# Chapter 4
# Local Area network

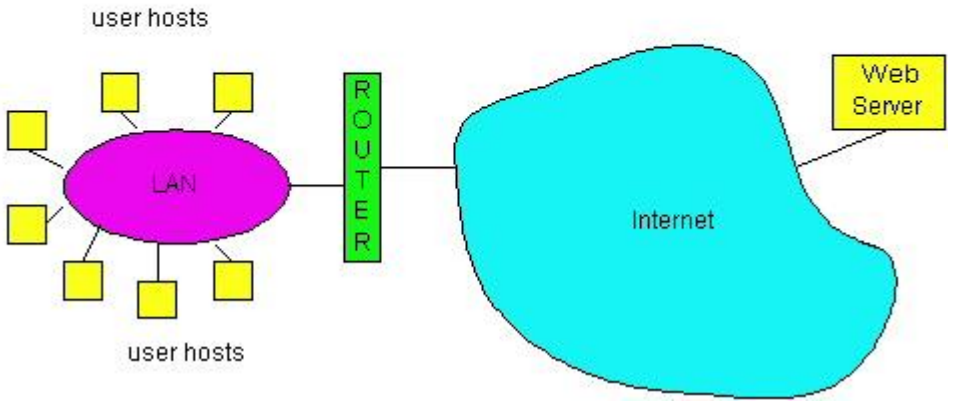
# LAN technologies

Data link layer so far:

- services, error detection/correction, multiple access

Next: LAN technologies

- LAN model
- addressing
- Ethernet
- hubs, switches
- 802.11
- 802.15



# Keypoints and Difficulties

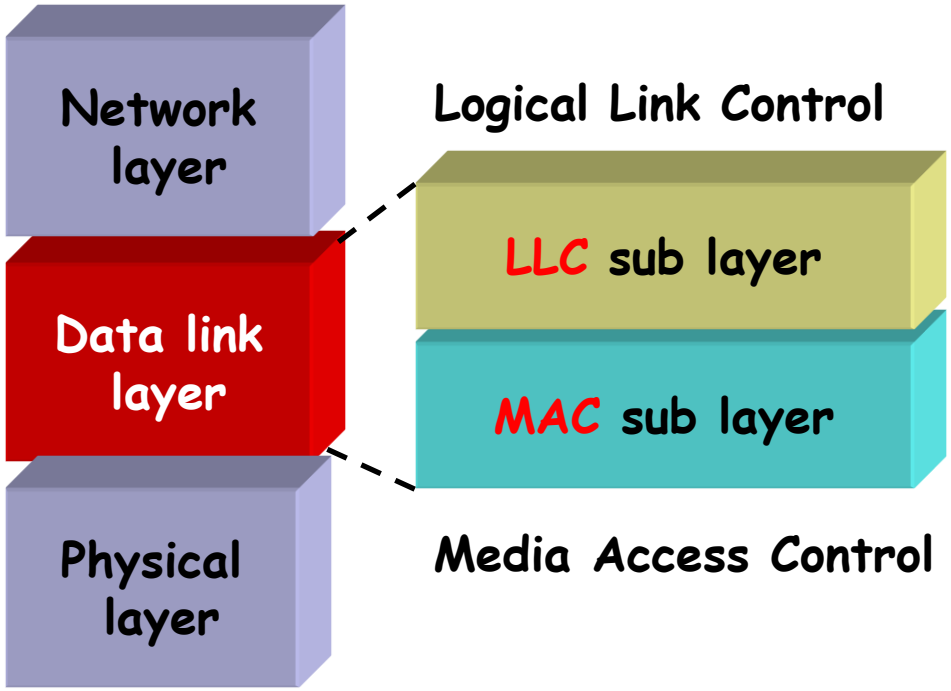
## Keypoints:

- LAN model
- Ethernet
- Hubs, switches
- Wireless LAN-IEEE 802.11

## Difficulties:

- The minimum frame length
- The exponential Backoff algorithm
- CSMA/CA

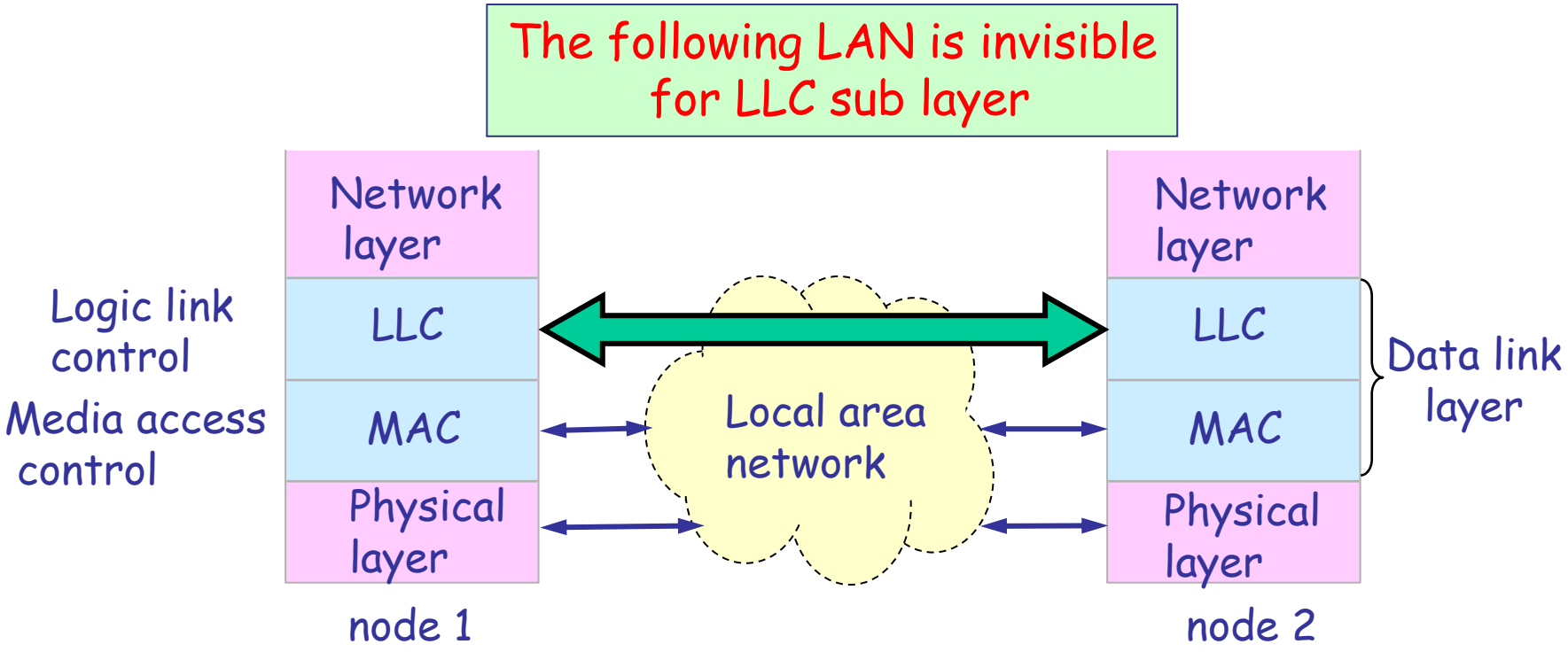
# LAN model




Provide the connection environment to the upper level

Providing media access to the lower layer

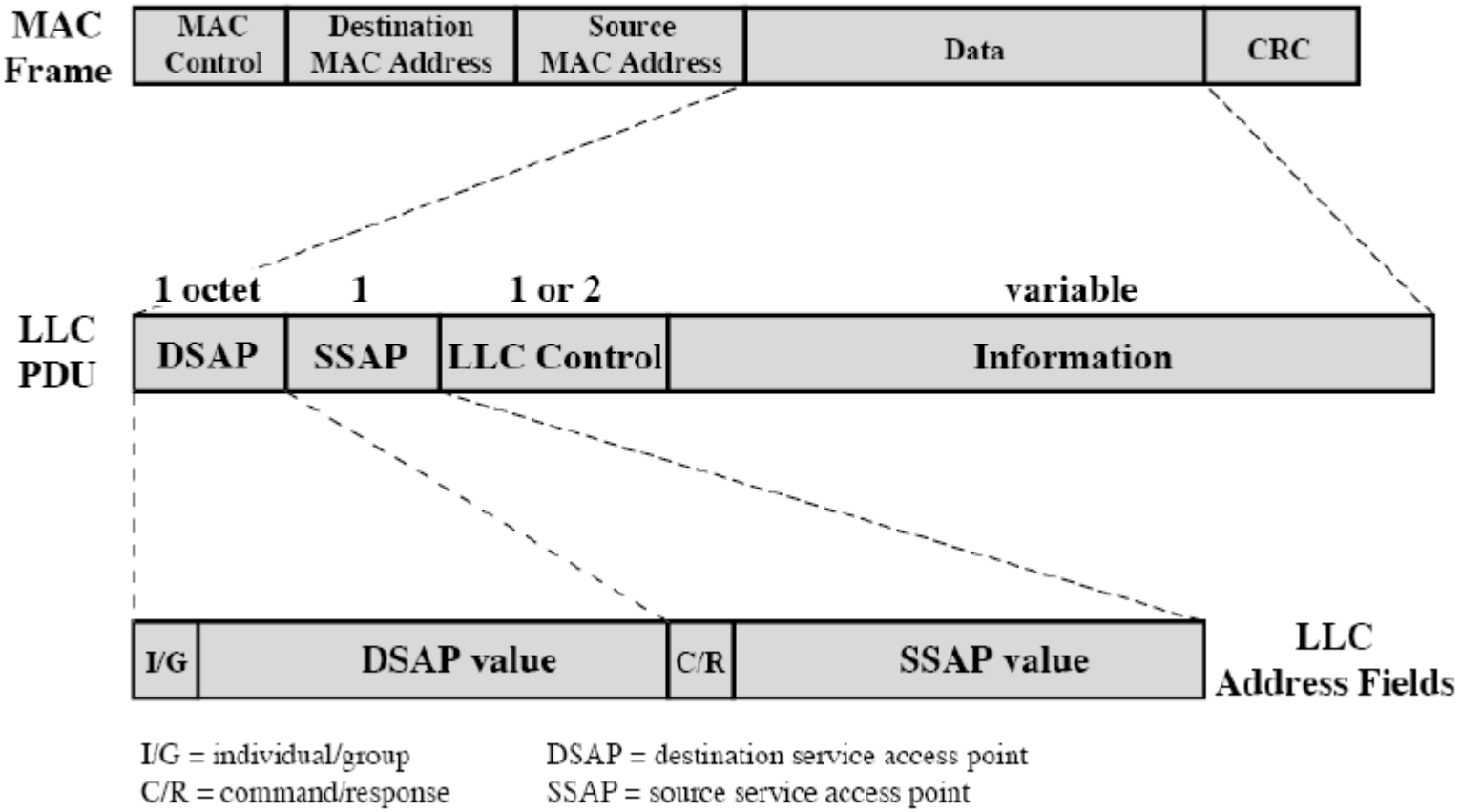
# LAN model



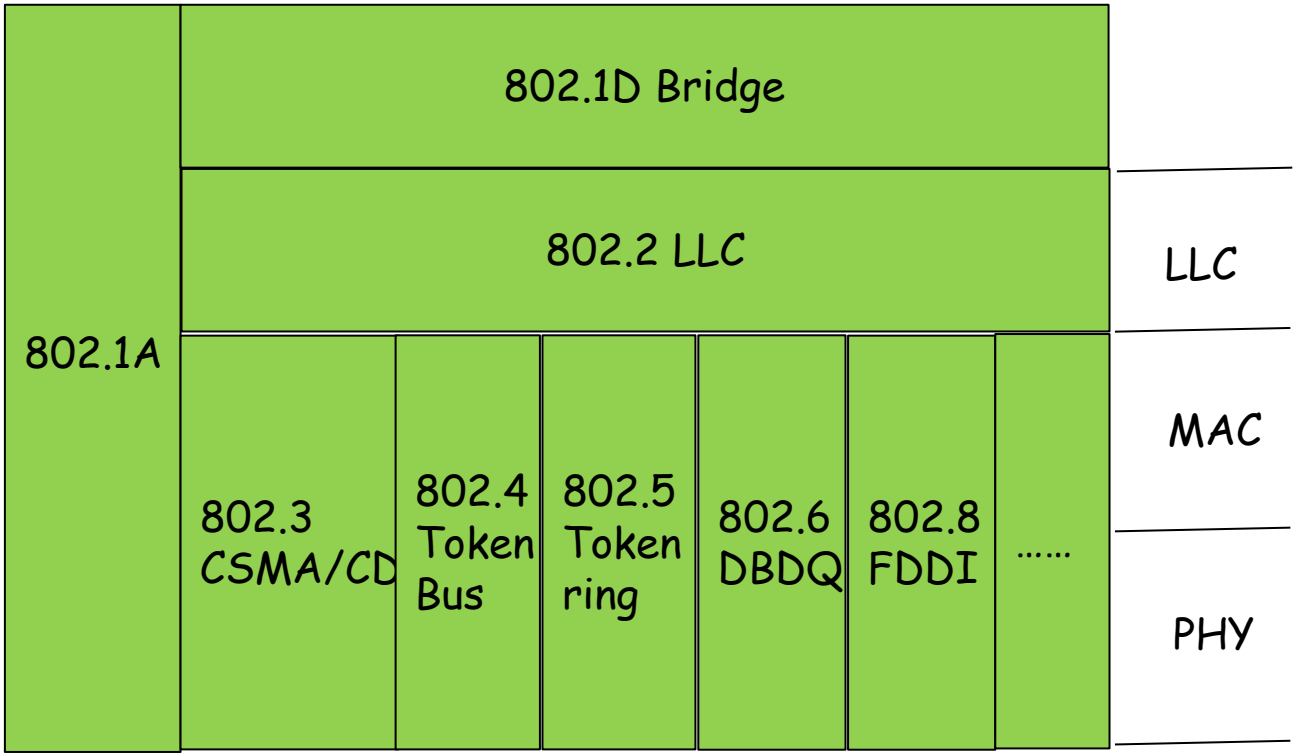

For the same LLC, several MAC options may be provided.

