3TC-MAC
Medium Access Control

Release 3.1b, May 2023

REASONABLE VERSION!

TO ADD:
- WI-FI CONTROLLER

INSTITUT NATIONAL DES SCIENCES APPLIQUÉES LYON

A course from:

- Philippe Isorce (now, retired)
- Razvan Stanica (razvan.stanica@insa-lyon.fr)
- Fabrice Valois (fabrice.valois@insa-lyon.fr)

INSA LYON

Course information

- 3TC-MAC
  - 2 ECTS
  - 5 classes, 4 TDs, 3 Labs (aka TP)
  - Slides in English, the rest in French (you should take notes, read books, blogs and articles)

Evaluation

- Live evaluation during the labs
- Written exam: 2h, documents & calculator allowed, subject in French, answers in French or English

Team (*classic*)

Fabrice Valois, CM/TD/TP
http://perso.citi-lab.fr/fvalois/

Frédéric Le Mouel, TD/TP
http://perso.citi.insa-lyon.fr/flemouel/

Sébastien Peychet, TP

Youssef Badra, TP

Gwendoline Hochet, CM/TD/TP
http://perso.citi-lab.fr/ghochet/

Course information

- Resources
  - No hard copy, only Moodle :)
  - A MOOC is available on OPC (only in French):

https://openclassrooms.com/fr/courses/5433211-reseau-et-communication-pour-lembarque-1

Dans ce cours, découvrez les concepts de base des réseaux de communication, permettant à des machines (ou plus particulièrement à des objets intelligents) de se connecter à un réseau local et ensuite à Internet, afin d'accéder à des services informatiques distants. Le cours présente les **bases des réseaux**, en s'intéressant notamment aux méthodes d'accès sur un réseau local et aux protocoles qui forment le cœur d'Internet : **IP et TCP**.

Course information (cont'd)

- Resources
  - A. Tanembaum – "Computer Networks" (at the library)
  - G. Pujolle – "Les Réseaux" (at the library)
  - O. Bonaventure – "Computer Networking : Principles, Protocols and Practice" (link on moodle)

  - Good materials (a little biased) from the Cisco Academy
  - Interesting discussions on Twitter and Reddit
  - Not everyone on the Internet is a reliable source of information

Disclaimer

- In networking (and also in telecommunications), a lot of abbreviations & acronyms are used…

MTU **802.11**
STP **DIFS**
CSMA **Wi-Fi** **802.3** **ARQ**
SDU
SIFS **CD** **PCF**
MAC **BEB**
VLAN
CS **CA** **CW**
RJ45
PDU **LAN**
DCF **EIFS**
ACK **CRC**
BSS
IEEE **NAV** **RTS**
CTS
UTP

- Take care and be patient…

Objectives

- Knowledges (*connaissances*)

- Skills (*compétences*)

Objectives

- Knowledges (*connaissances*)
  - Data link layer
  - How to share a medium?
  - How to manage collision?
  - Aloha and the CSMA family
  - CSMA/CD and CSMA/CA
  - Ethernet and Wi-Fi
  - Cable, hub and switch
  - Spanning tree
  - Virtual LAN
- Skills (*compétences*)

Objectives

- Knowledges (*connaissances*)
  - Data link layer
  - How to share a medium?
  - How to manage collision?
  - Aloha and the CSMA family
  - CSMA/CD and CSMA/CA
  - Ethernet and Wi-Fi
  - Cable, hub and switch
  - Spanning tree
  - Virtual LAN

- Skills (*compétences*)
  - Compute delay & throughput
  - Describe a protocol with a finite state machine
  - Illustrate frame exchanges using a chronogram
  - Deploy an Ethernet LAN
  - Connect cables properly
  - Configure a switch
  - Configure VLANs
  - Use Wireshark

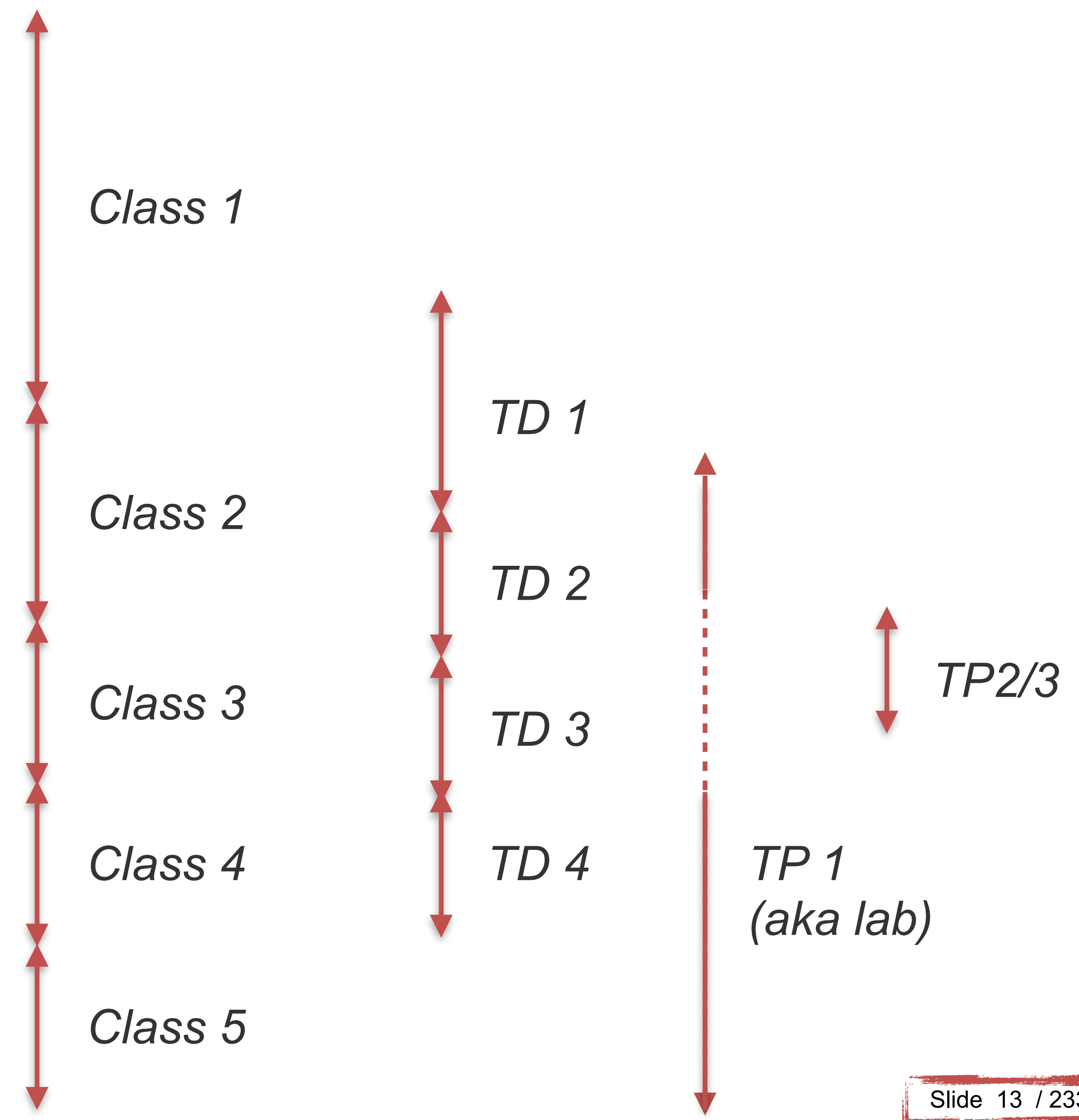
Agenda

What we will do

1. IEEE Family
2. General information on the physical layer
3. Data link layer
4. Medium access control
5. CSMA/CD and Ethernet/IEEE 802.3
6. CSMA/CA and Wi-Fi/IEEE 802.11
7. Network hardware for LAN
8. VLAN

What we will do & when…

1. IEEE Family
2. General information on the physical layer
3. Data link layer
4. Medium access control
5. CSMA/CD and Ethernet/IEEE 802.3
6. CSMA/CA and Wi-Fi/IEEE 802.11
7. Network hardware for LAN
8. VLAN



1. IEEE* 802 family

*Institute of Electrical and Electronics Engineers

IEEE 802

- Family of standards for *Local Area Networks* and *Metropolitan Area Networks*
- Define:
  - Physical layer
  - Data link layer
    - *Logical Link Control sublayer*
    - *Medium Access Control sublayer*

IEEE 802: Few standards committees

- 802.3: Ethernet & CSMA/CD (LAN)
- 802.4: Token Bus (LAN)
- 802.5: Token Ring (LAN)
- 802.7: Broadband LAN using coaxial cables
- 802.8: Fiber Optic
- 802.11: Wireless Networking (e.g. Wi-Fi)
- 802.15: Wireless PAN/Wireless BAN (e.g. Bluetooth, ZigBee)
- 802.16: Broadband Wireless Access (e.g. WiMax)

2. Physical Layer

Physical layer

- Connecting two hosts
  - Electrical cable
  - Optical fiber
  - Wireless
- Signal manipulation
  - To be seen in all the classes from the syscom domain

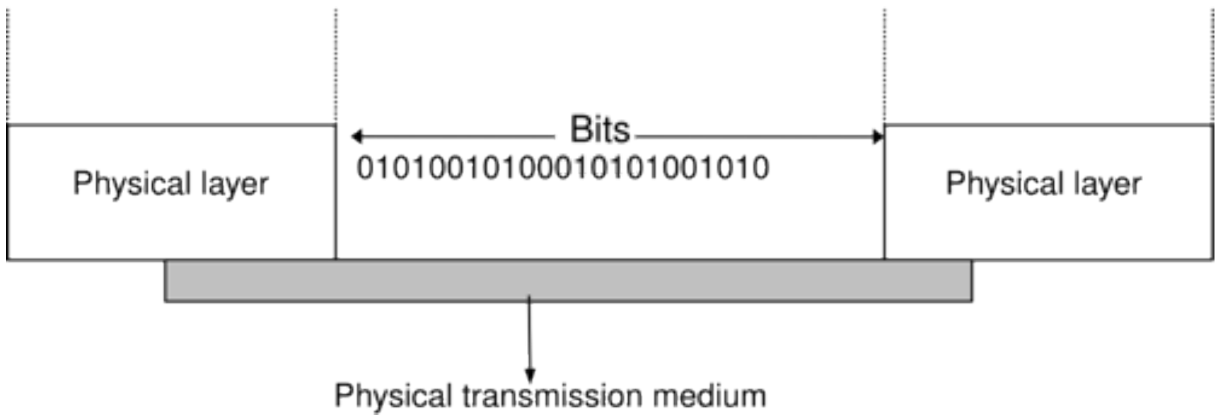
Physical layer

- Communication channel classification
  - The physical link (aka communication channel) between a source A and a destination B can be:
    - ***Serial**: only one bit at a time, sequentially, over a single communication channel*
    - ***Parallel**: using of several communication channels simultaneously*

    - *Unidirectionnal (**simplex**): only from A to B*
    - *Bidirectionnal (**half-duplex**): from A to B and from B to A but alternatively*
    - *Bidirectionnal (**full-duplex**): from A to B and from B to A simultaneously*

Physical layer

- Provided services
  - Transfers bits of information using an electromagnetic field
  - Unit: bits per second
  - 1 kbps = 1000 bps (unlike 1 Kbps = 1024 bps = 1 KiBps)

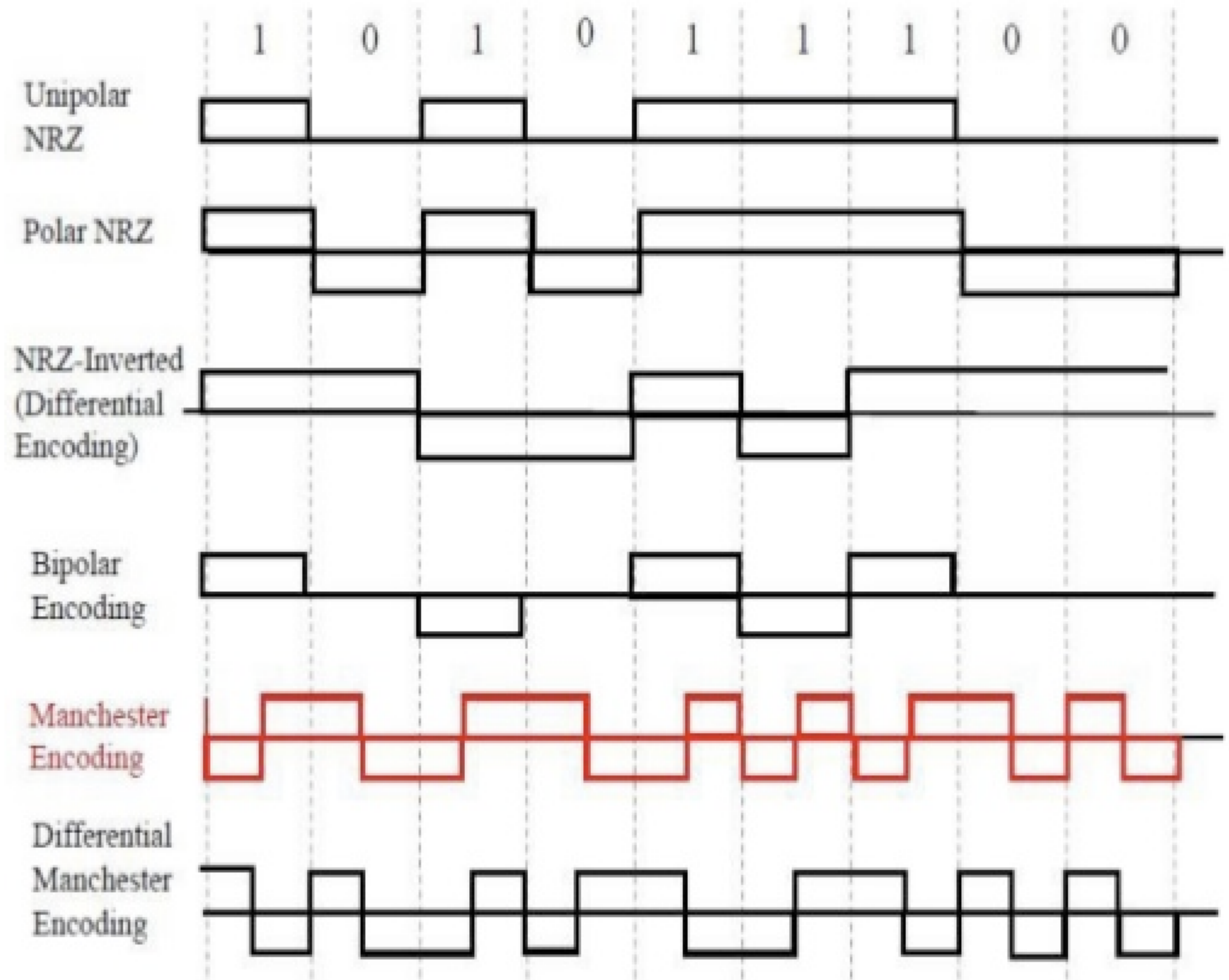


Physical layer

- Host synchronization
  - **Implicit**
    - *The receiver knows when and where to listen for data*
    - *The fastest solution*
    - *Requires control traffic and can waste ressources (padding)*
  - **Explicit**
    - *A known sequence is used to mark the start of a transmission*
    - *Simpler, but with some complications (the sequence can not be used during the communication)*
    - *What about the end? - another sequence or duration indication*

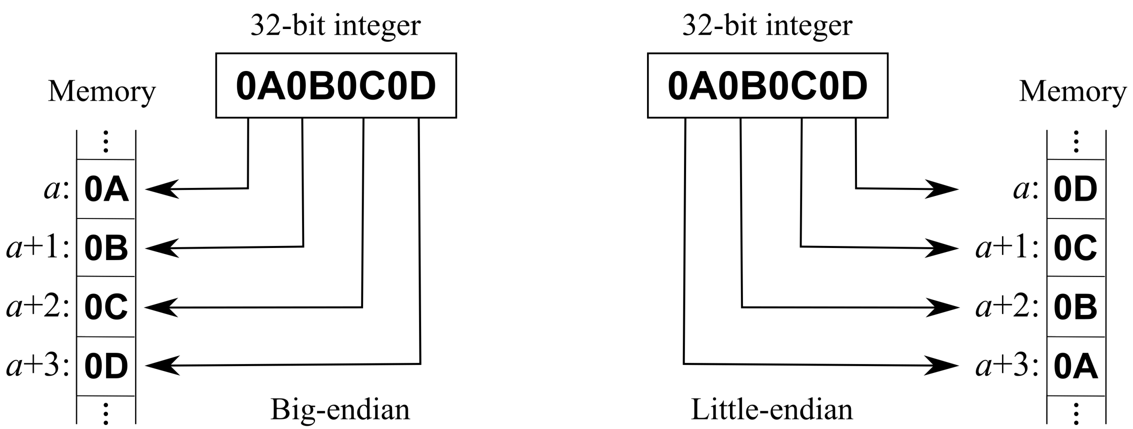
Physical layer

- Coding Scheme



Physical layer

- Physical transmission: Little Endian vs Big Endian
  - Order of transmission of bytes and bits over a medium

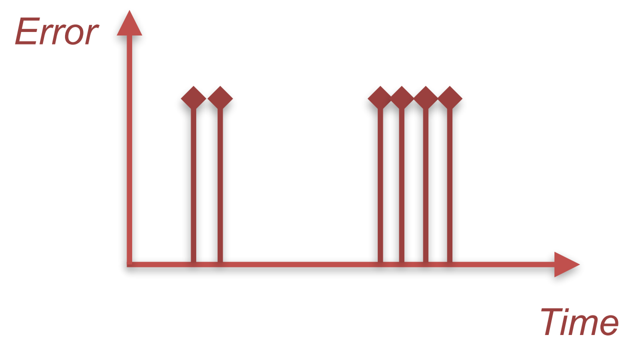


- In networking, mainly network byte order (*i.e.* big endian byte order)

3. Data link layer

Data link layer

- Framing
  - With a perfect PHY layer, simply send a continuous stream of bits (e.g. reading a DVD)
  - Real PHY layer introduces errors (less on an optical fiber ~10^{-12}, more on a wireless medium ~10^{-4}) – usually bursty
  - Split the stream of bits in frames
  - In case of errors, only concerned frames are lost

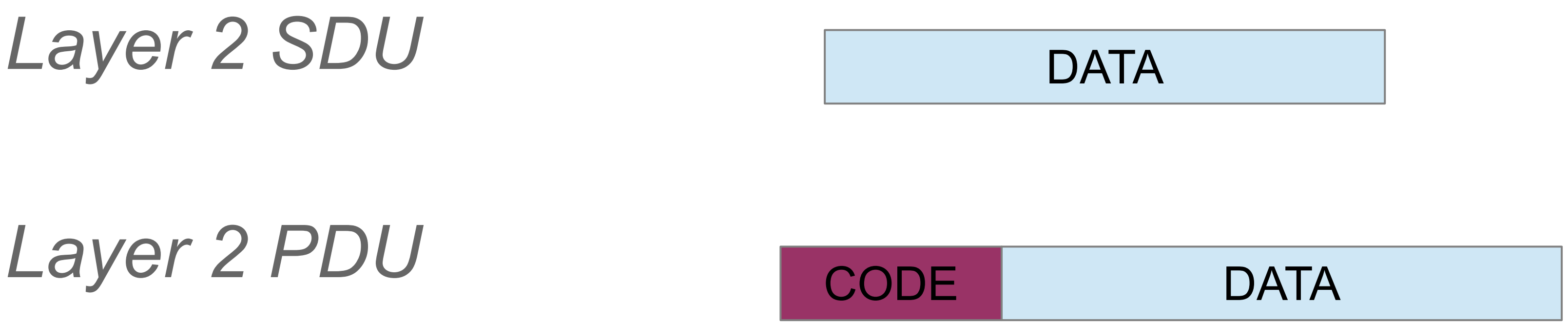


Data link layer

- Error control
  - Frames can be corrupted by transmission errors
    - *Random isolated errors modifying the value of one bit*
    - *Random bit creation of removal*
    - *Burst errors that impact n consecutive bits*
  - Frames can be lost entirely due to buffer overflow

Data link layer

- Transmission errors
  - Add redundant information as *error detection codes*
  - Instead of *N* bits, transmit *N*+*r* bits, *r* is the code length



Data link layer

- Error detection (1)
  - Simplest error detection code: parity bit
  - Even parity or odd parity
  - Create an even (or odd) number of 1 in the transmitted frame

3 bits string	Odd parity	Even parity
000	1	0
001	0	1
010	0	1
011	1	0
100	0	1
101	1	0
110	1	0
111	0	1

Data link layer

- Error detection (2)
  - Checksum – used by the TCP/IP stack and by most security mechanisms
  - Basic idea (but different flavours exist): break the data into *words* of *r* bits and compute the XOR of all those words
  - Easily implementable in software

0	0	1	0	0	1	0	0
1	0	1	1	1	0	0	0
1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	1
0	1	1	0	0	0	1	0

Data link layer

- Error detection (3)
  - Cyclic Redundancy Check (CRC) – used by data link protocols, disk reading solutions, presentation layer protocols (.zip, .png)
  - Better performance than checksum, but generally implemented in hardware
  - Check bits computed through polynomial division of the original data
  - Different polynomials, different CRCs – e.g. CRC-32, CRC-32K, CRC-32K2, all used in Ethernet

Data link layer

- Error recovery
  - What to do if an error is detected?
    - *Correct it*
    - *Send explicit feed-back*
    - *Send implicit feed-back*

Data link layer

- Error correction
  - Forward Error Correction (FEC) codes
  - Used also for reliable media storage (DVD, CD, hard disk)
  - The number of errors that can be corrected depends on the code
  - Convolutional codes – processed on a bit-by-bit basis
  - Block codes – processed on a block-by-block basis (Reed-Solomon, Turbo codes, LDPC)

Data link layer

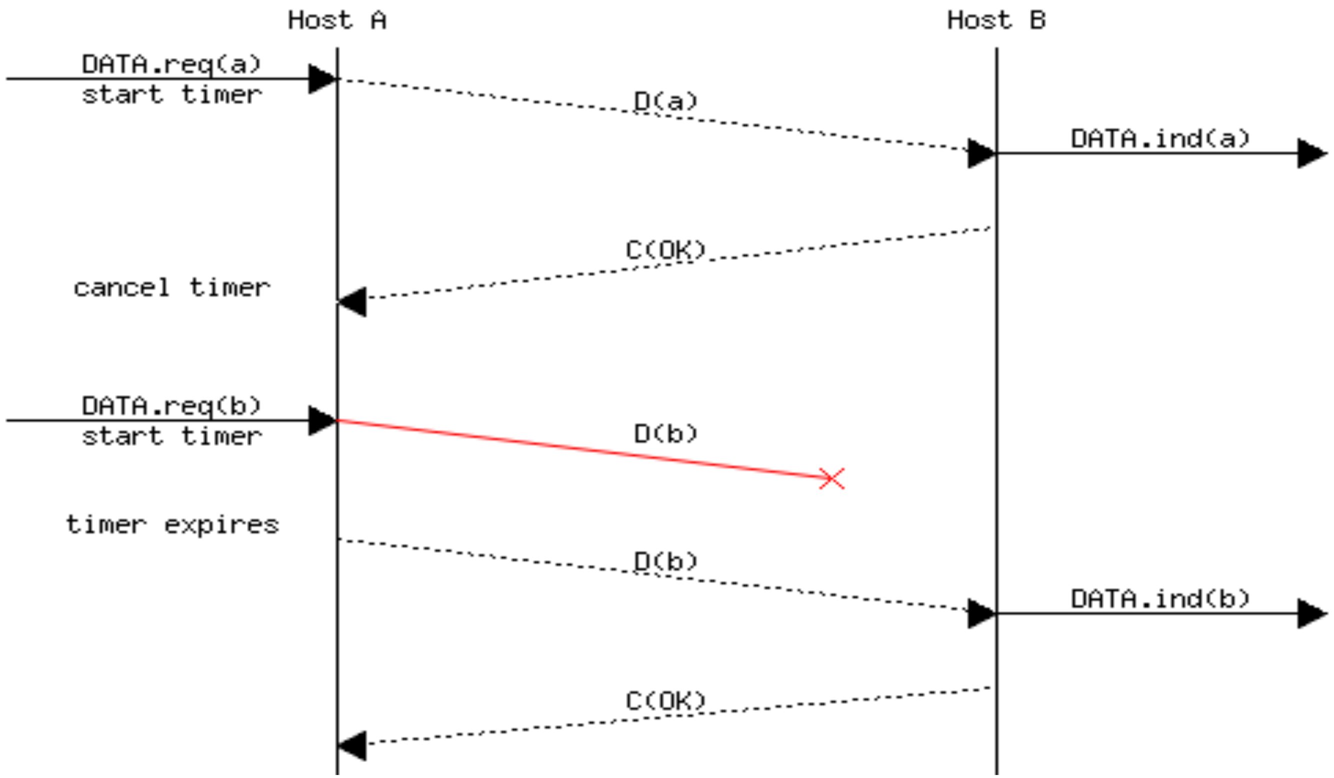
- Explicit feed-back
  - Send a negative acknowledgement (NACK)
  - Requires to know the identity of the transmitter
  - It can not be used on a shared medium

Data link layer

- Implicit feed-back
  - Automatic Repeat Request (ARQ)
  - Transmitter starts a timer for each frame
  - If ACK message not received by the end of the timer – frame lost
  - Retransmission until ACK, or until maximum number of retransmissions
  - If no ACK – Data_Link_Failed indication transmitted to upper layer
  - It can be combined with FEC – Hybrid ARQ (HARQ)

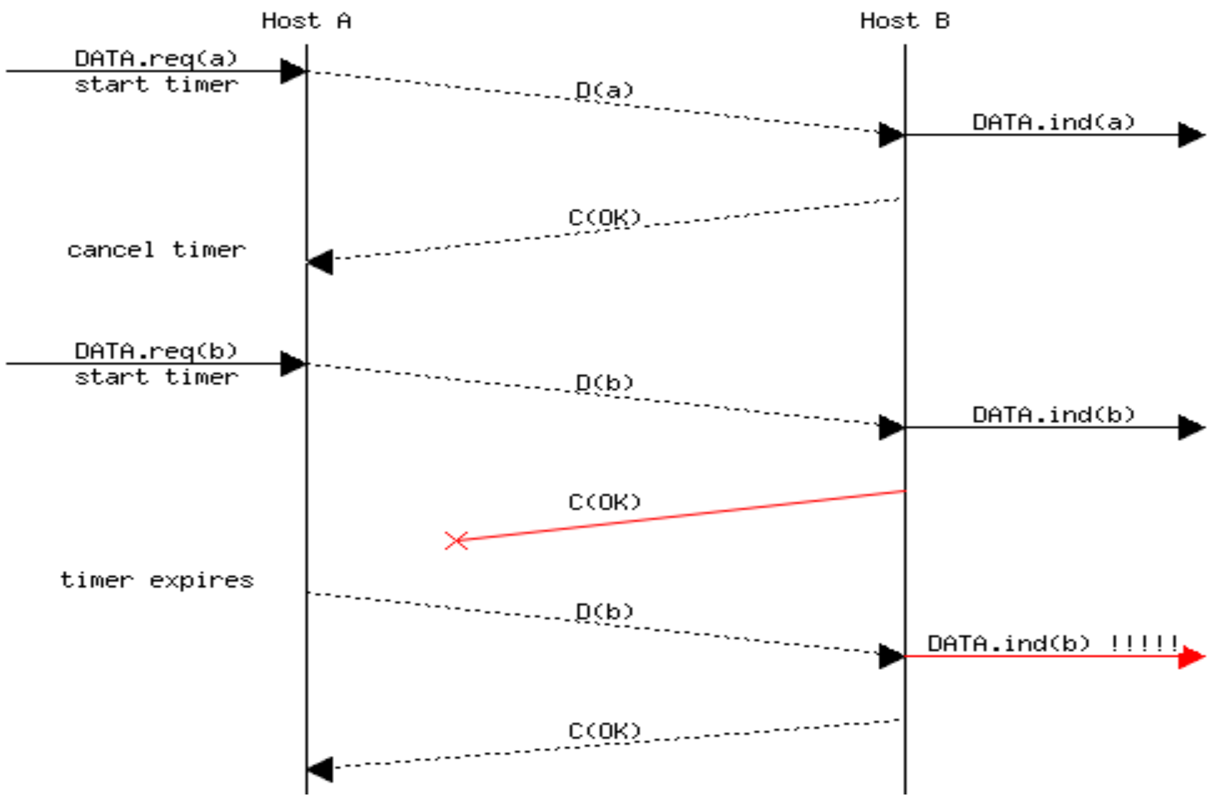
Data link layer

- ARQ



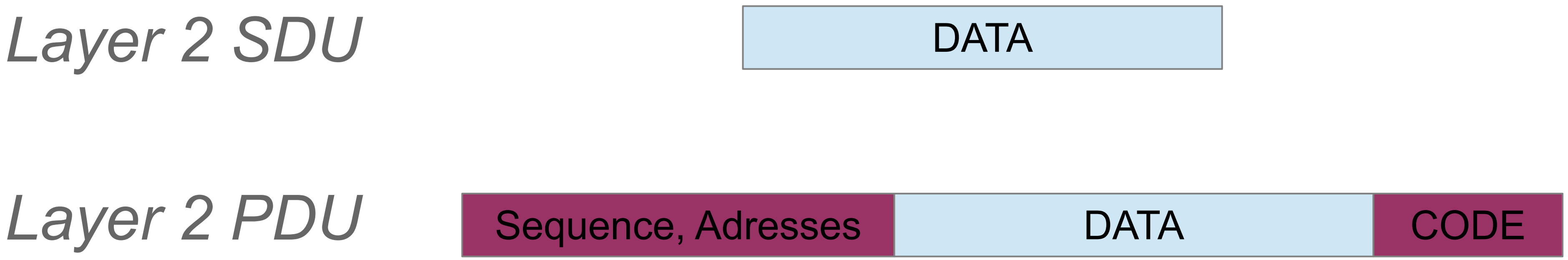
Data link layer

- ARQ
  - Need for sequence number to remove duplicated messages



Data link layer

- ARQ
  - Need for sequence number to remove duplicated messages

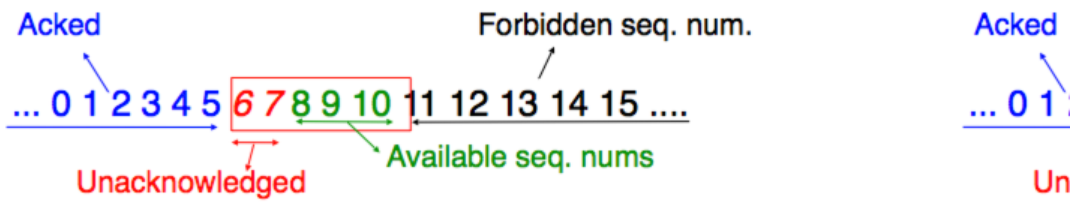


Data link layer

- Window mechanism
  - Waiting for an ACK after each transmission is slow
  - Pipelining frames can improve the performance …
  - … but it can overload the receiver as well
  - A maximum *window* of *W* frames can be transmitted
  - The window size is negotiated at the establishment of a connection, or never if the protocol is not connected

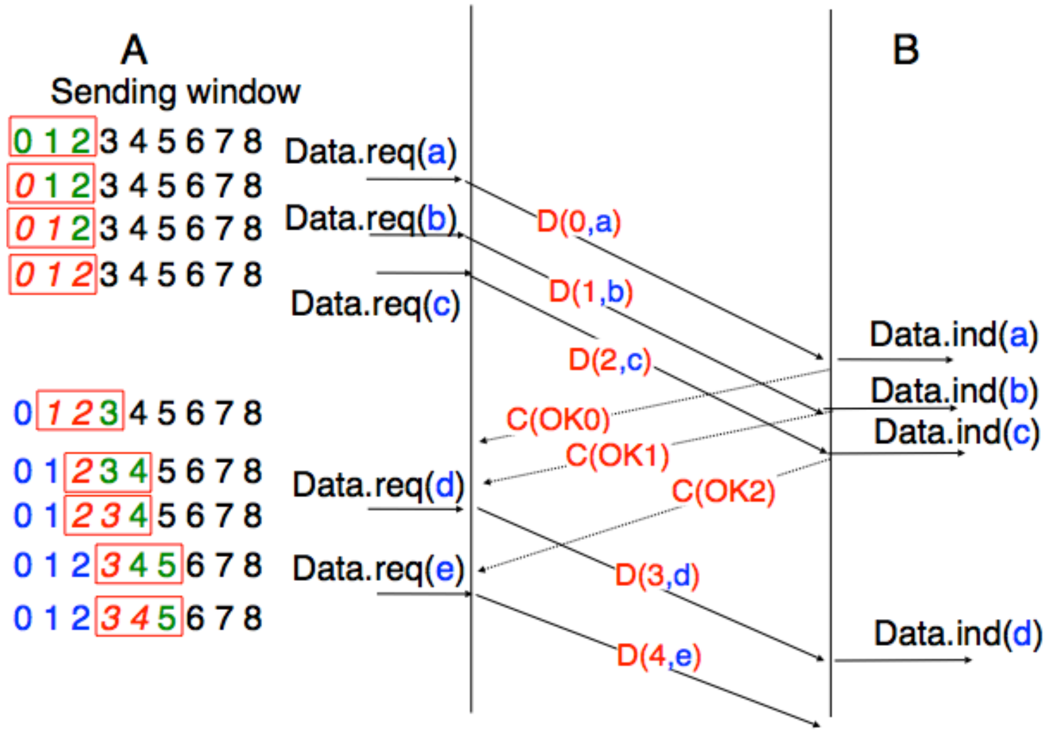
Data link layer

- Window mechanism
  - Four types of messages when using a sliding window
    - *Already ACKed messaged*
    - *Messages transmitted but not yet ACKed*
    - *Messages available for transmission*
    - *Messages with forbidden sequence numbers*



Data link layer

- Window mechanism



Data link layer

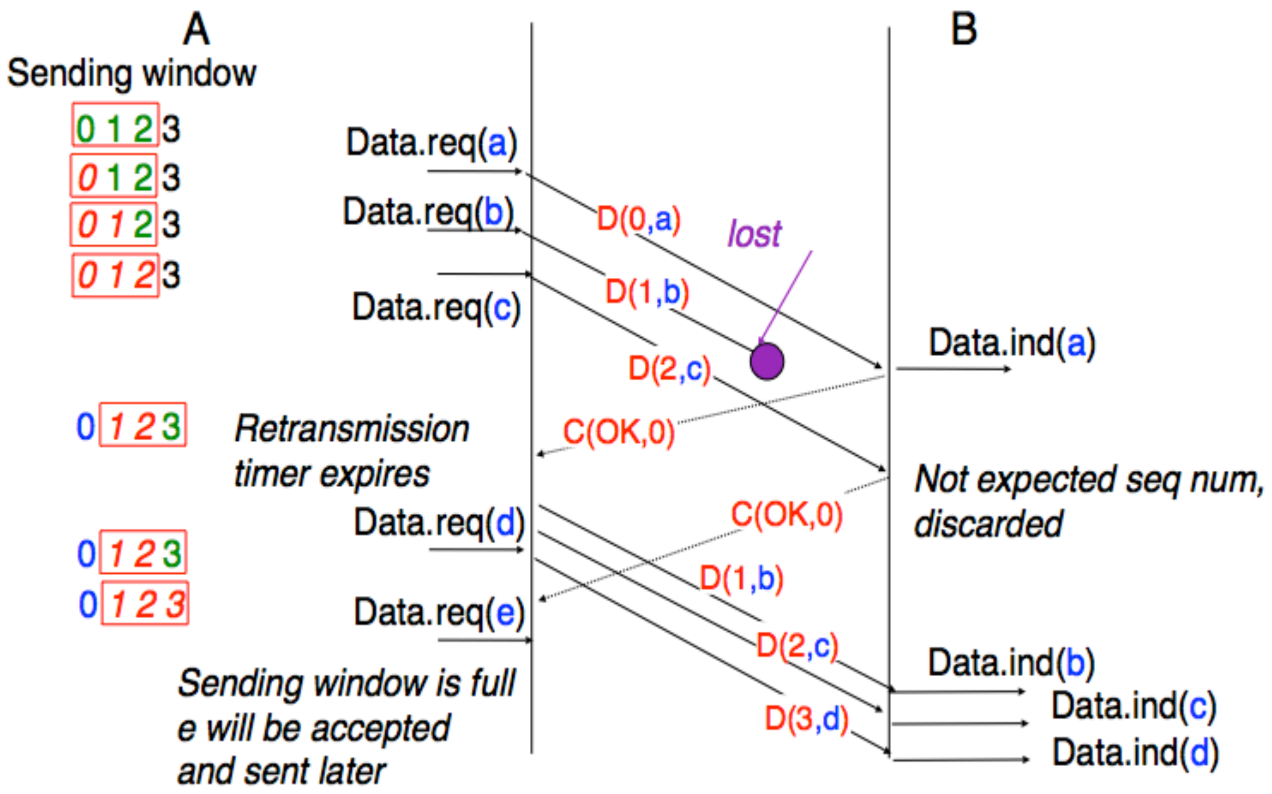
- Window mechanism
  - *n* bits used to encode the sequence number in the frame header
  - Only sequence numbers up to 2^{n-1} can be used
  - For a long transfer, use modulo arithmetic
  - A retransmission strategy is required for the lost frames

Data link layer

- Go-back-n
  - Frames are only accepted in order
  - Any out-of-sequence frame is discarded
  - Cumulative ACK – implicitly acknowledges the previous frames
  - When a loss is detected, everything is retransmitted
  - Easy to implement, good performance when only a few losses

Data link layer

- Go-back-n

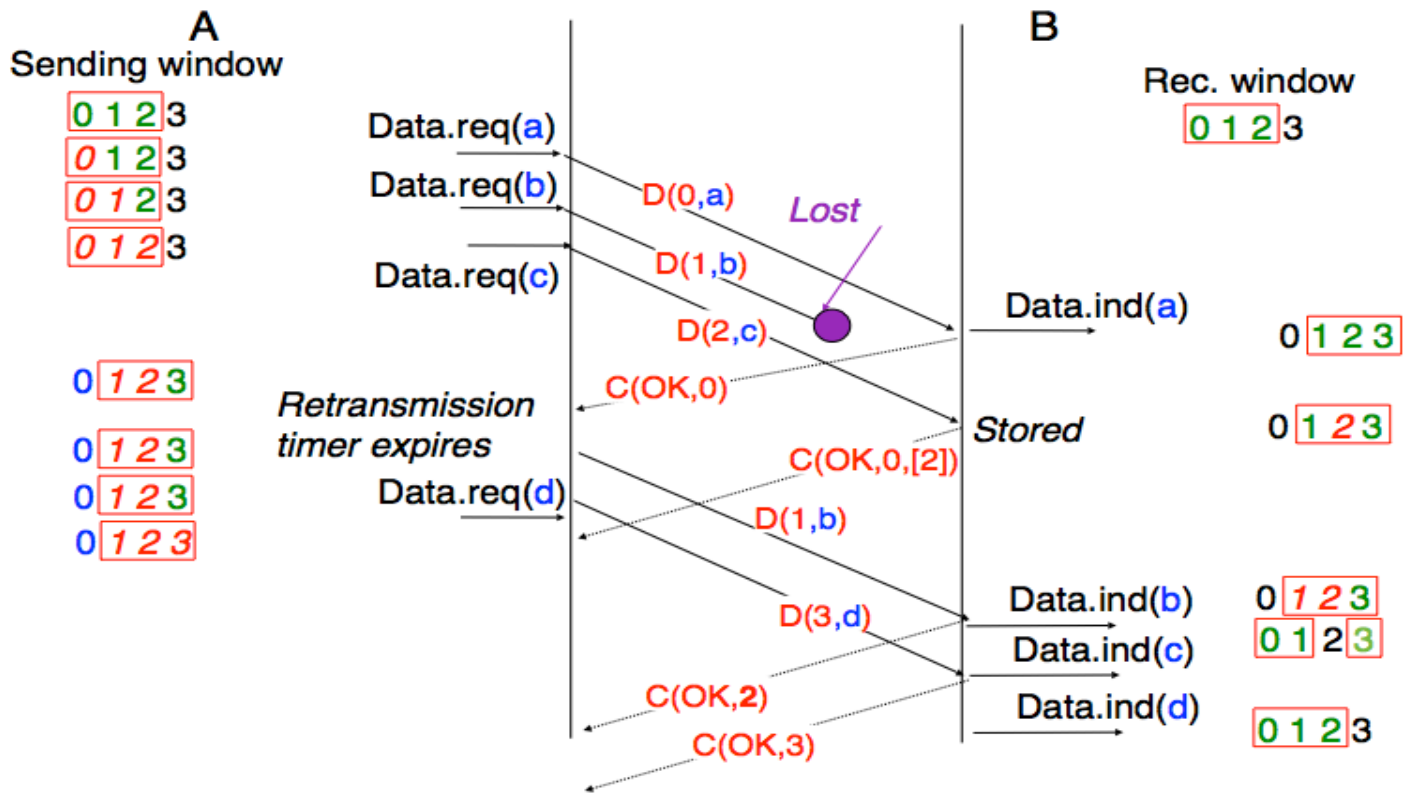


Data link layer

- Selective repeat
  - Accept out-of-sequence frames
  - When a loss is detected, only the lost frames are retransmitted
  - Out-of-order frames can be selectively ACKed
  - Buffers required at transmitter and receiver

