two nodes, which are hidden from each other, send complete packets to the base station where they interfere and are lost.
  - Wasted bandwidth for everyone!
- Solution:
  - Small reservation packages!
  - The nodes keep track of reserved time with their own “network allocation vector” (NAV)

802.11 Security & WiFi

- Goal
  - Access control
    - Only those who are given access will get it
  - DataIntegritet
    - No one should be able to change the contents of the data packets during transmission ("man in the middle attacks")
  - Confidentiality
    - Prevent eavesdropping and session hijacking
- Method
  - Encryption of the traffic between AP and user machine
- Techniques
  - WEP
    - Easy to crack due to repetitive 40 bit keys etc.; better with 128 bit key but still easy to crack
    - Static key
  - WPA 1 & 2
    - New encryption key for each package = better encryption
    - WPA 1 can crack,
    - WPA 2 can also be cracked
    - WPA 2 also allows you to use authentication server (more secure a PSK = common password))
    - CCMP encryption is stronger than TKIP.
  - EAP (Extensible Authentication Protocol)
    - Will make various WPA-Enterprise methods interoperable.

How to secure your own wireless network

- Do not use default settings against your own WLAN / ISP
- Update firmware on AP and drivers for WNIC (minimum annually)
- Turn off "Remote Administration" on the AP
  - Choose complicated / secure Admin password
- Select "unusual" IP network
  - preferably from the 172.16.0.0/12 area
  - limit DHCP pool
- Filter access to MAC addresses
- Turn off SSID broadcast
- Be sure to check the range of the signal!
- Use WPA2 with a long and complicated password