# LLC and MAC

## MAC Frame Format



# IEEE 802 working group



# LAN Addresses

## 32-bit IP address:

- *network-layer* address
- used to get datagram to destination network

## LAN (or MAC or physical) address:

- used to get datagram from one interface to another physically-connected interface (same network)
- 48 bit MAC address (for most LANs) burned in the adapter ROM

# LAN Address (more)

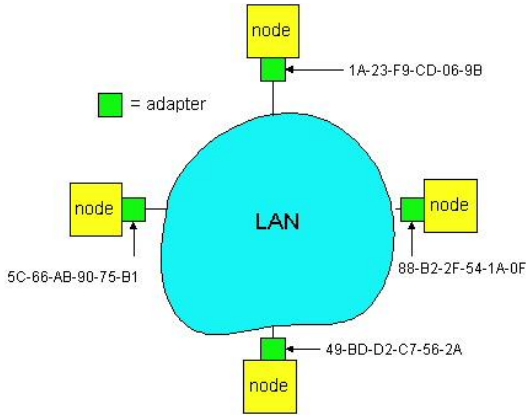
- MAC address allocation administered by IEEE
- manufacturer buys portion of MAC address space (to assure uniqueness)
- Analogy:

  (a) MAC address: like Social Security Number

  (b) IP address: like postal address
- MAC flat address => portability
  - can move LAN card from one LAN to another
- IP hierarchical address NOT portable
  - depends on network to which one attaches

# LAN Address

Each adapter on LAN has unique LAN address





**IEEE 802局域网的MAC地址格式**

**扩展的唯一标识符EUI**
**EUI-48**

| 组织唯一标识符OUI（由IEEE的注册管理机构分配） | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 第一字节 | | | | | | | | 第二字节 | | | | | | | | 第三字节 | | | | | | | |
| b7 | b6 | b5 | b4 | b3 | b2 | b1 | b0 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | b0 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | b0 |
| 十六进制 | X | | X | | X | | X | | X | | X | | | | | | | | | | | | |

| 网络接口标识符（由获得OUI的厂商自行随意分配） | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 第四字节 | | | | | | | | 第五字节 | | | | | | | | 第六字节 | | | | | | | |
| b7 | b6 | b5 | b4 | b3 | b2 | b1 | b0 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | b0 | b7 | b6 | b5 | b4 | b3 | b2 | b1 | b0 |
| X | | X | | X | | X | | X | | X | | X | | X | | X | | X | | X | | X | |

标准表示法：XX-XX-XX-XX-XX-XX　Windows　例如：00-0C-CF-93-8C-92

其他表示法：XX:XX:XX:XX:XX:XX　例如：00:0C:CF:93:8C:92

XXXX.XXXX.XXXX　Cisco Packet Tracer　例如：000C.CF93.8C92

# MAC Addresses


| 第一字节的b1位 | 第一字节的b0位 | MAC地址类型 | 地址数量占比 | 总地址数量 |
|---|---|---|---|---|
| 0 | 0 | 全球管理 单播地址 厂商生产网络设备（网卡，交换机，路由器）时固化 | 1/4 | $2^{48}$=281,474,976,710,656（二百八十多万亿） |
| | 1 | 全球管理 多播地址 标准网络设备所支持的多播地址，用于特定功能 | 1/4 | |
| 1 | 0 | 本地管理 单播地址 由网络管理员分配，覆盖网络接口的全球管理单播地址 | 1/4 | |
| | 1 | 本地管理 多播地址 用户对主机进行软件配置，以表明其属于哪些多播组<br>注意：剩余46位全为1时，就是广播地址FF-FF-FF-FF-FF-FF | 1/4 | |

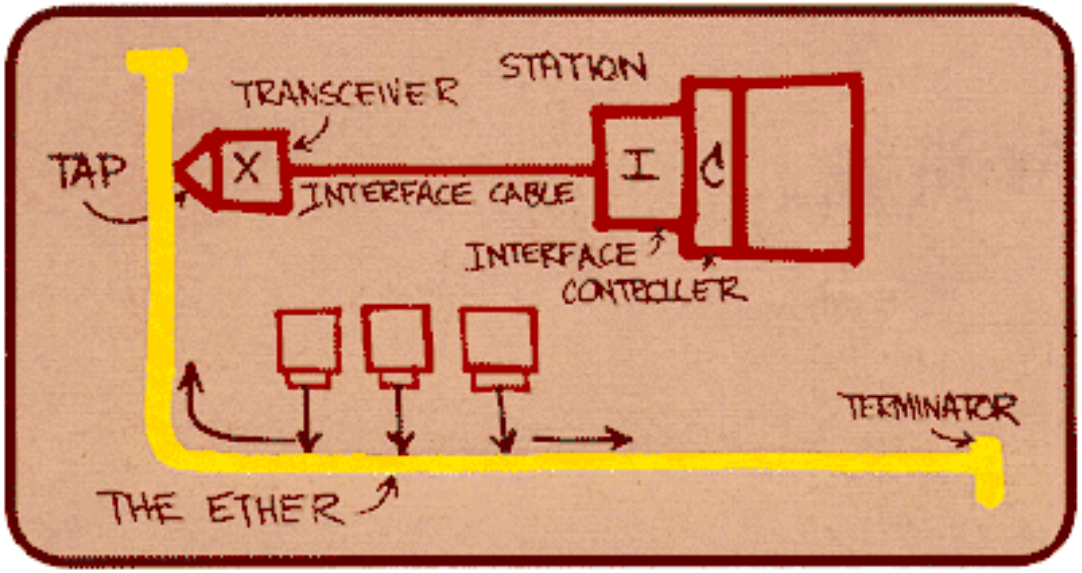
https://standards-oui.ieee.org/oui/oui.txt
MAC地址查询 - https://mac.bmcx.com/

What is the random MAC address technology?

# Ethernet

"dominant" LAN technology:

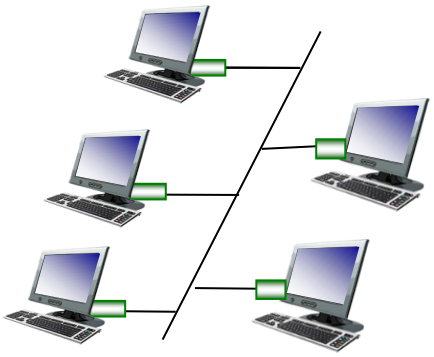
- cheap $20 for 100Mbs!
- first wildey used LAN technology
- Simpler, cheaper than token LANs and ATM
- Kept up with speed race: 10, 100, 1000 Mbps



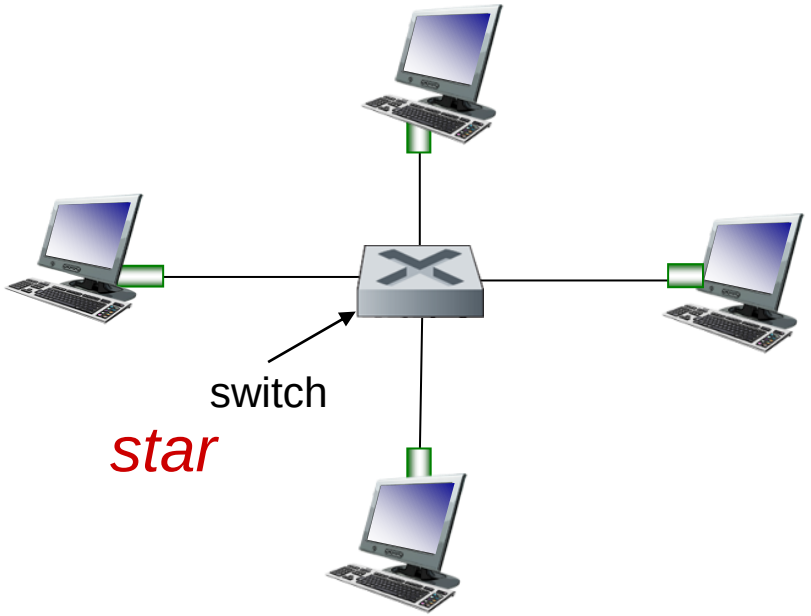

Metcalfe's Etheret sketch

# Ethernet: physical topology

- *bus:* popular through mid 90s
  - all nodes in same collision domain (can collide with each other)
- *star:* prevails today
  - active *switch* in center
  - each "spoke" runs a (separate) Ethernet protocol (nodes do not collide with each other)



*bus:* coaxial cable



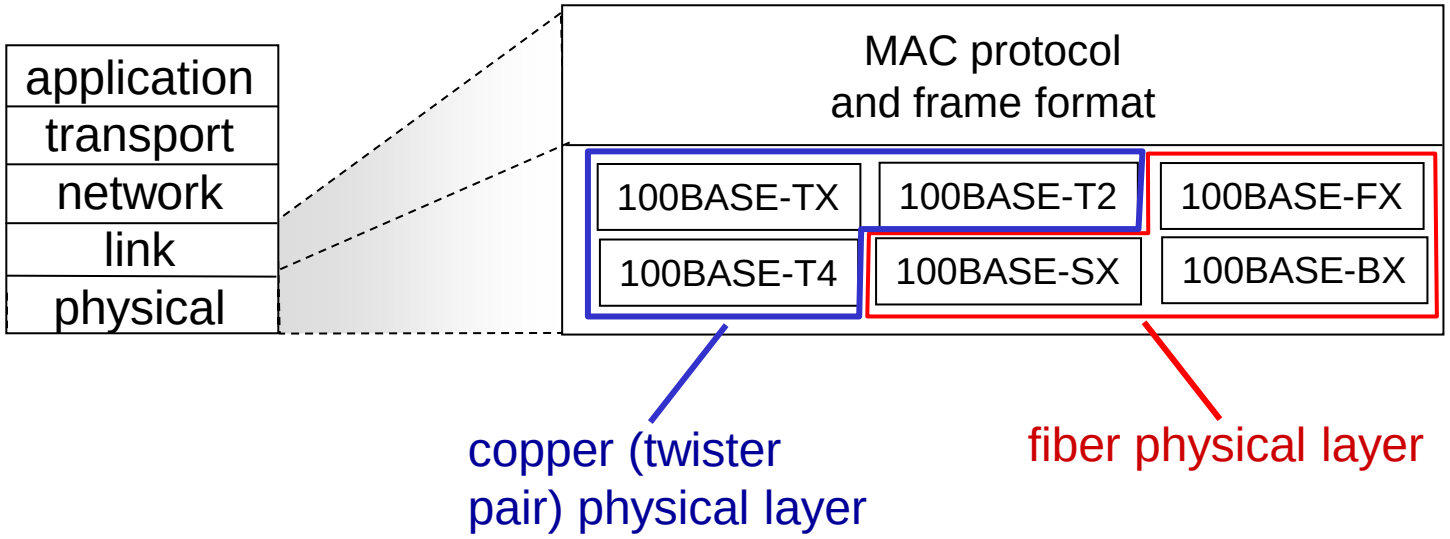

*star*

# Ethernet: unreliable, connectionless

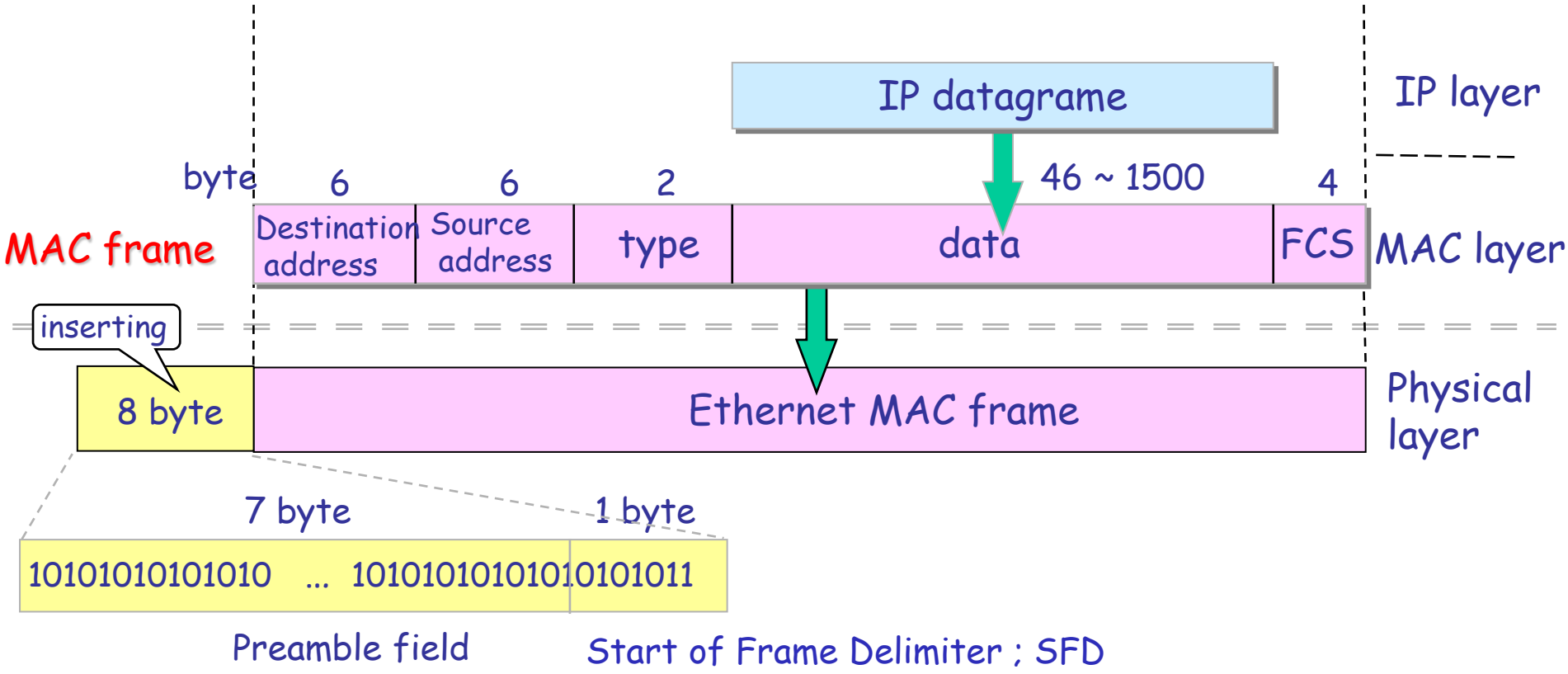
- *connectionless:* no handshaking between sending and receiving NICs
- *unreliable:* receiving NIC doesn't send acks or nacks to sending NIC
  - data in dropped frames recovered only if initial sender uses higher layer rdt (e.g., TCP), otherwise dropped data lost
- Ethernet's MAC protocol: unslotted *CSMA/CD with binary backoff*

# 802.3 Ethernet standards: link & physical layers

- *many* different Ethernet standards
  - common MAC protocol and frame format
  - different speeds: 10 Mbps, 100 Mbps, 1Gbps, 10 Gbps, 40 Gbps
  - different physical layer media: fiber, cable

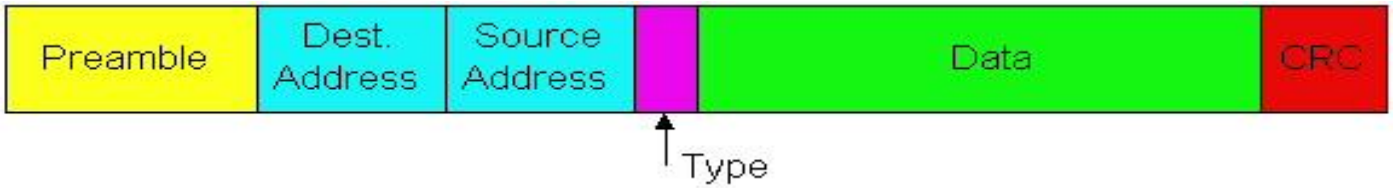


# Ethernet Frame Structure



# Ethernet Frame Structure

Sending adapter encapsulates IP datagram (or other network layer protocol packet) in Ethernet frame