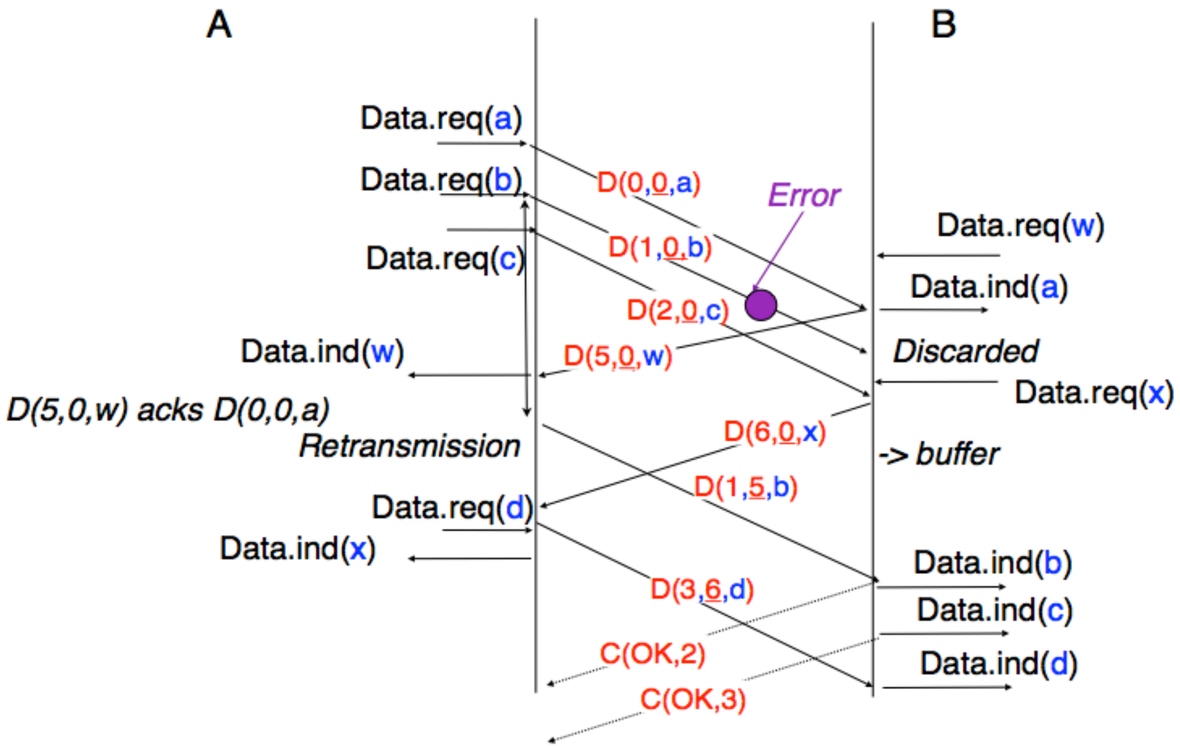
Data link layer

- Selective repeat



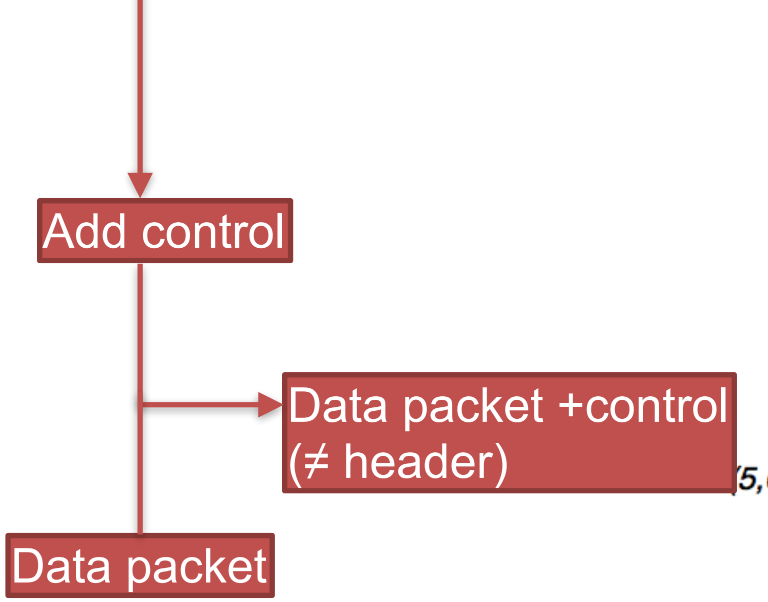
Data link layer

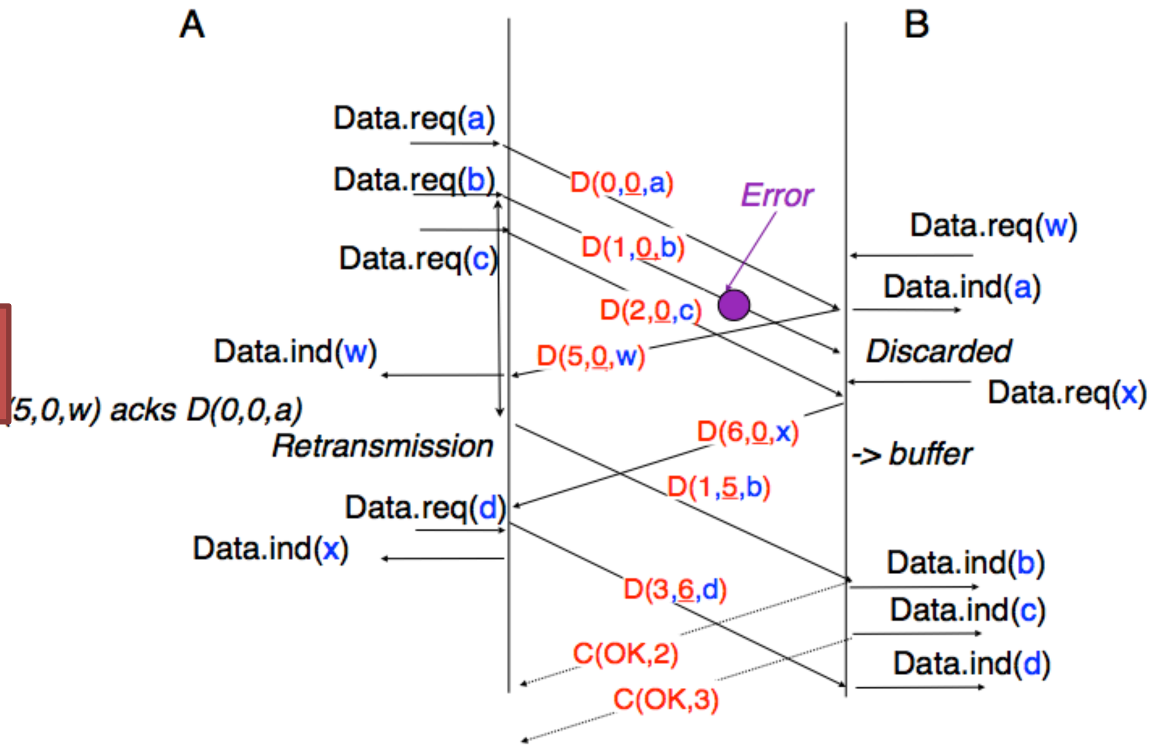
- Piggybacking
  - Data often needs to be transmitted in both directions
  - Append ACKs to data



Data link layer

- Piggybacking
  - Data often needs to be transmitted in both directions
  - Append ACKs to data





Data link layer

- Reliability
  - The data link layer can offer either a reliable or a non-reliable service
  - A reliable service requires retransmissions, sequence numbers, window for flow control, etc. → connection procedure
  - A reliable data link layer provides the SDUs to the upper layer in the correct order
  - *An unreliable protocol goes fast*

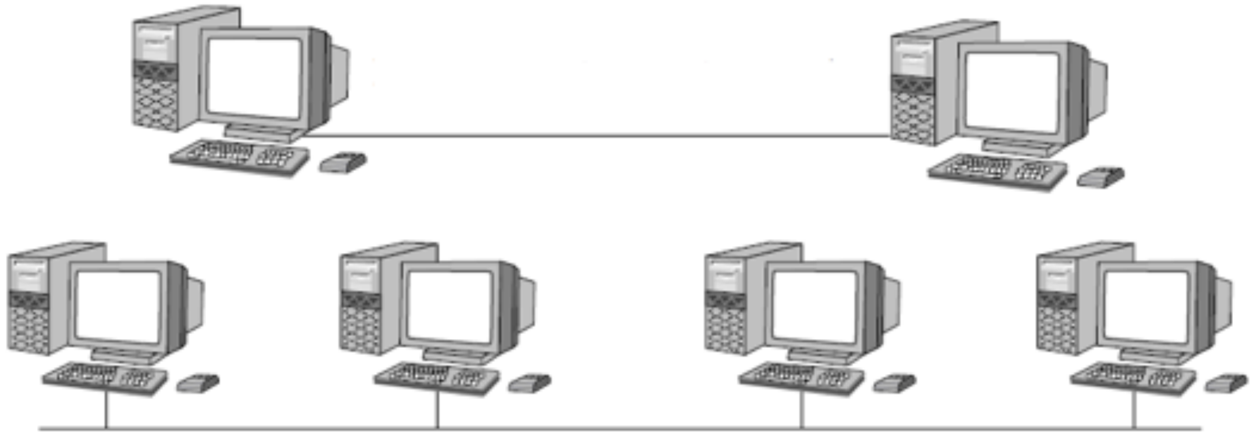
Data link layer

- MTU — Maximum Transmission Unit
  - Physical (or logical) maximum limit for a PDU (frame) due to the physical layer and the data link layer
  - Large value: overhead ↑
  - Small value: network delay ↑
  - For a frame size ≤ MTU: no fragmentation
  - For a frame size > MTU: fragmentation needed (but not necessarily allowed)
  - Default values (Bytes, including headers): Ethernet (1500), Jumbo Frame (1900), PPPoE (1492), ADSL (1468), Token Ring (4500), etc.

4. Medium access control

Medium access control

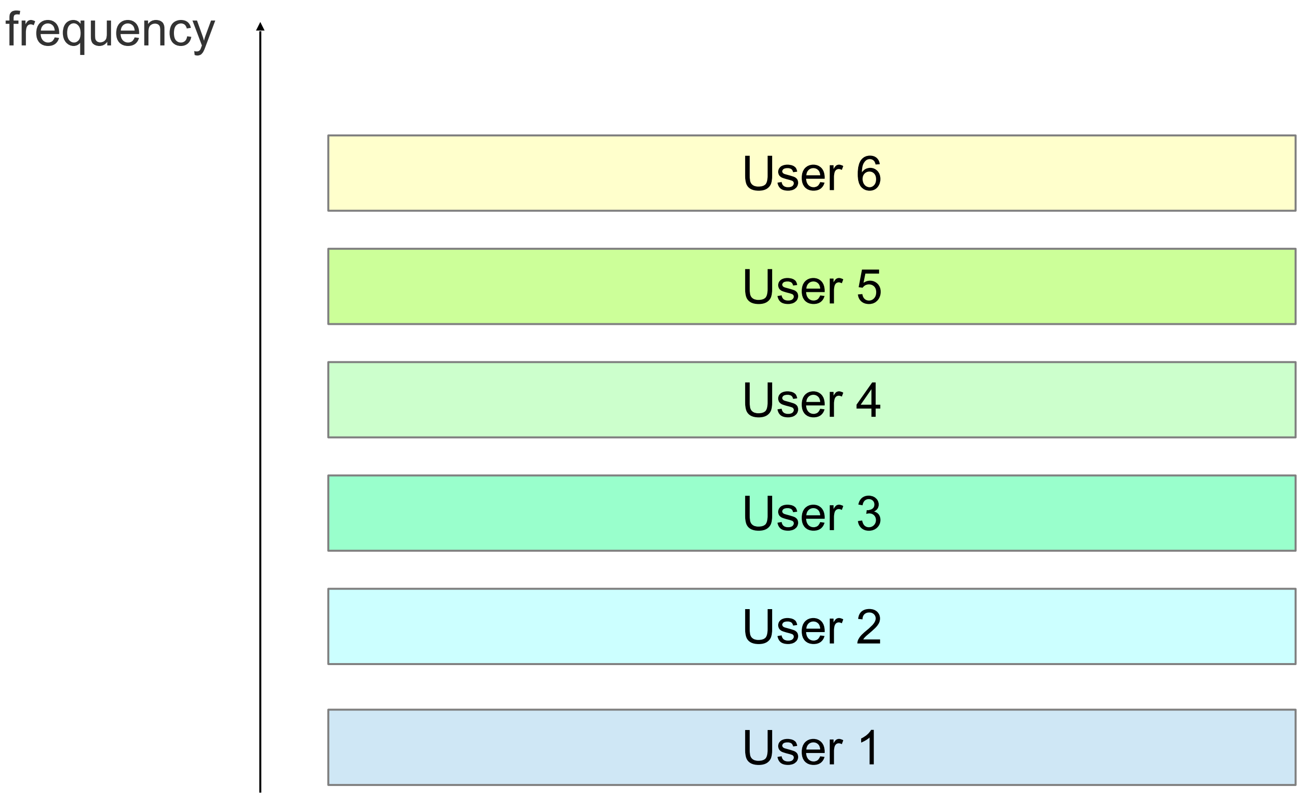
- Point-to-point link
- Shared link



→ How to share the medium & how to multiplex user?

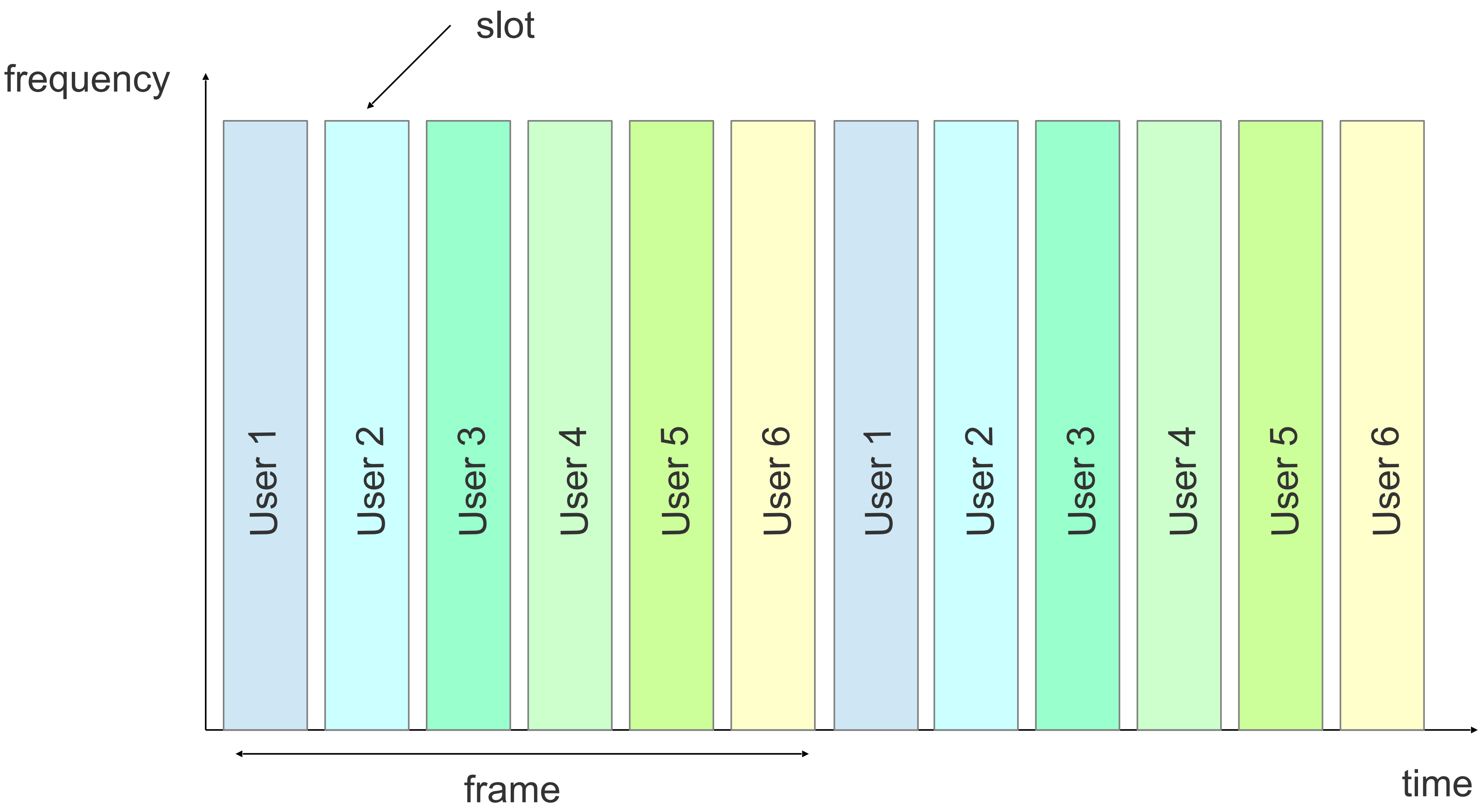
Multiplexing & sharing

- FDMA – Frequency Division Multiple Access



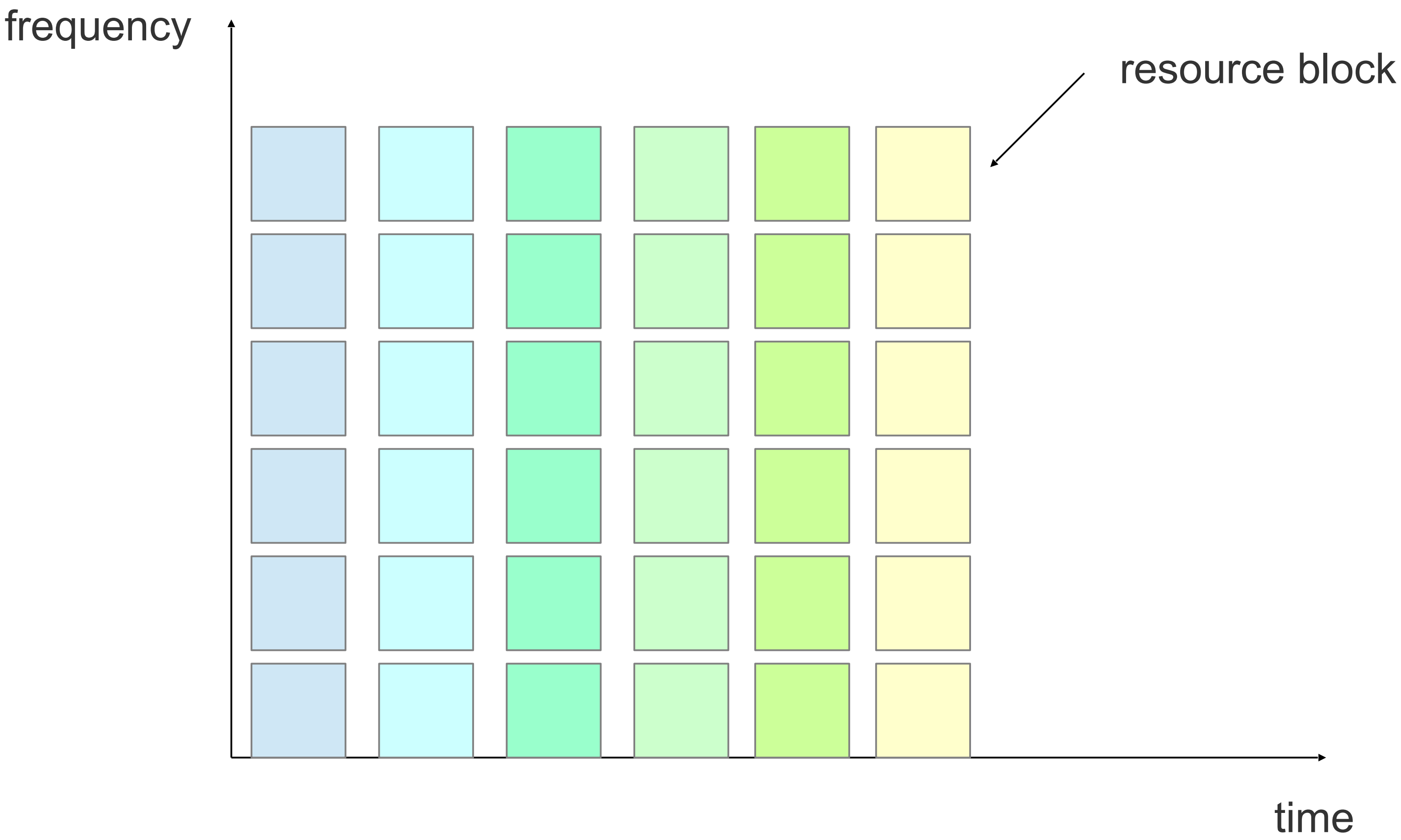
Multiplexing & sharing (cont'd)

- TDMA – Time Division Multiple Access



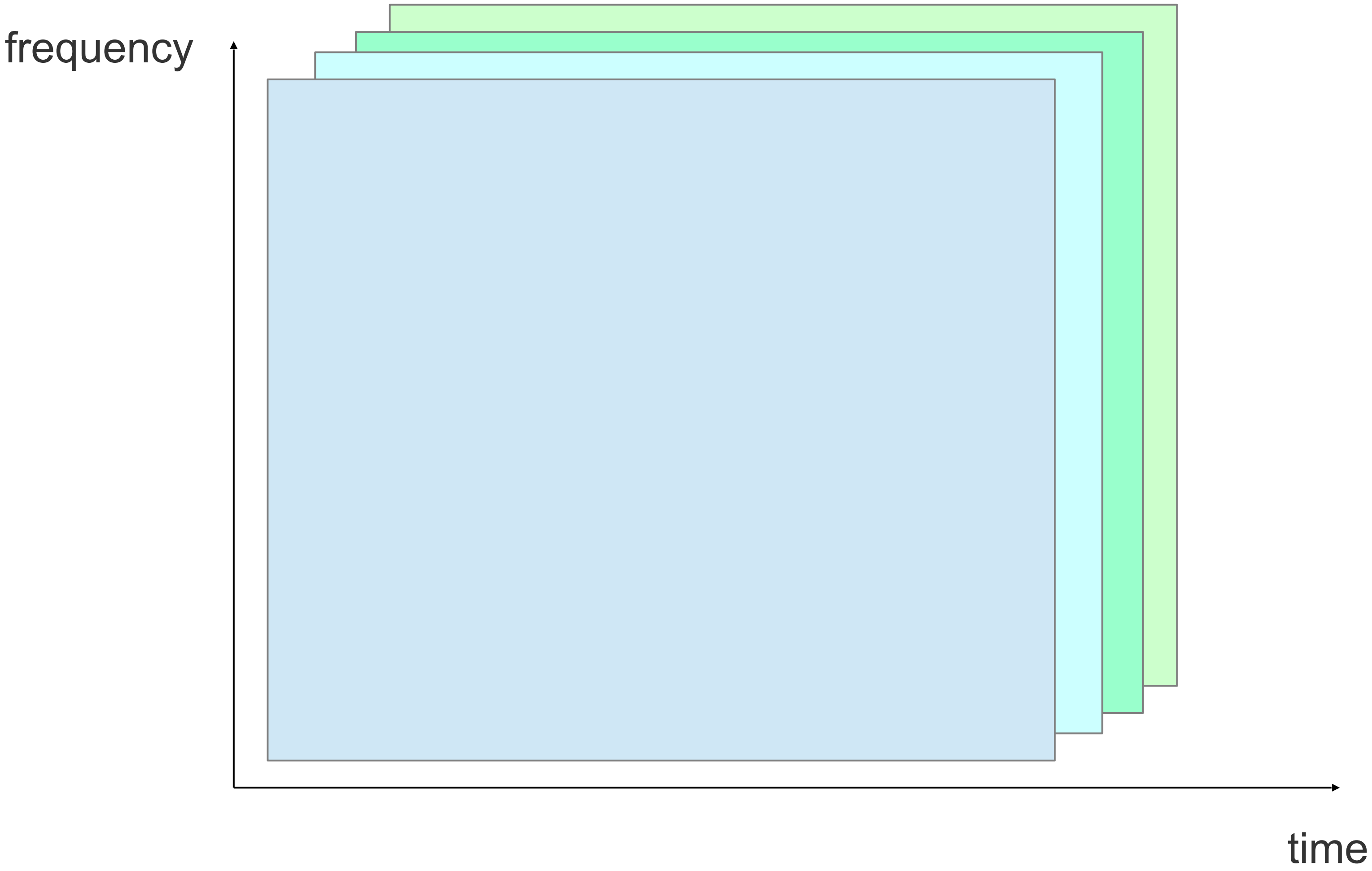
Multiplexing & sharing (cont'd)

- Time-frequency sharing (*e.g.*, OFDM)



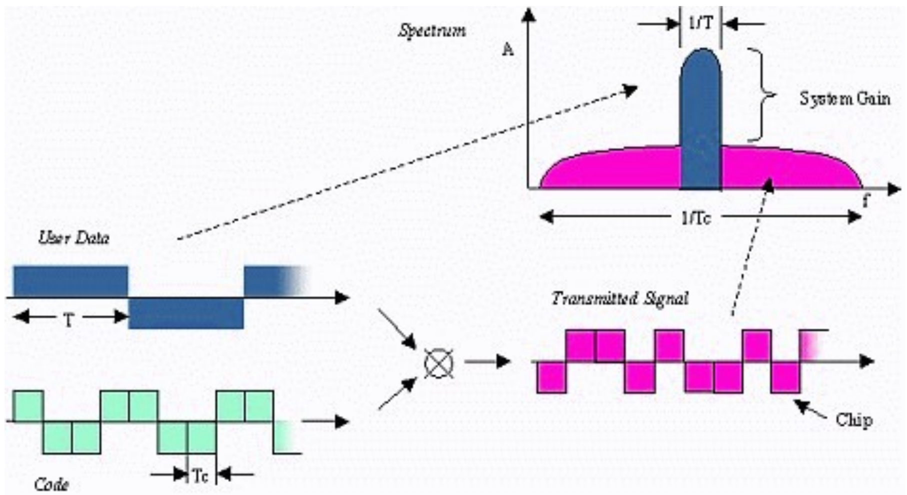
Multiplexing & sharing (cont'd)

- CDMA – Code Division Multiple Access

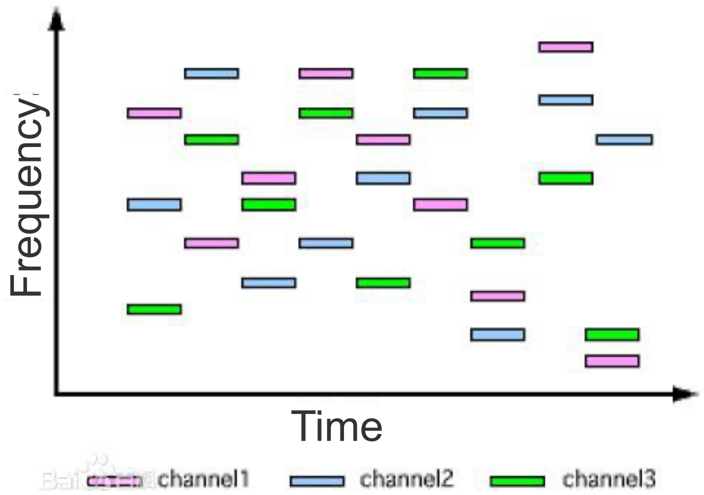


Multiplexing & sharing (cont'd)

- Spread Spectrum
  - DSSS: Direct Sequence Spread Spectrum
  - FHSS: Frequency Hopping Spread Spectrum



— DSSS —



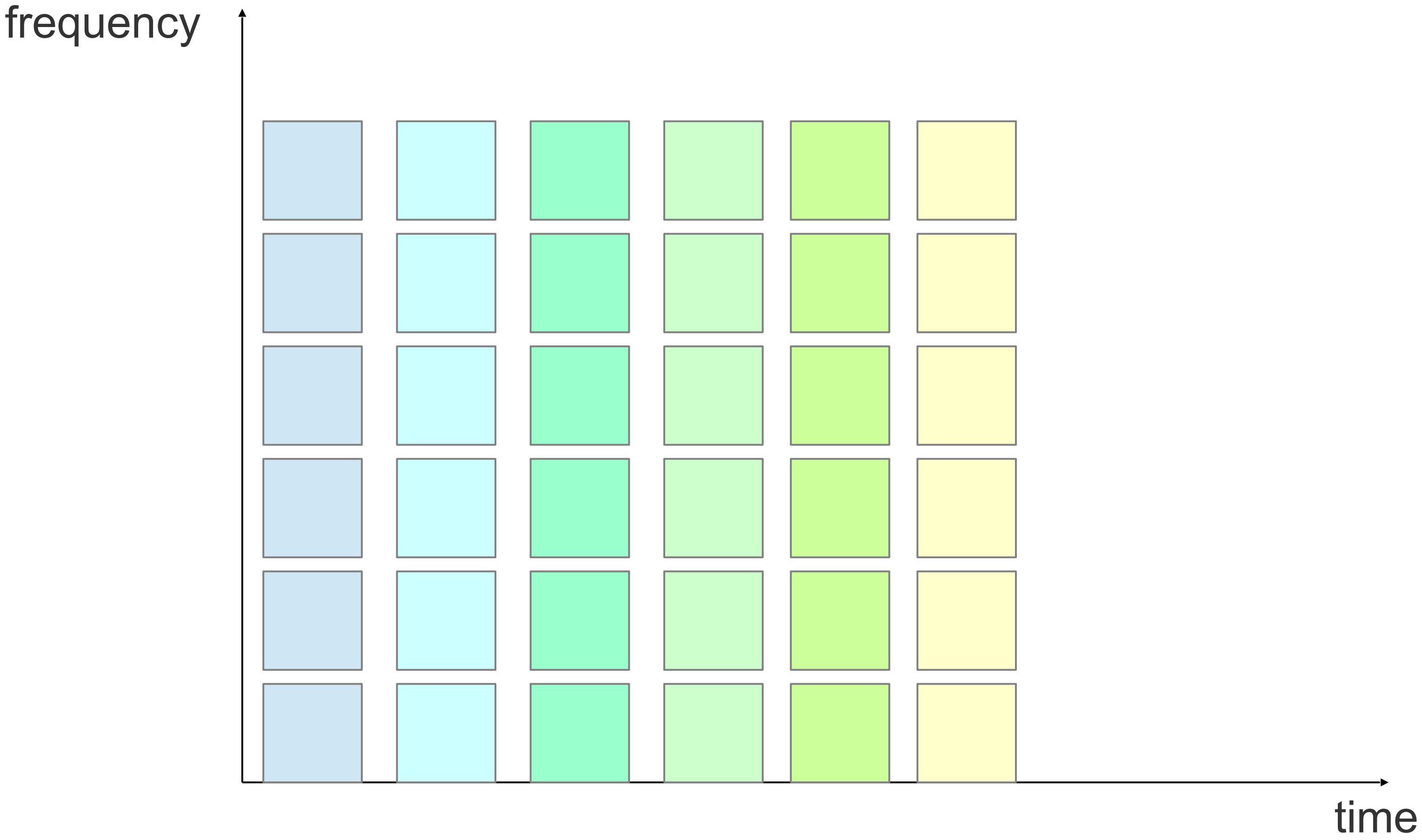
— FHSS —

Medium access control

- Role of the MAC layer
  - Share the different resources (frequency blocks, time slots, codes) among users
  - Manage collisions
- Classification
  - Static assignment
  - Dynamic assignment
    - *Centralized protocols*
    - *Distributed protocols*
      - *Deterministic protocols*
      - *Stochastic protocols*

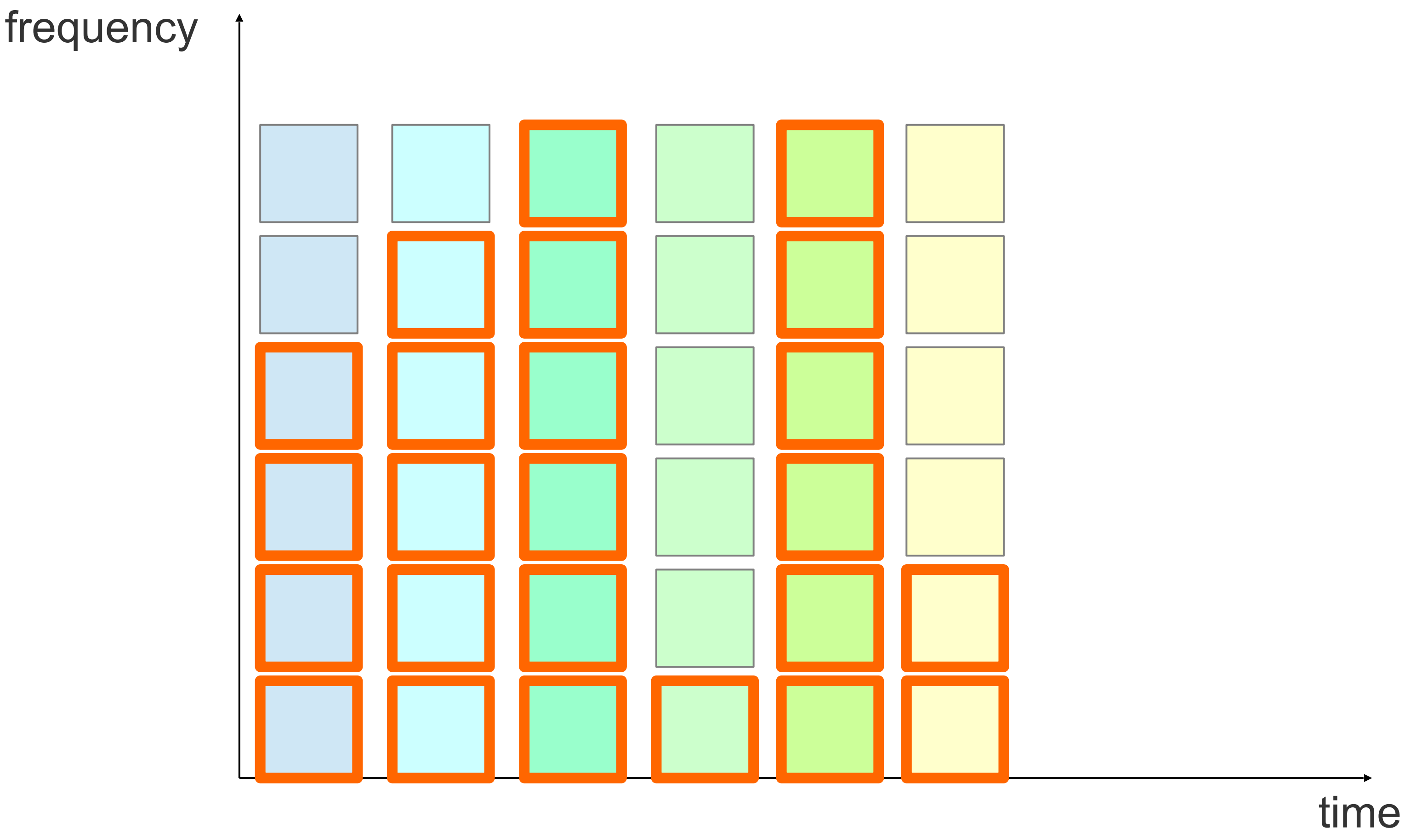
Medium access control

- Static resource assignment



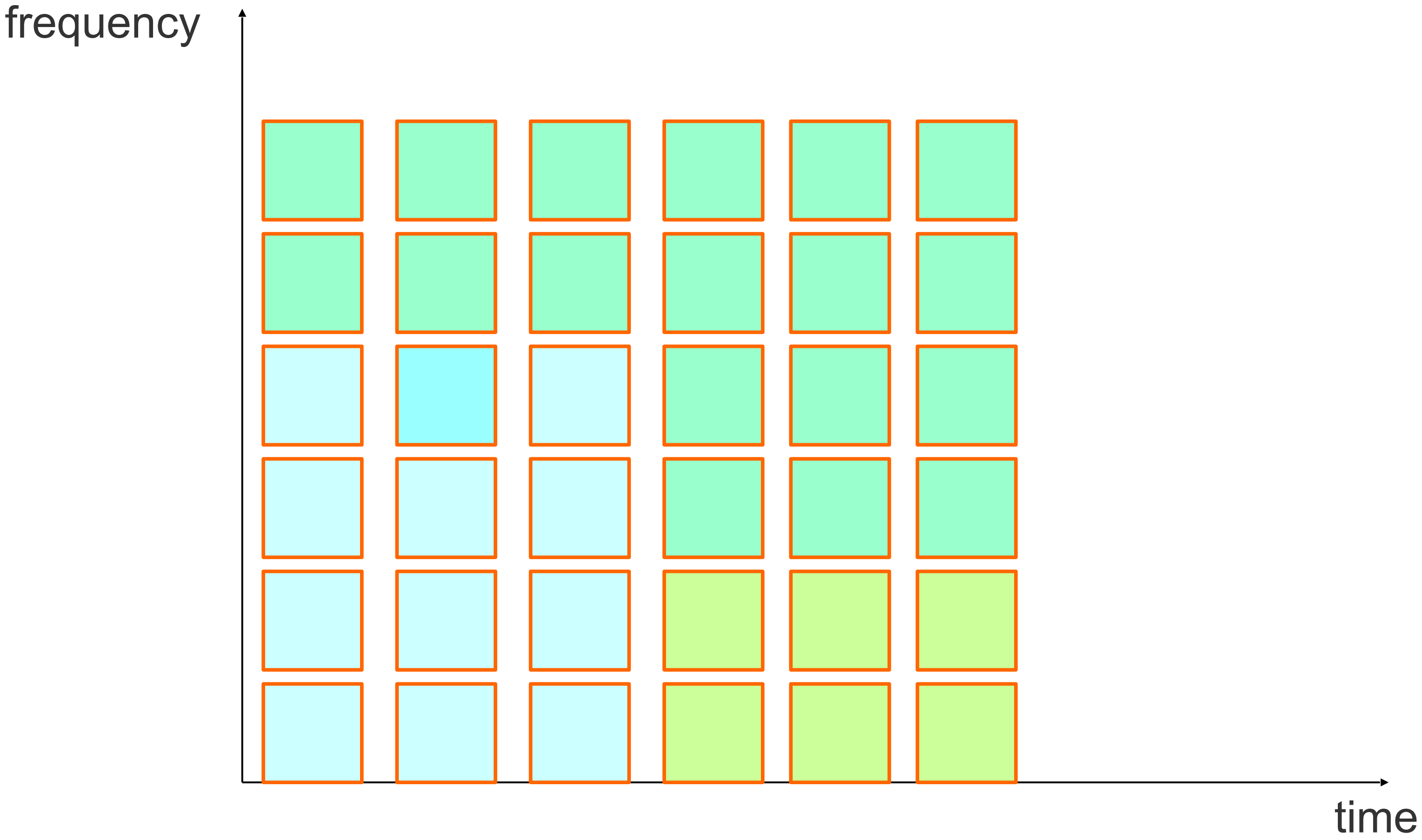
Medium access control

- Static resource assignment
  - Resource under-utilization



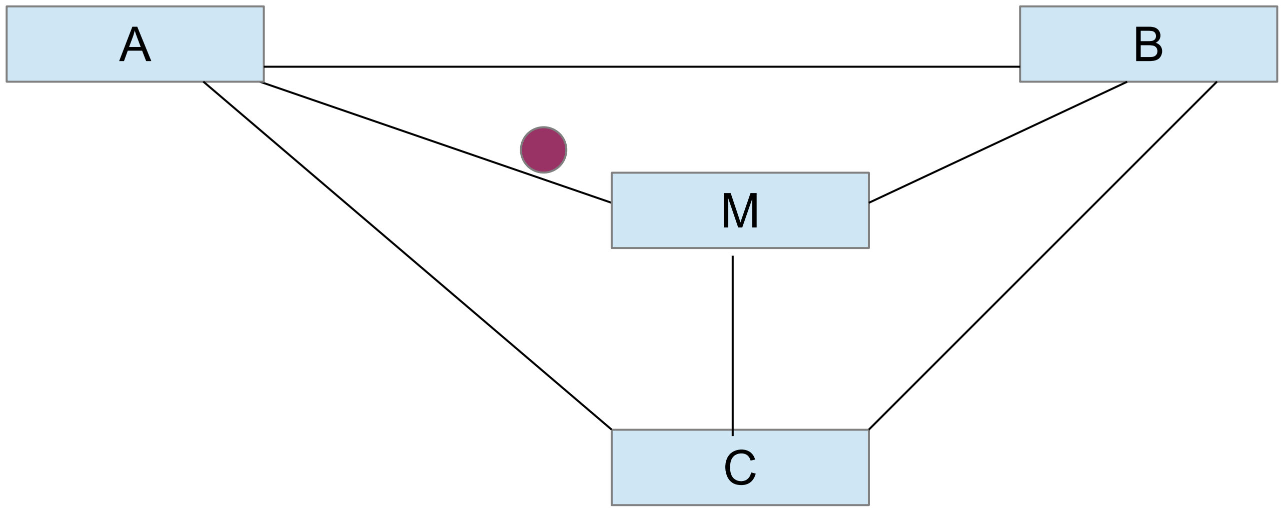
Medium access control

- Dynamic solutions
  - Users are given resources only when they need them



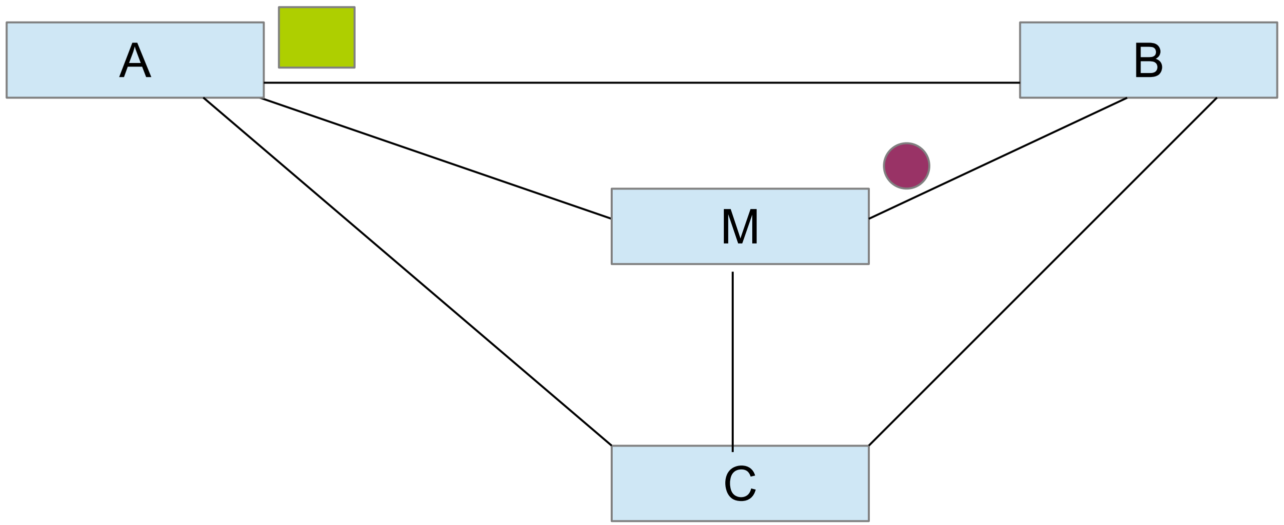
Medium access control

- Centralized protocols
  - A master granting channel access to the users
  - Close to optimal performance
  - Requires supplementary control traffic
  - The master is a single point of failure