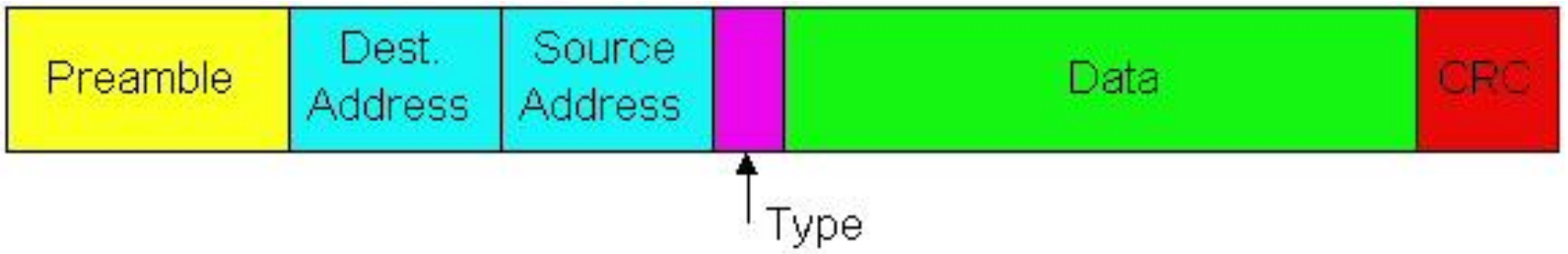



Preamble:

- 7 bytes with pattern 10101010 followed by one byte with pattern 10101011
- used to synchronize receiver, sender clock rates

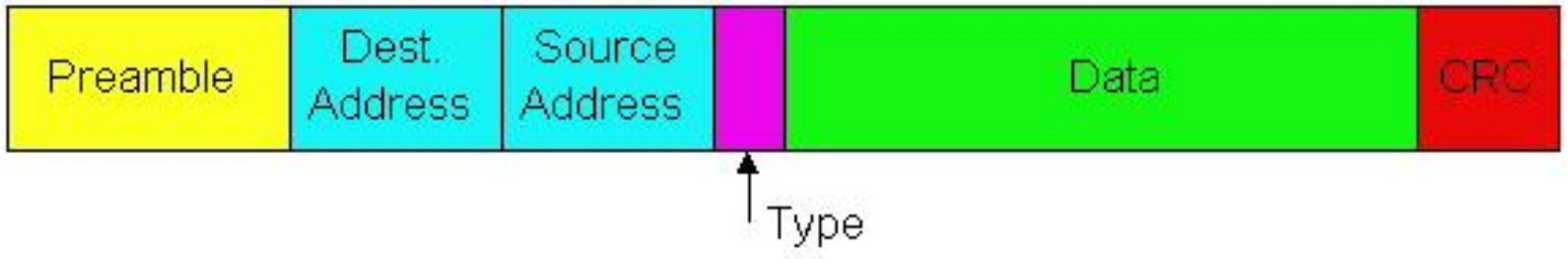
# Ethernet Frame Structure (more)

- Addresses: 6 bytes, frame is received by all adapters on a LAN and dropped if address does not match
- Type: 2 bytes, indicates the higher layer protocol, mostly IP but others may be supported such as Novell IPX and AppleTalk)
- CRC: 4 bytes, checked at receiver, if error is detected, the frame is simply dropped



# Ethernet Frame Structure (more)

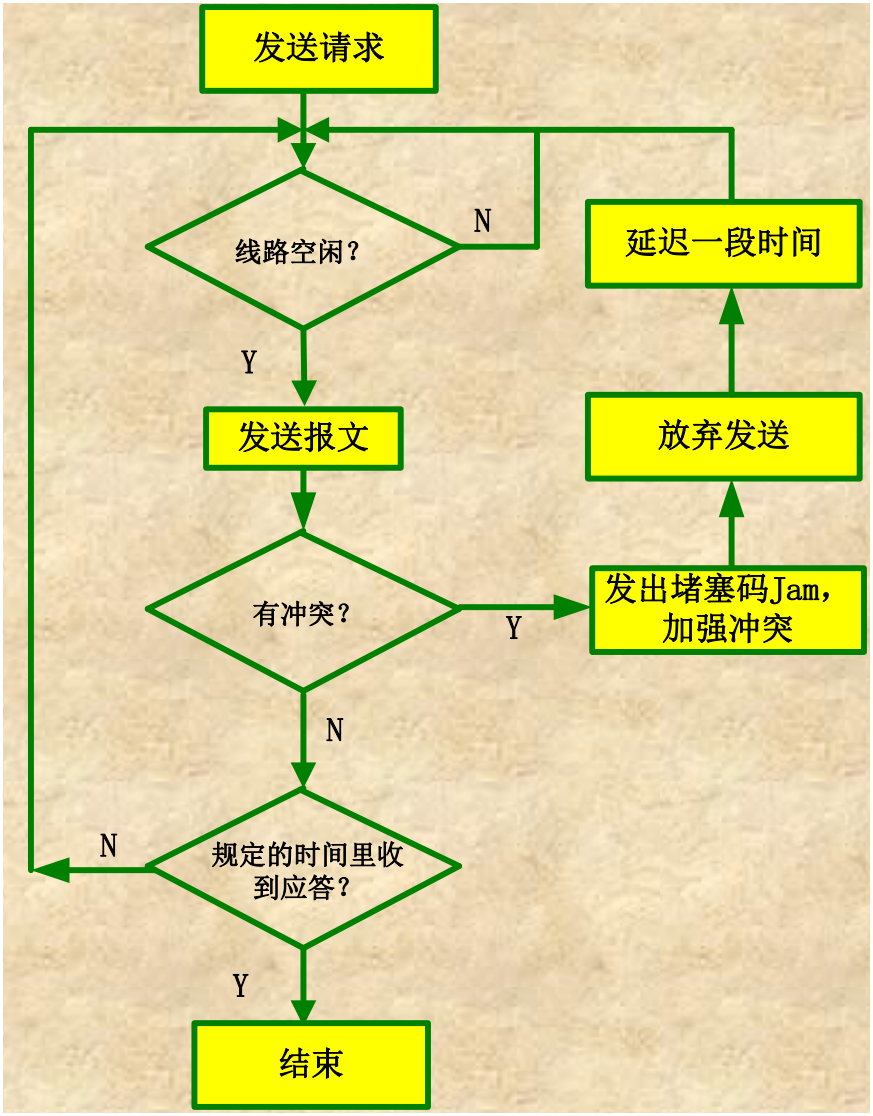
- Data: 46~1500 bytes
- Minimum frame length: 64 bytes, why? (contention period $2\tau$ is 51.2 $\mu$s for IEEE 802.3, R=10Mbps)
- Maximum frame length: 1518 bytes, why?



# Ethernet: uses CSMA/CD

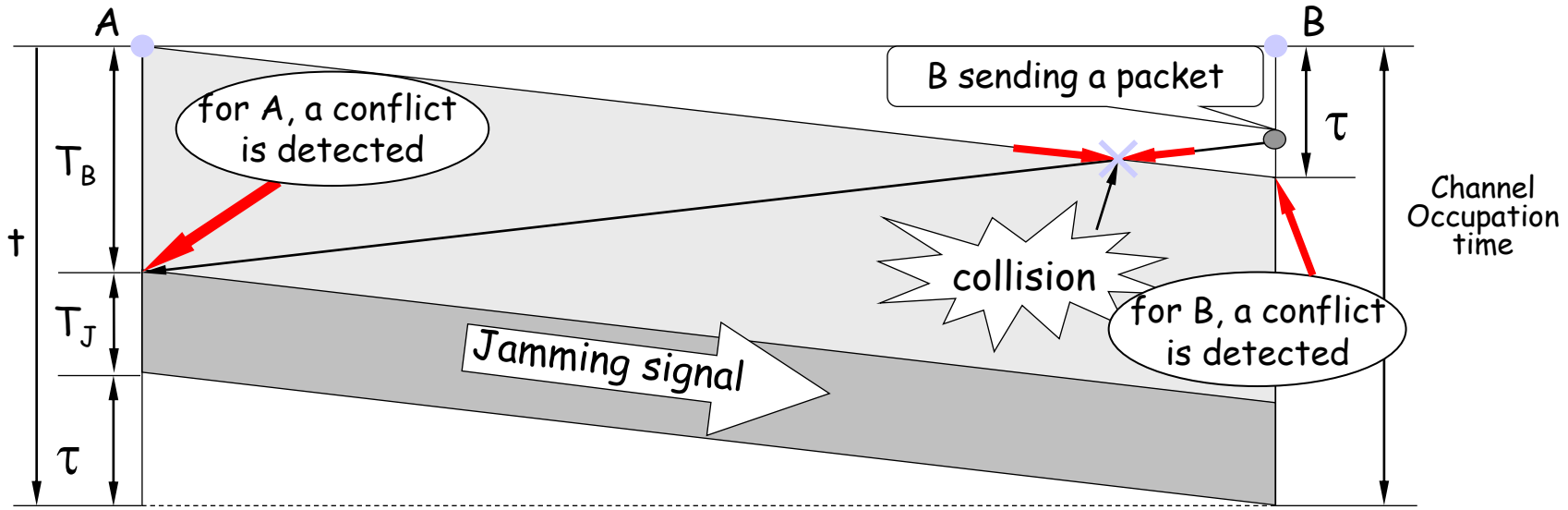
```
A: sense channel, if idle
    then {
            transmit and monitor the channel;
            If detect another transmission
              then {
                  abort and send jam signal;
                  update # collisions;
                  delay as required by exponential backoff algorithm;
                  goto A
                  }
             else {done with the frame; set collisions to zero}
        }
    else {wait until ongoing transmission is over and goto A}
```

# Ethernet: uses CSMA/CD



# Ethernet's CSMA/CD (more)

Jam Signal: make sure all other transmitters are aware of collision; 48 bits;



# Ethernet's CSMA/CD (more)

Exponential Backoff:

- *Goal*: adapt retransmission attemtps to estimated current load
  - heavy load: random wait will be longer
- delay is K x 512 bit transmission times (contention period: $2\tau$)
- first collision: choose K from {0,1};
- after second collision: choose K from {0,1,2,3}…
- after ten or more collisions, choose K from {0,1,2,3,4,…,1023}
- K=min(n,i),n: # collisions,n≤j(attempt limit);i:back off limit
- For Ethernet, i=10,j=16

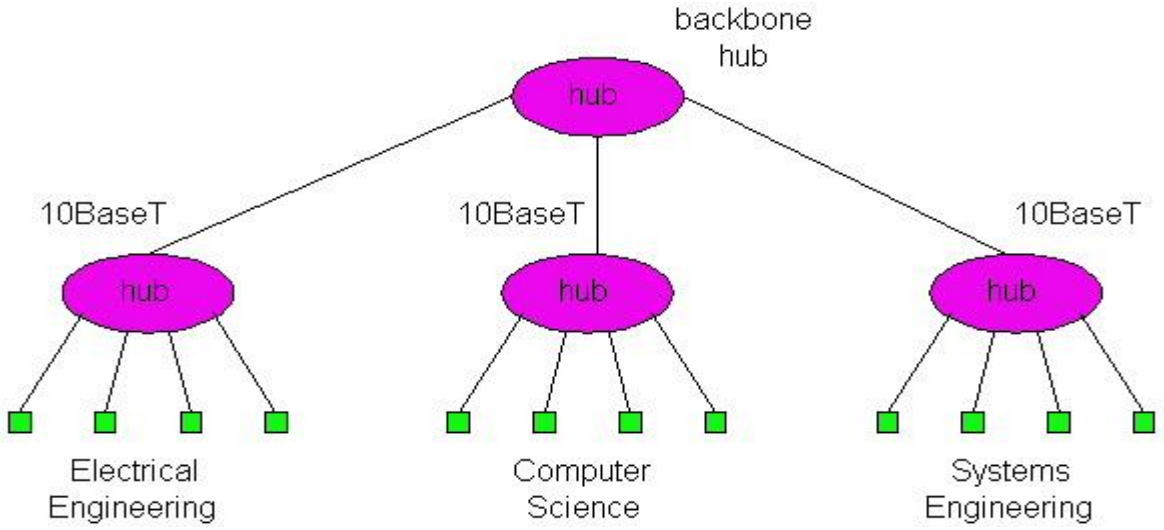
# Interconnecting LANs

Q: Why not just one big LAN?

- Limited amount of supportable traffic: on single LAN, all stations must share bandwidth
- limited length: 802.3 specifies maximum cable length
- large "collision domain" (can collide with many stations)

# Hubs

- Physical Layer devices: essentially repeaters operating at bit levels: repeat received bits on one interface to all other interfaces
- Hubs can be arranged in a hierarchy (or multi-tier design), with backbone hub at its top



# Hubs (more)

- Each connected LAN referred to as LAN **segment**
- Hubs do not isolate collision domains: node may collide with any node residing at any segment in LAN
- Hub Advantages:
  - simple, inexpensive device
  - Multi-tier provides graceful degradation: portions of the LAN continue to operate if one hub malfunctions
  - extends maximum distance between node pairs (100m per Hub)

# Hub limitations

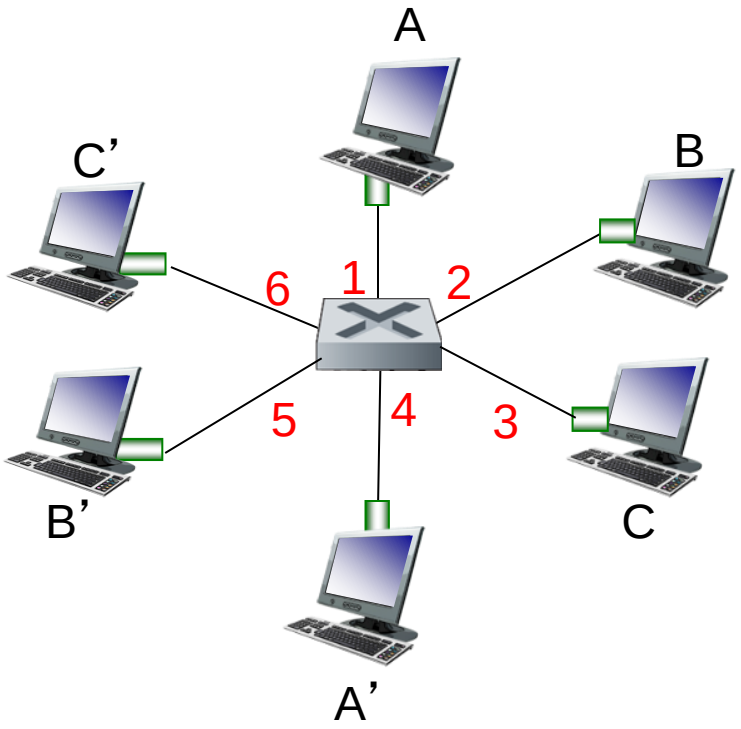
- single collision domain results in no increase in max throughput
  - multi-tier throughput same as single segment throughput
- individual LAN restrictions pose limits on number of nodes in same collision domain and on total allowed geographical coverage
- cannot connect different Ethernet types (e.g., 10BaseT and 100baseT)