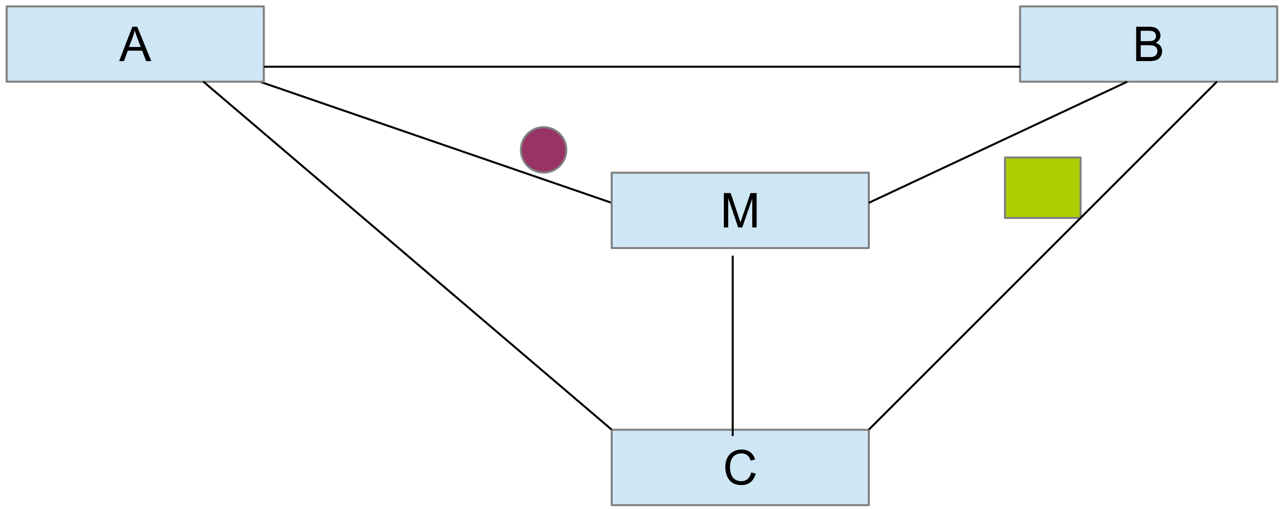
Medium access control

- Centralized protocols
  - A master granting channel access to the users
  - Close to optimal performance
  - Requires supplementary control traffic
  - The master is a single point of failure



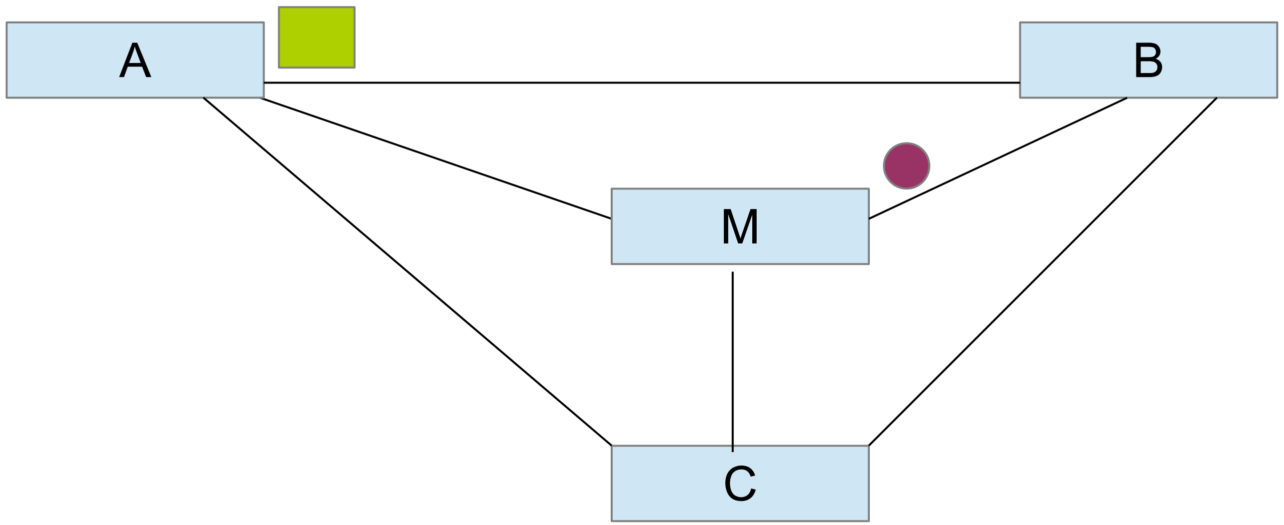
Medium access control

- Centralized protocols
  - A master granting channel access to the users
  - Close to optimal performance
  - Requires supplementary control traffic
  - The master is a single point of failure



Medium access control

- Centralized protocols
  - A master granting channel access to the users
  - Close to optimal performance
  - Requires supplementary control traffic
  - The master is a single point of failure

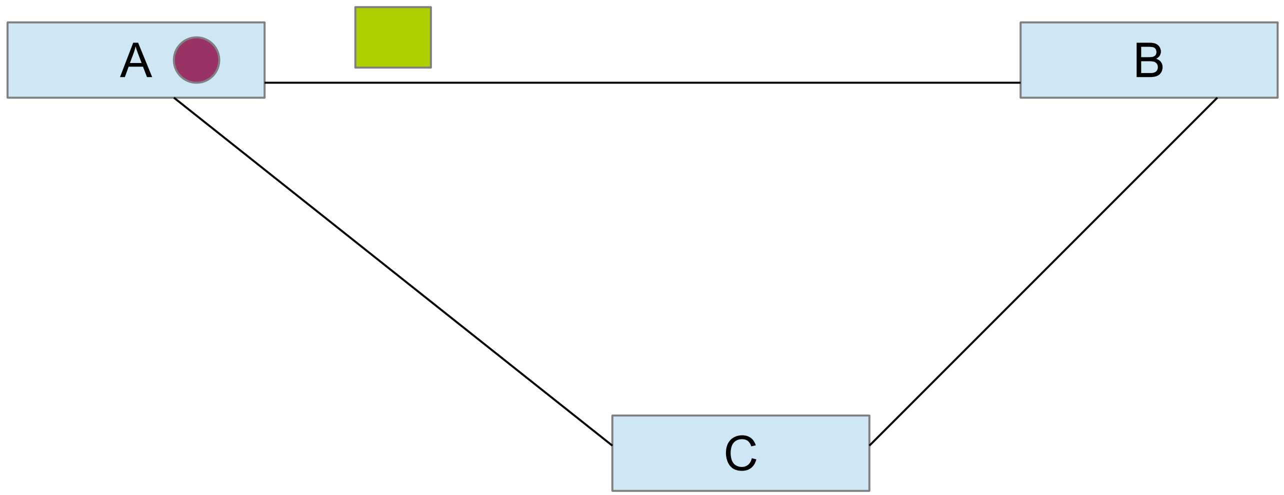


Medium access control

- Distributed protocols
  - All the machines play a similar role
  - Consensus is required
  - Synchronization is required
  - Network robustness increases

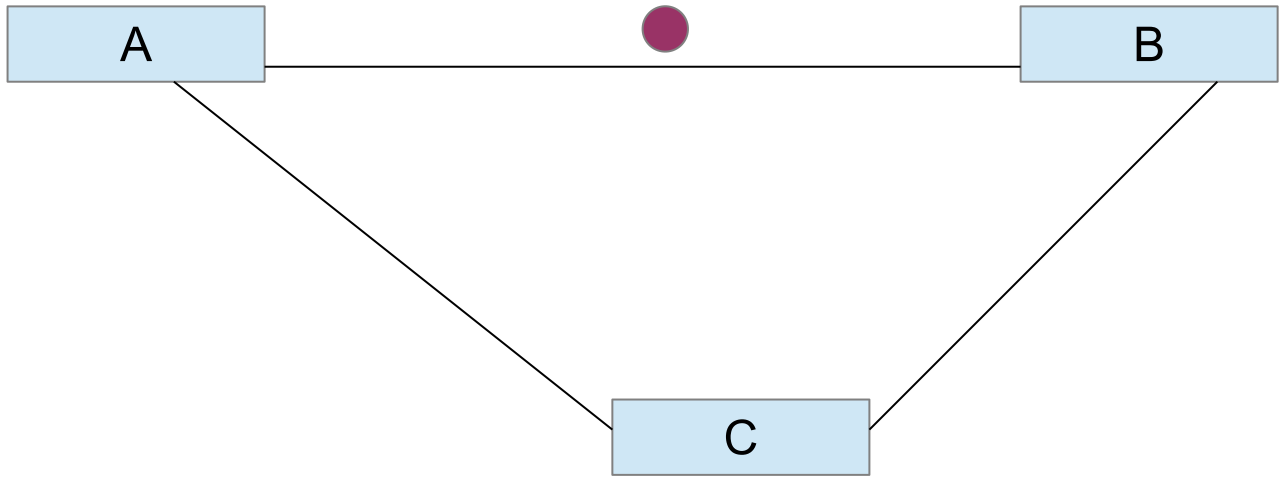
Distributed MAC protocols

- Deterministic protocols
  - Guarantee access to the medium in a finite time
  - Based on the token-sharing mechanism
  - The machine owning the token has the right to transmit



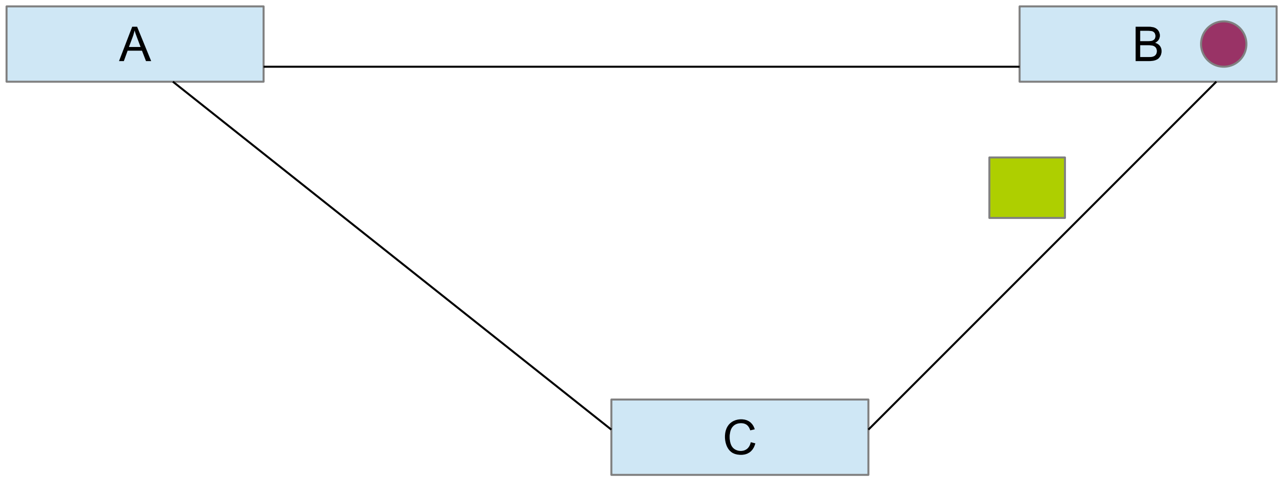
Distributed MAC protocols

- Deterministic protocols
  - Guarantee access to the medium in a finite time
  - Based on the token-sharing mechanism
  - The machine owning the token has the right to transmit



Distributed MAC protocols

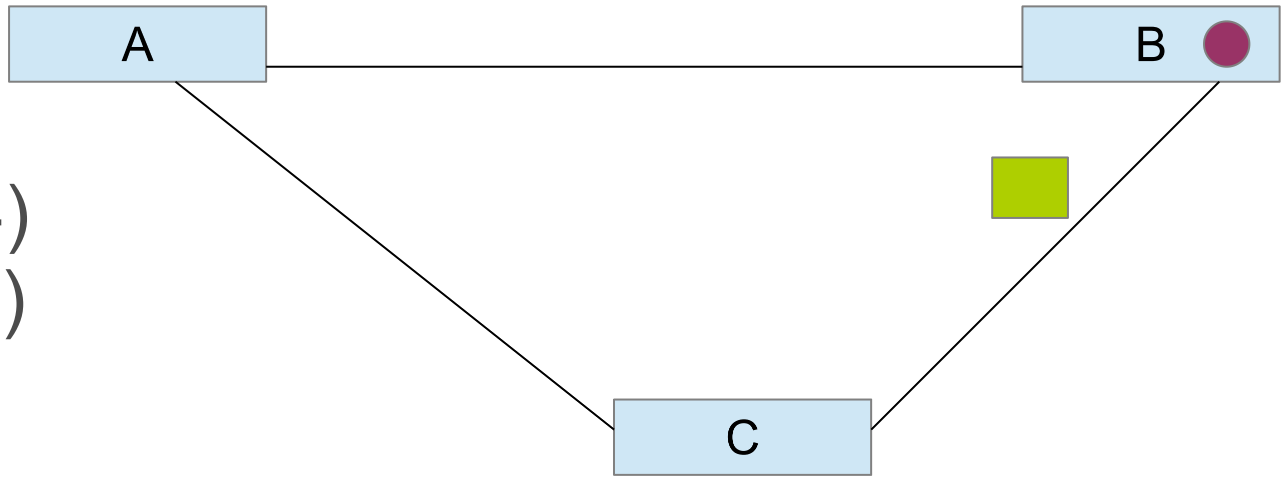
- Deterministic protocols
  - Guarantee access to the medium in a finite time
  - Based on the token-sharing mechanism
  - The machine owning the token has the right to transmit
  - Resource under-utilization



Distributed MAC protocols

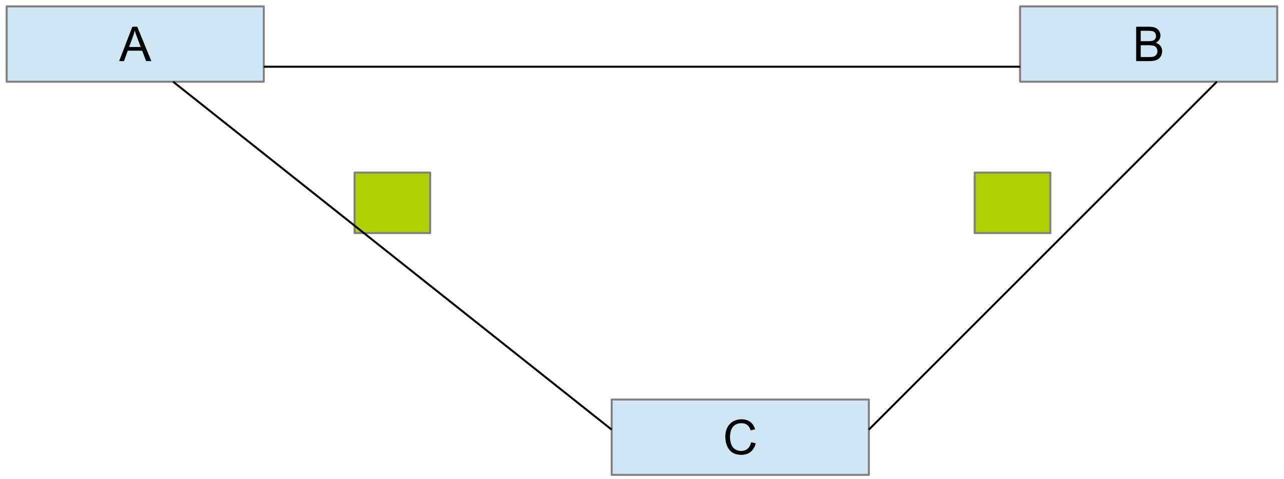
- Deterministic protocols
  - Guarantee access to the medium in a finite time
  - Based on the token-sharing mechanism
  - The machine owning the token has the right to transmit
  - Resource under-utilization

  - See: Token Bus (IEEE 802.4) and Token Ring (IEEE 802.5)



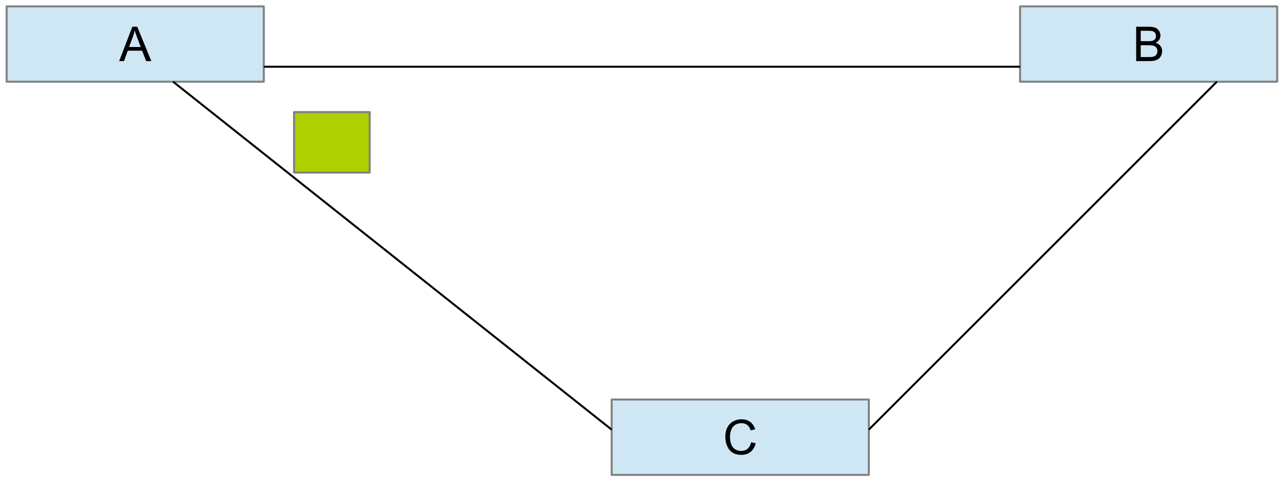
Stochastic MAC protocols

- Randomised mechanisms
  - No guarantee regarding channel access time
  - Collisions are possible between transmitters
  - Good performance *on average*



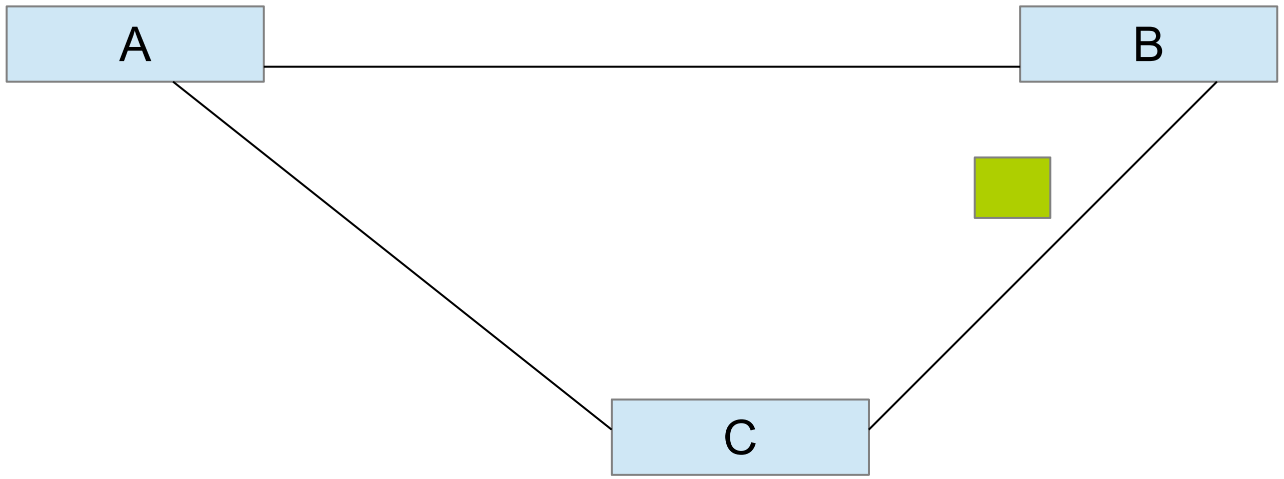
Stochastic MAC protocols

- Randomised mechanisms
  - No guarantee regarding channel access time
  - Collisions are possible between transmitters
  - Good performance *on average*



Stochastic MAC protocols

- Randomised mechanisms
  - No guarantee regarding channel access time
  - Collisions are possible between transmitters
  - Good performance *on average*



Stochastic MAC protocols

- Aloha
  - '60s : connecting terminals to mainframes
  - Usually through phone lines

Stochastic MAC protocols

- Aloha
  - Two frequency channels: mainframe to terminals and terminals to mainframe
  - A terminal sends data as soon as it becomes available
  - Collision (and propagation error) possibility
  - ACK message from mainframe to terminal
  - If ACK not received, retransmission after a random delay

Stochastic MAC protocols

- Aloha
  - Good performance in lightly loaded networks
  - Collisions cascade under high load
  - Maximum channel utilization at 18.6% of the bandwidth

Stochastic MAC protocols

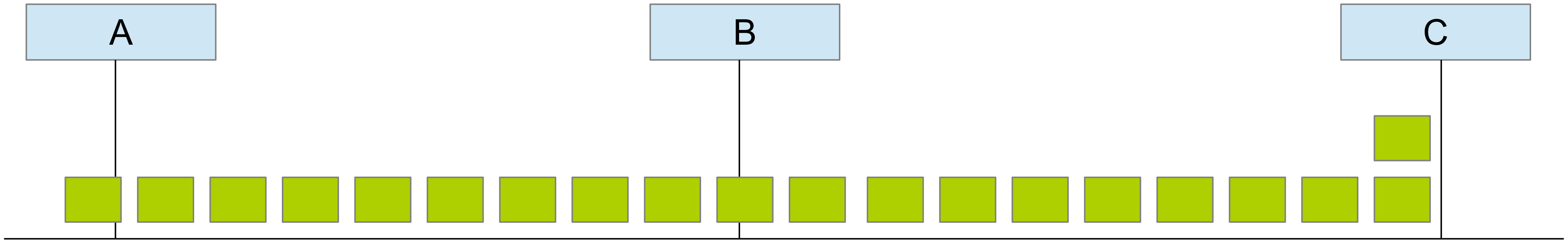
- Slotted Aloha
  - Simple improvement if temporal synchronization available
  - Time divided in slots
  - Transmissions can only begin at the beginning of a slot
  - Doubles the maximum channel utilization with respect to Pure Aloha

Stochastic MAC protocols

- CSMA – Carrier Sense Multiple Access
  - Based on the carrier sense mechanism
  - Can be summarized as *listen before you talk*
  - If medium is busy, wait and transmit later
  - Waiting time based on a random back-off

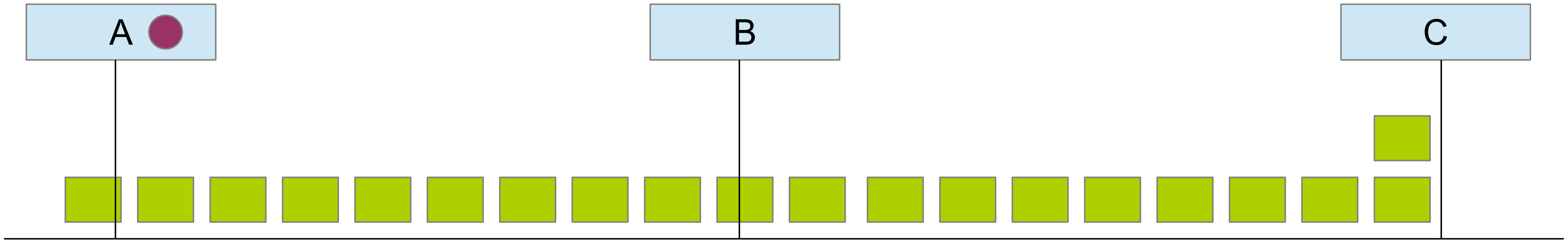
Stochastic MAC protocols

- CSMA flavours
  - Persistent CSMA
    - *If the channel is busy, wait until it becomes free and then transmit*
  - Non-persistent CSMA
  - *p*-persistent CSMA



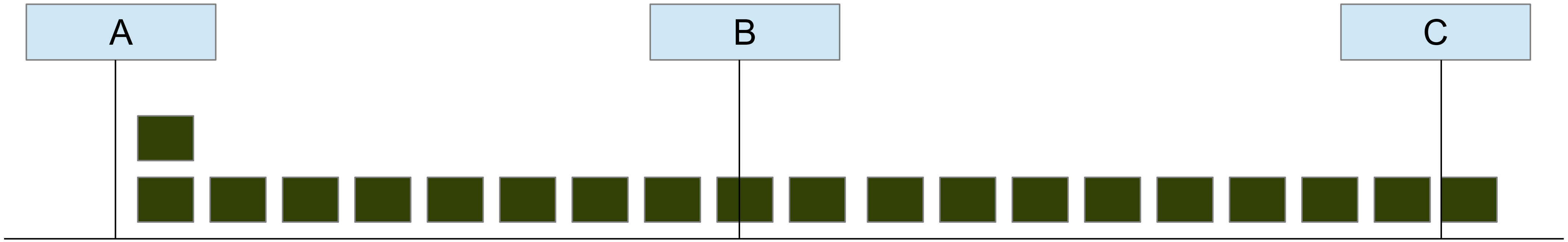
Stochastic MAC protocols

- CSMA flavours
  - Persistent CSMA
    - *If the channel is busy, wait until it becomes free and then transmit*
  - Non-persistent CSMA
  - *p*-persistent CSMA



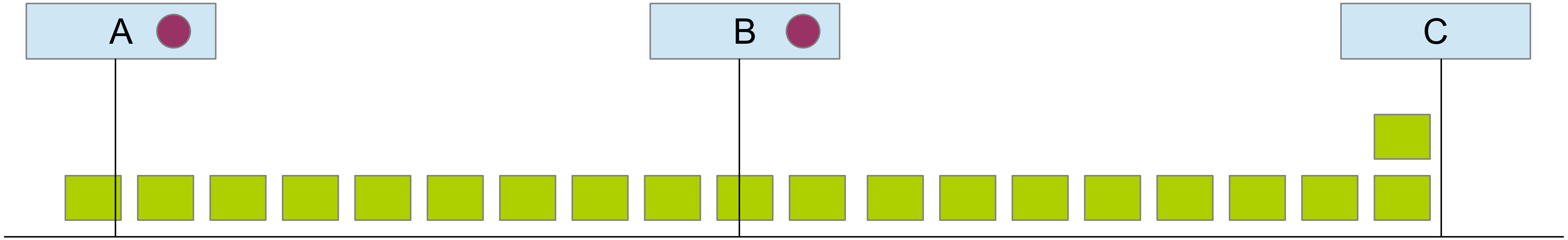
Stochastic MAC protocols

- CSMA flavours
  - Persistent CSMA
    - *If the channel is busy, wait until it becomes free and then transmit*
  - Non-persistent CSMA
  - *p*-persistent CSMA



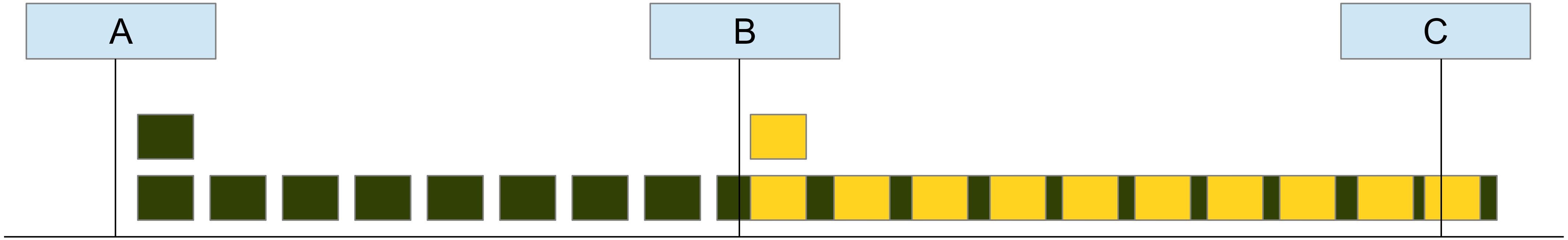
Stochastic MAC protocols

- CSMA flavours
  - Persistent CSMA
    - *If the channel is busy, wait until it becomes free and then transmit*
  - Non-persistent CSMA
  - *p*-persistent CSMA



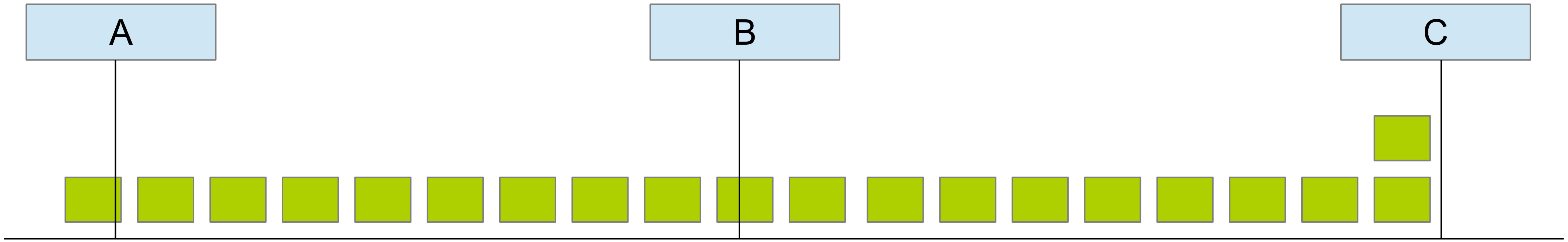
Stochastic MAC protocols

- CSMA flavours
  - Persistent CSMA
    - *If the channel is busy, wait until it becomes free and then transmit*
  - Non-persistent CSMA
  - *p*-persistent CSMA



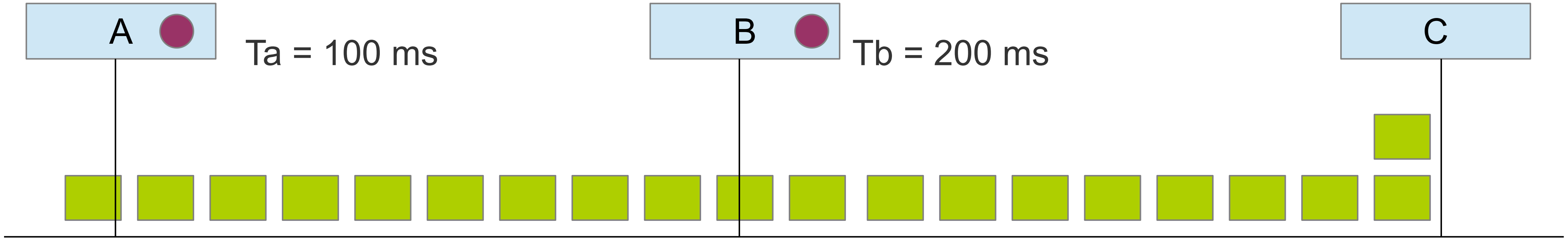
Stochastic MAC protocols

- CSMA flavours
  - Persistent CSMA
  - Non-persistent CSMA
    - *If the channel is busy, wait random time before checking again*
  - *p*-persistent CSMA



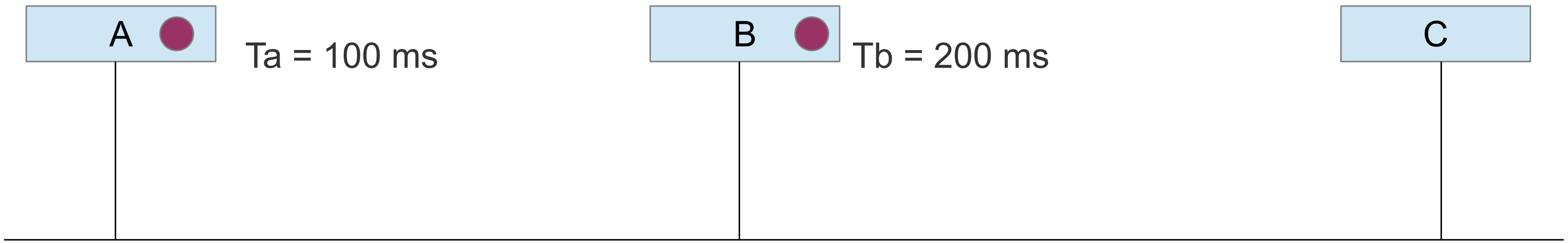
Stochastic MAC protocols

- CSMA flavours
  - Persistent CSMA
  - Non-persistent CSMA
    - *If the channel is busy, wait random time before checking again*
  - *p*-persistent CSMA



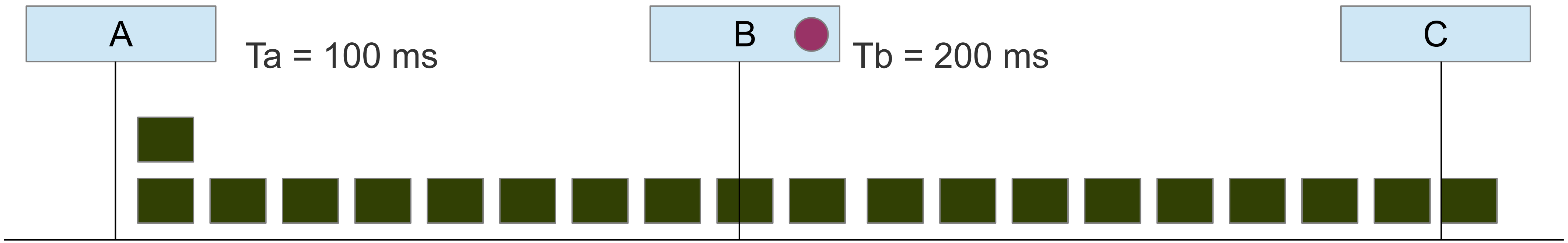
Stochastic MAC protocols

- CSMA flavours
  - Persistent CSMA
  - Non-persistent CSMA
    - *If the channel is busy, wait random time before checking again*
  - *p*-persistent CSMA



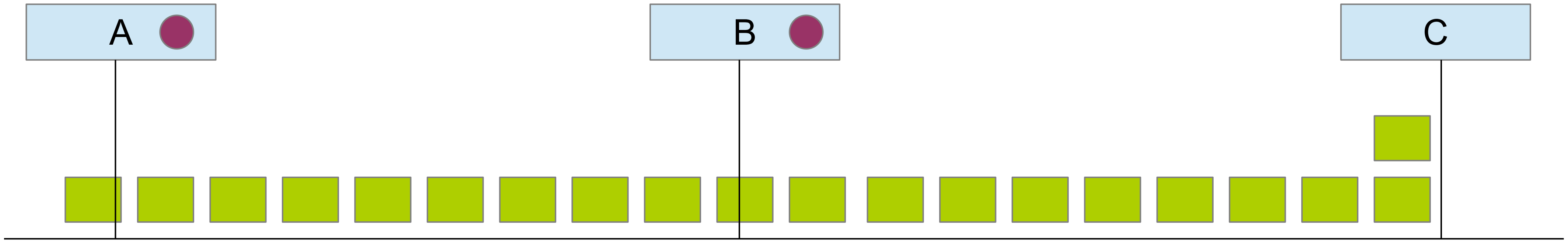
Stochastic MAC protocols

- CSMA flavours
  - Persistent CSMA
  - Non-persistent CSMA
    - *If the channel is busy, wait random time before checking again*
  - *p*-persistent CSMA



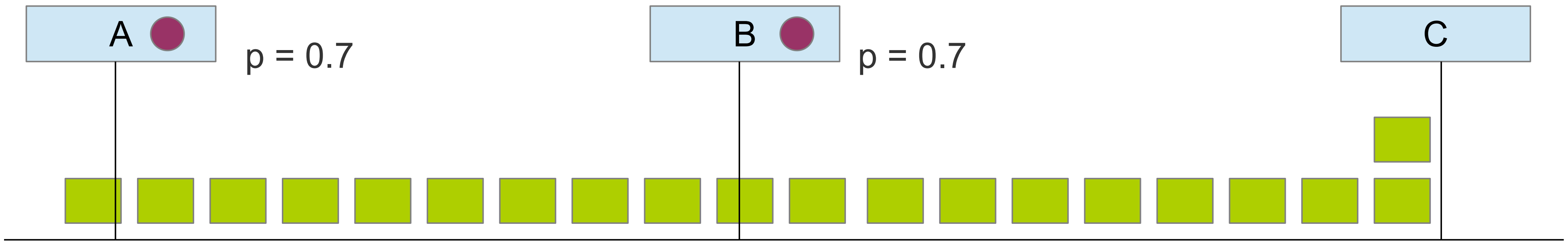
Stochastic MAC protocols

- CSMA flavours
  - Persistent CSMA
  - Non-persistent CSMA
  - *p*-persistent CSMA
    - *Persistent solution, but transmission with probability p when channel idle*