# Ethernet switch

- link-layer device: takes an *active* role
  - store, forward Ethernet frames
  - examine incoming frame's MAC address, selectively forward frame to one-or-more outgoing links when frame is to be forwarded on segment, uses CSMA/CD to access segment
- *transparent*
  - hosts are unaware of presence of switches
- *plug-and-play, self-learning*
  - switches do not need to be configured

# Switch: *multiple* simultaneous transmissions

- hosts have dedicated, direct connection to switch
- switches buffer packets
- Ethernet protocol used on *each* incoming link, but no collisions; full duplex
  - each link is its own collision domain
- *switching:* A-to-A' and B-to-B' can transmit simultaneously, without collisions




*switch with six interfaces (1,2,3,4,5,6)*

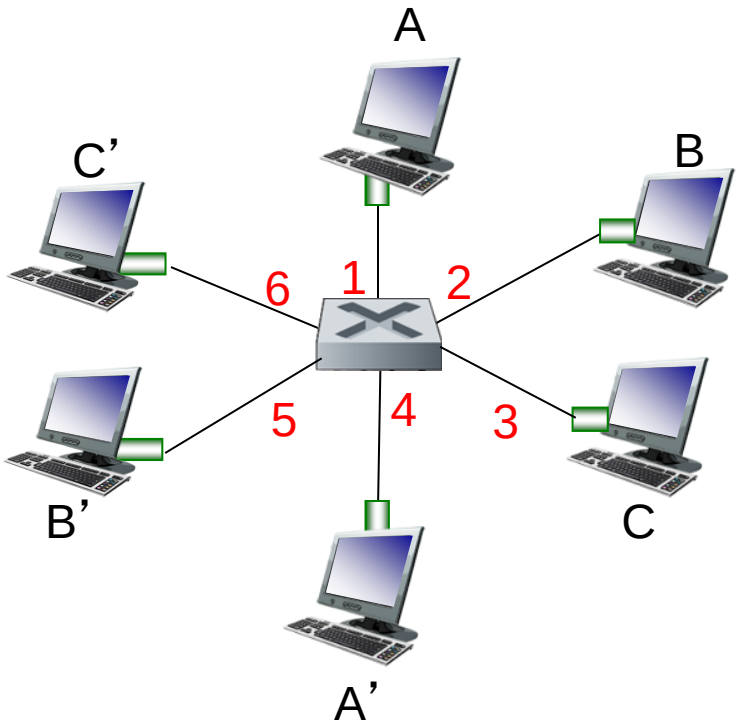
# Switch forwarding table

Q: how does switch know A' reachable via interface 4, B' reachable via interface 5?

- A: each switch has a switch table, each entry:
  - (MAC address of host, interface to reach host, time stamp)
  - looks like a routing table!

Q: how are entries created, maintained in switch table?

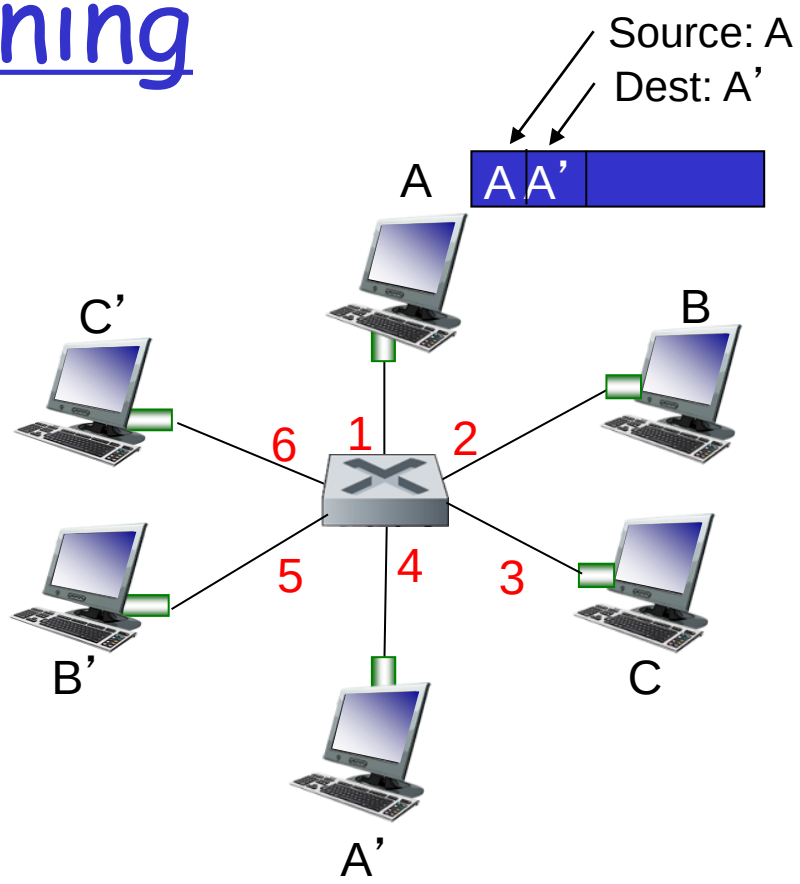
- something like a routing protocol?




*switch with six interfaces (1,2,3,4,5,6)*

# Switch: self-learning

- switch *learns* which hosts can be reached through which interfaces
  - when frame received, switch "learns" location of sender: incoming LAN segment
  - records sender/location pair in switch table




| MAC addr | interface | TTL |
|---|---|---|
| *A* | *1* | *60* |

*Switch table (initially empty)*

# Switch: frame filtering/forwarding

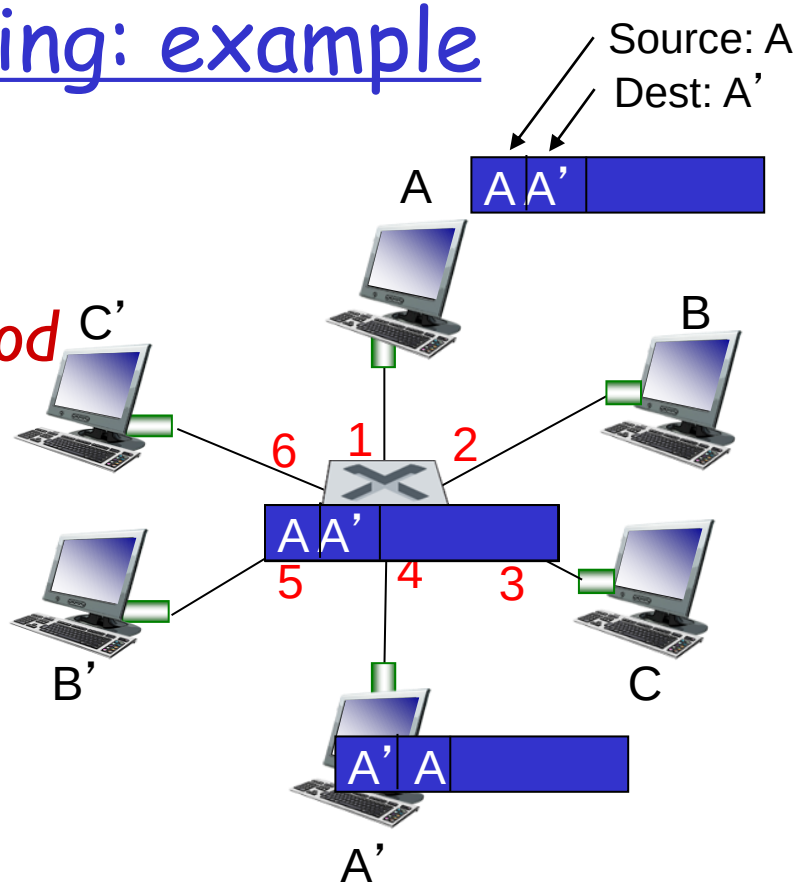
when frame received at switch:

1. record incoming link, MAC address of sending host
2. index switch table using MAC destination address
3. if entry found for destination
   then {
   if destination on segment from which frame arrived
   then drop frame
   else forward frame on interface indicated by entry
   }
   else flood /* forward on all interfaces except arriving
   interface */

# Self-learning, forwarding: example

- frame destination, A', location unknown: *flood*
- destination A location known:

  selectively send on just one link

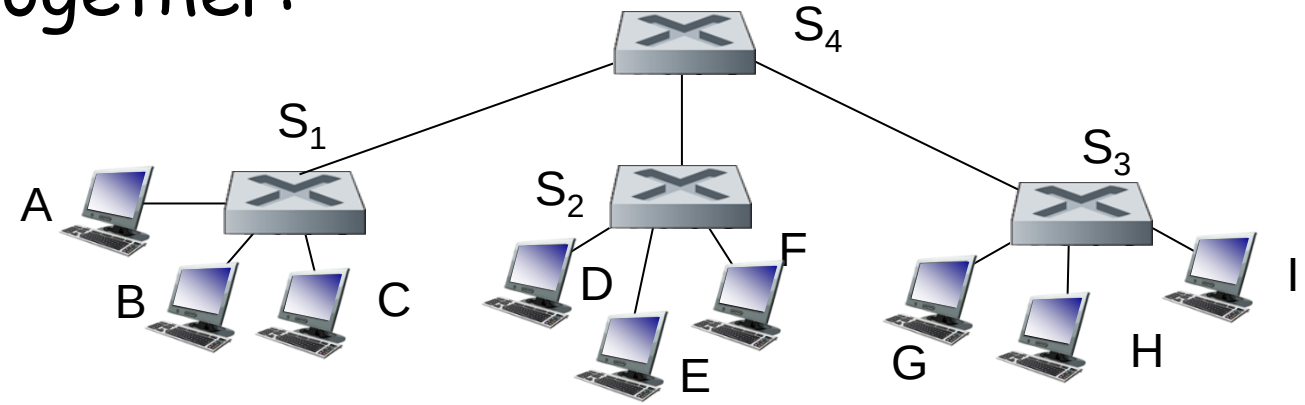



| MAC addr | interface | TTL |
|---|---|---|
| *A* | *1* | *60* |
| *A'* | *4* | *60* |

*switch table (initially empty)*

# Interconnecting switches

self-learning switches can be connected together:

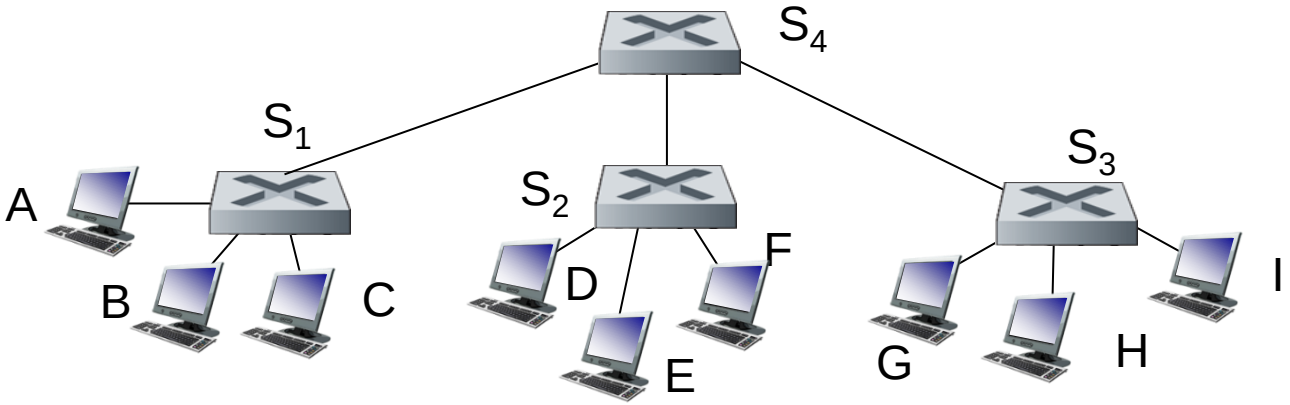



Q: sending from A to G - how does $S_1$ know to forward frame destined to G via $S_4$ and $S_3$?

- A: self learning! (works exactly the same as in single-switch case!)

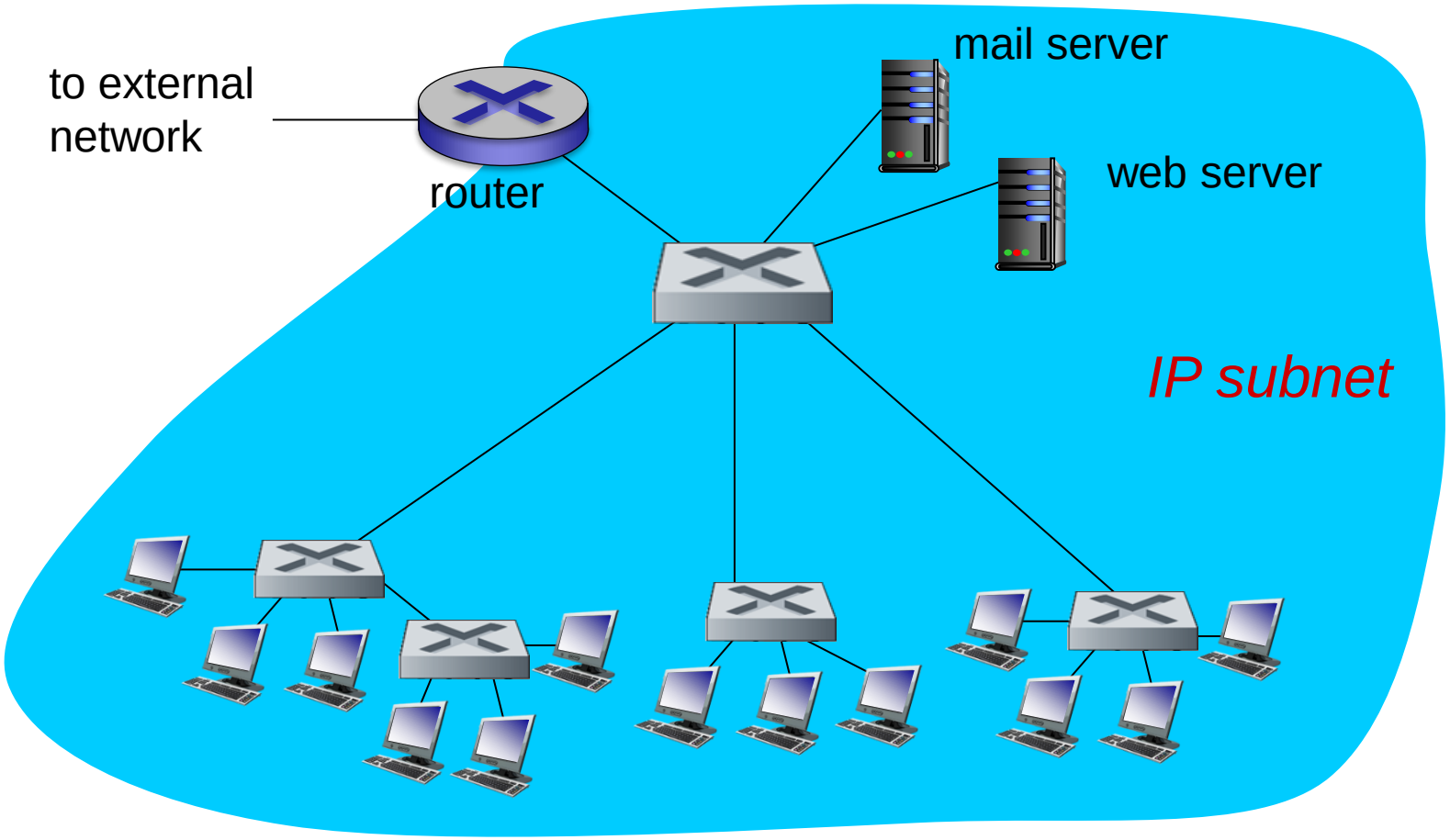
# Self-learning multi-switch example

Suppose C sends frame to I, I responds to C




- Q: show switch tables and packet forwarding in $S_1$, $S_2$, $S_3$, $S_4$

# Institutional network



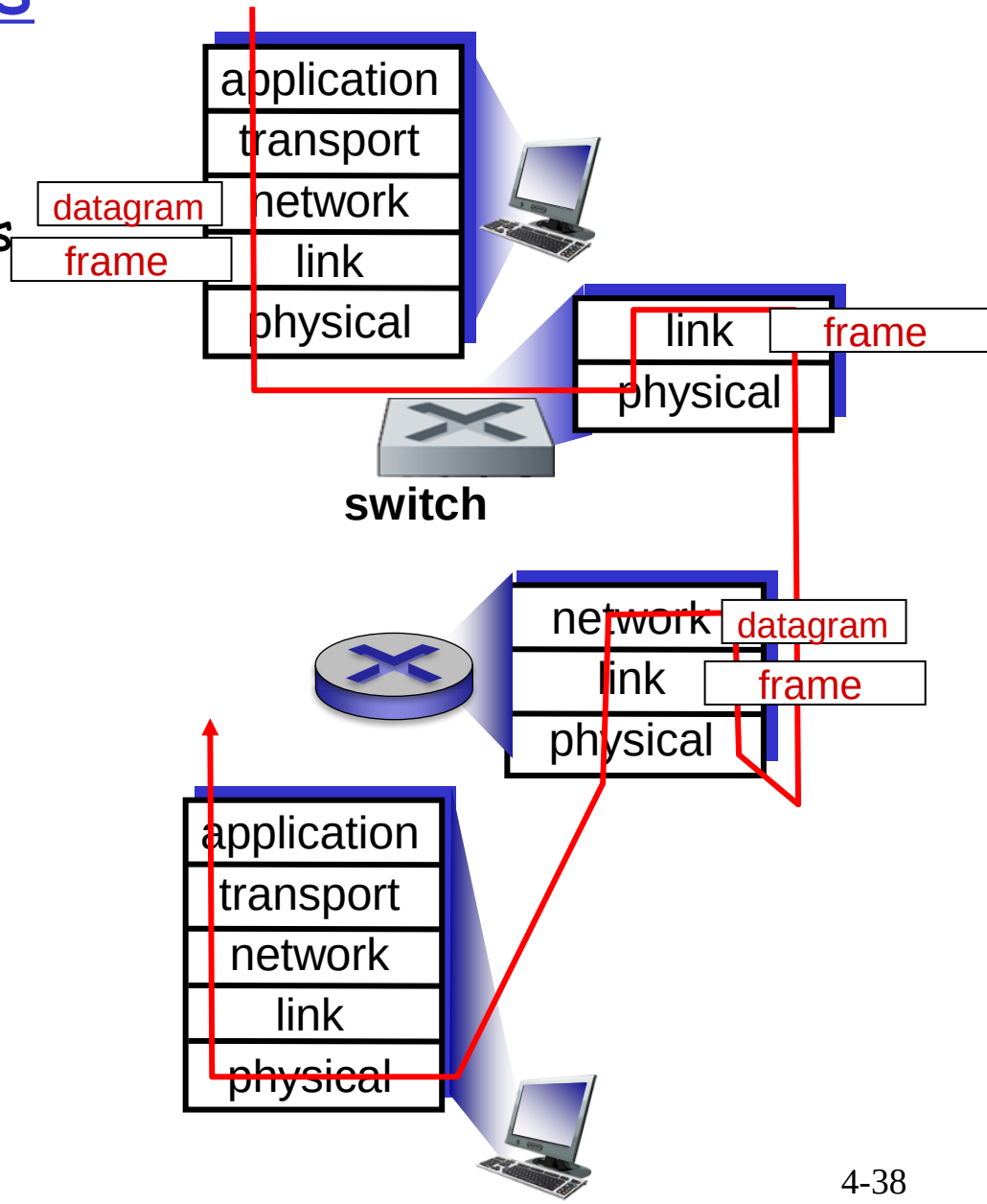
# Switches vs. routers

both are store-and-forward:

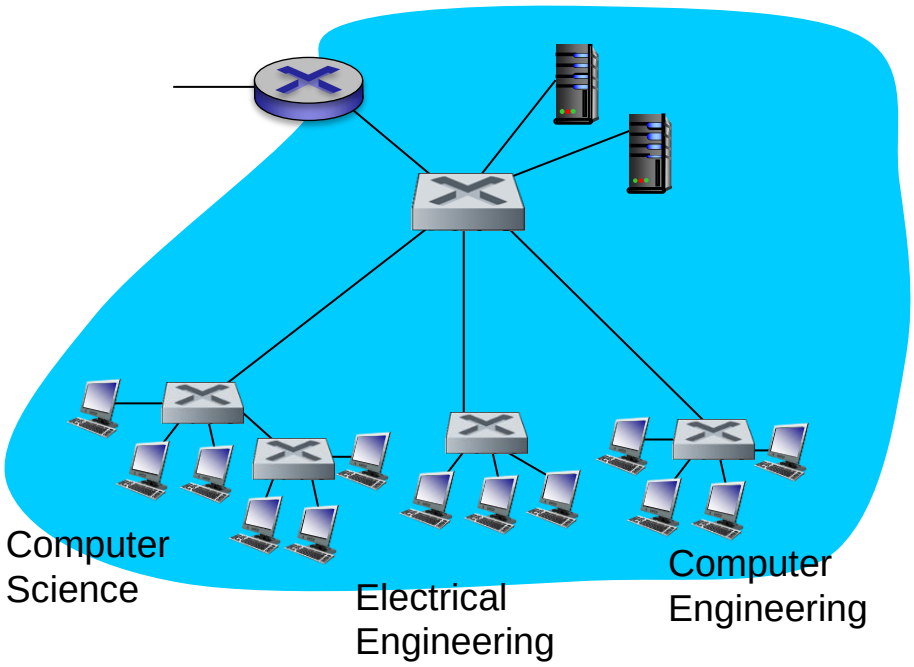
- *routers:* network-layer devices (examine network-layer headers)
- *switches:* link-layer devices (examine link-layer headers)

both have forwarding tables:

- *routers:* compute tables using routing algorithms, IP addresses
- *switches:* learn forwarding table using flooding, learning, MAC addresses



# VLANs: motivation




*consider:*

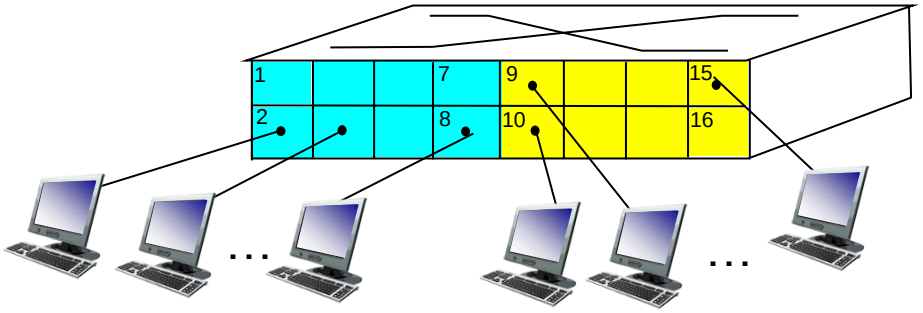
- CS user moves office to EE, but wants connect to CS switch?
- single broadcast domain:
  - all layer-2 broadcast traffic (ARP, DHCP, unknown location of destination MAC address) must cross entire LAN
  - security/privacy, efficiency issues

# VLANs

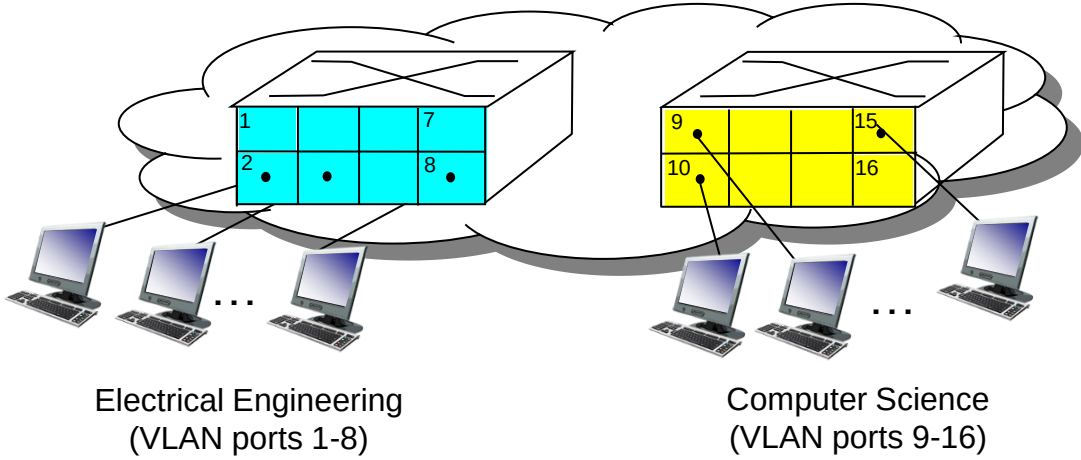
***Virtual Local Area Network***

switch(es) supporting VLAN capabilities can be configured to define multiple ***virtual*** LANS over single physical LAN infrastructure.

port-based VLAN: switch ports grouped (by switch management software) so that *single* physical switch ……

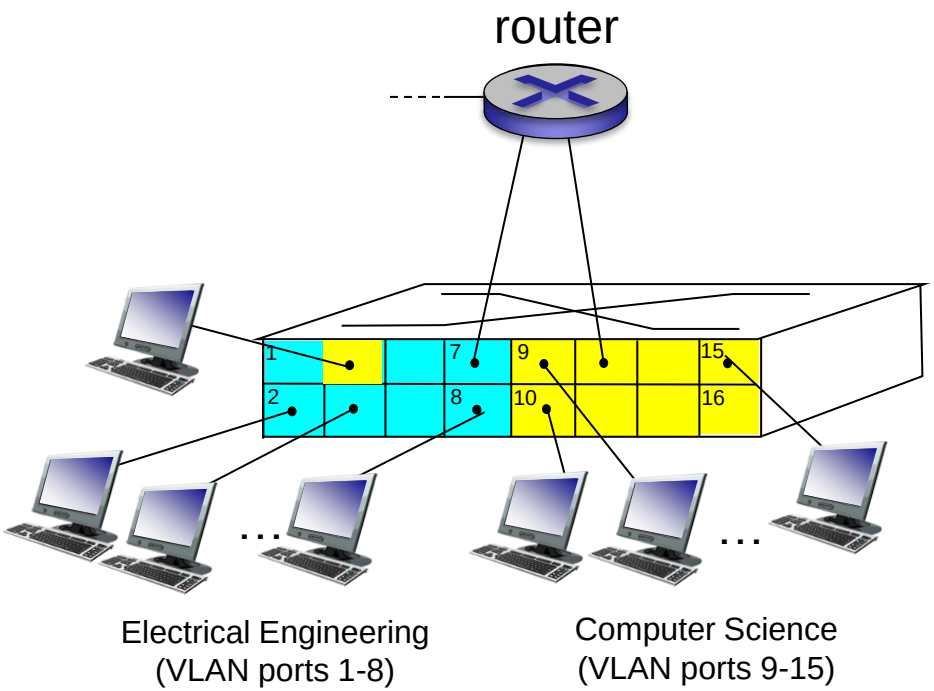



… operates as multiple virtual switches



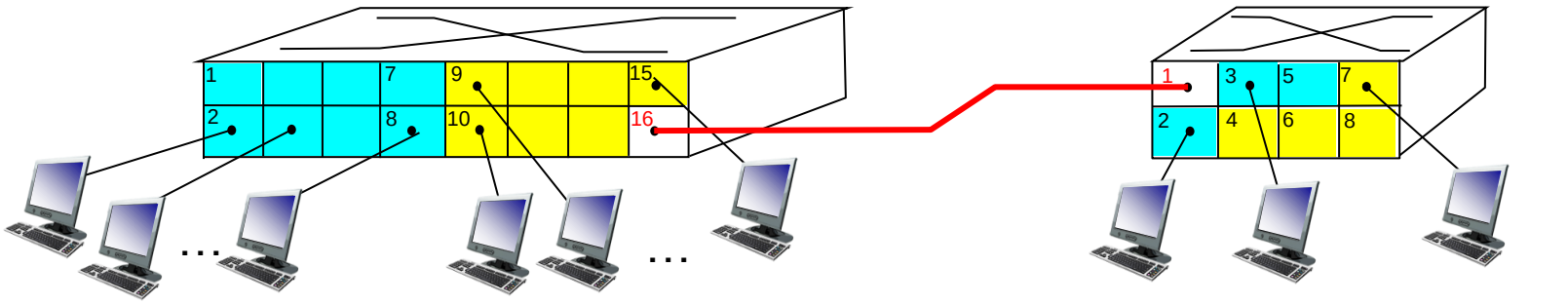
# Port-based VLAN

- *traffic isolation:* frames to/from ports 1-8 can *only* reach ports 1-8
  - can also define VLAN based on MAC addresses of endpoints, rather than switch port
- dynamic membership: ports can be dynamically assigned among VLANs