Stochastic MAC protocols

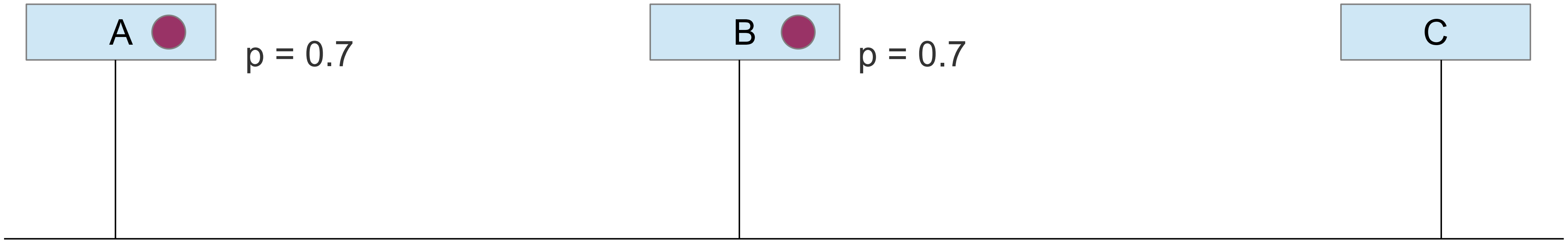
- CSMA flavours
  - Persistent CSMA
  - Non-persistent CSMA
  - *p*-persistent CSMA
    - *Persistent solution, but transmission with probability p when channel idle*



Stochastic MAC protocols

- CSMA flavours
  - Persistent CSMA
  - Non-persistent CSMA
  - *p*-persistent CSMA
    - *Persistent solution, but transmission with probability p when channel idle*

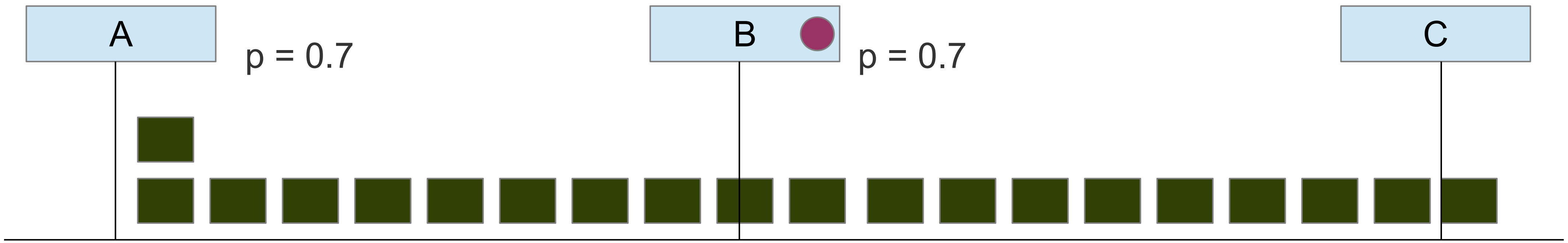
Case 1



Stochastic MAC protocols

- CSMA flavours
  - Persistent CSMA
  - Non-persistent CSMA
  - *p*-persistent CSMA
    - *Persistent solution, but transmission with probability p when channel idle*

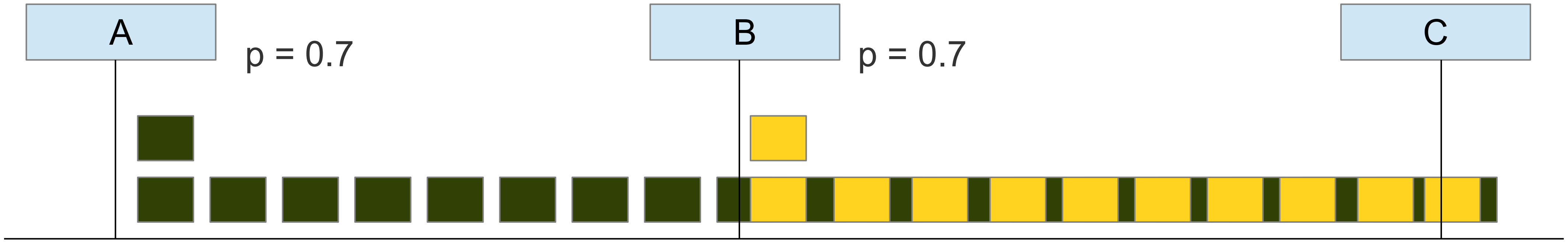
Case 2



Stochastic MAC protocols

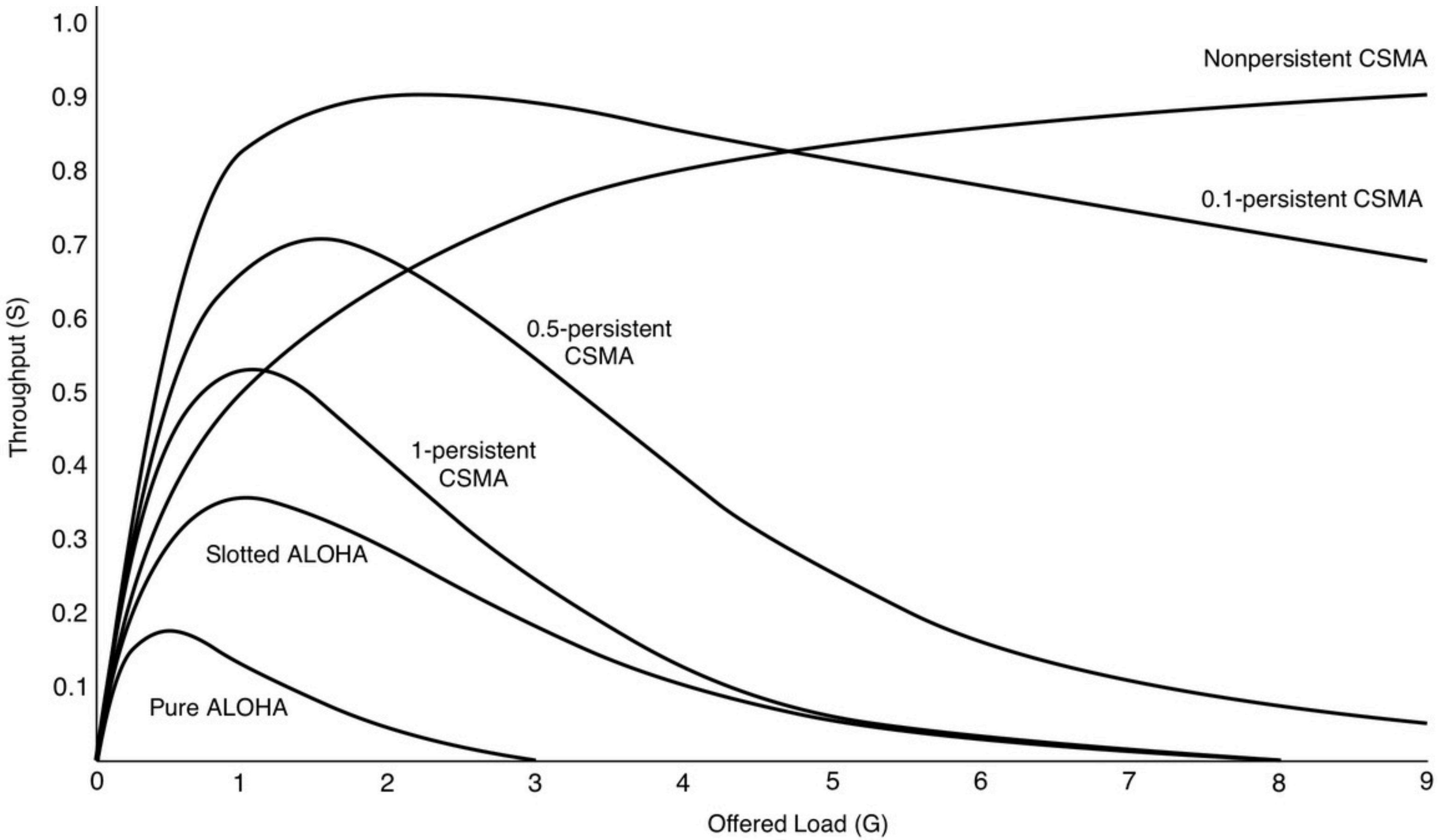
- CSMA flavours
  - Persistent CSMA
  - Non-persistent CSMA
  - *p*-persistent CSMA
    - *Persistent solution, but transmission with probability p when channel idle*

Case 3



Stochastic MAC protocols

- Overall performance



Source: Thanh Hai To, *Energy saving protocols for the Internet of Things,* PhD Thesis, Université Grenoble Alpes, 2020

Stochastic MAC protocols

- CSMA flavours
  - Two types of CSMA largely used today
  - CSMA with Collision Detection (CSMA/CD)
    - *Used in Ethernet*
  - CSMA with Collision Avoidance (CSMA/CA)
    - *Used in WiFi*

5. CSMA/CD

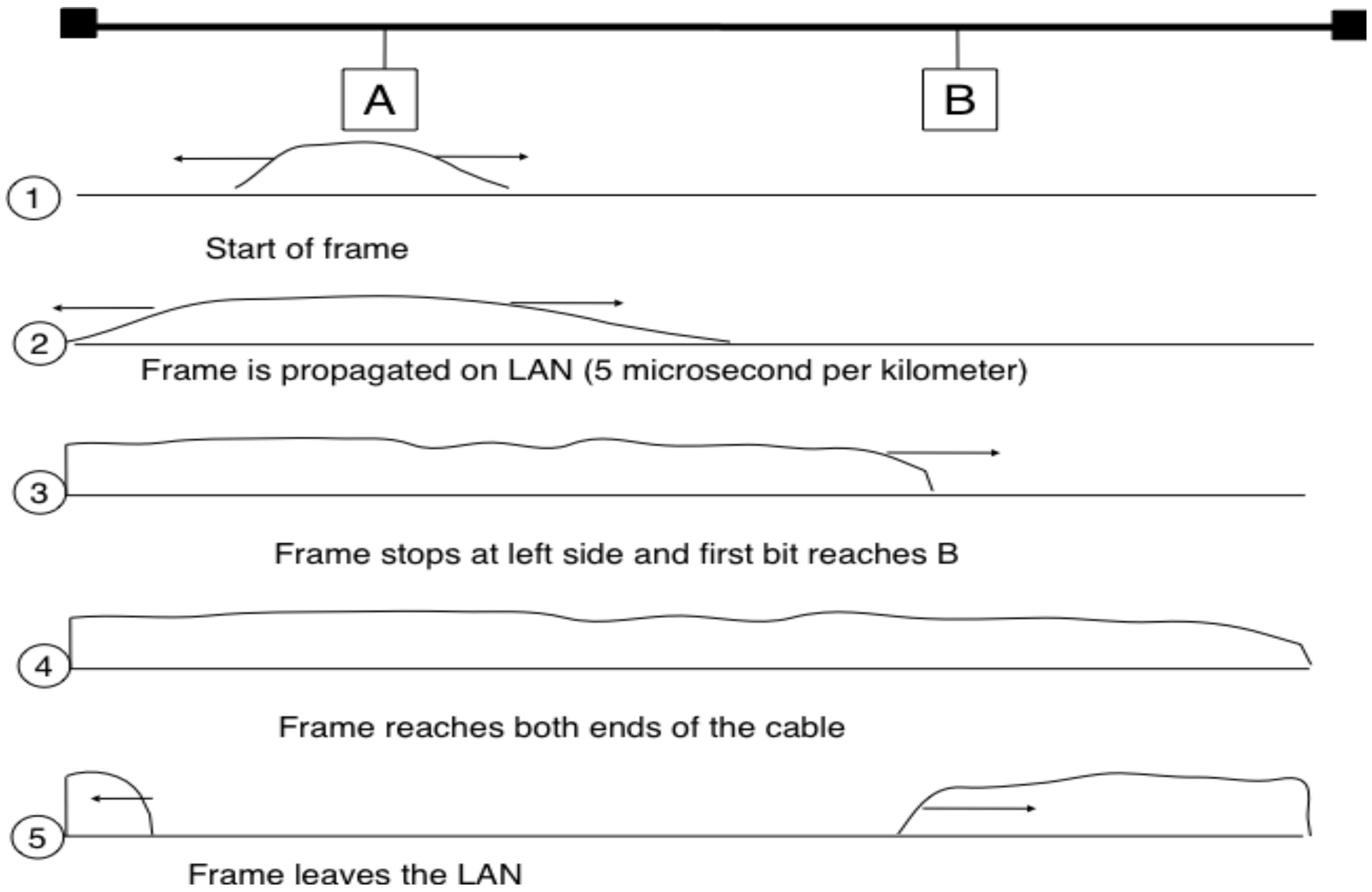
Medium access control for Ethernet and IEEE 802.3

CSMA/CD

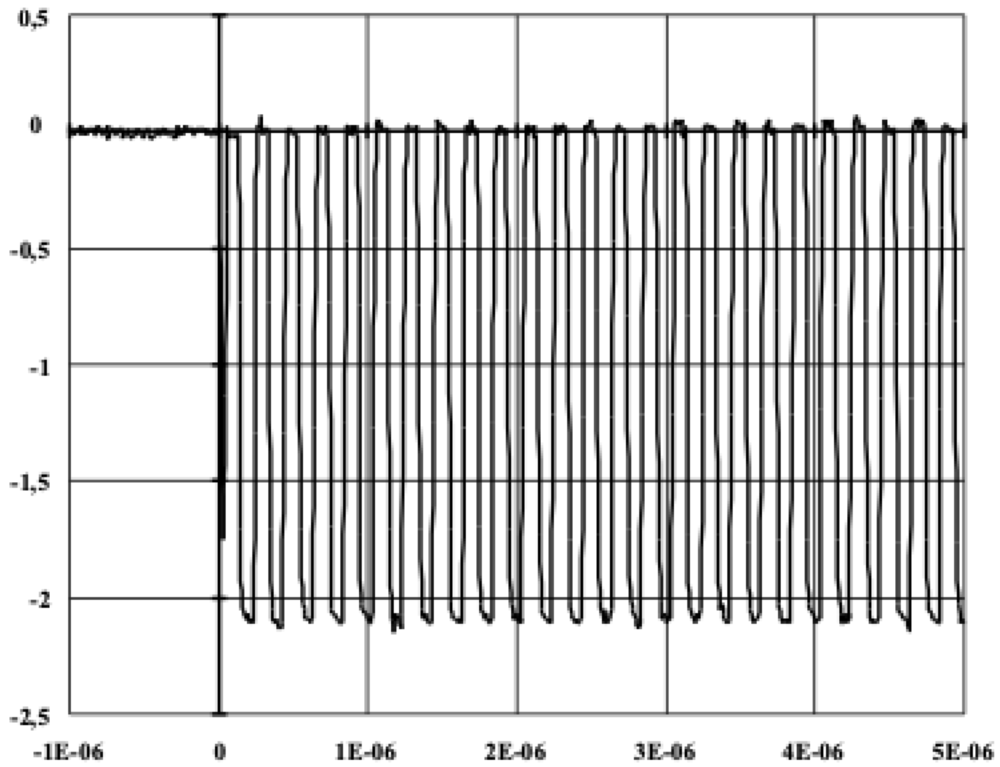
- Basic principles
  - Carrier Sense – listen the medium to detect ongoing transmissions
  - Collision Detection – notice a collision as soon as possible and enter a back-up mode
  - Requires to listen and transmit at the same time
  - Compare transmitted and received signals to detect collisions

CSMA/CD

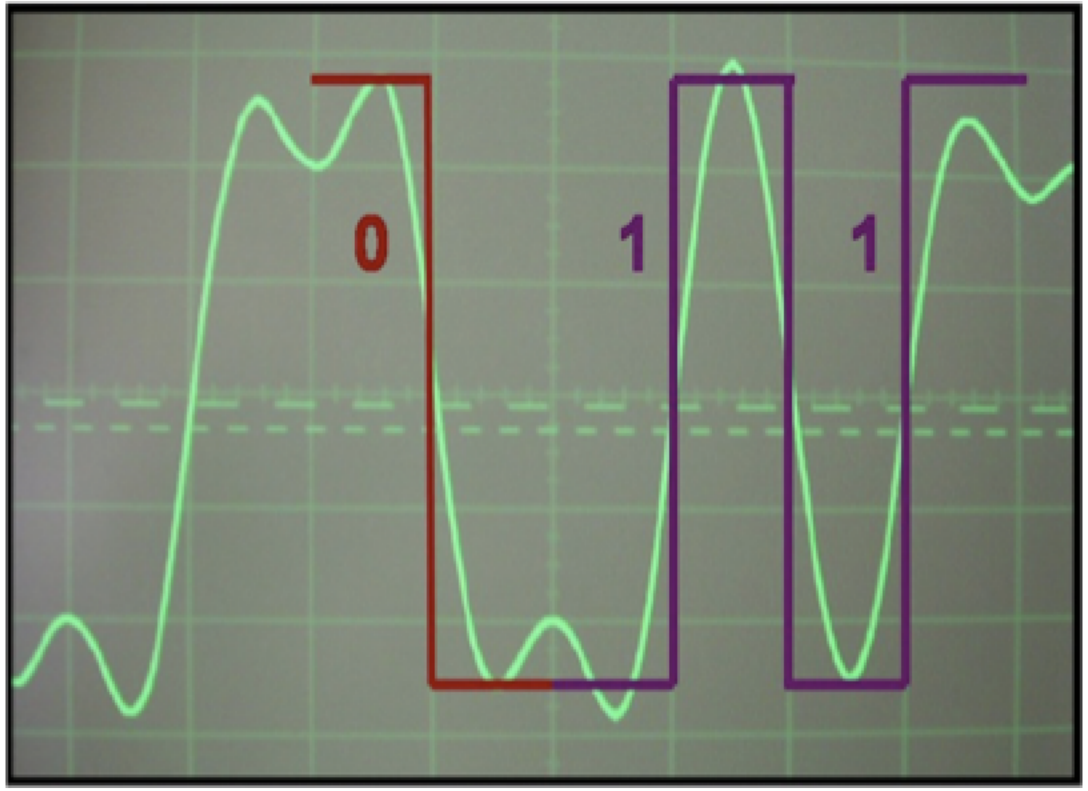
- Basic principles
  - Signal propagation on an electrical cable



CSMA/CD



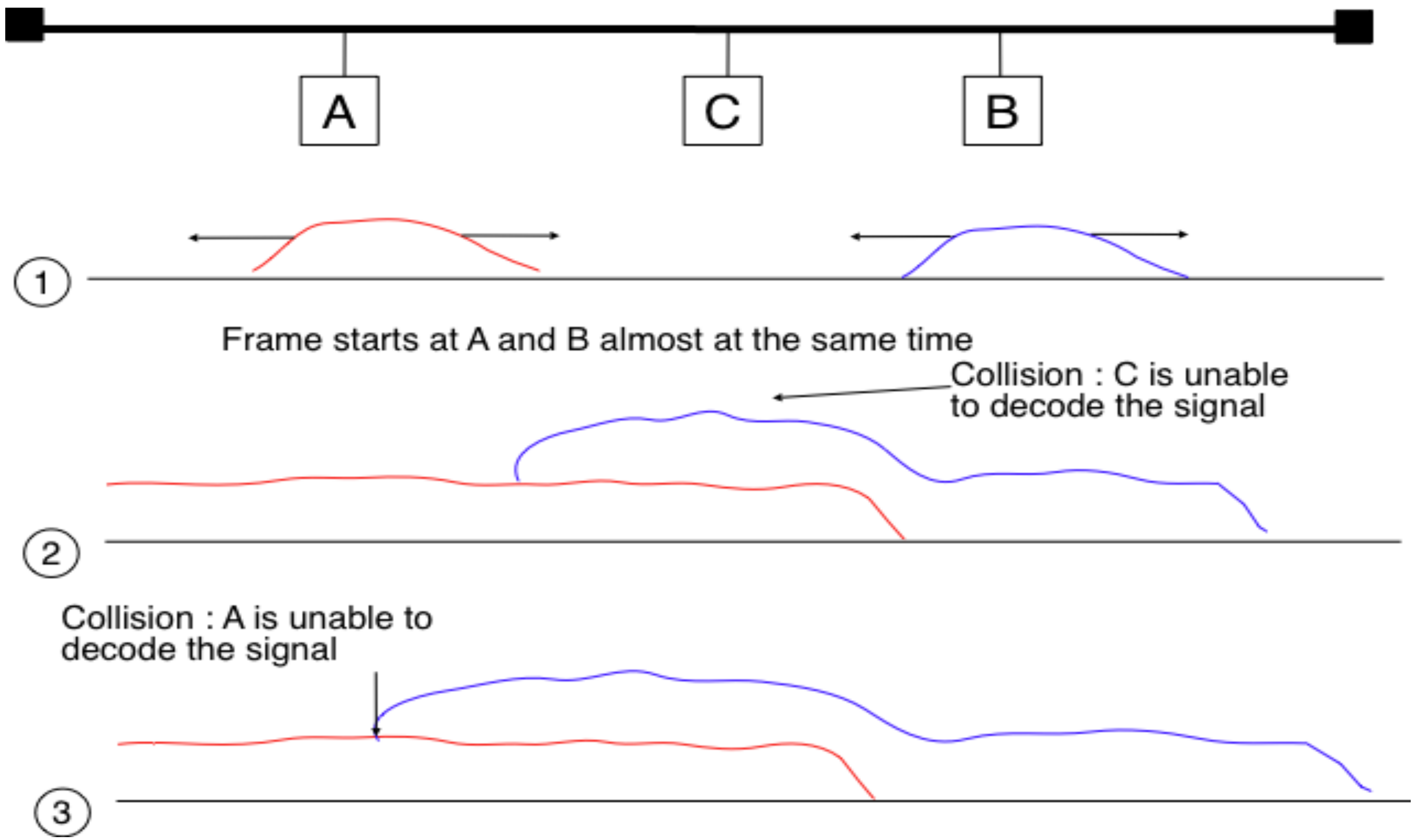
The preamble allow the synchronization of the receiver



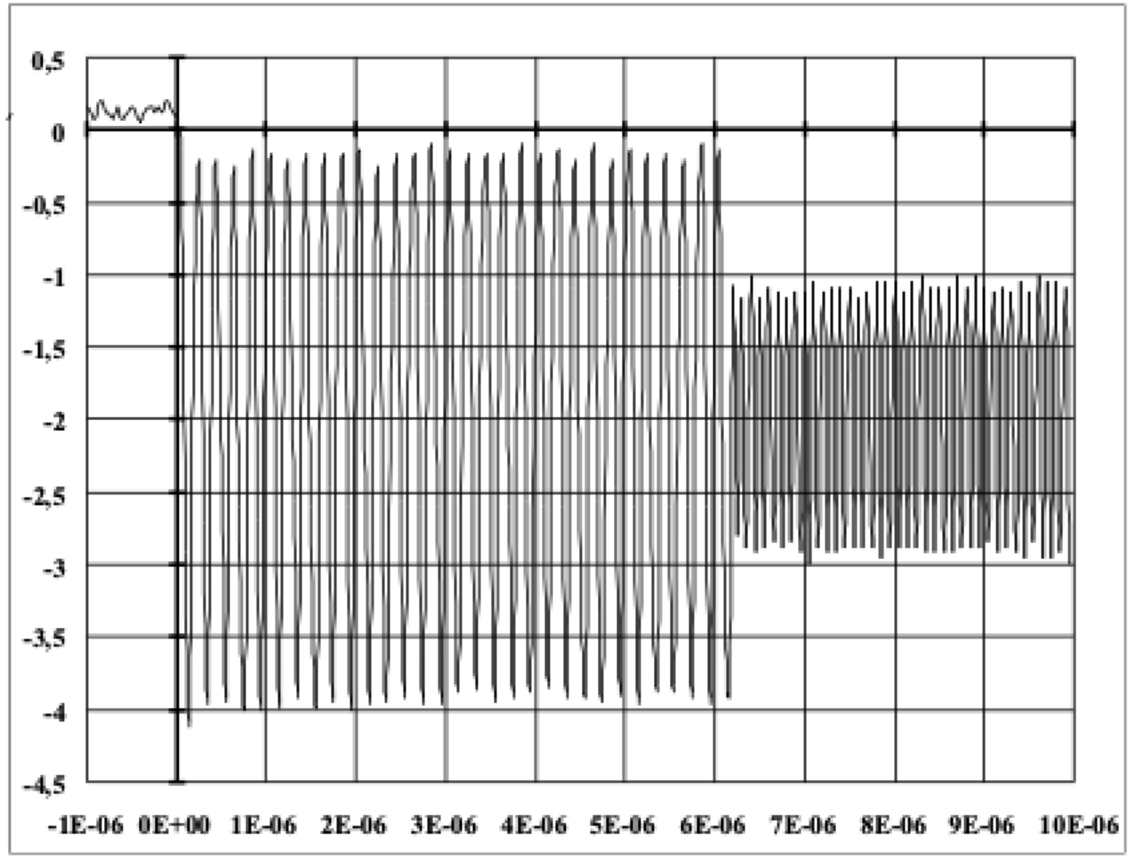
Transmission in Ethernet, 10Base2

CSMA/CD

- Basic principles
  - Collision on an electrical cable



CSMA/CD



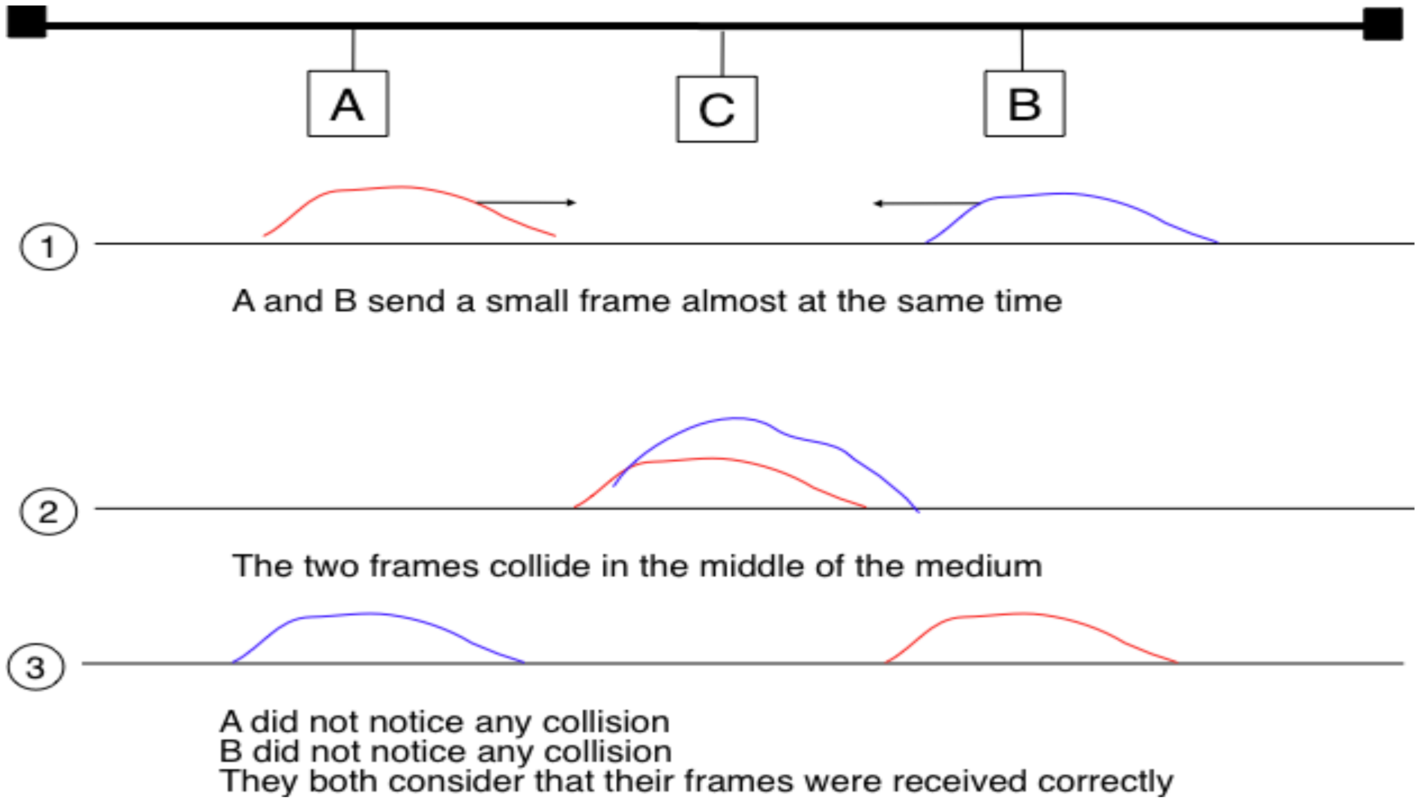
When a collision occurs...

CSMA/CD

- Basic principles
  - To properly handle collisions, a station needs to detect an incoming frame before the end of its own transmission

CSMA/CD

- Basic principles
  - To properly handle collisions, a station needs to detect an incoming frame before the end of its own transmission

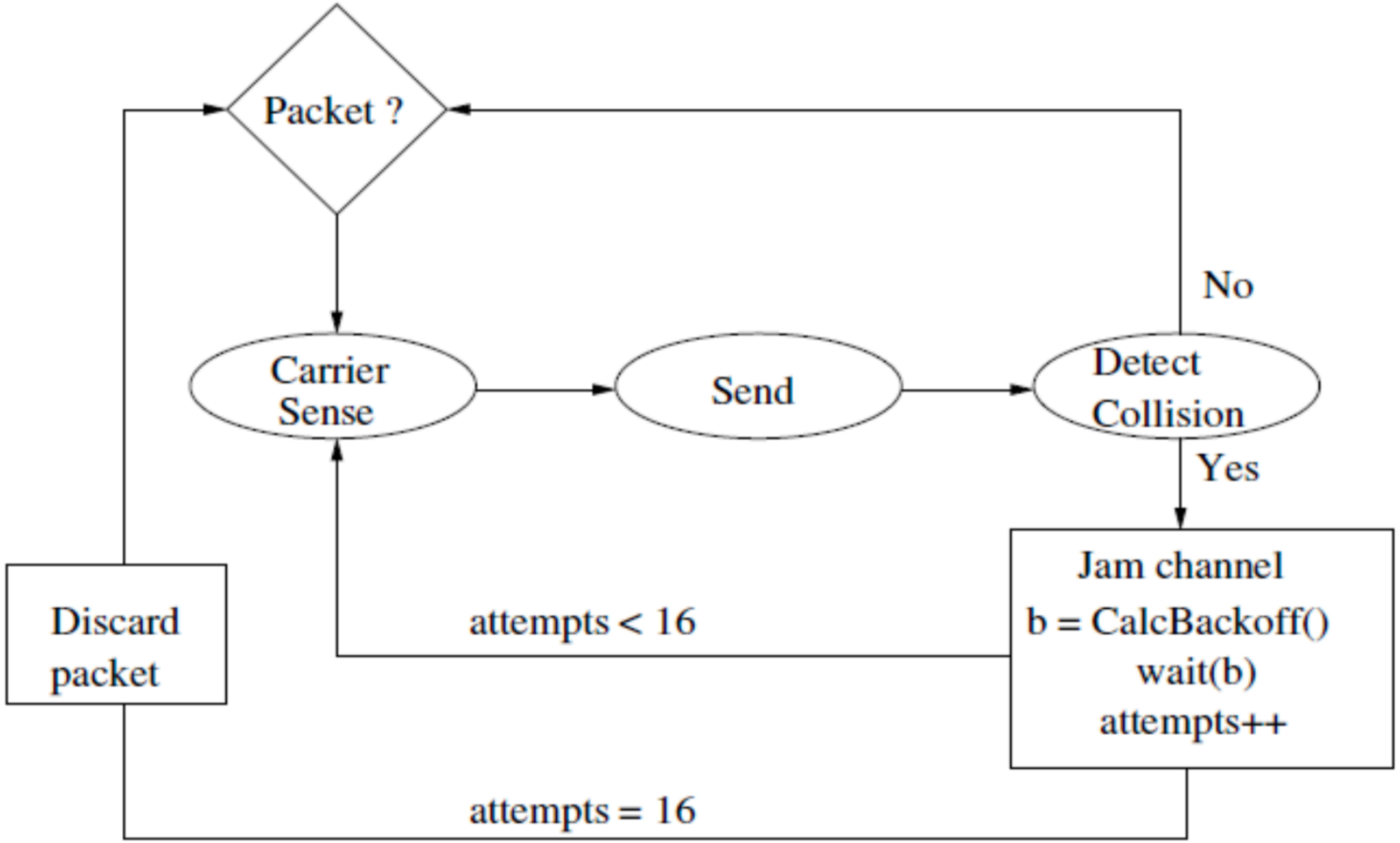


CSMA/CD

- Basic principles
  - Minimum frame length: a transmission needs to last for at least 2 times the maximum propagation time
  - Jam signal: when a collision is detected, do not stop until the minimum frame length is reached
  - All the other stations need to start receiving a frame before the transmission ends

CSMA/CD

- Protocol state machine

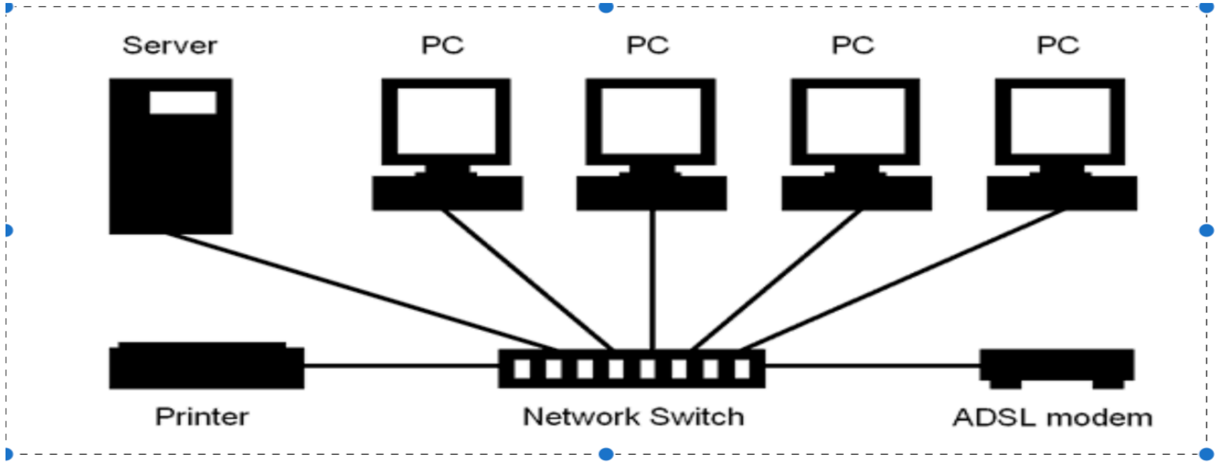


CSMA/CD

- Binary Exponential Back-off (BEB)
  - When a collision is detected, stations need to be desynchronized
  - All the contending and transmitting stations detecting a collision choose a random timer
  - Time becomes slotted – a slot is the time during which a collision can occur at the beginning of a frame
  - For the *i*-th consecutive collision – uniform back-off choice *b* in the window $[0, 2^i - 1]$
  - Station waits for *b* slots before trying a transmission

From CSMA/CD to Ethernet

- Implementation
  - Ethernet – developed in the early '70s at the Xerox Palo Alto Research Center
  - The dominant technology today
  - Evolutions in terms of data rate, physical support and topology (Ethernet switches)



From CSMA/CD to Ethernet

- Implementation
  - In 1983, a slightly modified version of Ethernet was standardized by the IEEE 802.3 working group
  - The most recent version – IEEE 802.3cc (25 Gbps over single mode fiber)
  - Current work, mostly on optical networks, where IEEE 802.3 is becoming the dominant technology

Ethernet

- Implementation
  - Ethernet frame

Preamble	Destination	Source	Type	Data	CRC
8 bytes	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes

  - IEEE 802.3 frame

Preamble	Destination	Source	Length	802.2 header	Data	CRC
8 bytes	6 bytes	6 bytes	2 bytes	8 bytes	38-1492 bytes	4 bytes

Ethernet

- Implementation
  - Ethernet frame

Preamble 8 bytes	Destination 6 bytes	Source 6 bytes	Type 2 bytes	Data 46-1500 bytes	CRC 4 bytes

  - IEEE 802.3 frame

Preamble 8 bytes	Destination 6 bytes	Source 6 bytes	Length 2 bytes	802.2 header 8 bytes	Data 38-1492 bytes	CRC 4 bytes

Ethernet

- Implementation
  - Ethernet frame

Preamble	Destination	Source	Type	Data	CRC
8 bytes	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes

  - Preamble – synchronize the clock of the transmitter and receiver

Ethernet

- Implementation
  - Ethernet frame

Preamble	Destination	Source	Type	Data	CRC
8 bytes	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes

  - Destination and Source – 48 bits MAC addresses

Ethernet

- Implementation
  - Ethernet frame

Preamble 8 bytes	Destination 6 bytes	Source 6 bytes	Type 2 bytes	Data 46-1500 bytes	CRC 4 bytes

  - Type – unique code for the encapsulated protocol (e.g. 0X0800 for IP)

Ethernet

- Implementation
  - Ethernet frame

Preamble	Destination	Source	Type	Data	CRC
8 bytes	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes

  - Data – possibly with padding to reach the minimum frame size

Ethernet

- Implementation
  - Ethernet frame

Preamble	Destination	Source	Type	Data	CRC
8 bytes	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes

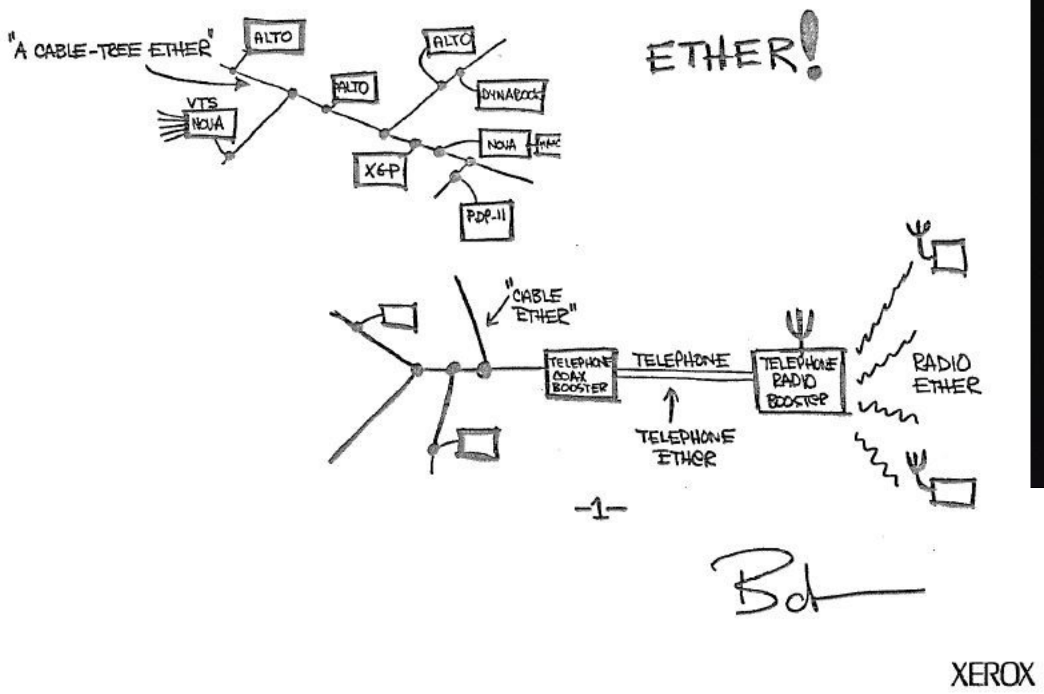
  - CRC – Cyclic Redundancy Check for error control

Ethernet

- MAC address
  - Physical address
  - Encoded on 6 bytes (48 bits)
  - Theoretically unique address, assigned by the manufacturer
  - 3 bytes to identify the manufacturer, 3 bytes to identify the network card
  - Today, it can be easily modified in software
  - All frames are received by all stations sharing the medium
  - Dropped by stations that do not match the destination address
  - Special broadcast (FF:FF:FF:FF:FF:FF) and multicast addresses

Thanks Bob Metcalfe!