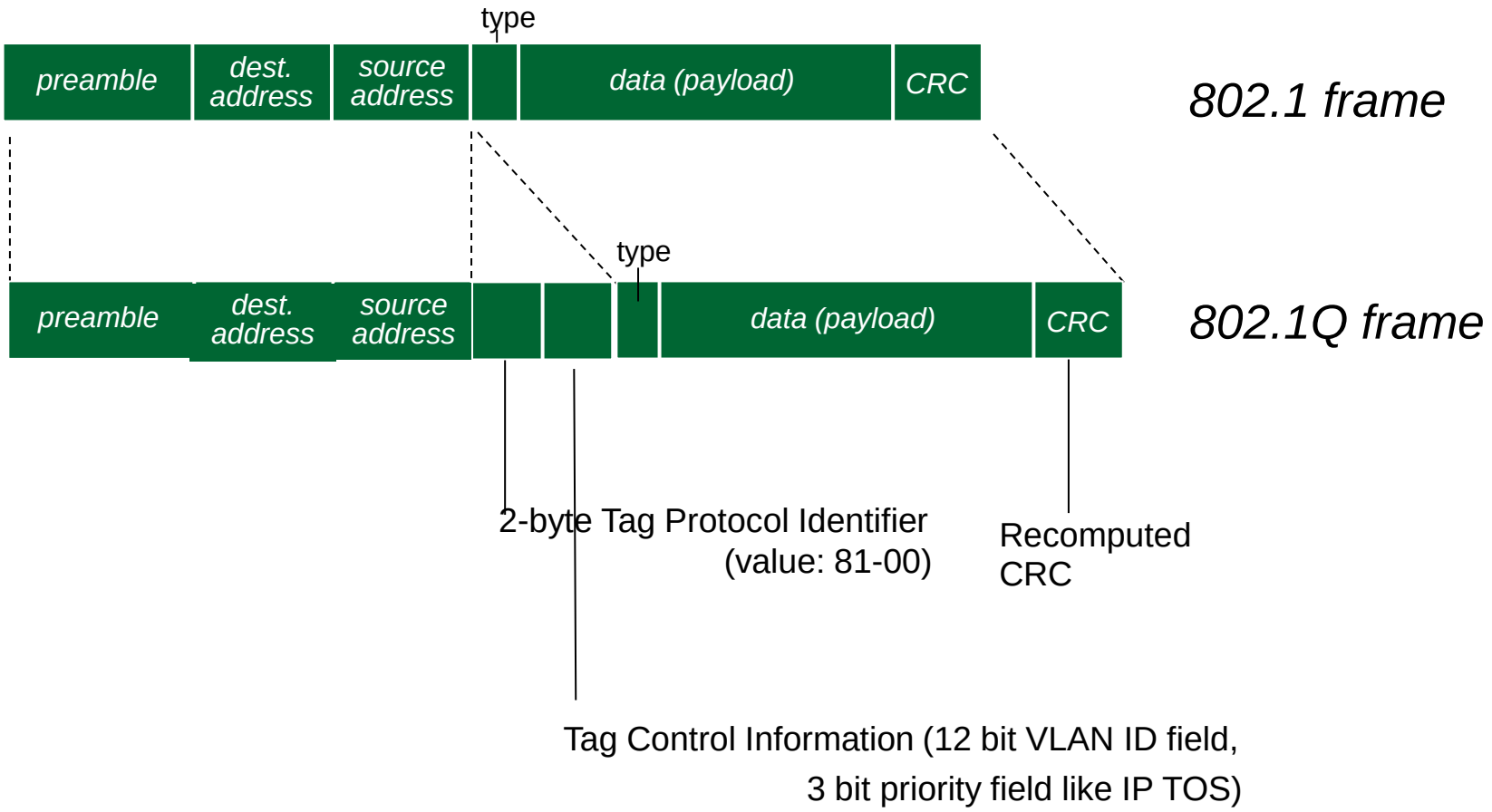

- forwarding between VLANS: done via routing (just as with separate switches)
  - in practice vendors sell combined switches plus routers

# VLANS spanning multiple switches




- *trunk port:* carries frames between VLANS defined over multiple physical switches
  - frames forwarded within VLAN between switches can't be vanilla 802.1 frames (must carry VLAN ID info)
  - 802.1q protocol adds/removed additional header fields for frames forwarded between trunk ports

# 802.1Q VLAN frame format



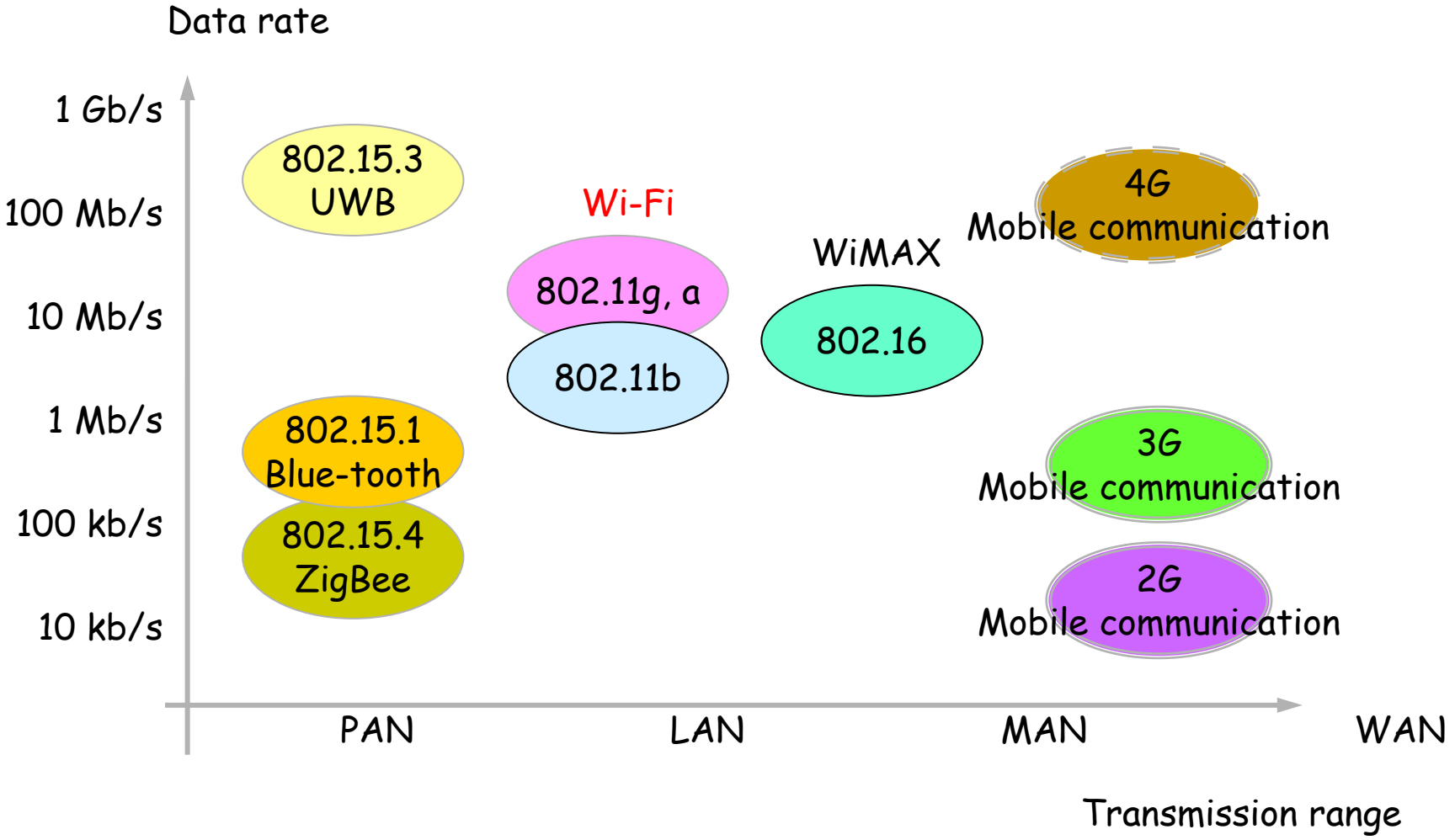
# Wireless communications

- the challenges of wireless communications
- wireless communication standards
- IEEE 802.11
- IEEE 802.15.4
- 5G?

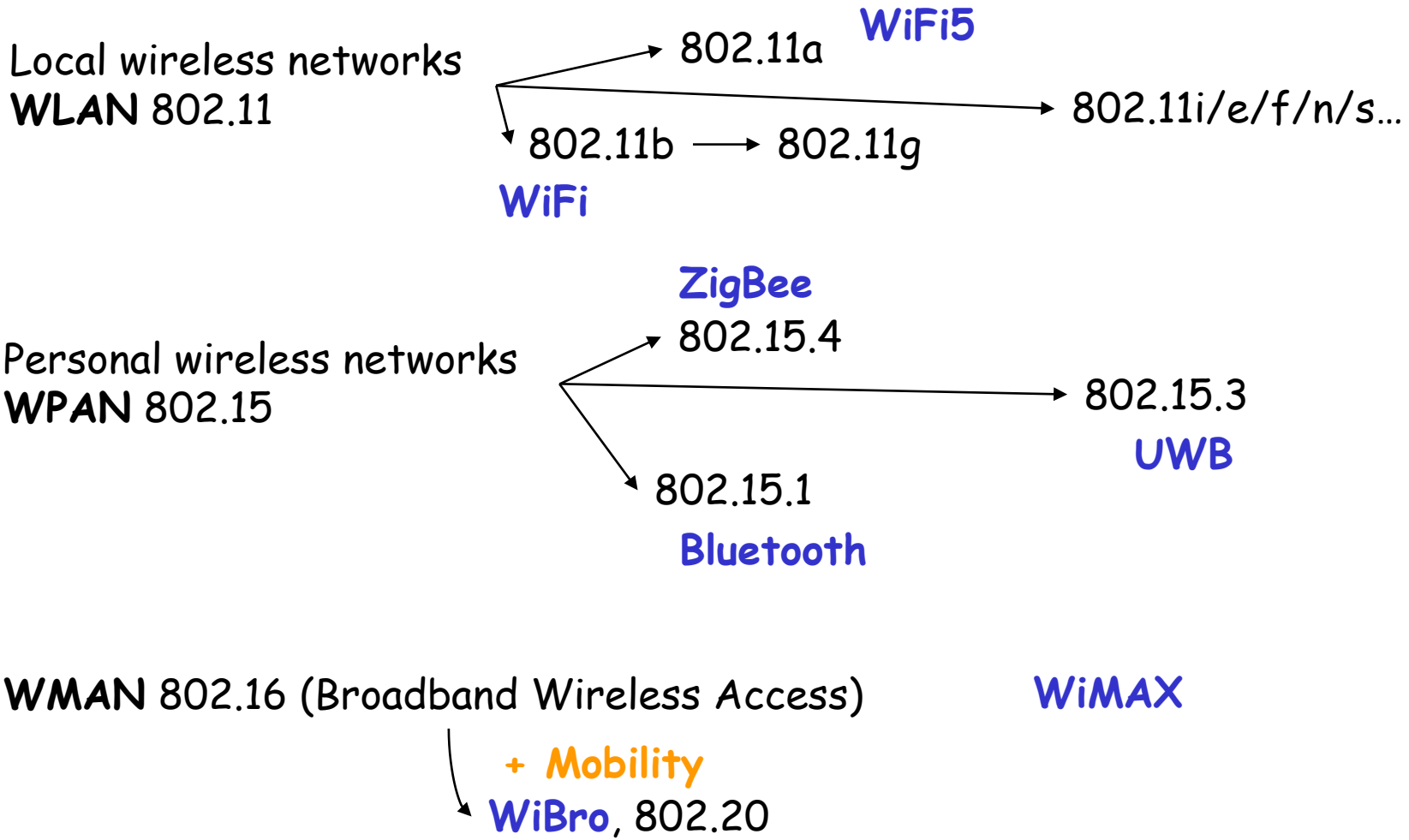
# the challenges of Wireless communications

- fading: path loss, multipath effect, shadow effect, Doppler effect
- interference: from other wireless communications
- hidden terminal problem
- security
- mobility