- Ethernet was invented by Bob Metcalfe,
  - Xerox, 1973
  - Turing Prize, 2022



Credit: @AlexArchambault, https://twitter.com/alexarchambault/status/1660610708554514432?s=61&t=WpYBM8FaF0drm6tqOm_-2A

6. CSMA/CA

Medium access control for Wi-Fi and IEEE 802.11

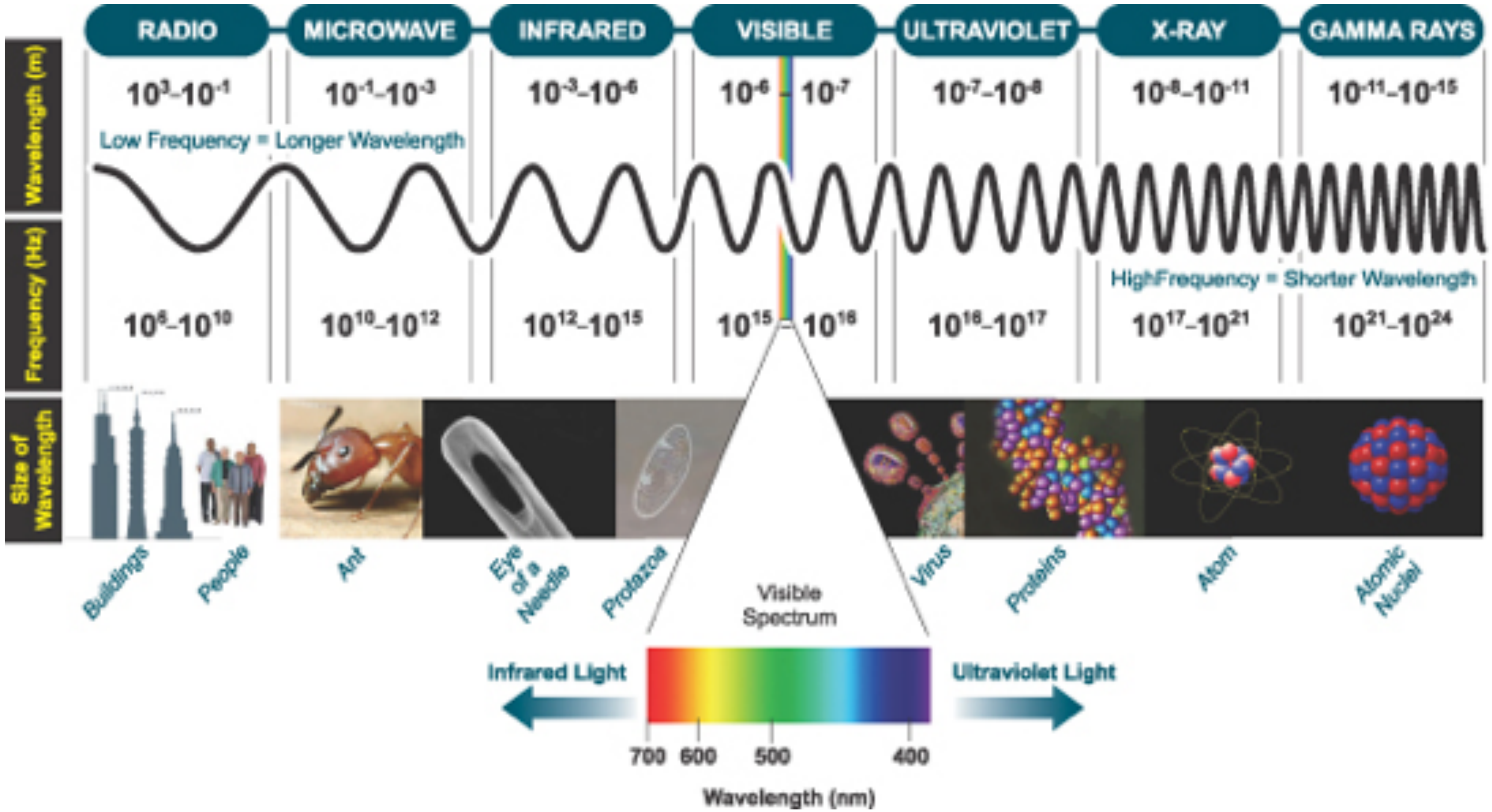
The plan of today

- What makes wireless so special?
- Carrier Sense Multiple Access with Collision Avoidance Why? How?
- What else is in IEEE 802.11?

Basic concepts: wireless

- Electromagnetic frequency spectrum

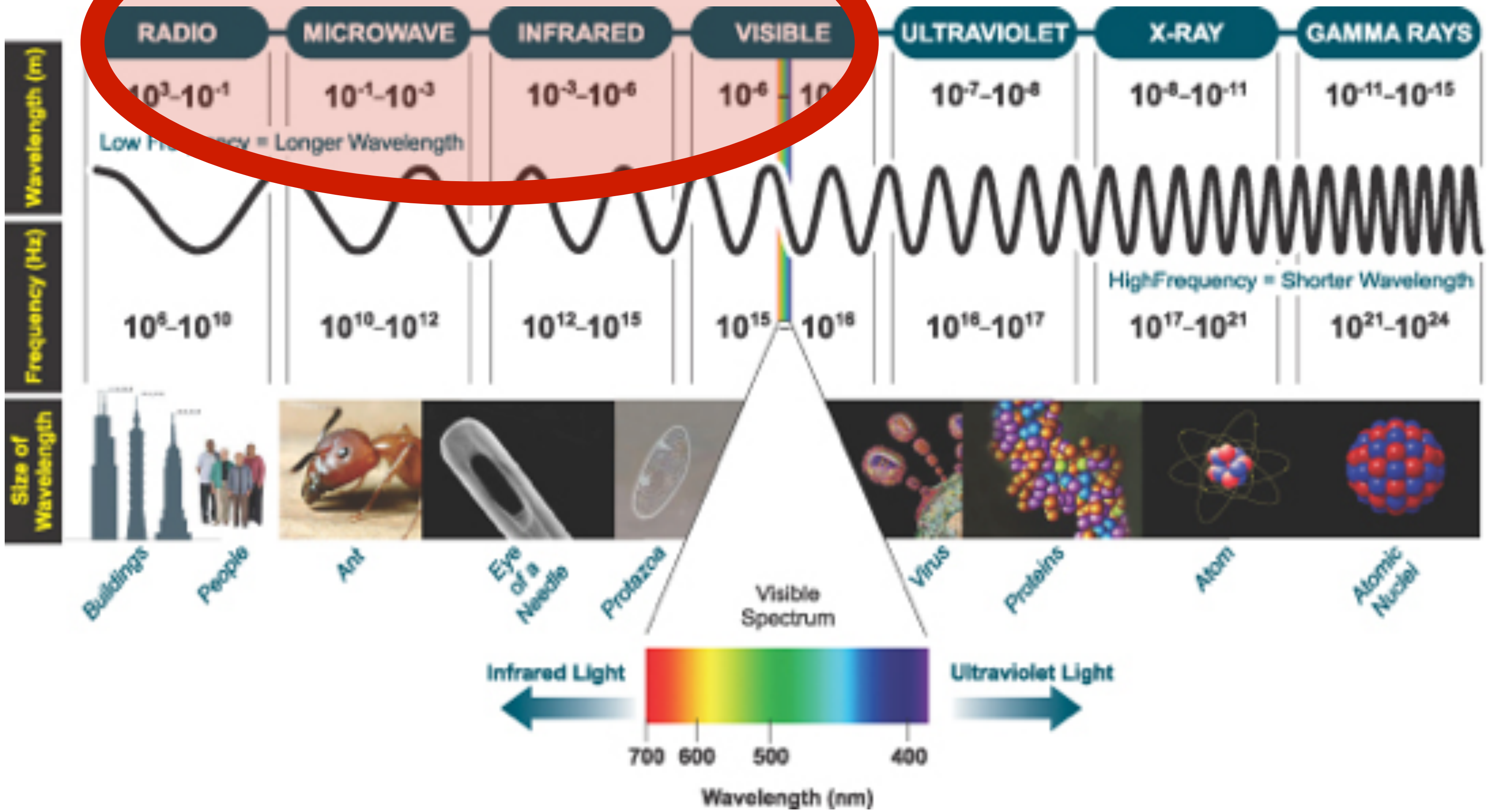
$\lambda = c/f$



Basic concepts: wireless

- Where wireless communication happens

$\lambda = c/f$



Basic concepts: wireless spectrum

Name	f	λλ	Usage
Low Frequency	30 KHz	10 Km	Aeronautical & maritime navigation, metereology
Medium Frequency	300 KHz	1 Km	AM radio
High Frequency	3 MHz	100 m	Amateur radio (Morse code), marine, aviation, military
Very High Frequency	30 MHz	10 m	FM radio
Ultra High Frequency	300 MHz	1 m	Television, Cellular networks, WiFi
Super High Frequency	3 GHz	10 cm	WiFi, Satellite transmission, Bluetooth, Wireless USB
Extremely High Frequency	30 GHz	1 cm	Radar, Satellite sensing, Wireless HD, WiFi(?)
Infrared	300 GHz	1 mm	Lasers, LEDs, Free Space Optical Communication

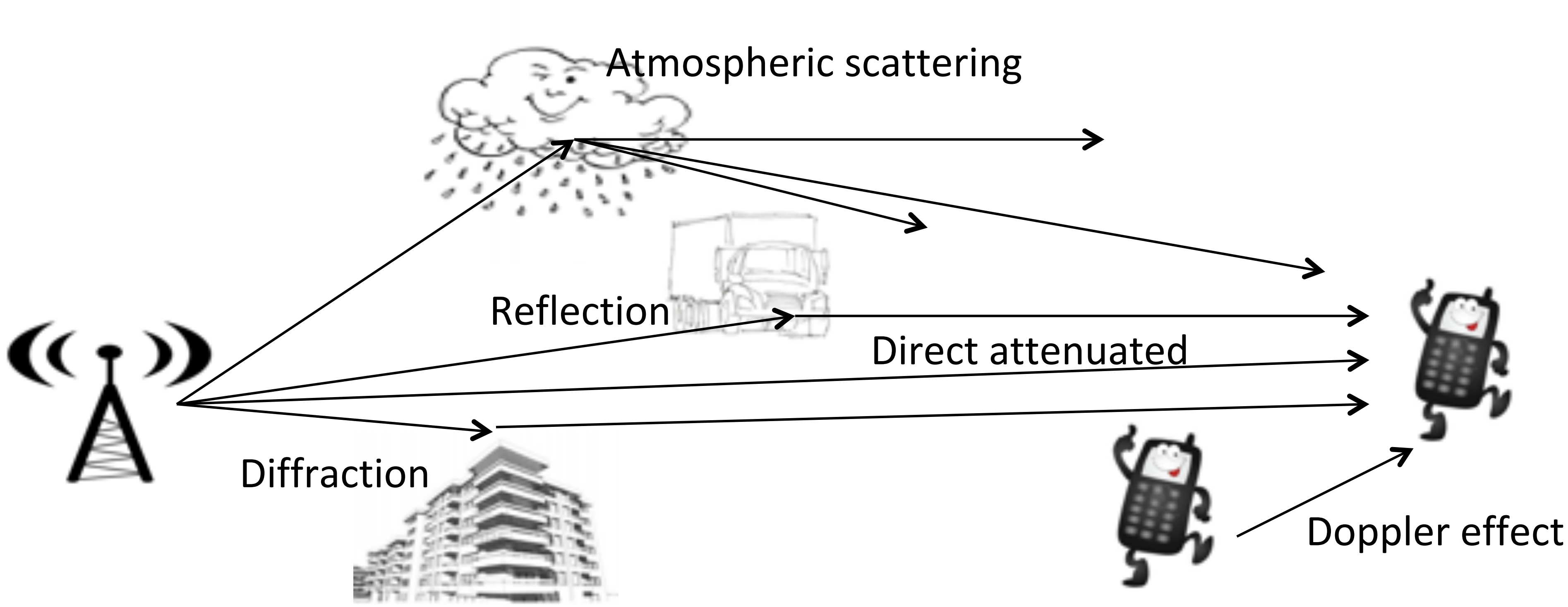
Basic concepts: wireless spectrum

Name	f	λλ	Usage
Low **F**requency	30 KHz	10 Km	Aeronautical & maritime navigation, metereology
Medium **F**requency	300 KHz	1 Km	AM radio
High **F**requency	3 MHz	100 m	Amateur radio (Morse code), marine, aviation, military
Very **H**igh **F**requency	30 MHz	10 m	FM radio
Ultra **H**igh **F**requency	300 MHz	1 m	Television, Cellular networks, WiFi
Super **H**igh **F**requency	3 GHz	10 cm	WiFi, Satellite transmission, Bluetooth, Wireless USB
Extremely **H**igh **F**requency	30 GHz	1 cm	Radar, Satellite sensing, Wireless HD, WiFi(?)
Infrared	300 GHz	1 mm	Lasers, LEDs, Free Space Optical Communication

Cordeless Telephony, Cellular,
IoT, Wireless LAN/MAN

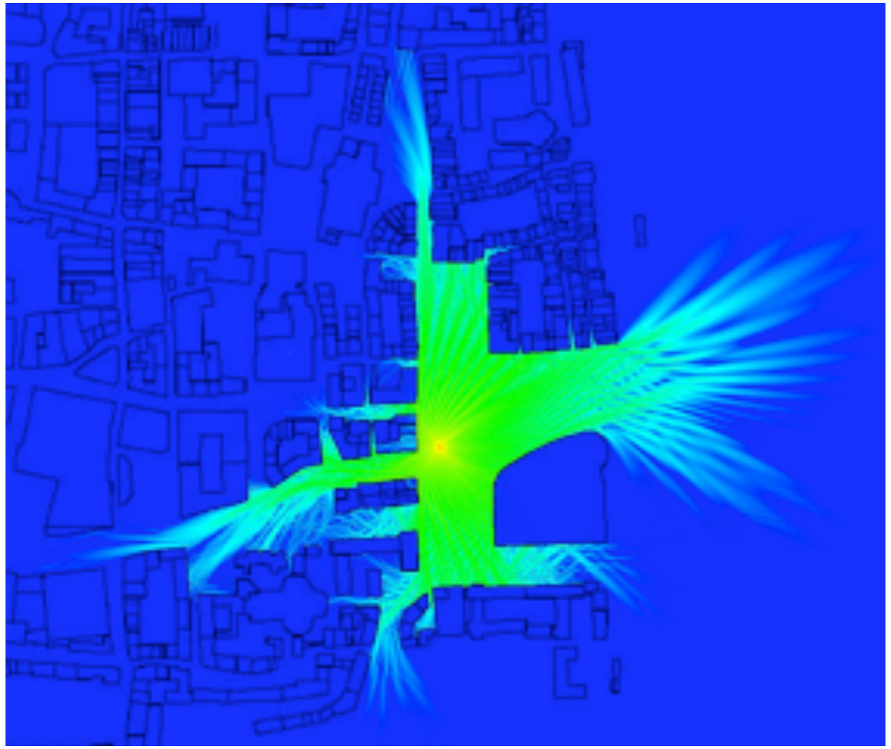
Basic concepts: wireless propagation irl

- Everything you know from EM physics
- Free space attenuation: $P_r \sim P_t \left(\frac{\lambda}{R}\right)^2$



Basic concepts: wireless propagation irl

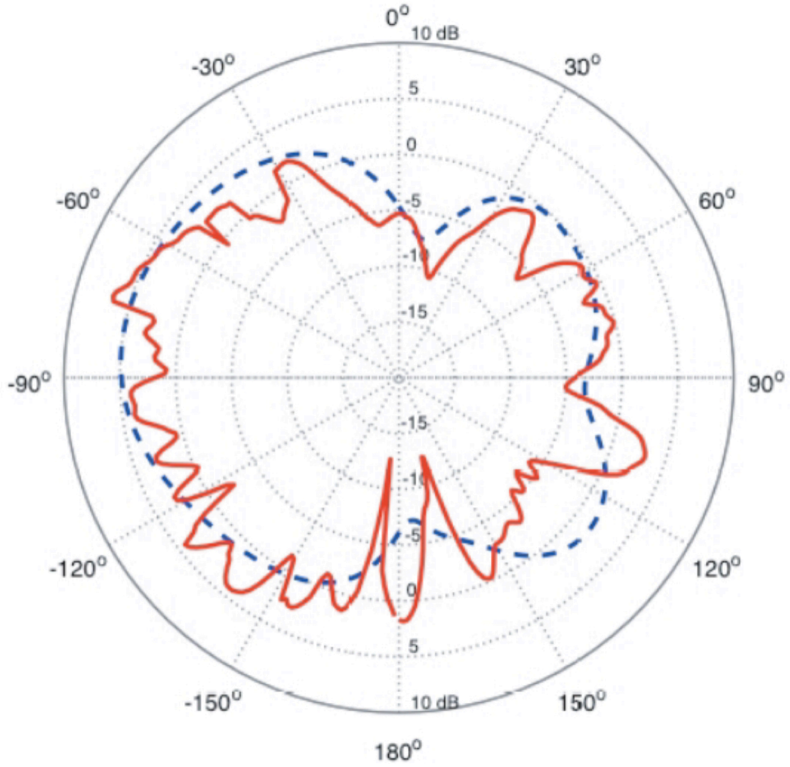
- As a result of the complex RF propagation the strength of the received signal is highly irregular



[City of Koln, 100mW at 2.4GHz]

Basic concepts: antenna design irl

- Not really omnidirectionnal
  - Impact on the connectivity



Source: D. K. Rongas, A. S. Paraskevopoulos, L. D. Marantis, and A. G. Kanatas, “An integrated shark-fin reconfigurable antenna for v2x communications,” Progress In Electromagnetics Research C, vol. 100, pp. 1–16, 2020, Progress In Electromagnetics Research.

Basic concepts: MAC layer

- Goal of a MAC layer:
  - fair sharing* of the medium among users and computers
  - manage collisions

- Impressive number of different protocols: TDMA, CDMA, FDMA, OFDMA, Token, Token Ring, Aloha, etc.

* *Same access to the medium (not the same use)*

CSMA: The principle

Listen before you talk

- Every station senses the channel for a certain time before transmitting
- If the channel is idle, transmission goes on
- If the channel is busy, wait and
  - Send as soon as it becomes idle (1-persistent)
  - Choose a random back-of and try again (non-persistent)
  - Send with probability p when idle (p-persistent)

CSMA: The flavours

- Two types of CSMA largely used today:
  - CSMA with Collision Detection (CSMA/CD)
    - *Used in Ethernet*
  - CSMA with Collision Avoidance (CSMA/CA)
    - *Used in WiFi and Zigbee*

CSMA/CD: A remainder

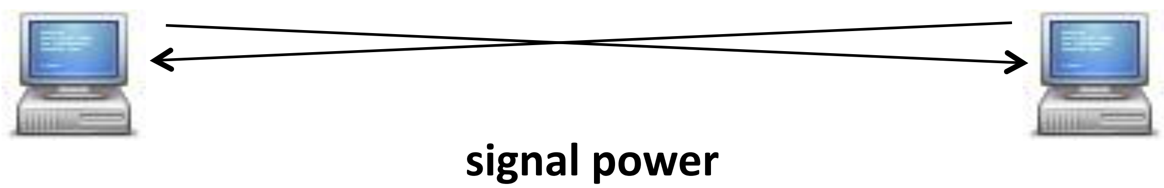
- How does it work?
- It's CSMA, so we listen before we talk.
- The CD part explains what happens when two stations start transmitting at the same time.
- The collision detected procedure:
  - *Keep transmitting a jamming signal for one slot. This way everybody detects the collision.*
  - *Check if you are allowed to retransmit (retransmission limit).*
  - *Double the contention window and back-off.*

b= rand(0,CW-1)

CW_{min}= 1

CSMA/CD: A remainder

- How does it work?



  - Ethernet uses a wired physical layer
  - Full-duplex medium
  - Small signal attenuation
  - CSMA with Collision Avoidance (CSMA/CA)

CSMA/CD: A remainder

- How does it work?

Station A	ii						
Station B	ii						
Station C							

CSMA/CD: A remainder

- How does it work?

Station A	ii	x				
Station B	ii	x				
Station C						

CSMA/CD: A remainder

- How does it work?

Station A	ii	x				
Station B	ii	x				
Station C						

- 4 possibilities for the back-off:
  - *b(A)=0, b(B)=0*
  - *b(A)=0, b(B)=1*
  - *b(A)=1, b(B)=0*
  - *b(A)=1, b(B)=1*

CSMA/CD: A remainder

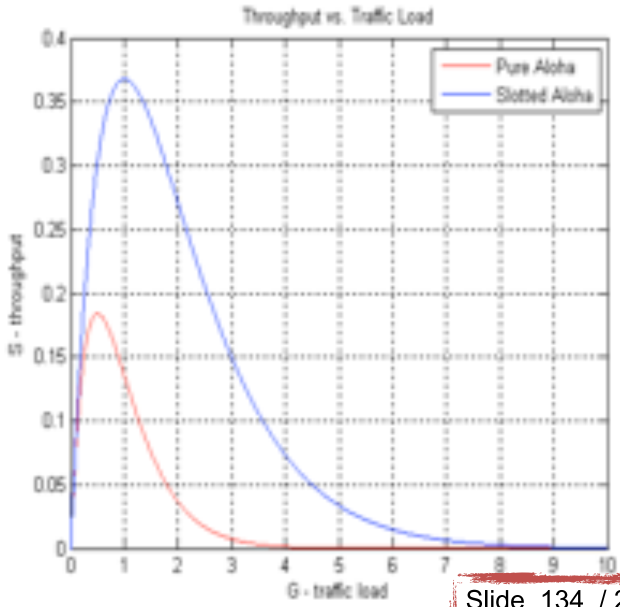
- How does it work?

Station A	ii	x	x				
Station B	ii	x					
Station C							

- On Ethernet, a small back-off can solve collisions quickly with high probability

CSMA/CA: The origins

- Wireless needs something different
- Aloha
  - AlohaNet: first wireless packet network (‘70s)
  - No carrier sense, just transmit as soon as a packet is available
  - No ACK message means back-off
- Slotted Aloha
  - Stations are synchronized
  - Transmissions can only start at the beginning of a slot



CSMA/CA: The origins

- Wireless needs something different
- Aloha is not efficient: too many collisions as the load increases
- The idea of using missing ACKs to schedule retransmissions is valid (and used in CSMA/CA)
- However, missing ACKs **are not collision detection**. They are just a mechanism for error control (Automatic Repeat reQuest (ARQ))

CSMA/CA: The origins

- Wireless needs something different
- CSMA/CA appears in the ‘80s, originally as a MAC protocol in the Apple LocalTalk network
- It becomes the basis of the IEEE 802.11 standard, aka Wi-Fi
- It is the most successful wireless communications technology up to date

CSMA/CA: The principles

- A station that wants to transmit
  - Listen the channel (carrier sense)
  - If the channel is idle, transmit
  - If the channel is busy, choose a random back-off
  - During back-off, time becomes slotted
  - If a slot is idle, decrement the back-off timer
  - If a slot is busy, freeze the back-off timer
  - When the time reaches 0, transmit
  - If no ACK message is received, double the contention window and restart the procedure

b= rand(0,CW-1)

CW_{min}= 32

CSMA/CA: The principles

- A station that wants to transmit
  - Listen the channel (carrier sense)
  - If the channel is idle, transmit
  - If the channel is busy, choose a random back-off
  - During back-off, time becomes slotted
  - If a slot is idle, decrement the back-off timer
  - If a slot is busy, freeze the back-off timer
  - When the time reaches 0, transmit
  - If no ACK message is received, double the contention window and restart the procedure

b= rand(0,CW-1)

CW_{min}= 32

CSMA/CA: The principles

- Why does it work?
- The relatively high value for CW is essential

Station A	i					
Station B	i					
Station C						

CSMA/CA: The principles

- Why does it work?
- The relatively high value for CW is essential

i= idle, t= transmission,
W= wait for ACK,
x= collision detected

Station A	i	t	t	t	t	t	w	w	x		
Station B	i	t	t	t	t	t	w	w	x		
Station C											

- On Ethernet, a collision was detected in maximum 5.12 µs
- On Wi-Fi, a missing ACK (not necessarily a collision) is detected after several ms

CSMA/CA: The principles

- Why does it work?
- The relatively high value for CW is essential

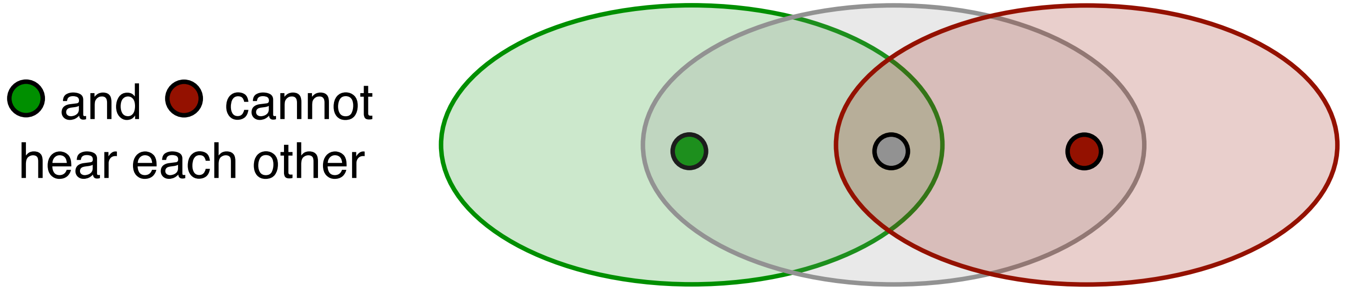
i= idle, t= transmission,
W= wait for ACK,
x= collision detected

Station A	i	t	t	t	t	t	w	w	x		
Station B	i	t	t	t	t	t	w	w	x		
Station C											

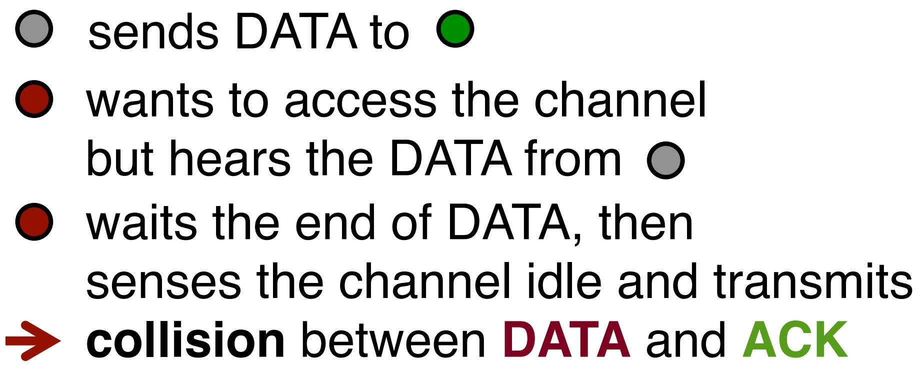
- Using CWmin, on CSMA/CD, we have a 50% probability for another collision
- Using CWmin, on CSMA/CA, it is ~3%

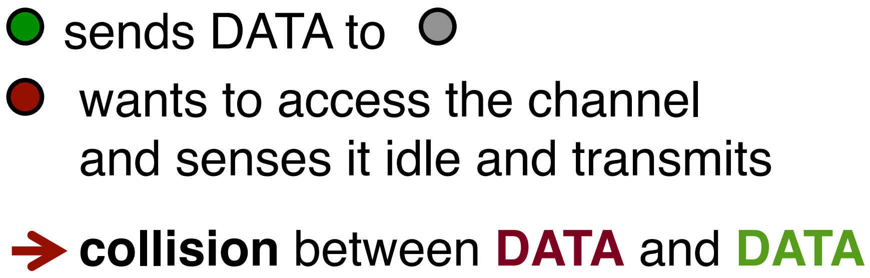
CSMA/CA: The problems

- Great, this solves everything!
- … not exactly: hidden terminals



Common scenarios





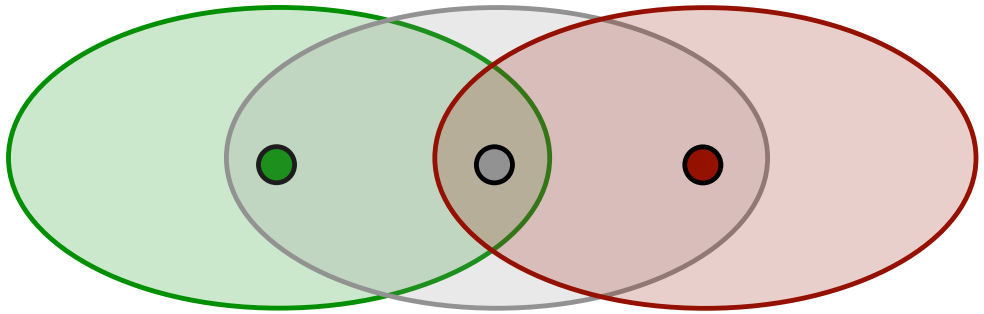
CSMA/CA: The problems

- The RTS/CTS handshake
  - The collision probability between hidden terminals increases with the size of the messages
  - The idea: use two short control messages to reserve the medium:
    - Request-to-Send (RTS)
    - Clear-to-Send (CTS)
  - RTS and CTS contain information about the duration of the following transmission (DATA + ACK)

CSMA/CA: The problems

- The RTS/CTS handshake

and cannot hear each other



- sends RTS to
- sends CTS to
- hears the CTS and considers the channel busy for the announced duration
- sends DATA to
- sends ACK to

The RTS/CTS handshake is also known as <u>virtual carrier sense</u>.

6bis. IEEE 802.11

IEEE 802.11: The beginnings

- In 1985, the US Federal Communications Commission (FCC) created the Industrial, Scientific and Medical band (ISM) for non-licensed applications (2.4 GHz)
- In 1990, the IEEE establishes the 802.11 committee
- The IEEE 802.11 standard was finalized in 1997 and became the do-facto standard for WLAN

IEEE 802.11: Evolutions

- Higher (theoretical) data rate: 11 Mbps (b), 54 Mbps (g), 100+ Mbps (n), 500+ Mbps (ac), 10 Gbps (ax)
- Use of different frequencies: 2.5Ghz, 5GHz (a), 60GHz (ad)
- Use of multiple antennas (n, ac, ax)
- Integrating quality of service (e)
- Dedicated environments: mesh (s), vehicular (p)
- Security enhancements (i, ax)

Wi-Fi Generations

Wi-Fi generations

Generation/IEEE Standard	Maximum Linkrate	Adopted	Frequency
Wi-Fi 6 (802.11ax)	600–9608 Mbit/s	2019	2.4/5 GHz 1–6 GHz ISM
Wi-Fi 5 (802.11ac)	433–6933 Mbit/s	2014	5 GHz
Wi-Fi 4 (802.11n)	72–600 Mbit/s	2009	2.4/5 GHz
Wi-Fi 3 (802.11g)	3–54 Mbit/s	2003	2.4 GHz
Wi-Fi 2 (802.11a)	1.5 to 54 Mbit/s	1999	5 GHz
Wi-Fi 1 (802.11b)	1 to 11 Mbit/s	1999	2.4 GHz
(Wi-Fi 1, Wi-Fi 2, Wi-Fi 3 are unbranded[41] but have unofficial assignments[42])			

- Wi-Fi 5 and Wi-Fi 6 are just different flavors of Wi-Fi

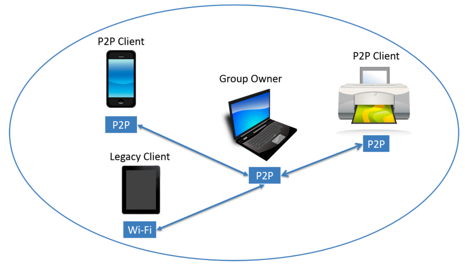
Wider RF bandwidth, more MIMO spatial streams (up to 8), downlink multi-user MIMO (up to 4 clients), high density modulation (256 QAM), etc.

Power-control methods to avoid interference with neighboring networks, orthogonal frequency-division multiple access (OFDMA), higher order 1024-QAM, and up-link direction added with the down-link of MIMO and MU-MIMO to further increase throughput, better security, lower energy consumption, etc.

Source: *WIkipédia, last viewed: September 2020*

IEEE 802.11: Wi-Fi Direct

- Standard for P2P wireless connections without a physical access point
  - At least one device compliant with Wi-Fi Direct
  - One device becomes a software AP
  - Clique topology
  - Local and global IP connectivities



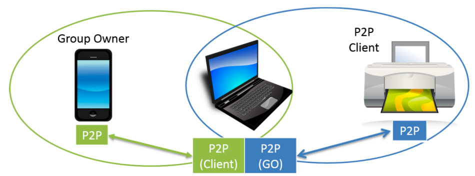


Fig. 2. Communication between two Wi-Fi Direct groups.

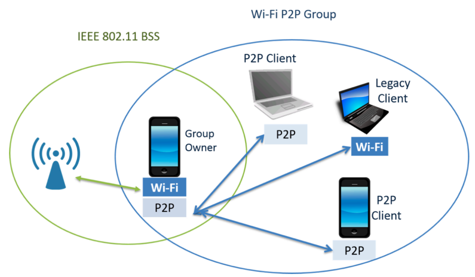
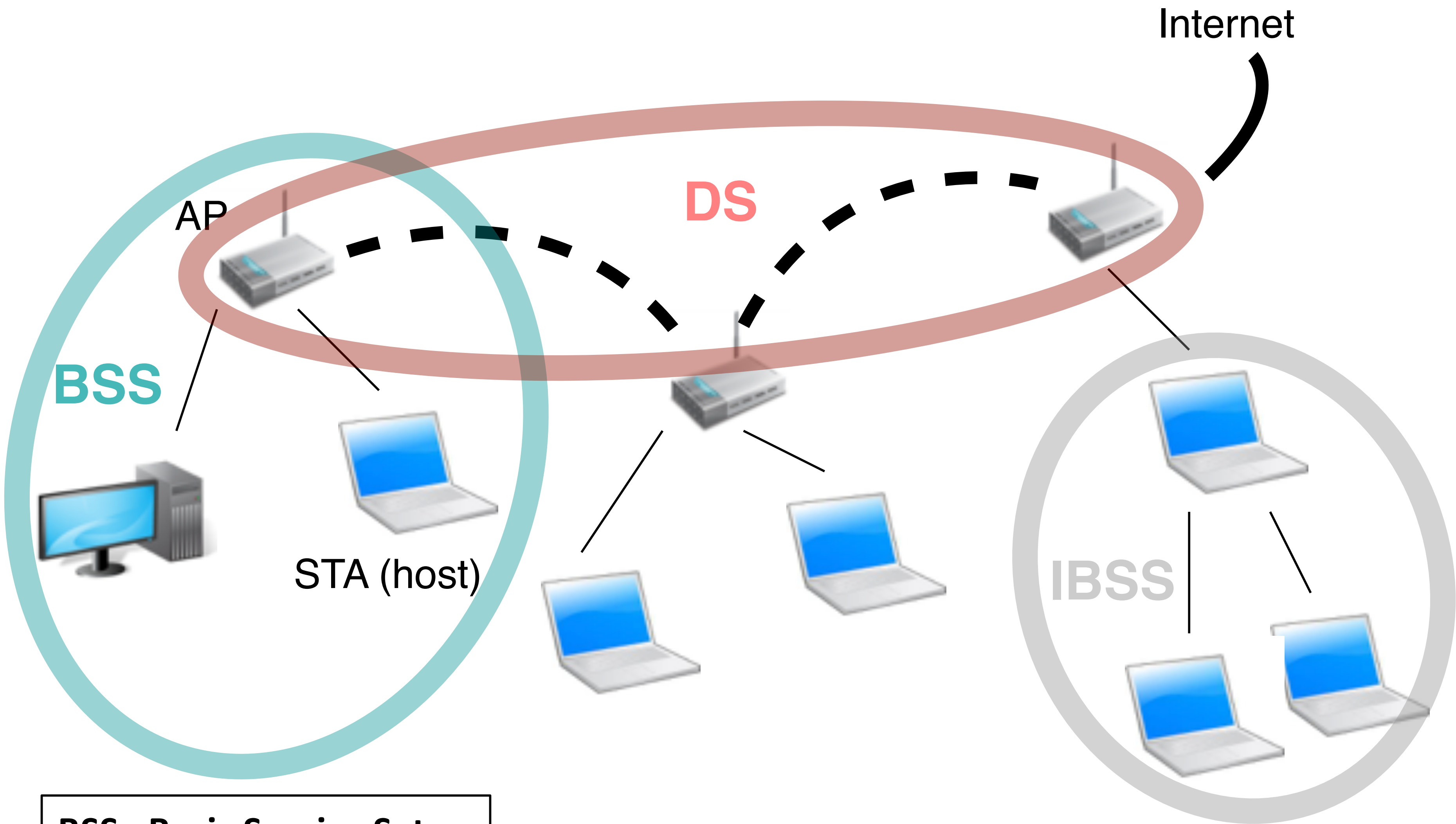


Fig. 3. Communication between a Wi-Fi Direct group and a Wi-Fi BSS.

Source: *Content-centric Routing in Wi-Fi Direct Multi-group Networks*, Casetti & al., arXiv1412.0880v1

IEEE 802.11: General architecture



BSS= Basic Service Set
IBSS= Independent BSS
DS= Distribution System

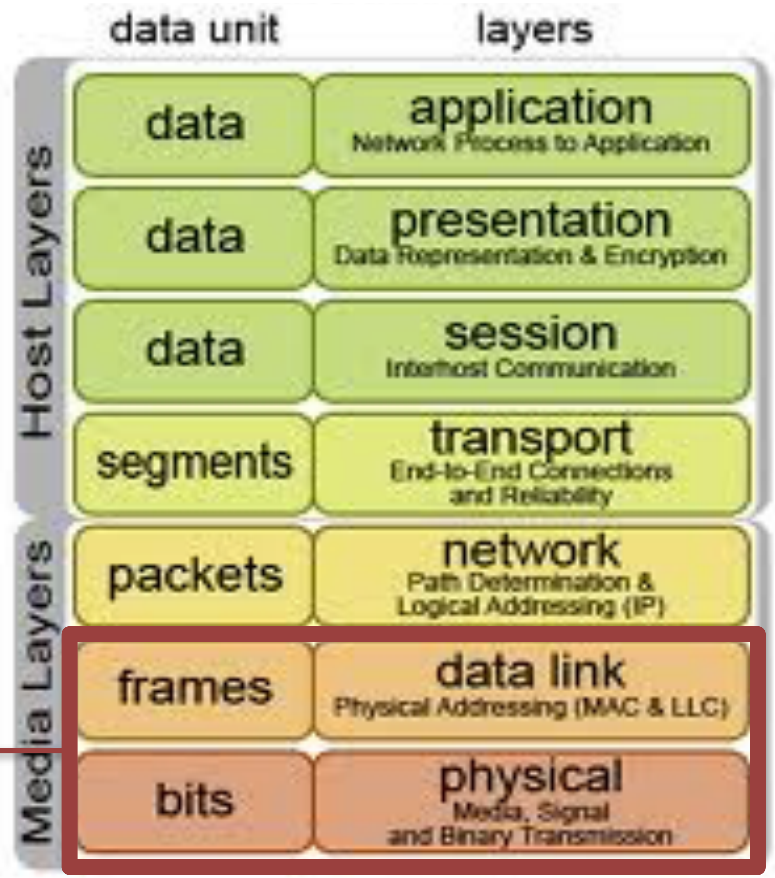
IEEE 802.11: BSS Association

- **Scanning** – STA looks for (chooses) an AP nearby
  - Passive: just wait for the periodic AP beacon
  - Active: probe APs for beacons
- **Authentication** – STA proves to have access
  - Open: skip this phase
  - Secure: challenge by the AP, the STA needs to have a shared key to respond correctly
- **Association** – STA enters the BSS
  - STA → AP: association request, followed by AP → STA: association response
  - AP informs old AP via the DS in case of roaming

IEEE 802.11: Protocol stack

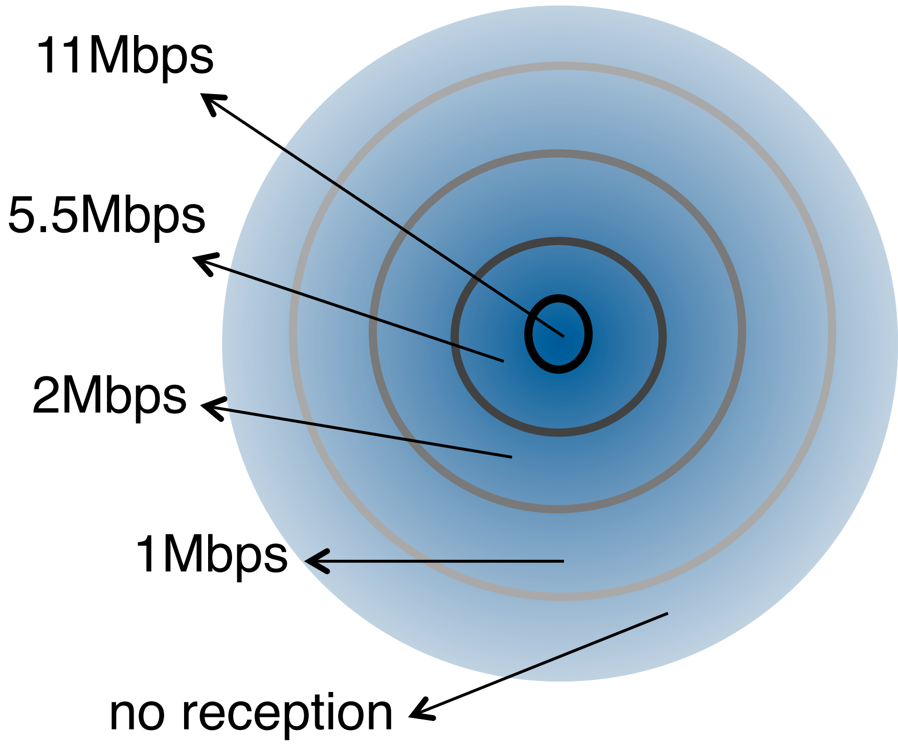
- 802.11 is not only about the MAC

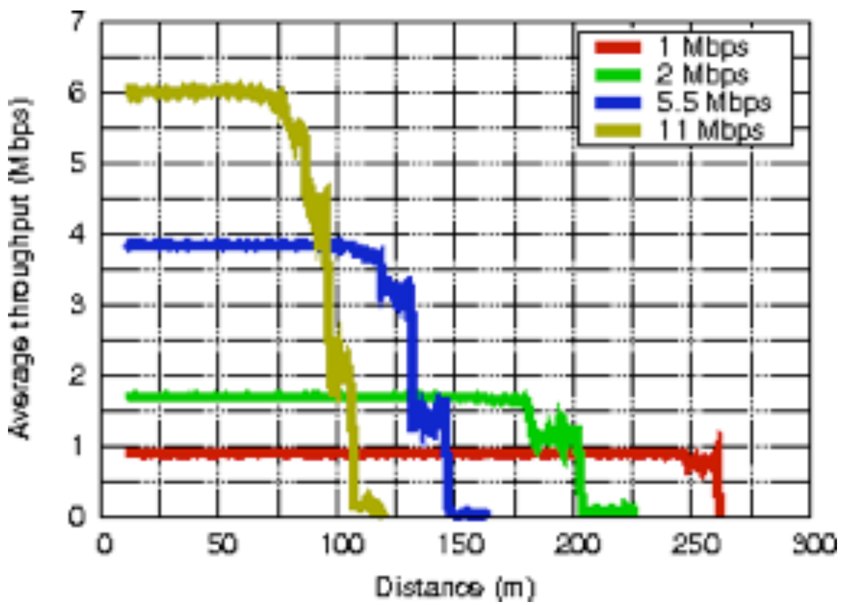
- IEEE 802.11 defines the protocols for the PHY and MAC



802.11: PHY basics

- Modulation gives us the data rate
  - To decode a more complex modulation, we need a higher signal strength
  - Trade-off between data rate and transmission range





[ns-2 simulation, 802.11b]

802.11: PHY basics

- Modulation and coding scheme
  - Dynamic adaptation of the modulation and the coding scheme according to the channel condition
  - Dynamic adaptation of the data rate

- MCS for 802.11n & ac
  - See: http://mcsindex.com/

MCS	Modulation	Coding	40 MHz			
			Data Rate		Min. SNR	Min. RSSI
			800 ns	400 ns		
0	BPSK	1/2	13.5	15	5	-79
1	QPSK	1/2	27	30	8	-76
2	QPSK	3/4	40.5	45	12	-74
3	16-QAM	1/2	54	60	14	-71
4	16-QAM	3/4	81	90	18	-67
5	64-QAM	2/3	108	120	21	-63
6	64-QAM	3/4	121.5	135	23	-62
7	64-QAM	5/6	135	150	28	-61
8	256-QAM	3/4	162	180	32	-56
9	256-QAM	5/6	180	200	34	-54

802.11: PHY basics

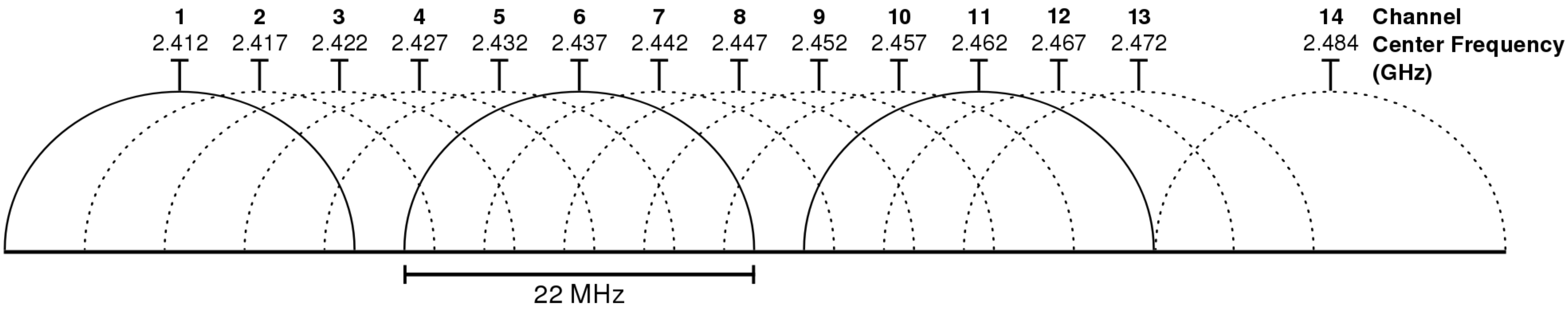
Full MCS Table (HT/VHT/HE) | MCS Table 3SS (HT/VHT/HE) | MCS Table HE | MCS Table HE (OFDM) | MCS Table HE (OFDMA) | The Math Behind it | Credit

MCS Index			Spatial Stream	Modulation	Coding	OFDM (Prior 11ax) 20MHz		40MHz		80MHz		160MHz		OFDM (802.11ax) 20MHz			40MHz			80MHz			160MHz		
HT	VHT	HE				0.8µs GI	0.4µs GI	0.8µs GI	0.4µs GI	0.8µs GI	0.4µs GI	0.8µs GI	0.4µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI	0.8µs GI	1.6µs GI	3.2µs GI
0	0	0	1	BPSK	1/2	6.5	7.2	13.5	15	29.3	32.5	58.5	65	8.6	8.1	7.3	17.2	16.3	14.6	36	34	30.6	72.1	68.1	61.3
1	1	1	1	QPSK	1/2	13	14.4	27	30	58.5	65	117	130	17.2	16.3	14.6	34.4	32.5	29.3	72.1	68.1	61.3	144.1	136.1	122.5
2	2	2	1	QPSK	3/4	19.5	21.7	40.5	45	87.8	97.5	175.5	195	25.8	24.4	21.9	51.6	48.8	43.9	108.1	102.1	91.9	216.2	204.2	183.8
3	3	3	1	16-QAM	1/2	26	28.9	54	60	117	130	234	260	34.4	32.5	29.3	68.8	65	58.5	144.1	136.1	122.5	288.2	272.2	245
4	4	4	1	16-QAM	3/4	39	43.3	81	90	175.5	195	351	390	51.6	48.8	43.9	103.2	97.5	87.8	216.2	204.2	183.8	432.4	408.3	367.5
5	5	5	1	64-QAM	2/3	52	57.8	108	120	234	260	468	520	68.8	65	58.5	137.6	130	117	288.2	272.2	245	576.5	544.4	490
6	6	6	1	64-QAM	3/4	58.5	65	121.5	135	263.3	292.5	526.5	585	77.4	73.1	65.8	154.9	146.3	131.6	324.3	306.3	275.6	648.5	612.5	551.3
7	7	7	1	64-QAM	5/6	65	72.2	135	150	292.5	325	585	650	86	81.3	73.1	172.1	162.5	146.3	360.3	340.3	306.3	720.6	680.6	612.5
	8	8	1	256-QAM	3/4	78	86.7	162	180	351	390	702	780	103.2	97.5	87.8	206.5	195	175.5	432.4	408.3	367.5	864.7	816.7	735
	9	9	1	256-QAM	5/6	N/A	N/A	180	200	390	433.3	780	866.7	114.7	108.3	97.5	229.4	216.7	195	480.4	453.7	408.3	960.8	907.4	816.7
		10	1	1024-QAM	3/4									129	121.9	109.7	258.1	243.8	219.4	540.4	510.4	459.4	1080.9	1020.8	918.8
		11	1	1024-QAM	5/6									143.4	135.4	121.9	286.8	270.8	243.8	600.5	567.1	510.4	1201	1134.3	1020.8
8	0	0	2	BPSK	1/2	13	14.4	27	30	58.5	65	117	130	17.2	16.3	14.6	34.4	32.5	29.3	72.1	68.1	61.3	144.1	136.1	122.5
9	1	1	2	QPSK	1/2	26	28.9	54	60	117	130	234	260	34.4	32.5	29.3	68.8	65	58.5	144.1	136.1	122.5	288.2	272.2	245
10	2	2	2	QPSK	3/4	39	43.3	81	90	175.5	195	351	390	51.6	48.8	43.9	103.2	97.5	87.8	216.2	204.2	183.8	432.4	408.3	367.5
11	3	3	2	16-QAM	1/2	52	57.8	108	120	234	260	468	520	68.8	65	58.5	137.6	130	117	288.2	272.2	245	576.5	544.4	490
12	4	4	2	16-QAM	3/4	78	86.7	162	180	351	390	702	780	103.2	97.5	87.8	206.5	195	175.5	432.4	408.3	367.5	864.7	816.7	735
13	5	5	2	64-QAM	2/3	104	115.6	216	240	468	520	936	1040	137.6	130	117	275.3	260	234	576.5	544.4	490	1152.9	1088.9	980
14	6	6	2	64-QAM	3/4	117	130	243	270	526.5	585	1053	1170	154.9	146.3	131.6	309.7	292.5	263.3	648.5	612.5	551.3	1297.1	1225	1102.5
15	7	7	2	64-QAM	5/6	130	144.4	270	300	585	650	1170	1300	172.1	162.5	146.3	344.1	325	292.5	720.6	680.6	612.5	1441.2	1361.1	1225
	8	8	2	256-QAM	3/4	156	173.3	324	360	702	780	1404	1560	206.5	195	175.5	412.9	390	351	864.7	816.7	735	1729.4	1633.3	1470
	9	9	2	256-QAM	5/6	N/A	N/A	360	400	780	866.7	1560	1733.3	229.4	216.7	195	458.8	433.3	390	960.8	907.4	816.7	1921.6	1814.8	1633.3
		10	2	1024-QAM	3/4									258.1	243.8	219.4	516.2	487.5	438.8	1080.9	1020.8	918.8	2161.8	2041.7	1837.5
		11	2	1024-QAM	5/6									286.8	270.8	243.8	573.5	541.7	487.5	1201	1134.3	1020.8	2402	2268.5	2041.7
16	0	0	3	BPSK	1/2	19.5	21.7	40.5	45	87.8	97.5	175.5	195	25.8	24.4	21.9	51.6	48.8	43.9	108.1	102.1	91.9	216.2	204.2	183.8
17	1	1	3	QPSK	1/2	39	43.3	81	90	175.5	195	351	390	51.6	48.8	43.9	103.2	97.5	87.8	216.2	204.2	183.8	432.4	408.3	367.5
18	2	2	3	QPSK	3/4	58.5	65	121.5	135	263.3	292.5	526.5	585	77.4	73.1	65.8	154.9	146.3	131.6	324.3	306.3	275.6	648.5	612.5	551.3
19	3	3	3	16-QAM	1/2	78	86.7	162	180	351	390	702	780	103.2	97.5	87.8	206.5	195	175.5	432.4	408.3	367.5	864.7	816.7	735
20	4	4	3	16-QAM	3/4	117	130	243	270	526.5	585	1053	1170	154.9	146.3	131.6	309.7	292.5	263.3	648.5	612.5	551.3	1297.1	1225	1102.5
21	5	5	3	64-QAM	2/3	156	173.3	324	360	702	780	1404	1560	206.5	195	175.5	412.9	390	351	864.7	816.7	735	1729.4	1633.3	1470
22	6	6	3	64-QAM	3/4	175.5	195	364.5	405	N/A	N/A	1579.5	1755	232.3	219.4	197.4	464.6	438.8	394.9	972.8	918.8	826.9	1945.6	1837.5	1653.8
23	7	7	3	64-QAM	5/6	195	216.7	405	450	877.5	975	1755	1950	258.1	243.8	219.4	516.2	487.5	438.8	1080.9	1020.8	918.8	2161.8	2041.7	1837.5
	8	8	3	256-QAM	3/4	234	260	486	540	1053	1170	2106	2340	309.7	292.5	263.3	619.4	585	526.5	1297.1	1225	1102.5	2594.1	2450	2205
	9	9	3	256-QAM	5/6	260	288.9	540	600	1170	1300	N/A	N/A	344.1	325	292.5	688.2	650	585	1441.2	1361.1	1225	2882.4	2722.2	2450
		10	3	1024-QAM	3/4									387.1	365.6	329.1	774.3	731.3	658.1	1621.3	1531.3	1378.1	3242.6	3062.5	2756.3
		11	3	1024-QAM	5/6									430.1	406.3	365.6	860.3	812.5	731.3	1801.5	1701.4	1531.3	3602.9	3402.8	3062.5
24	0	0	4	BPSK	1/2	26	28.9	54	60	117	130	234	260	34.4	32.5	29.3	68.8	65	58.5	144.1	136.1	122.5	288.2	272.2	245
25	1	1	4	QPSK	1/2	52	57.8	108	120	234	260	468	520	68.8	65	58.5	137.6	130	117	288.2	272.2	245	576.5	544.4	490
26	2	2	4	QPSK	3/4	78	86.7	162	180	351	390	702	780	103.2	97.5	87.8	206.5	195	175.5	432.4	408.3	367.5	864.7	816.7	735
27	3	3	4	16-QAM	1/2	104	115.6	216	240	468	520	936	1040	137.6	130	117	275.3	260	234	576.5	544.4	490	1152.9	1088.9	980

Source: http://mcsindex.com/

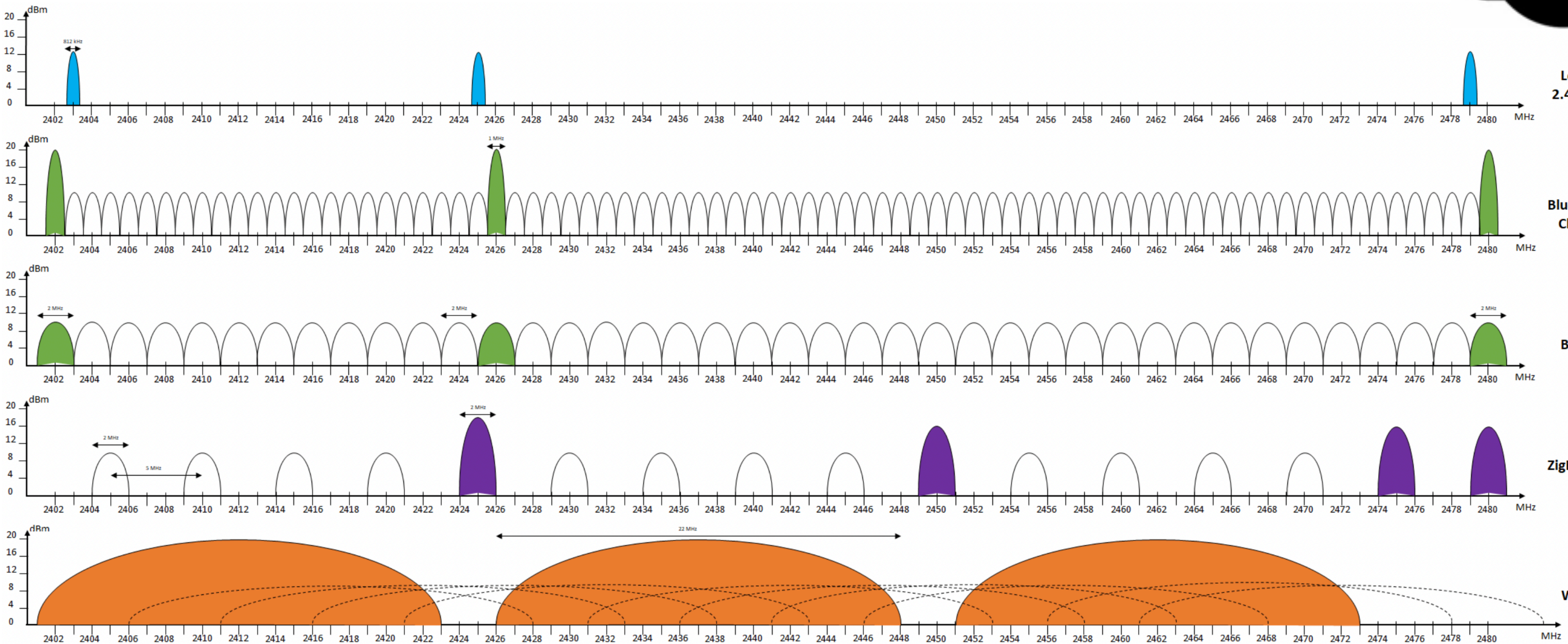
802.11: Radio spectrum

- Several channels… but not totally independent



802.11: Radio spectrum

- Several channels… in a very crowded environment



Courtesy by Gwendoline Hochet-Derévianckine

IEEE 802.11: Outdoor/indoor deployment

- French regulation provided by ARCEP
- Limited power transmission (2.4 GHz):
  - Indoor: 100mW
  - Outdoor: 100mW
- Limited power transmission (5 GHz):
  - Outdoor and indoor: 5470-5725 MHz: 500mW – 1W
  - Indoor only
    - 5150-5250 MHz: 200mW
    - 5250-5350 MHz: 100 mW - 200mW

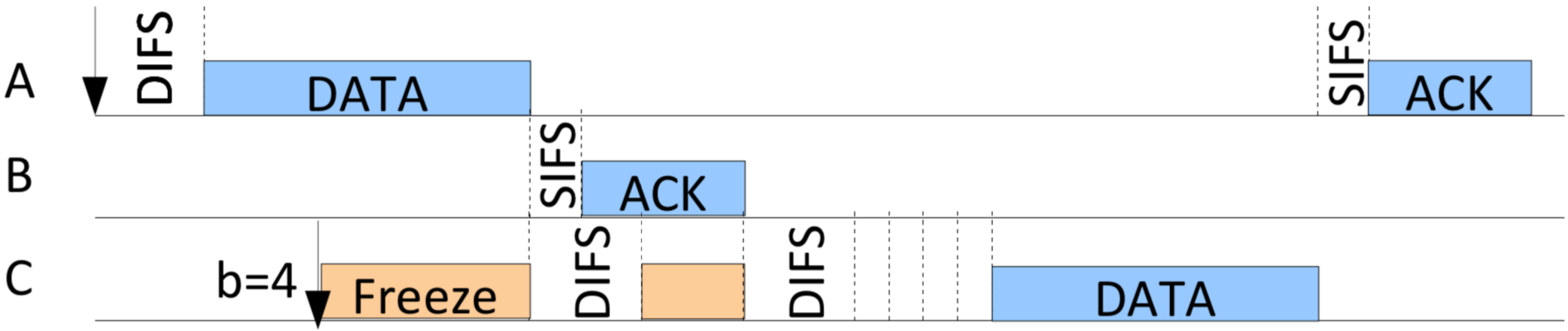
IEEE 802.11: DCF

- CSMA/CA implementation: Distributed Coordination Function
- Four types of InterFrame Space (IFS)
  - Short InterFrame Space (SIFS): used to separate transmissions belonging to a same dialogue (before a CTS or an ACK)
  - Point coordination InterFrame Space (PIFS): for data in the contention-free period (see later), to preempt any contention-based traffic
  - Distributed InterFrame Space (DIFS): standard IFS, used to separate transmissions of different dialogue
  - Extended InterFrame Space (EIFS): used by a station that received an erroneous frame

SIFS < PIFS < DIFS < EIFS

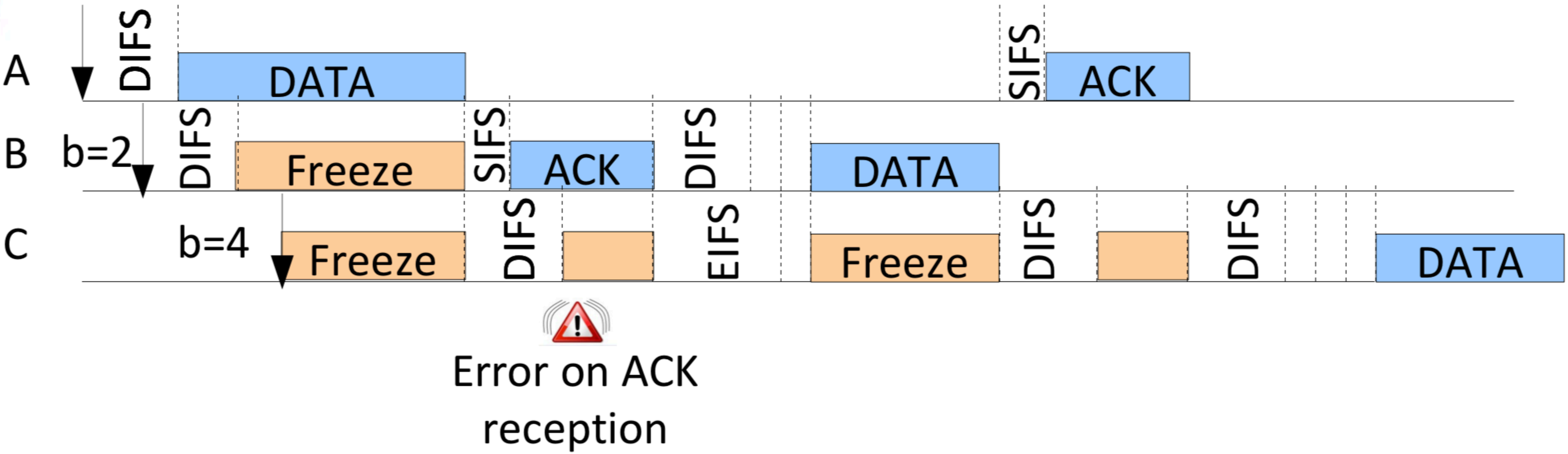
802.11: DCF

- Scenarios



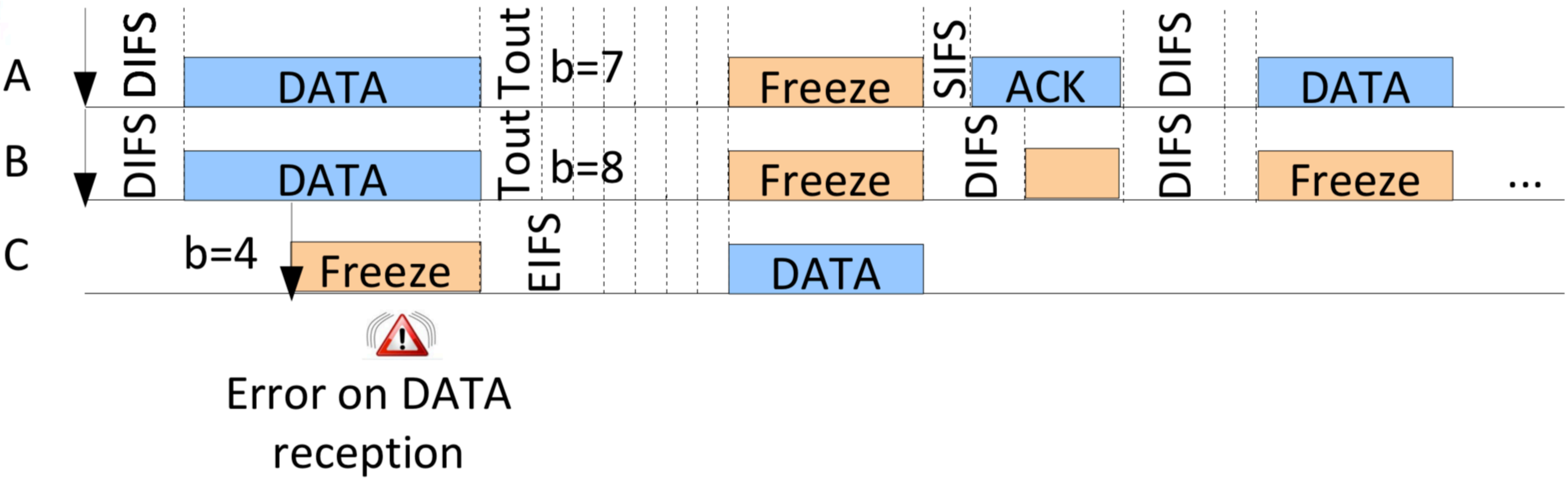
802.11: DCF

- Scenarios



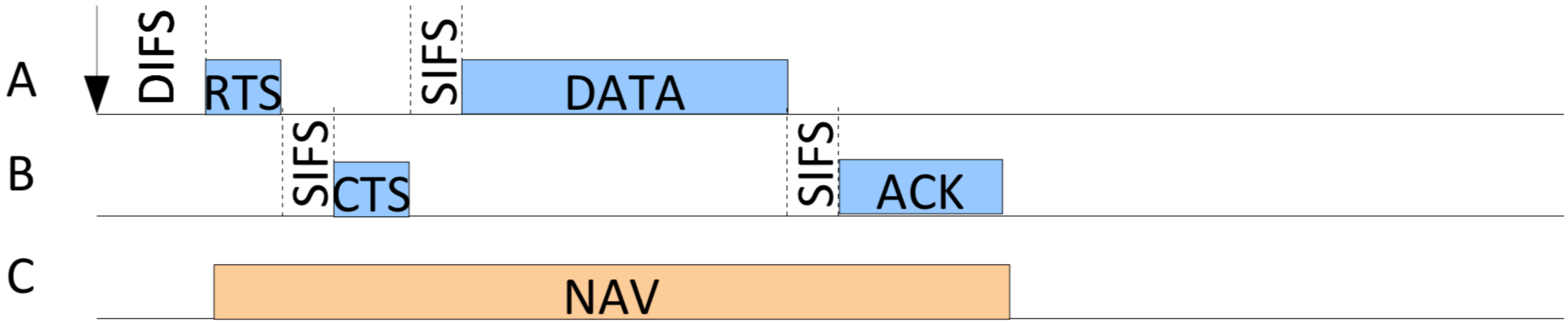
802.11: DCF

- Scenarios



802.11: DCF

- Scenarios



- NAV = Network Allocation Vector = Virtual Carrier Sense
- The RTS/CTS handshake is optional in IEEE 802.11

IEEE 802.11: DCF

- Broadcast messages
  - Broadcast = one transmitter, multiple receivers
  - If all receivers transmit CTS or ACK after SIFS, collisions are unavoidable
  - Broadcast messages are transmitted only once using the minimum CW, and their transmission is unreliable (no ACK)

IEEE 802.11: DCF

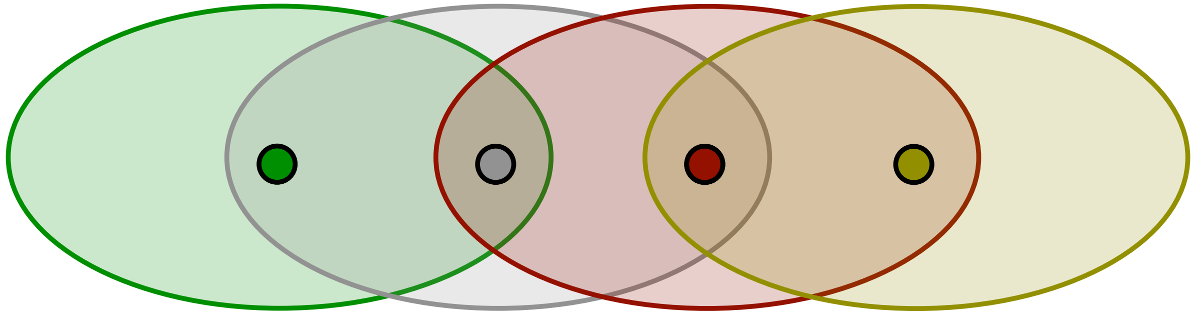
- Why do we still get collisions with collision avoidance?
  - CA mitigates collisions, but it does not eliminate them
  - The collision probability depends on
    - *The number of contending stations*
    - *The size of the contention window*
  - A higher CW reduces the collision probability, but increases the delay introduced by back-off

IEEE 802.11: DCF

- But the DCF is too:
  - Only a MAC layer solution among others (cellular networks use CDMA or OFDMA)
  - A mediocre protocol when mobility is considered
  - An unusable technology under high node density

IEEE 802.11: DCF

- An example: multi-hop networks
- Exposed terminal: a tremendous reduction in throughput



sends RTS to

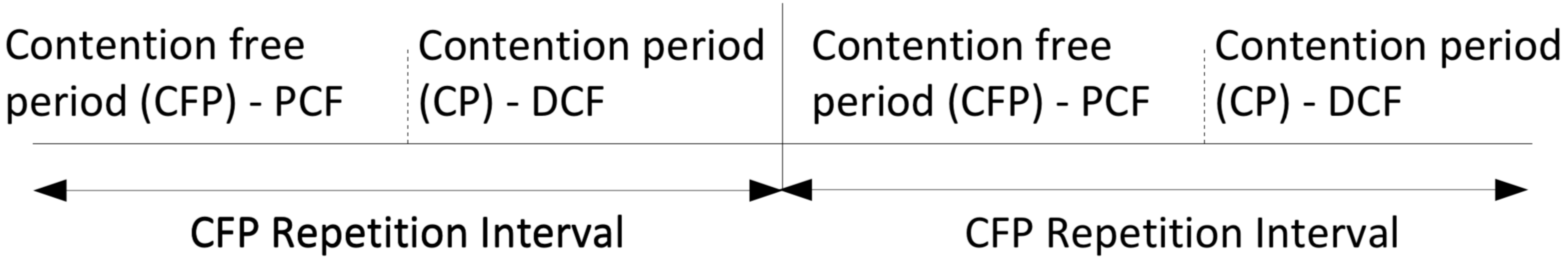
sends CTS to

receives RTS from and refrain from transmitting to

...but transmission from to would not cause a collision!

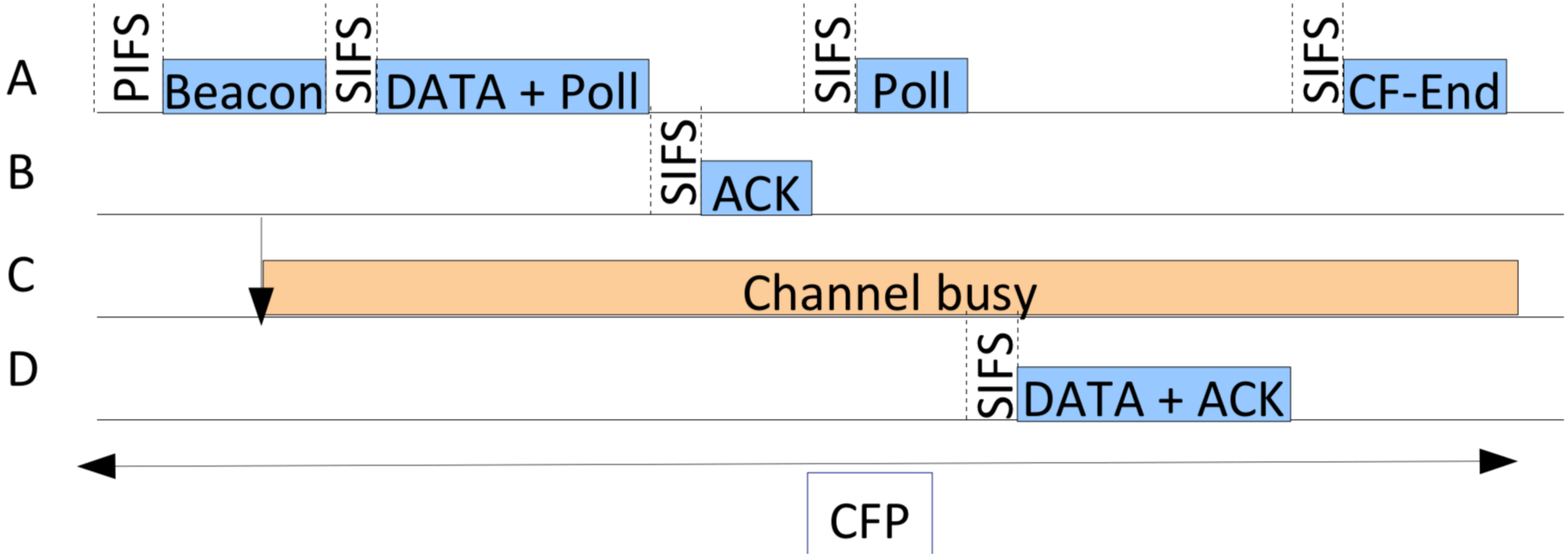
IEEE 802.11: PCF

- There is more than DCF in IEEE 802.11
  - Point Coordination Function (PCF)
  - Contention-Free frame transfer protocol
  - Based on polling made by the access point
  - Coexists with DCF



IEEE 802.11: PCF

- How does it work?



IEEE 802.11: Frame format

- The 802.11 frame

Preamble	PLCP	MAC Data	CRC

- The MAC data

Frame Control	Duration	Address1	Address2	Address3	Sequence Control	Address4	Frame Body	CRC

IEEE 802.11: Frame format

- Why do we need 4 adresses?
  - The Frame Control field contains (among others) two bits named To DS and From DS
  - The value of To DS and From DS gives the meaning of the 4 addresses

To DS	From DS	Address1	Address2	Address3	Address4
0	0	Destination	Source	BSSID	N/A
0	1	Destination	BSSID	Source	N/A
1	0	BSSID	Source	Destination	N/A
1	1	Receiver	Transmitter	Destination	Source

IEEE 802.11: Performance

- Performance anomaly
  - N hosts compete for the radio channel
  - N-1 hosts use the high transmission
  - 1 host transmits at a degraded rate
- Conclusion: all hosts the same throughput

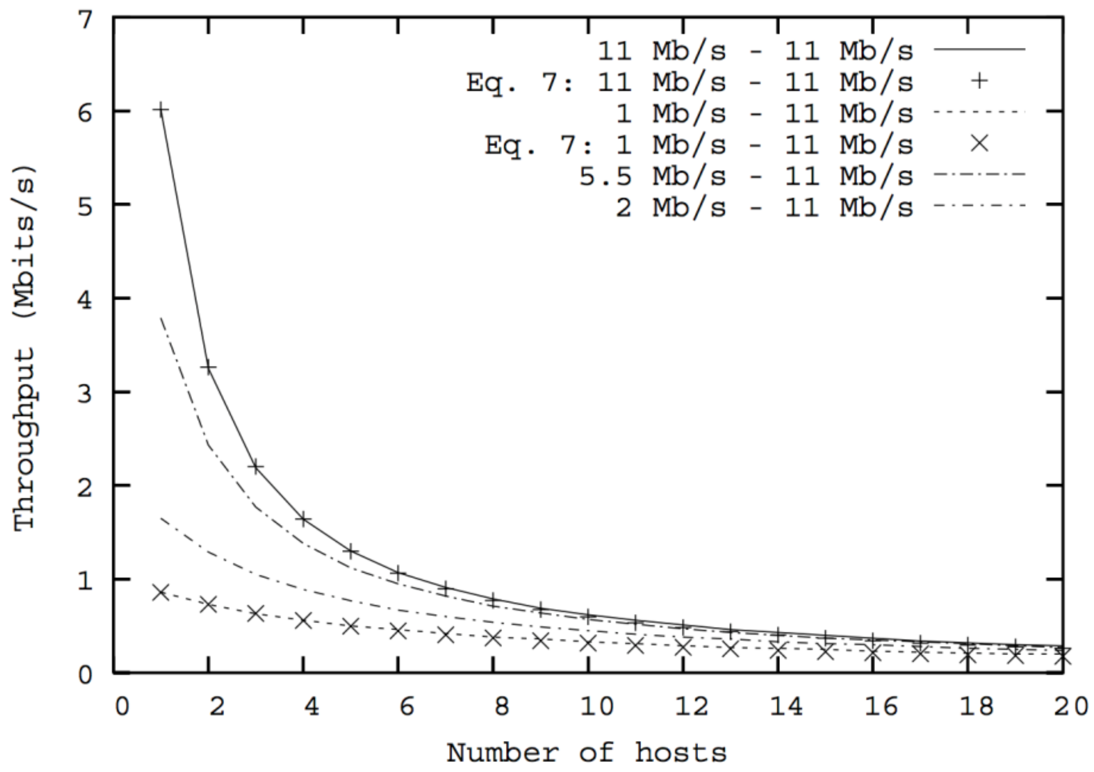


Fig. 3. Throughput experienced by a 802.11b host when all hosts except one transmit at 11Mb/s

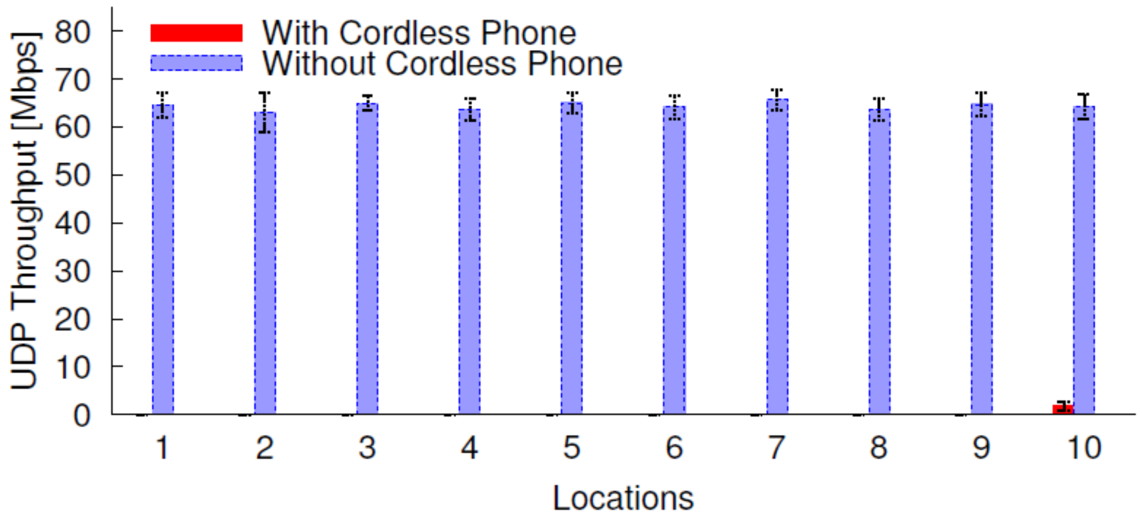
M. Heusse, F. Rousseau, G. Berger-Sabbatel, A. Duda, Performance Anomaly of 802.11b, Infocom 2003

IEEE 802.11: Performance

- Wi-Fi functions on the 2.4GHz (*Industrial, Scientific and Medical* (ISM) band)
- Available worldwide without license
- But also used by:
  - dielectric heating, microwave ovens, physical therapy machines, cordless phones, Bluetooth, Near Field Communication, wireless sensor networks, etc.