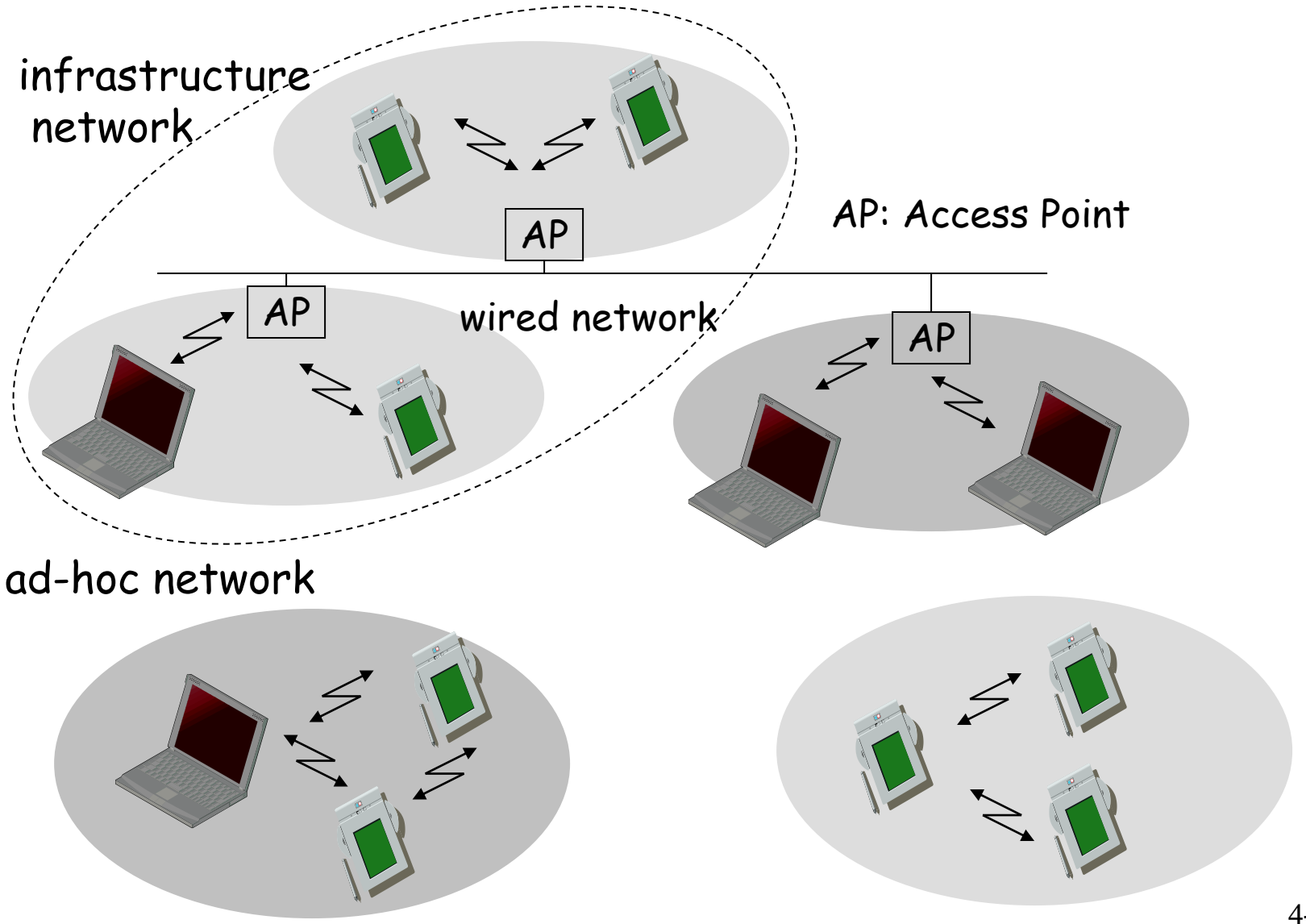
# Wireless communication technology



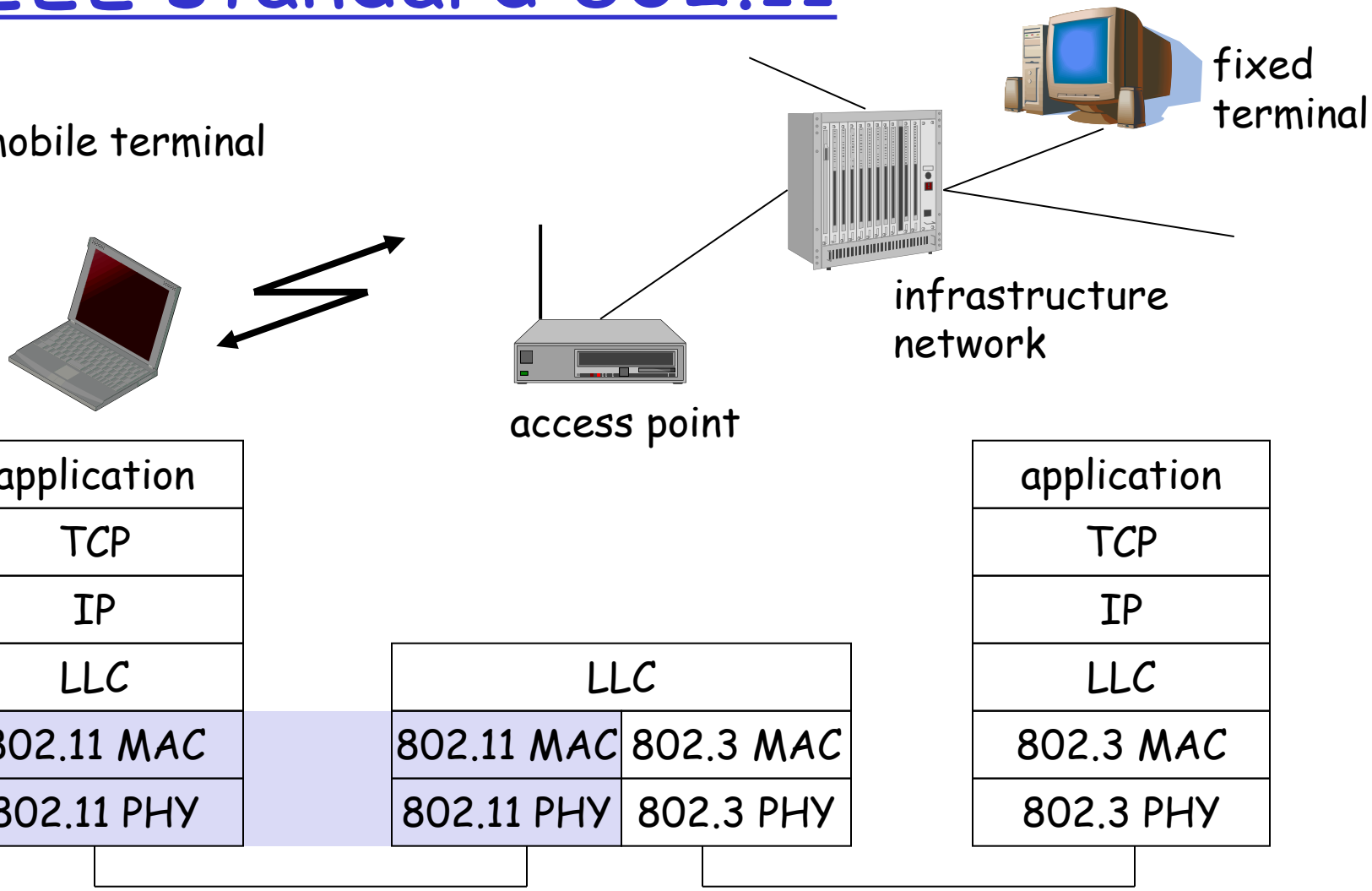
# IEEE Wireless Technology



# infrastructure vs. ad-hoc networks



# IEEE standard 802.11



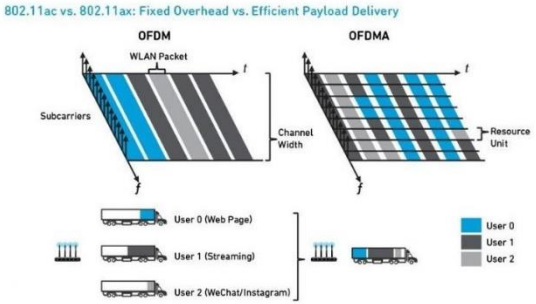
# IEEE 802.11 physical layer

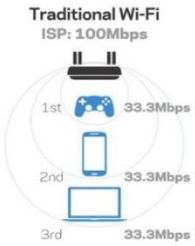
| WiFi 版本 | WiFi 标准 | 发布时间 | 最高速率 | 工作频段 |
|---|---|---|---|---|
| WiFi 7 | IEEE 802.11be | 2022年 | 30Gbits | 2.4GHz，5GHz，6GHz [4] |
| WiFi 6 | IEEE 802.11ax | 2019 年 | 11Gbps | 2.4GHz 或 5GHz |
| WiFi 5 | IEEE 802.11ac | 2014 年 | 1Gbps | 5GHz |
| WiFi 4 | IEEE 802.11n | 2009 年 | 600Mbps | 2.4GhHz 或 5GHz |
| WiFi 3 | IEEE 802.11g | 2003 年 | 54Mbps | 2.4GHz |
| WiFi 2 | IEEE 802.11b | 1999 年 | 11Mbps | 2.4GHz |
| WiFi 1 | IEEE 802.11a | 1999 年 | 54Mbps | 5GHz |
| WiFi 0 | IEEE 802.11 | 1997 年 | 2Mbps | 2.4GHz |

2.4GHz（802.11b/g/n/ax），5GHz（802.11a/n/ac/ax）

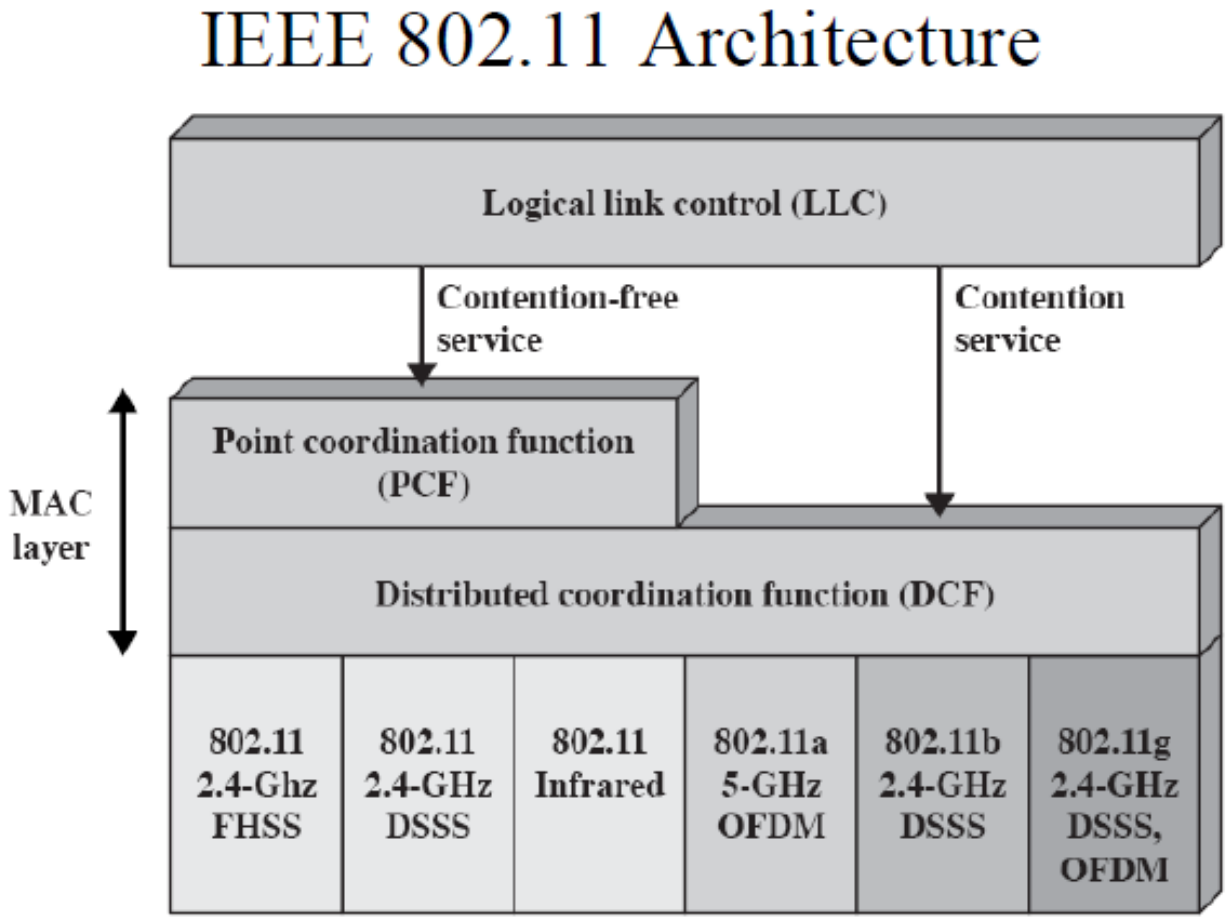
## WiFi 6

- OFDMA
- MU-MIMO
- 1024-QAM
- Spatial Reuse & BBS Coloring




# IEEE 802.11 protocol architecture




**IEEE 802.11 Protocol Architecture**

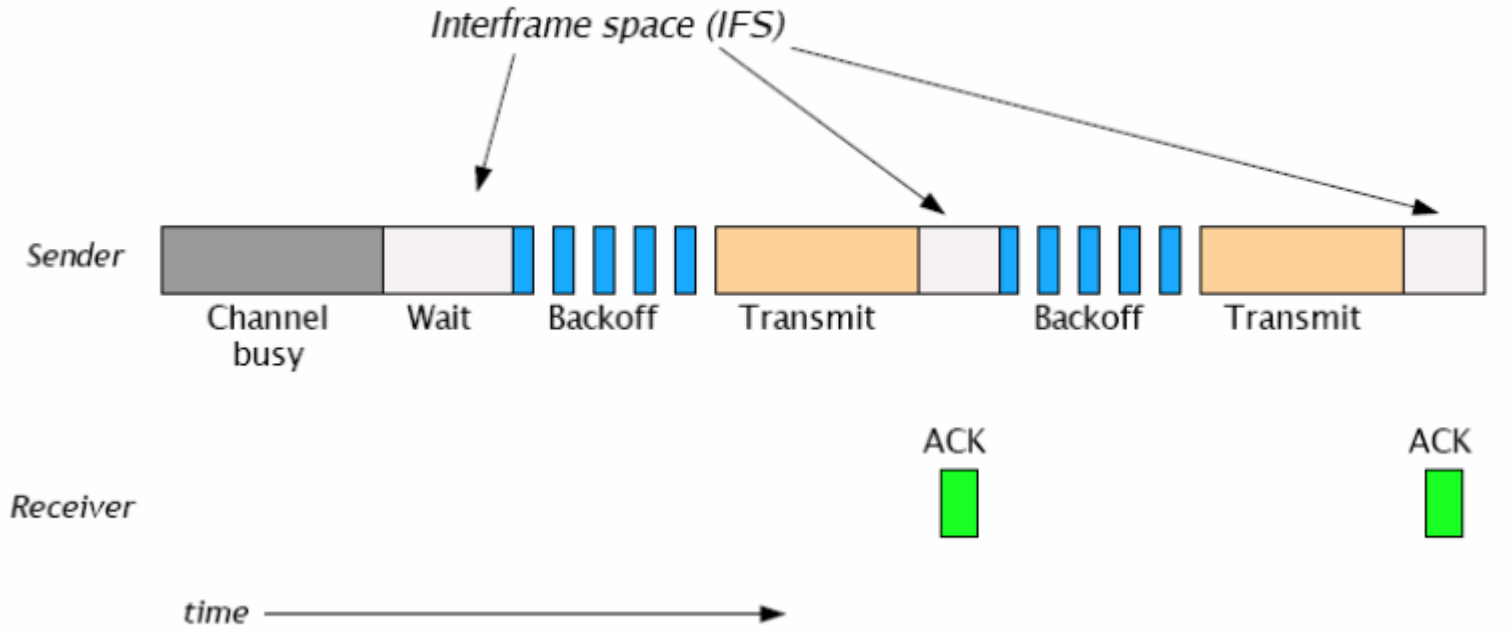
# 802.11 - MAC layer

- Traffic services
  - Asynchronous Data Service (mandatory)
    - implemented using DCF (Distributed Coordination Function)
  - Time-Bounded Service (optional)
    - implemented using PCF (Point Coordination Function)
- Access methods
  - DCF CSMA/CA (mandatory)
    - Distributed Wireless MAC
    - collision avoidance via randomized „back-off" mechanism
    - minimum distance between consecutive packets
    - ACK packet for acknowledgements (not for broadcasts)
  - DCF w/ RTS/CTS (optional)
    - avoids hidden terminal problem
  - PCF (optional)
    - access point polls terminals
    - Contention free

# 802.11 MAC functions

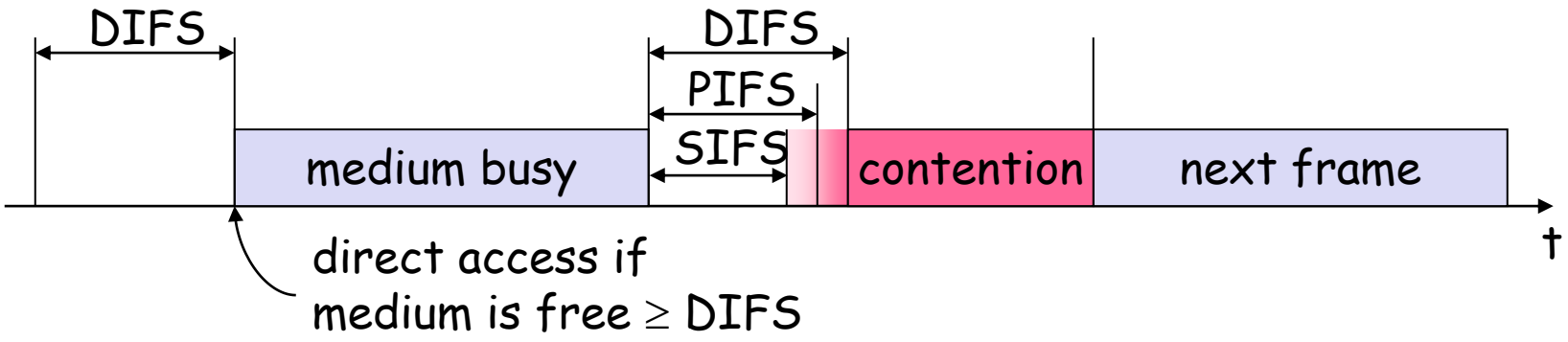
- MAC layer covers three functional areas:
  - Reliable data delivery
    - ACK-based scheme for reliability (receiver sends ACK after each successful transmission)
  - Medium access control
    - CSMA/CA; collision avoidance, not collision detection, Why? How?
  - Security
    - Wired Equivalent Privacy (WEP),WEP relies on a secret key being shared by end hosts and APs