IEEE 802.11: Performance

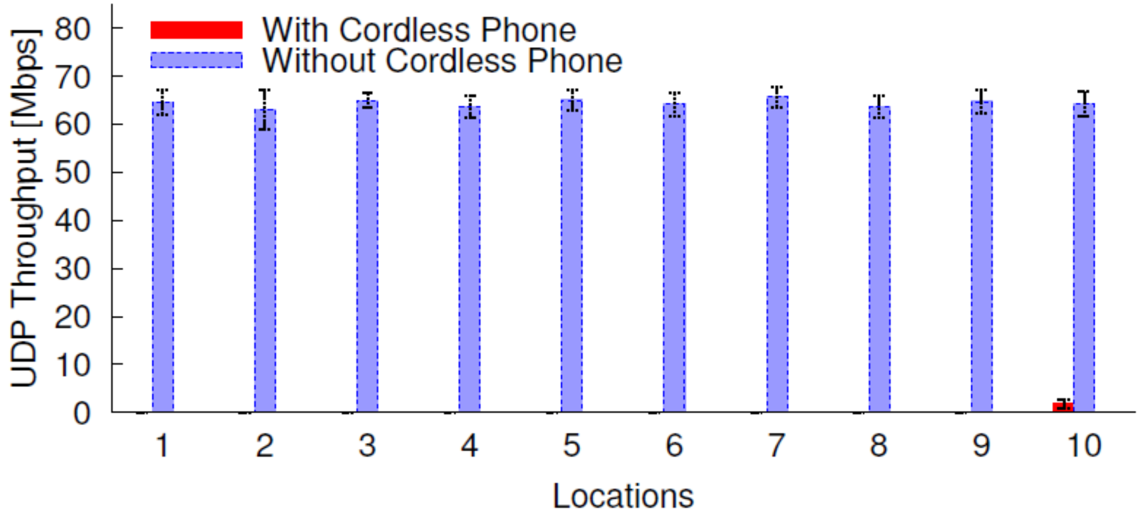
- The RF Smog
  - Impact of cordless telephone on 802.11n



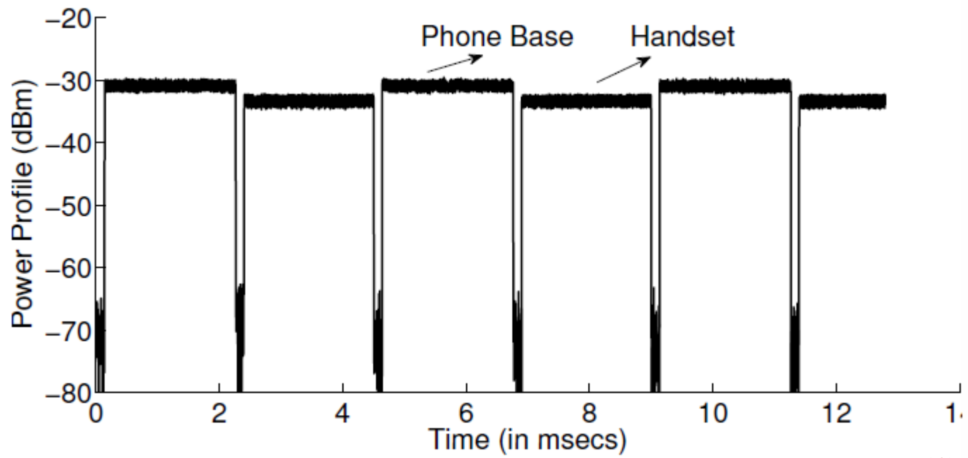
Close to 0 throughput for IEEE 802.11 when a cordless phone is active.

IEEE 802.11: Performance

- The RF Smog
  - Impact of cordless telephone on 802.11n



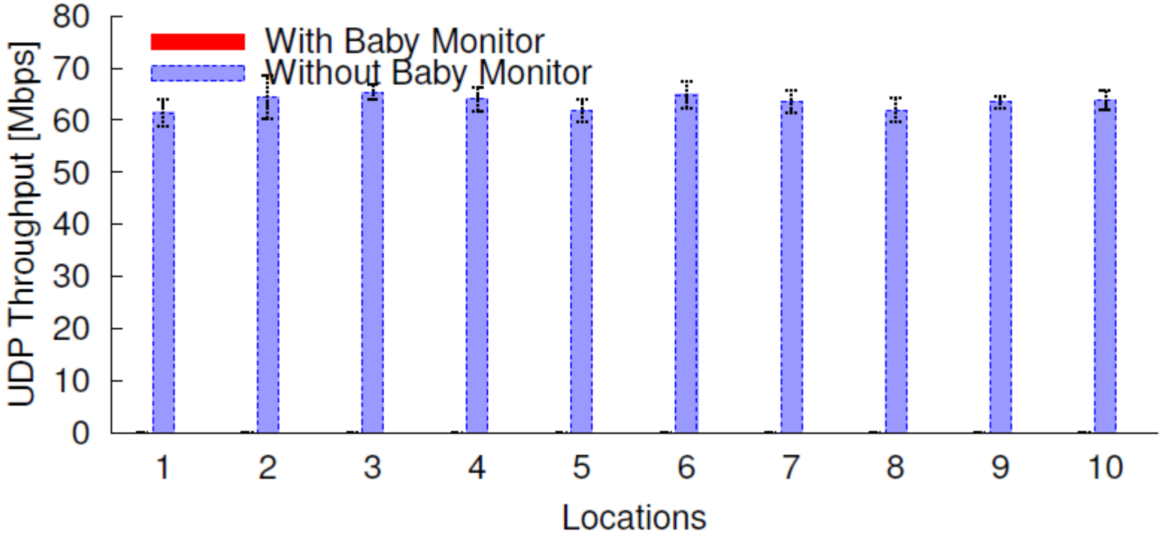
Close to 0 throughput for IEEE 802.11 when a cordless phone is active.



The energy detection mechanism of the carrier sense function blocks any transmission.

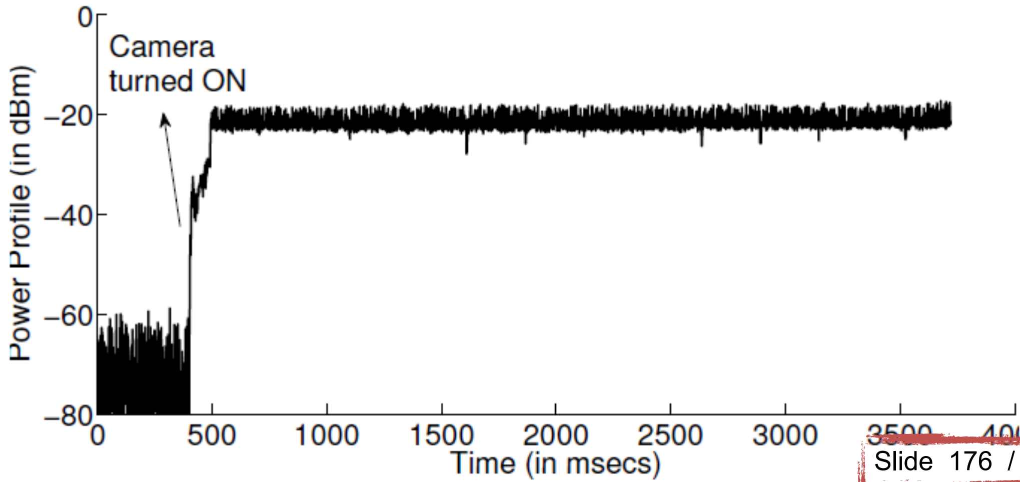
IEEE 802.11: Performance

- The RF Smog
  - Baby monitor



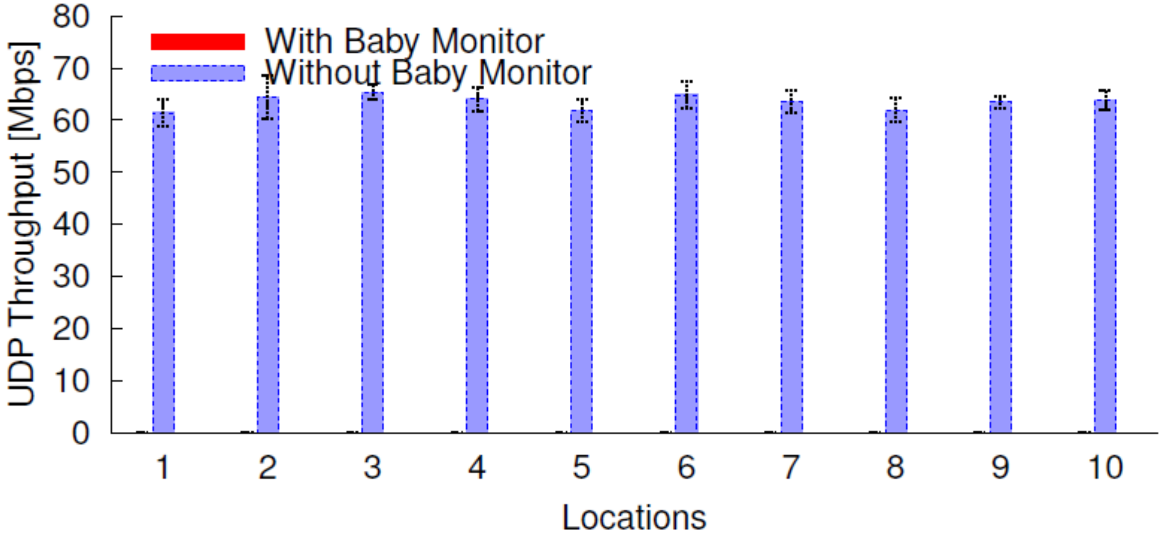
0 throughput for IEEE 802.11 when a baby monitor is active.

The camera transmits continuously at a relatively high power: carrier sense blocks any transmission.



IEEE 802.11: Performance

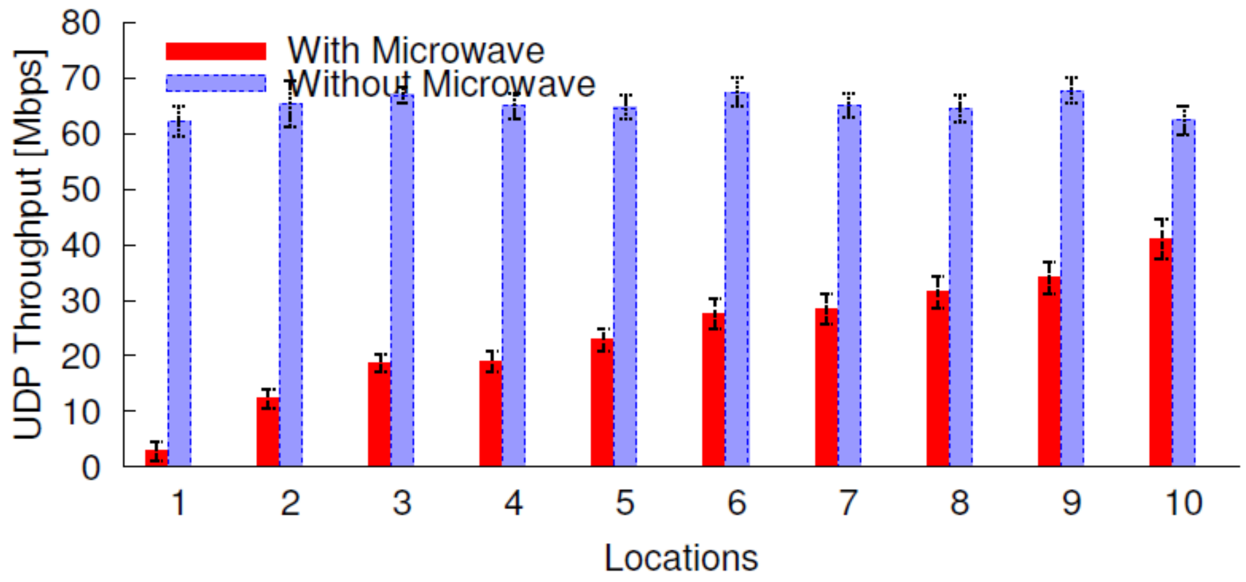
- The RF Smog
  - Baby monitor



0 throughput for IEEE 802.11 when a baby monitor is active.

IEEE 802.11: Performance

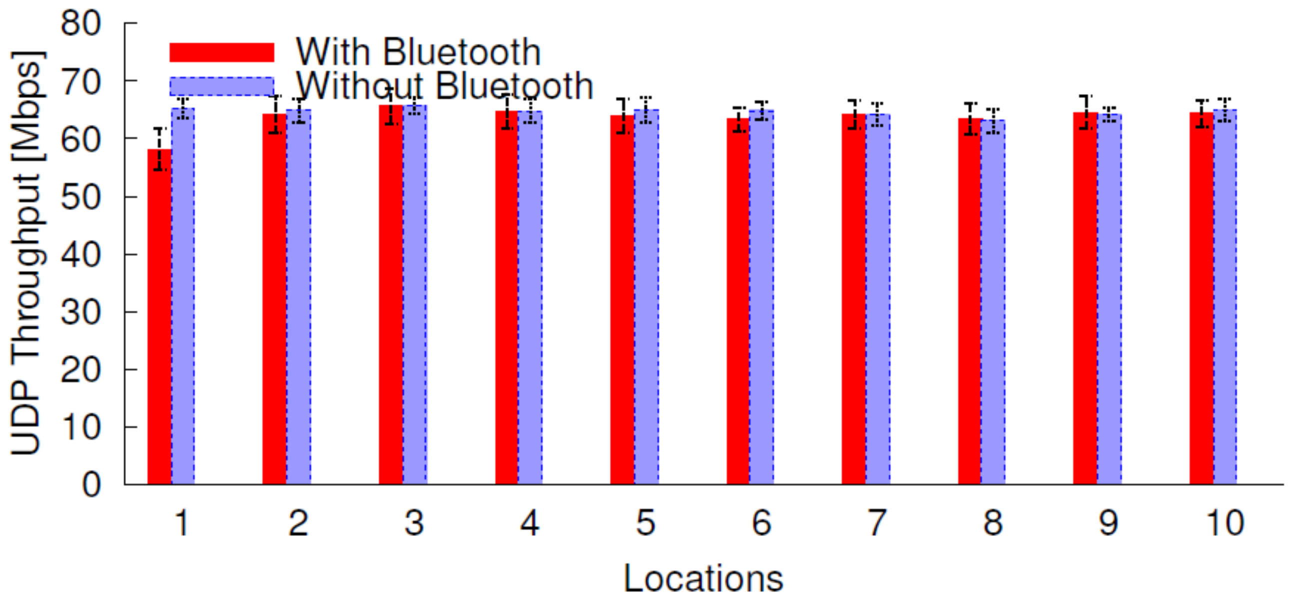
- The RF Smog
  - Microwave open…



Drastic reduction of the throughput…

IEEE 802.11: Performance

- The RF Smog
  - Bluetooth device



Bluetooth only has a significant impact when the interfering device is very close (location 1).

CSMA/CA and IEEE 802.11

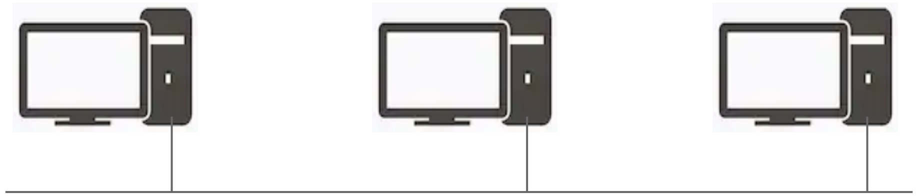
- Bibliography

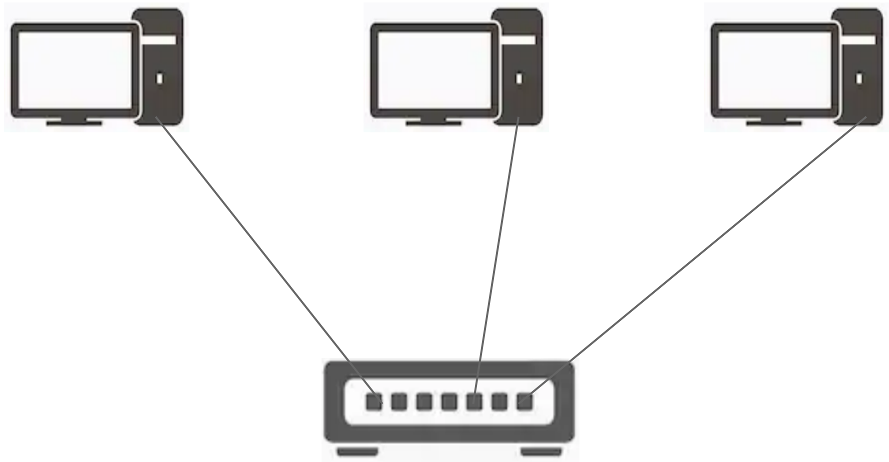
  - IEEE 802.11 Working Group, "802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE, 2007
  - G. Bianchi, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function", IEEE Journal on Selected Areas in Communication, March 2000
  - S. Xu, T. Saadawi, "Does the IEEE 802.11 MAC protocol work well in multi-hop wireless ad hoc networks?", IEEE Communications Magazine, June 2001
  - A. Colvin, "CSMA with Collision Avoidance", Computer Communications, October 1983

7. Network hardware (L1 and L2 only)

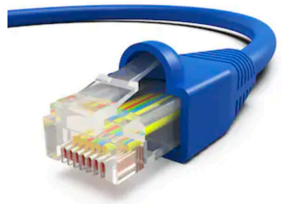
Network hardware for LAN (L1 & L2)

- Shared Ethernet *vs* Switched Ethernet



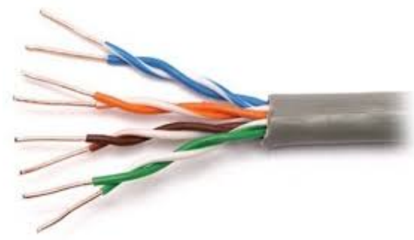


Ethernet cable and twisted pair



- Most widely used medium for telecommunication
- Copper wires that are twisted into pairs

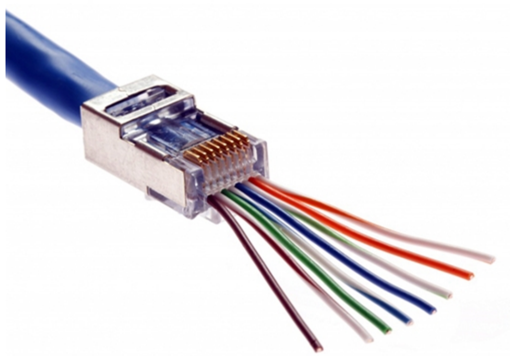
- Twister pairs reduce electromagnetic radiation
- Ethernet/802.3: 4 pairs of copper cabling

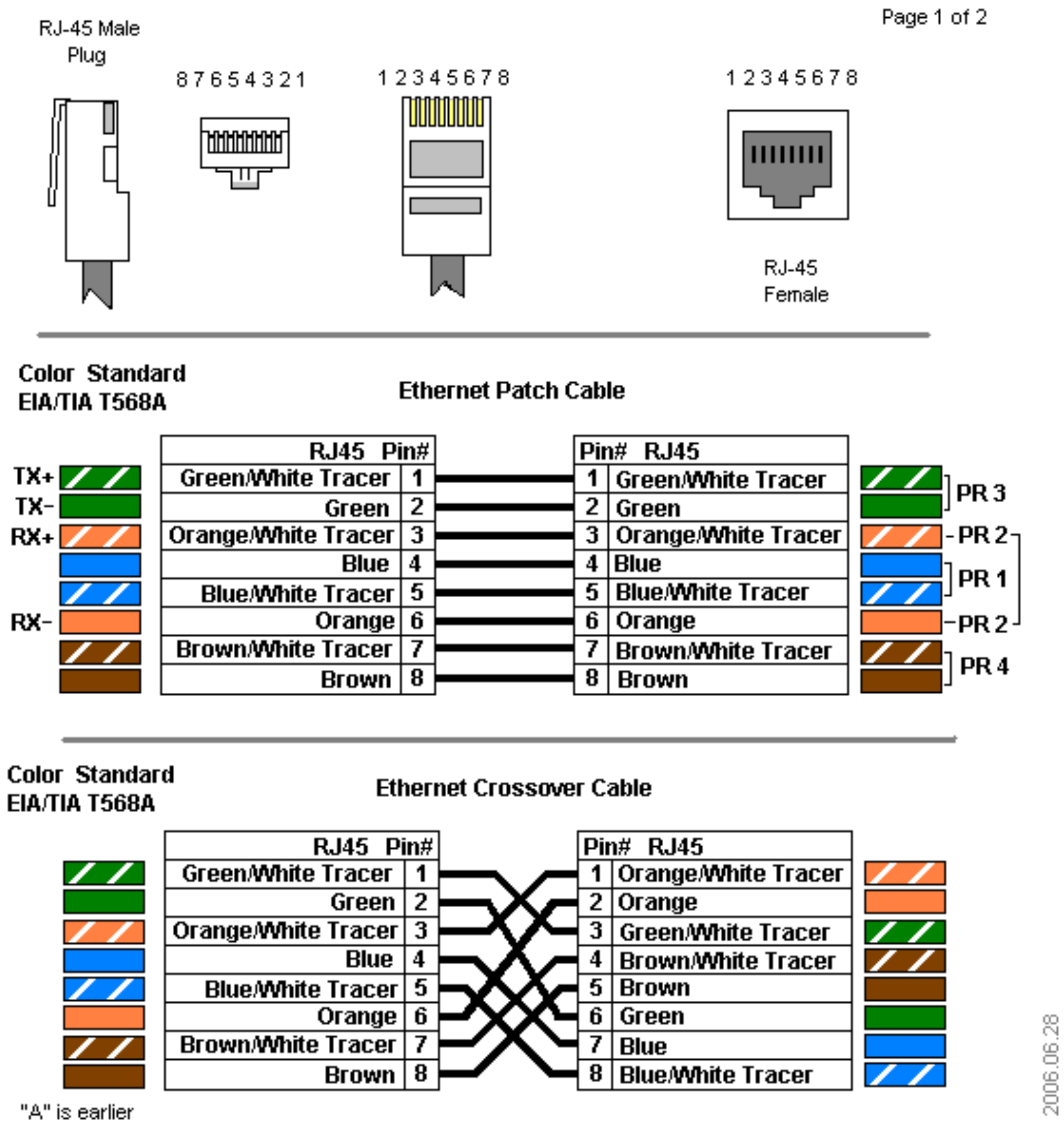


- Comes in 2 forms: unshielded twisted pair (UTP) and shielded twisted-pair (STP)

- Transmission speed ranges from 2 million bits per second to 10 billion bits per second

Ethernet (patch) cable *vs* crossover cable

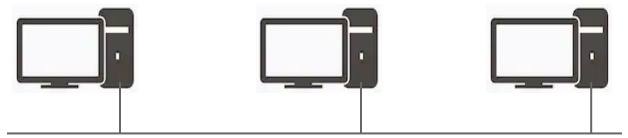




PoE (aka Power Over Ethernet)

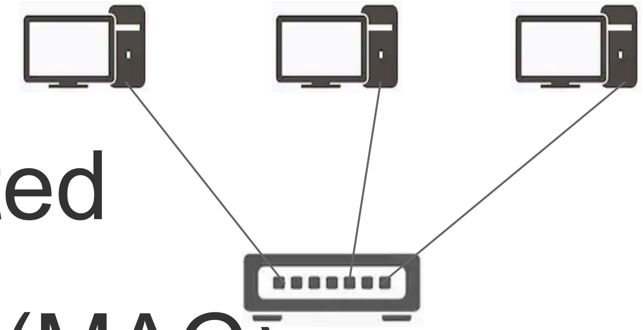
- Allow to pass electric power along with data on twisted pair Ethernet cables
- Allow to use only one cable to provide network connectivity for data trafic and electric power for devices (e.g. VoIP phones)
- Several implementations:
  - PoE: 15.40W, 350mA (802.3at Type 1)
  - PoE+: 30W, 600mA (802.3at Type 2)
  - 4PPoE: 60W, 600mA per pair (802.3bt Type 3)
  - Type 4: 100W, 900mA per pair (802.3bt Type 4)

Hub



- Multiple ports
- Repeats the received signal to all the others ports
  - In case of noise, the signal is cleaned, regenerated, and retransmitted at a higher power level
  - Only one collision domain
- Allow to extend the network size
- Cause a propagation delay
- Have been made obsolete by switches

Switch



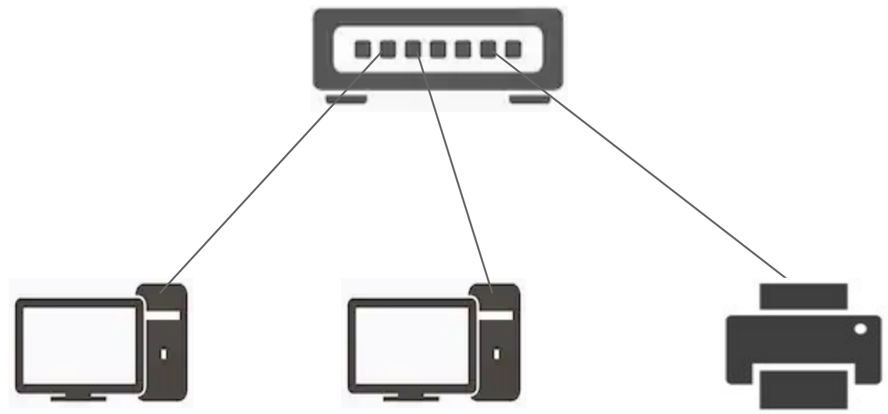
- Forward frames to the ports involved in the communication rather than all ports connected
- Port filter according to the physical address (MAC)
- Each port is in a different collision domain
- 1 monitoring port (read only port)
- Multi-layer switches are available (networking, application)

Switch functionalities

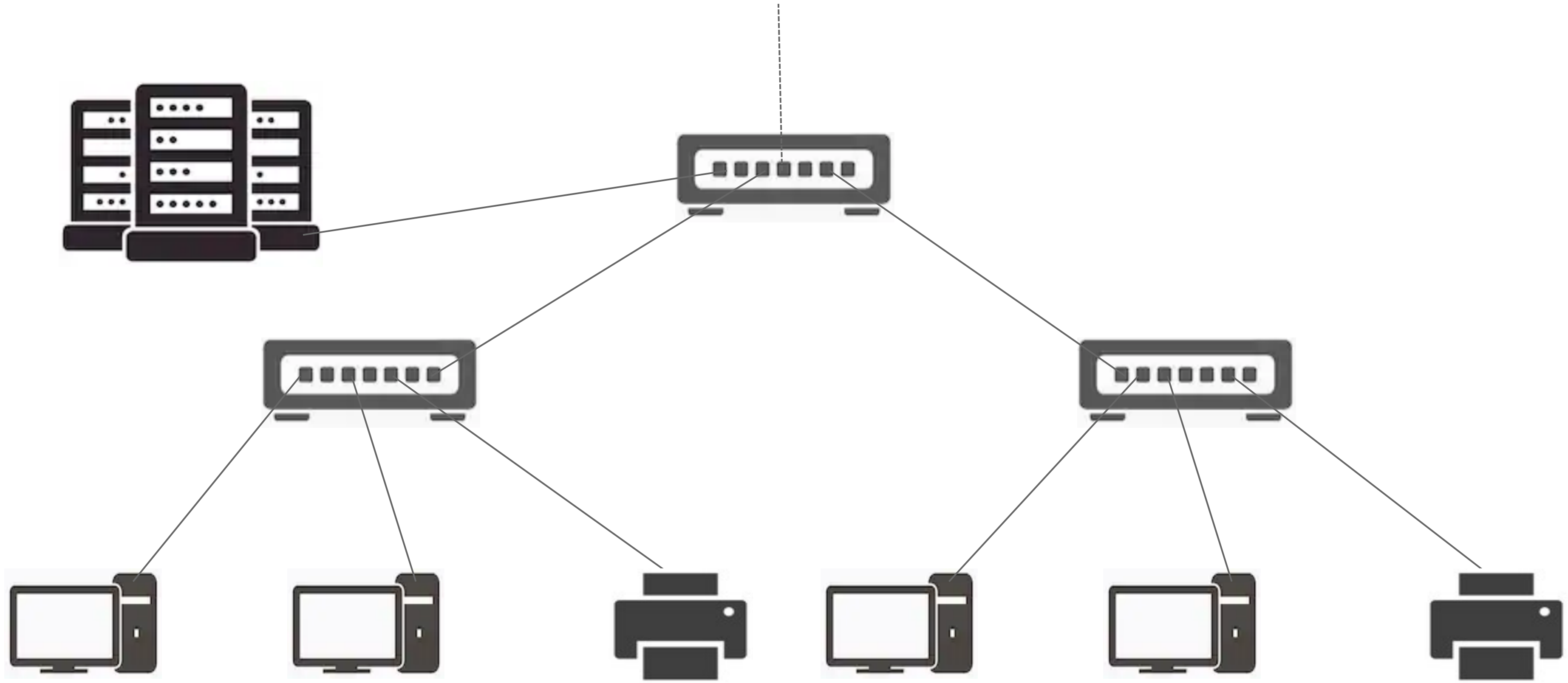
- MAC filtering
- Port filtering
- MTU modification
- Data rate management
- Loop management
- VLAN support
- PoE

Basic switch architecture

Switch



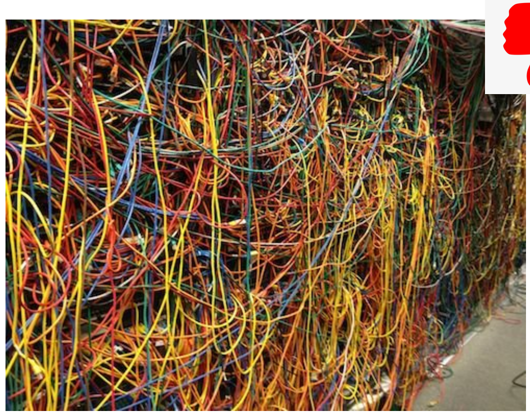
Complex switch architecture

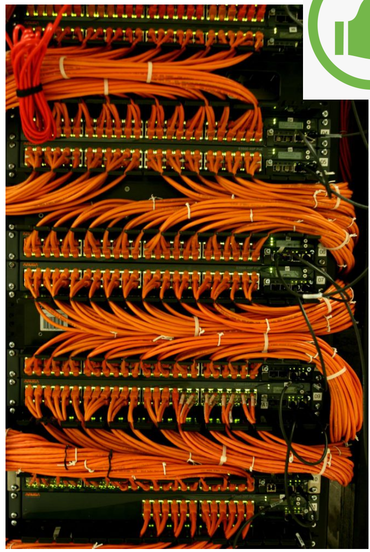


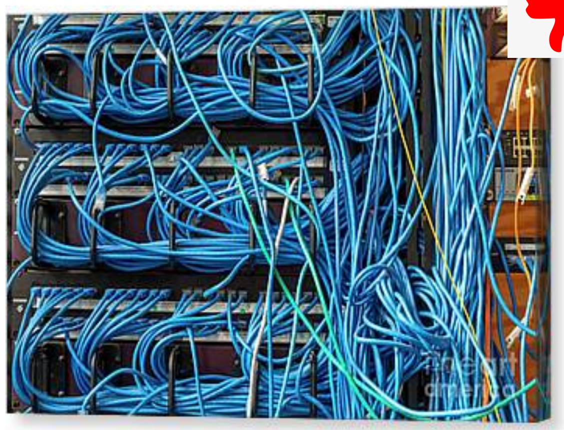
Backbone switch

Edge switches

Network cable and switch...

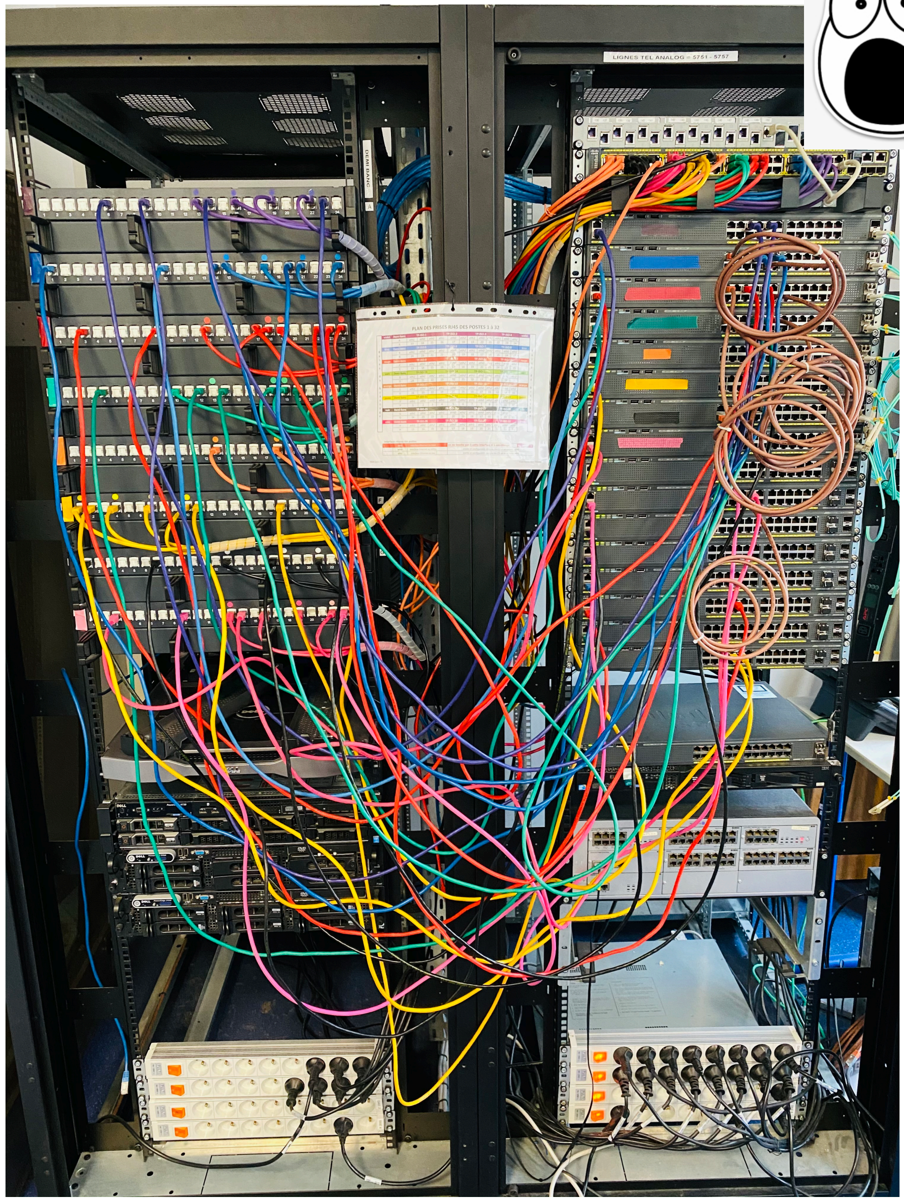






https://www.reddit.com/r/cableporn/

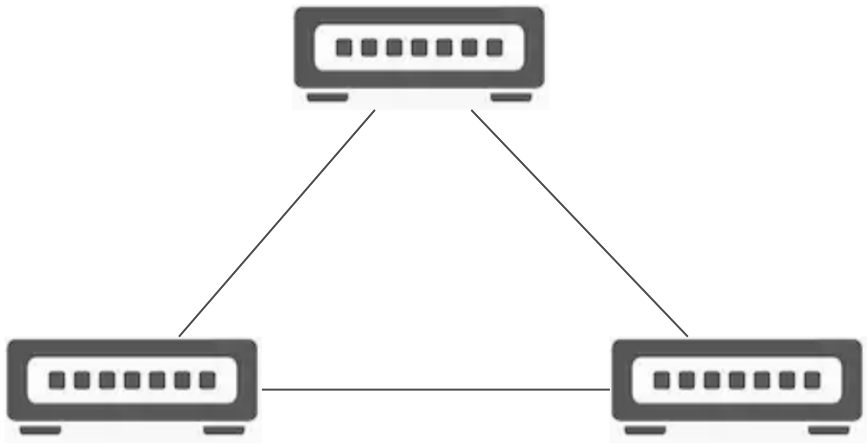
... but during the lab



Spanning tree protocol (STP, IEEE 802.1D)

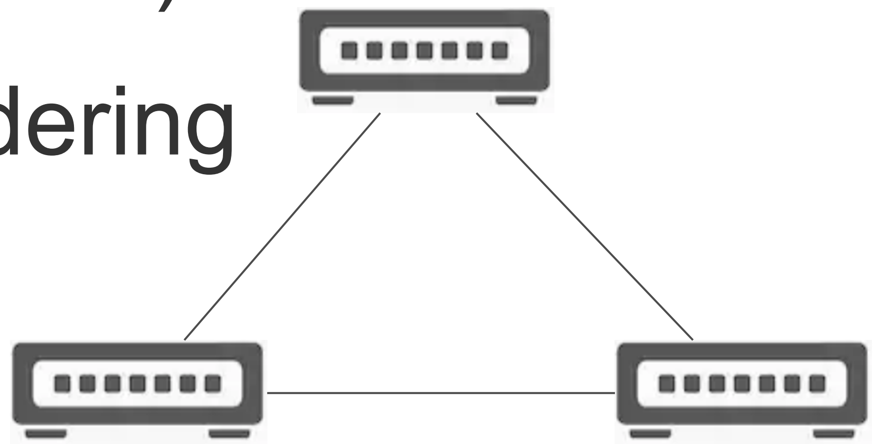
- Switches are interconnected using redundant links to improve resilience… but it creates loop!
- Bad network design also creates loops!

- STP protocol:
  - Builds a loop-free network topology
  - Avoid broadcast storm
  - Backup links and fault-tolerance

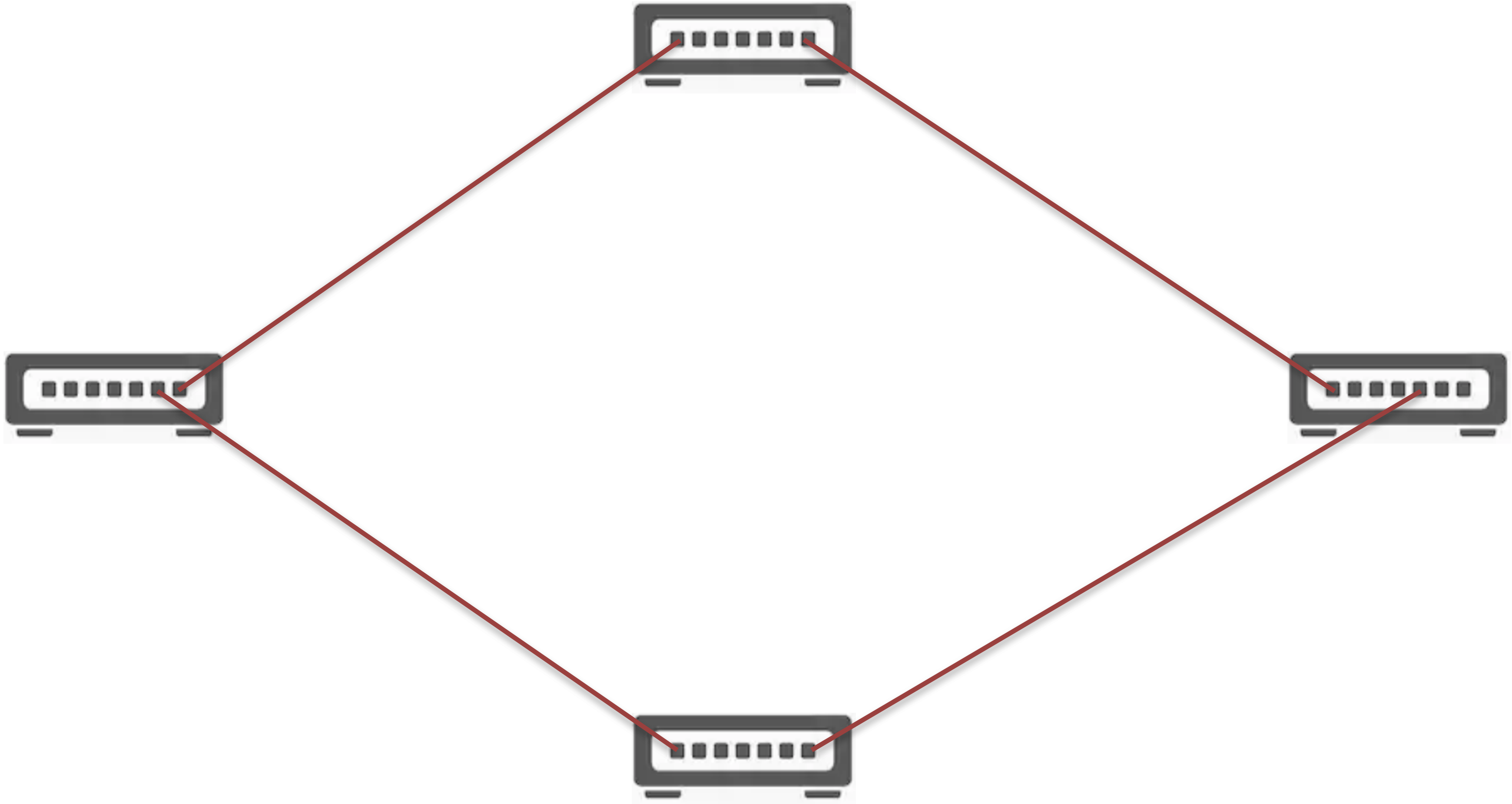


Spanning tree protocol

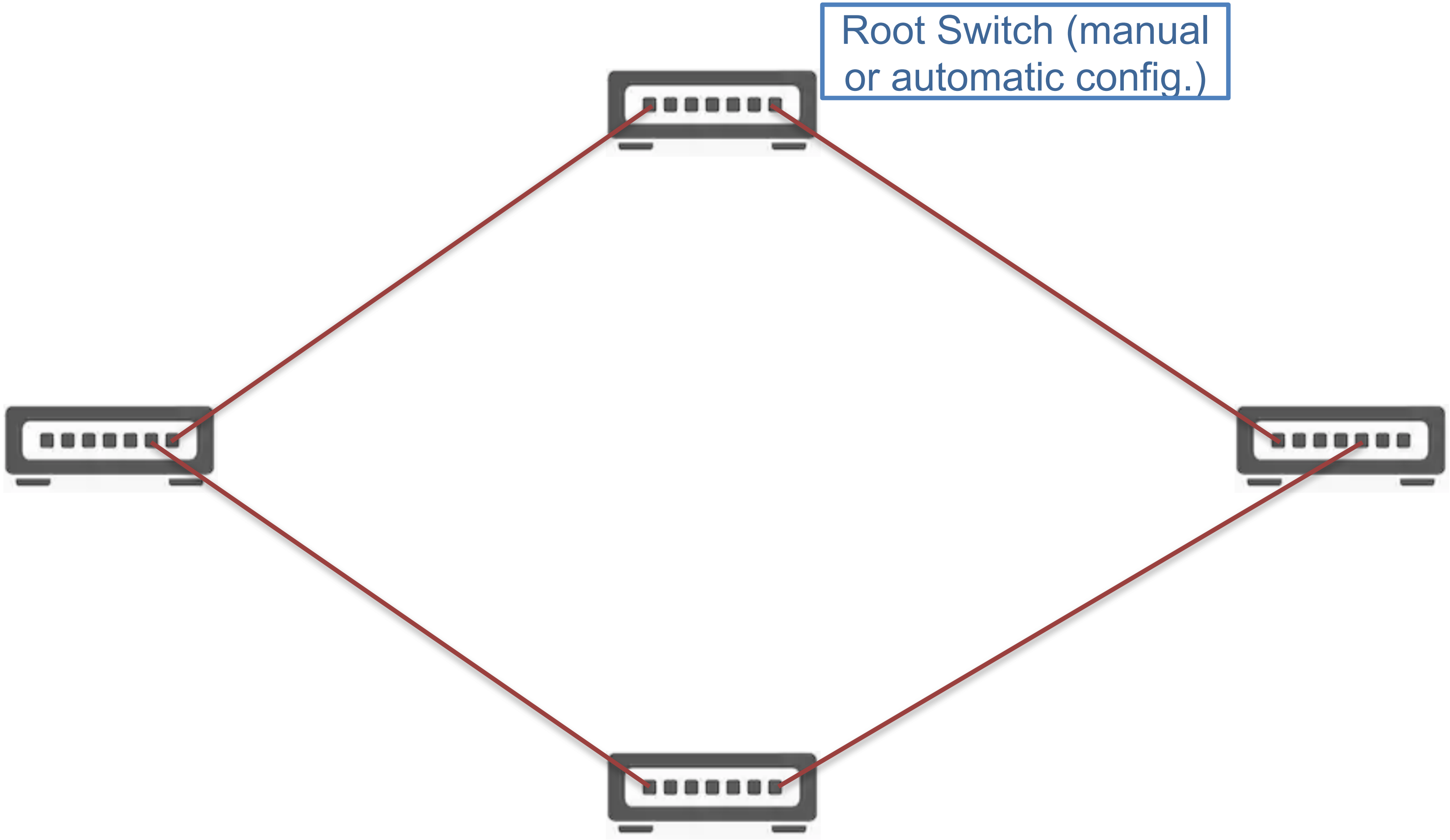
- Redundant links are identified
- Select *preferred* links ⇒ disable redundant links
- If the *preferred* link fails: a non-preferred redundant link is enabled (warning: convergence time…)
- Compute the cost of each path considering the highest bandwidth



Spanning tree protocol: how it works?

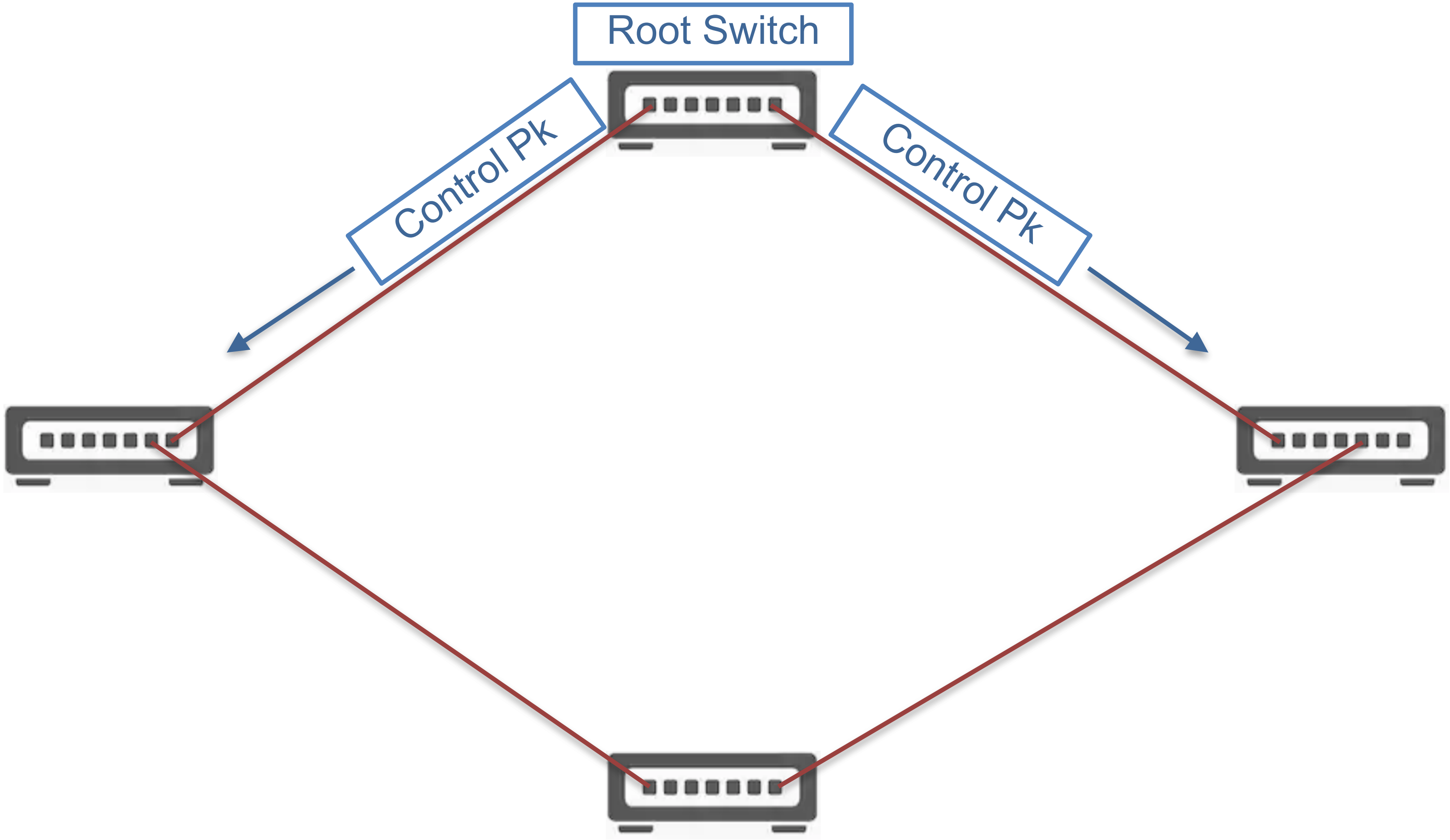


Spanning tree protocol: how it works?



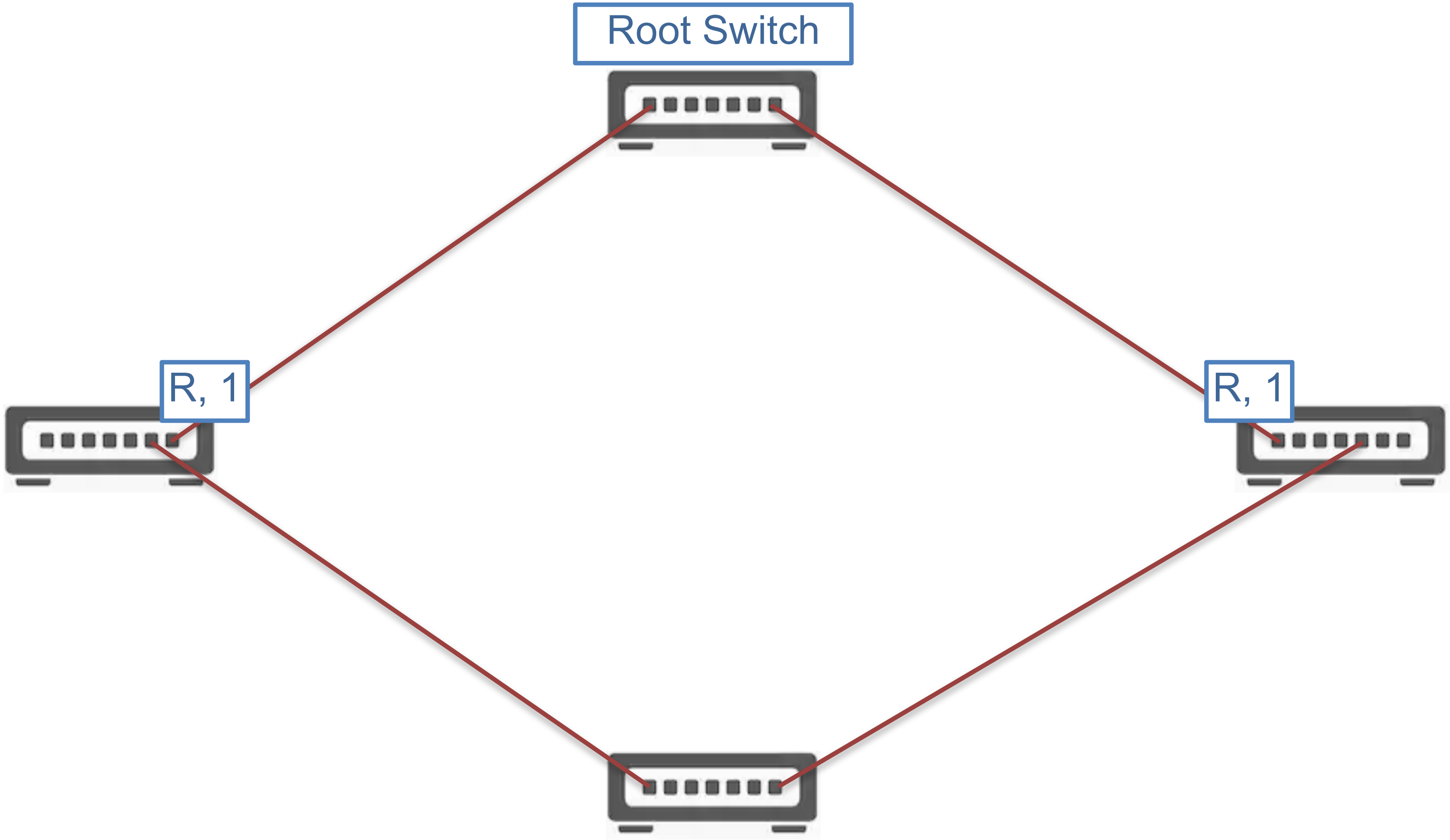
— R: Root Port — D: Disabled Port — B: Blocked Port —

Spanning tree protocol: how it works?



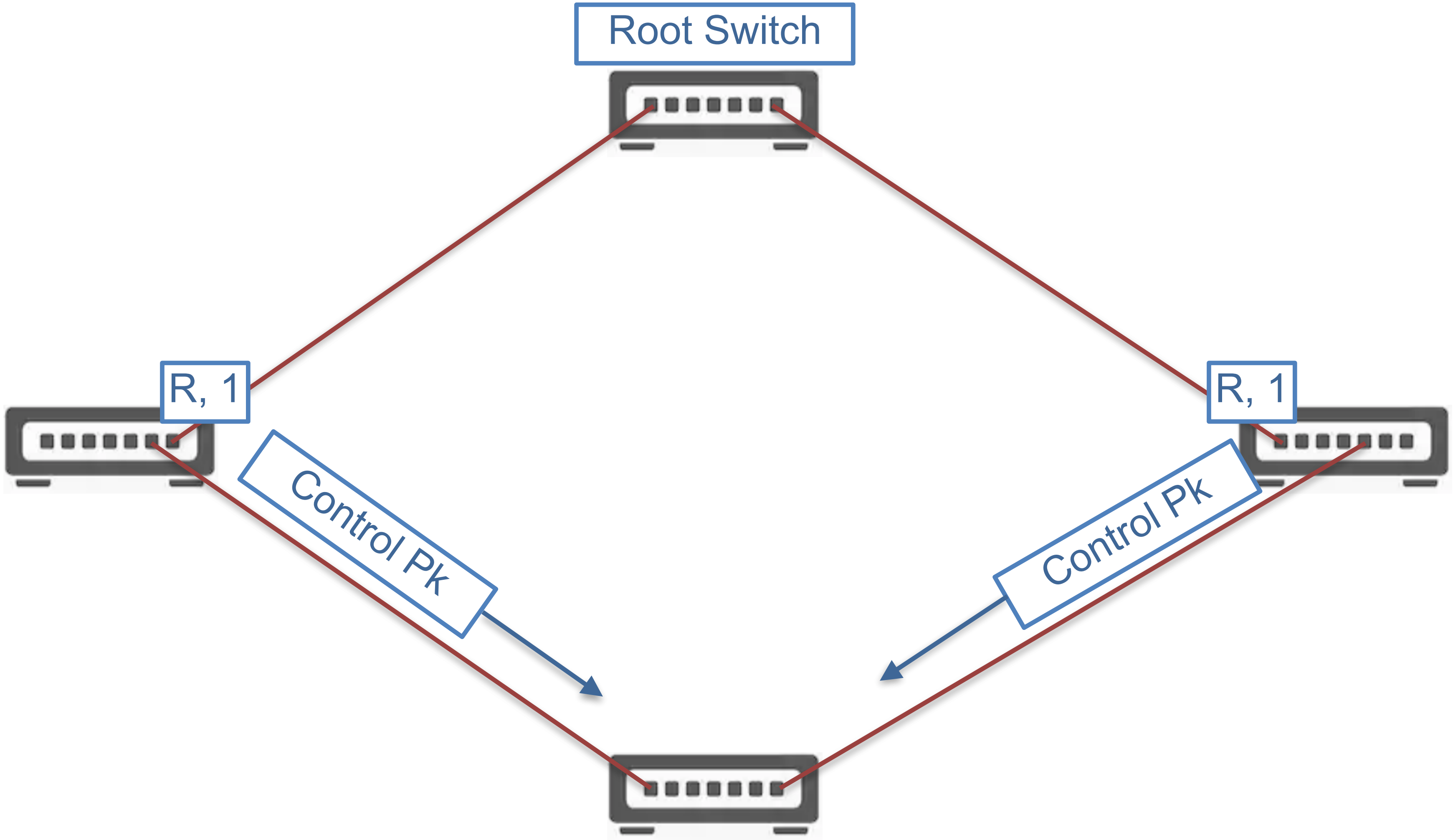
— R: Root Port — D: Disabled Port — B: Blocked Port —

Spanning tree protocol: how it works?



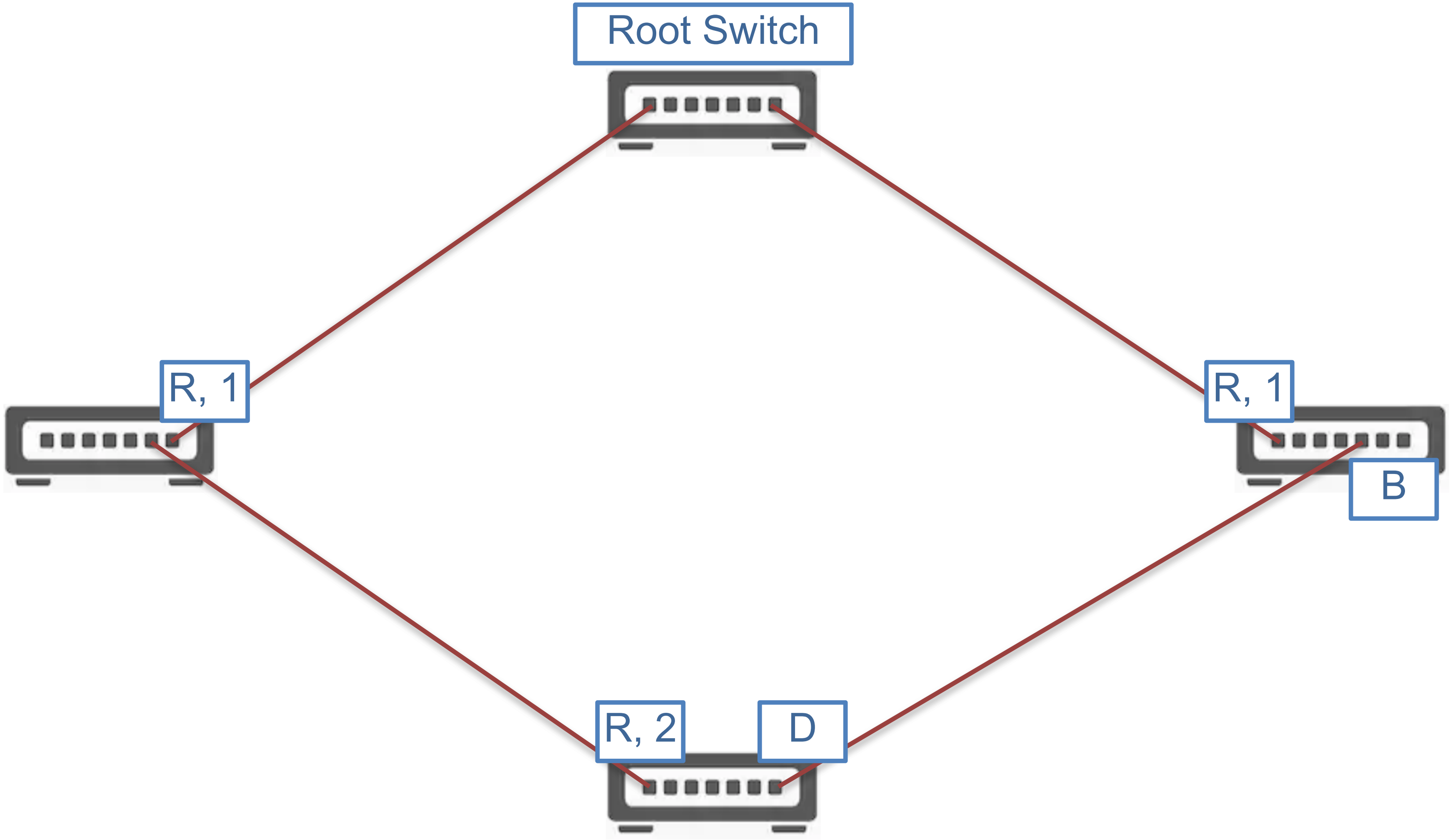
— R: Root Port — D: Disabled Port — B: Blocked Port —

Spanning tree protocol: how it works?



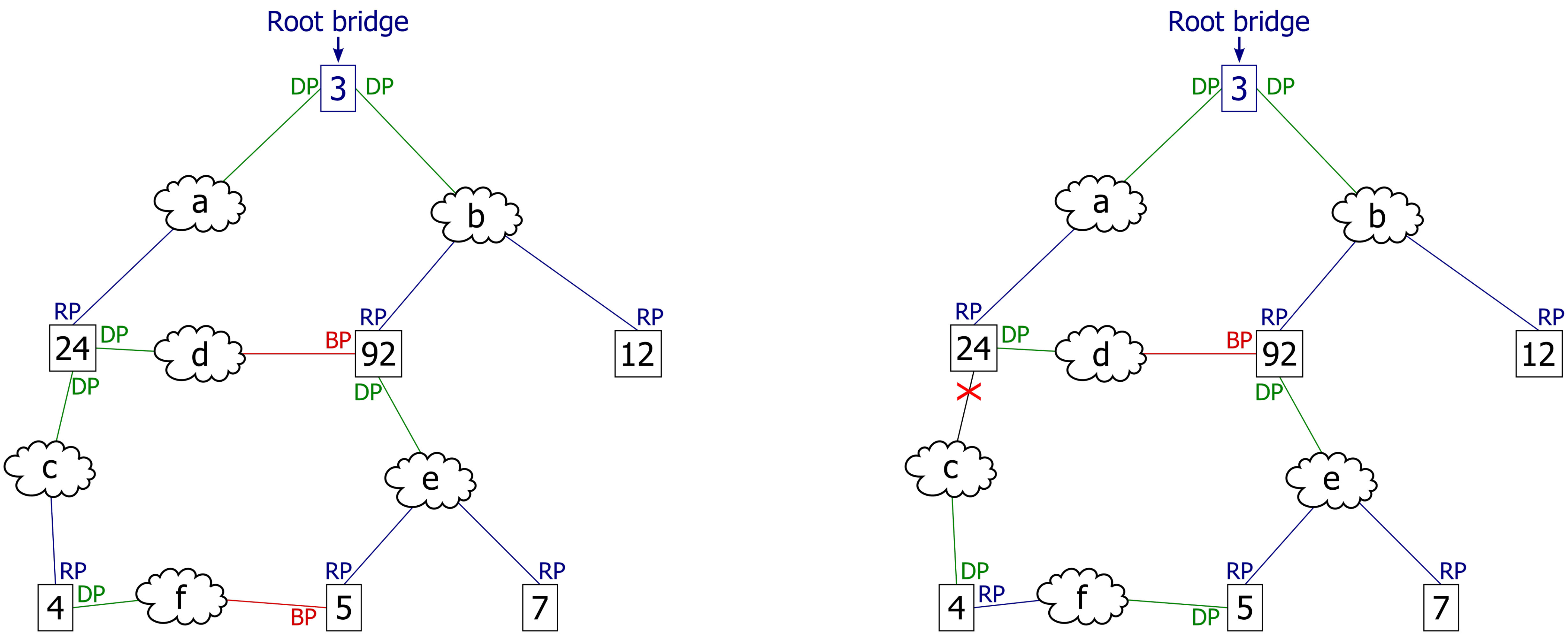
— R: Root Port — D: Disabled Port — B: Blocked Port —

Spanning tree protocol: how it works?



— R: Root Port — D: Disabled Port — B: Blocked Port —

Spanning tree protocol (link failure)



— RP: Root Port — DP: Disabled Port — BP: Blocked Port —

Source: wikicommons.wikimedia

8. Virtual Local Area Network – VLAN

VLAN

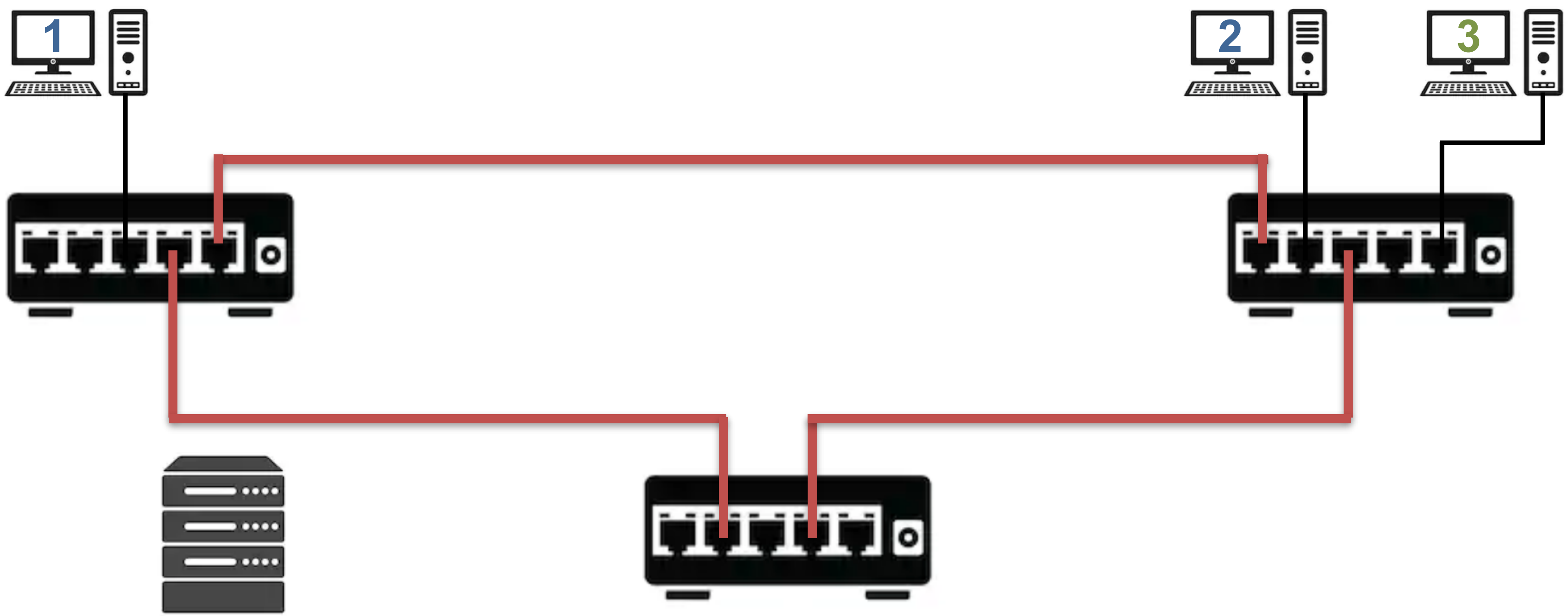
- Objectives:
  - Allow groups of users to be connected together
- Build a logical network on a physical LAN
- Flows are isolated, *e.g.*:
  - Telephony over IP *vs* others IP traffics
  - Demilitarized area (DMZ)
  - Storage access network

VLAN: Benefits

- Segmentation of a physical network
- Reduce the broadcast trafic (up to 30%)
- Several independent (*virtual*) partitions
- VLANs can be propagated and can decouple the users' network location from their physical location
- Advanced feature thanks to *trunk*
- Scalability of Ethernet networks
- Simplification of the network administration

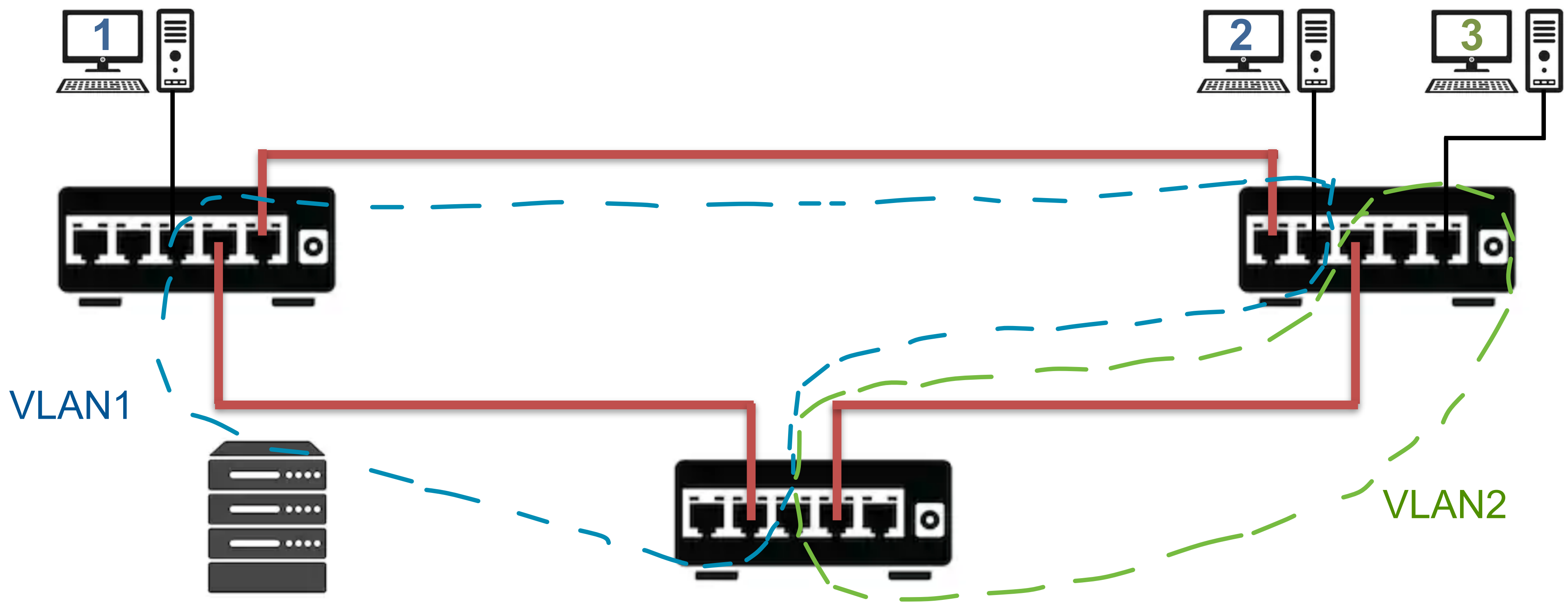
VLAN: Big Picture

- No modification on the computers
- VLANs are only managed by switches



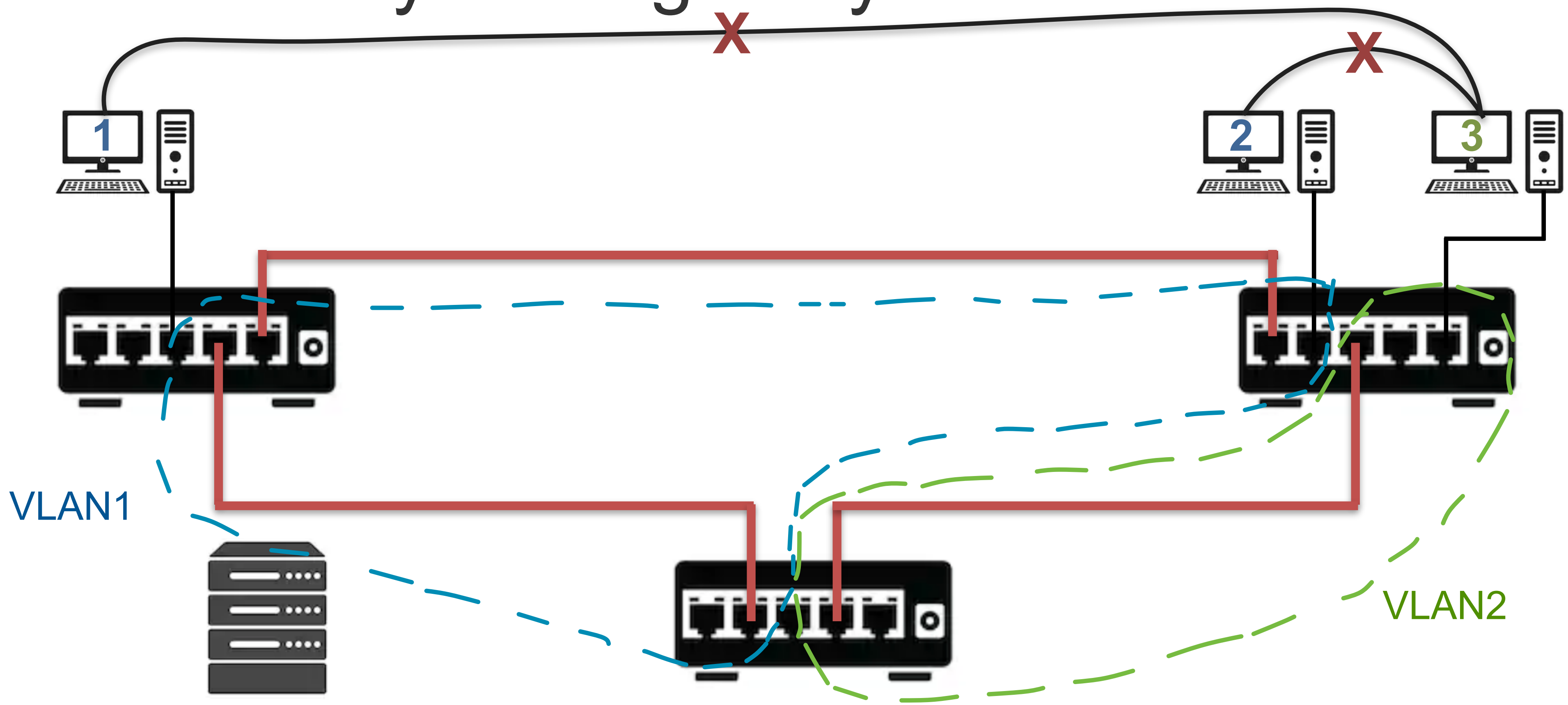
VLAN: Big Picture

- No modification on the computers
- VLANs are only managed by switches



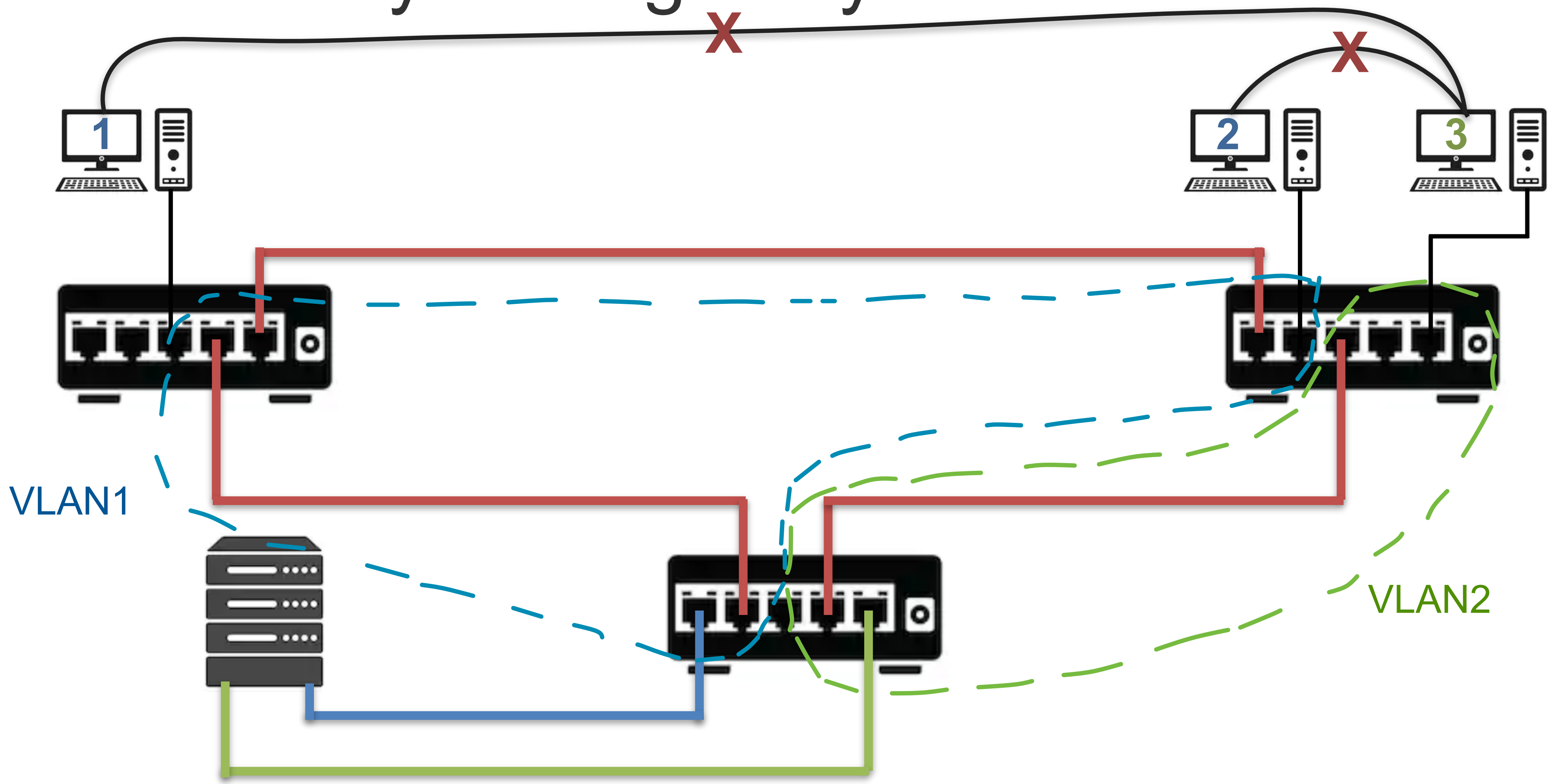
VLAN: Big Picture

- No modification on the computers
- VLANs are only managed by switches



VLAN: Big Picture

- No modification on the computers
- VLANs are only managed by switches

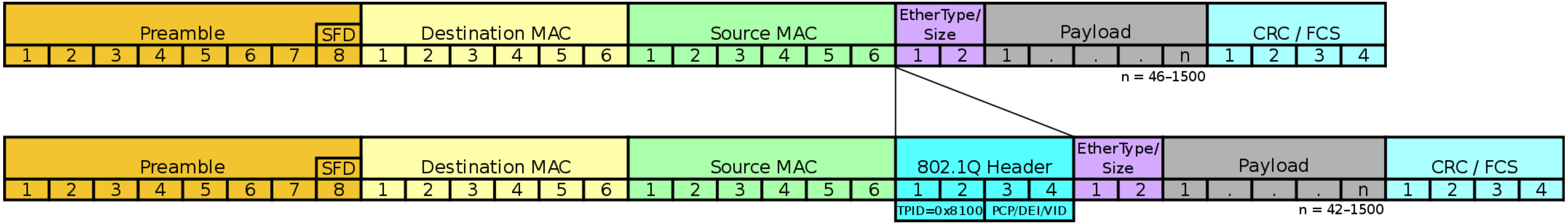


VLAN family

- Static: port-based VLAN
- Dynamic VLAN:
  - MAC address-based
  - IP-based
  - Protocol-based
  - User-based (using 802.1x authentication)

VLAN: 802.1Q

- Add 32 bytes of control in the Ethernet header for frame transmissions between switches and switches/routers



- This header is removed for frame delivery to computer

VLAN: 801.Q header

16 bits	3 bits	1 bit	12 bits
TPID	TCI		
	PCP	DEI	VID

- Tag Protocol ID, always set to: 0x8100, used to identify 802.1Q frames
- Tag Control Identification
  - Priority Code Point: support of different trafic priorities
  - Drop Eligible Indicator: frame can be dropped if congestion
  - VLAN identifier (4094 different ids.)

VLAN: Trunk mode

- Easy configuration & management of workstations connected to the same VLAN but on different switches
- Also used to interconnect several workstations which are in different VLANs (require routers)
- Two possibilities
  - VTP: VLAN Trunk Protocol by Cisco
  - GVRP: Generic VLAN Registration Protocol

Thanks for listening, reading and asking.

The end.

Title

- Level 1
- Level 1
  - Level 2
  - Level 2
- Level 1
  - Level 2
  - Level 2
    - *Level 3*
    - *Level 3*