# DCF CSMA/CA Illustrated

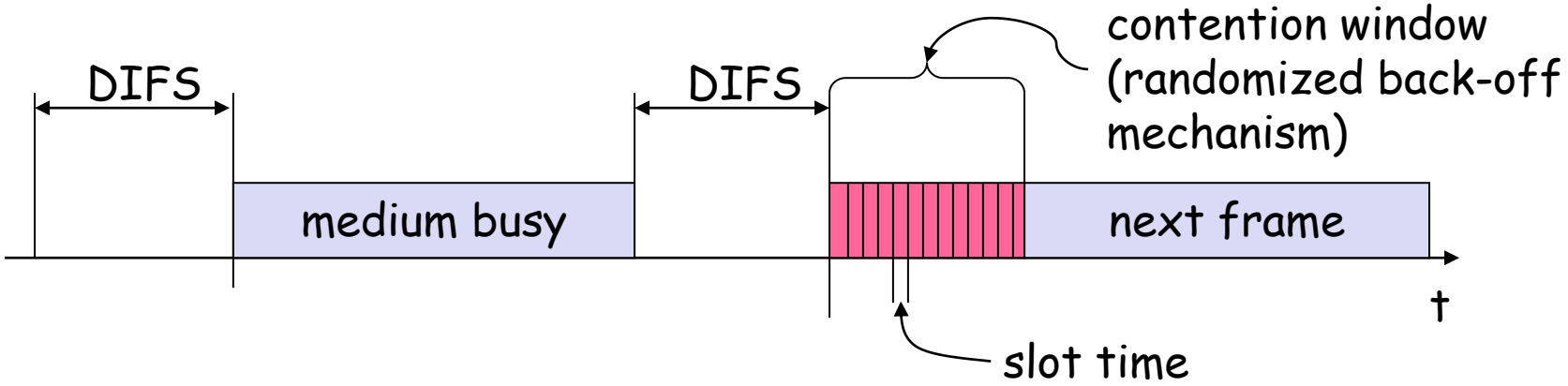


# 802.11 - MAC

- Priorities
  - defined through different inter frame spaces
  - SIFS (Short Inter Frame Spacing) :
    - 10µs (802.11b/g), 16 µs (802.11a)
    - High priority, for ACK, CTS, polling response
  - PIFS (PCF IFS) :
    - PIFS = SIFS + Slot time, which is 20 µs 802.11b, 9 µs 802.11a/g
    - medium priority, for time-bounded service using PCF
  - DIFS (DCF IFS):
    - DIFS = PIFS + Slot time
    - lowest priority, for asynchronous data service



# CSMA/CA access method

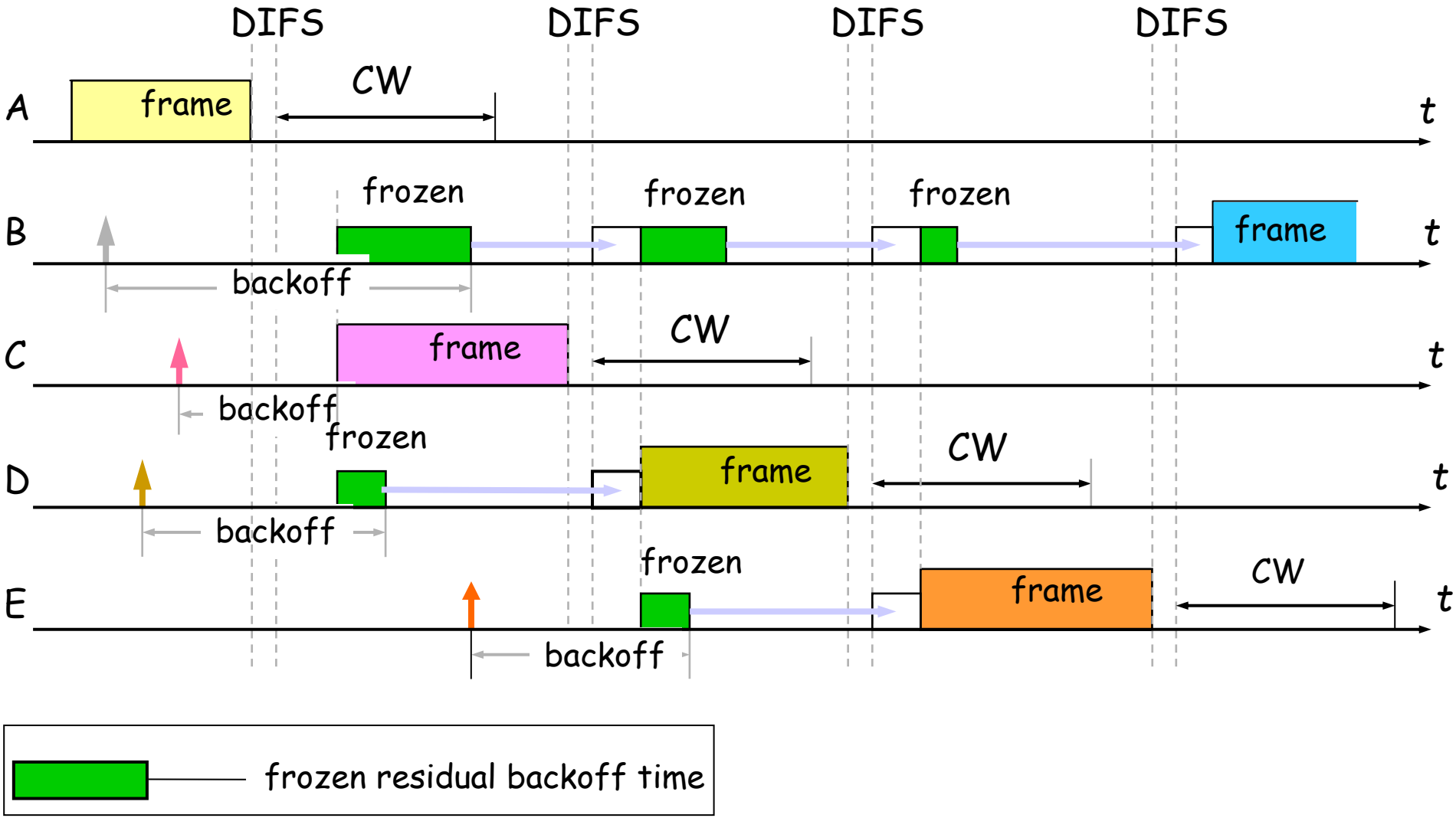



- station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
- if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- if the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
  - Slot time = 20 µs for 802.11b, 9 µs in 802.11a/g
  - CW_min = 16 for 802.11a, 32 for 802.11b
  - CW_max = 1024

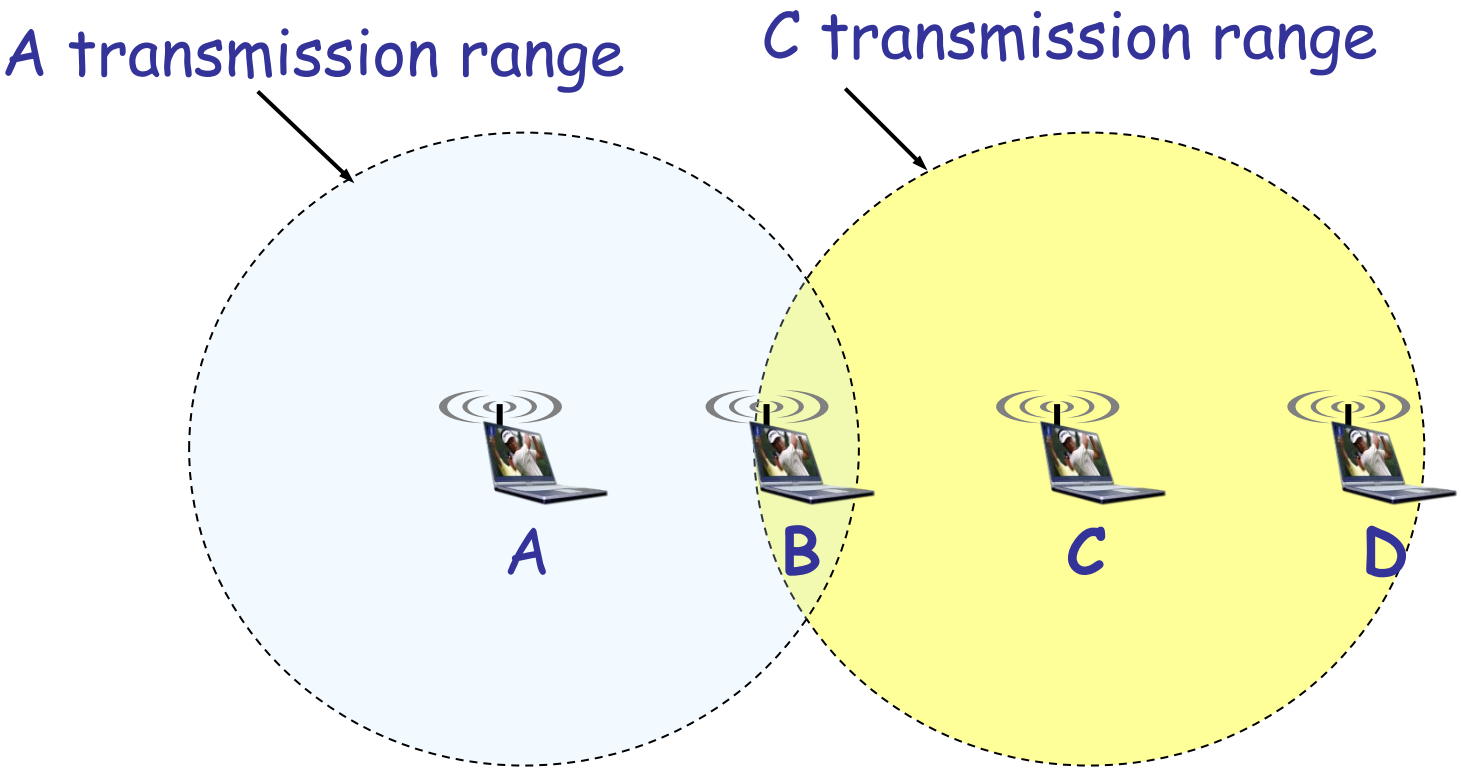
# CSMA/CA access method (Continued)

- If another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)
- When back-off timer reaches zero, start transmission
  - If more than one nodes decrement to zero at the same time, a collision will occur.
- If a collision occurs (missing ACK), the corresponding nodes double the CW size and choose their back-off time from the increase CW
- After successful transmission, CW size is reset to its min value.

# A simplified example

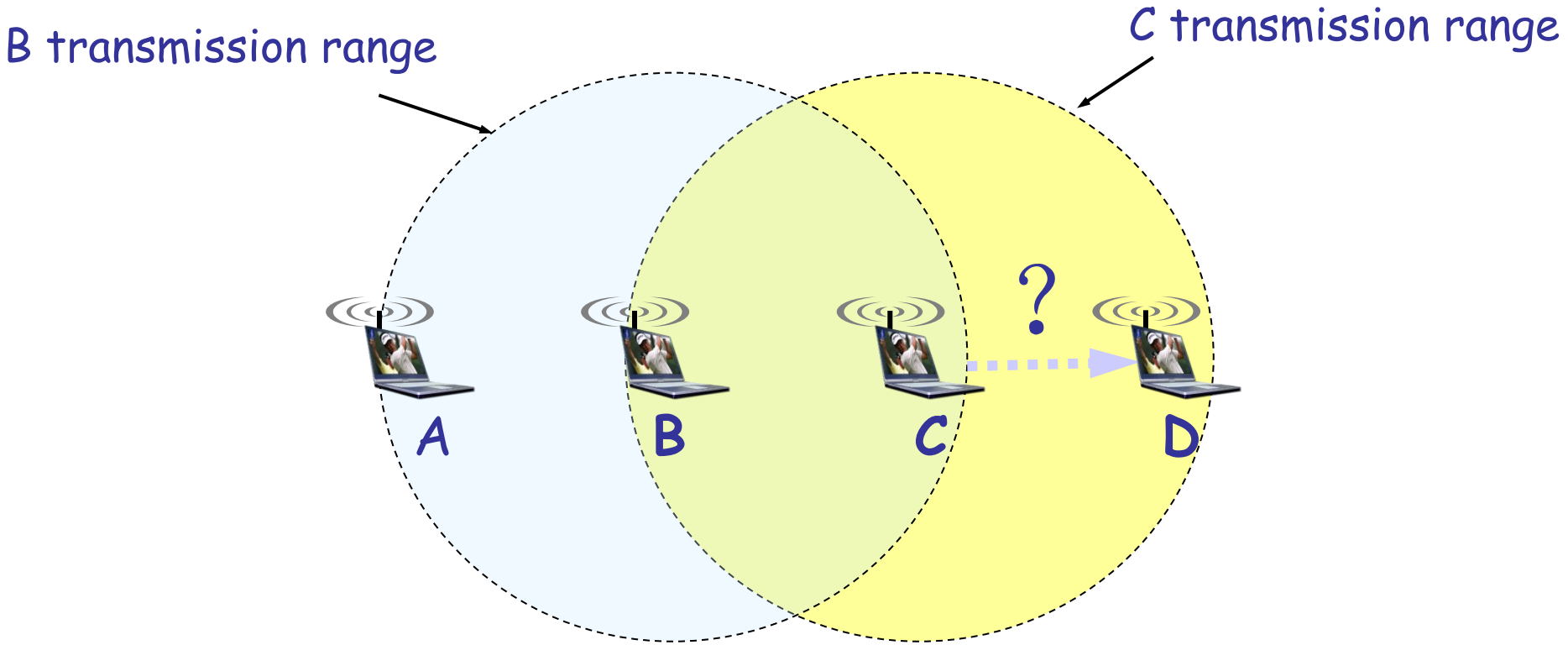


# LAN hidden terminal problem




A and C cannot hear each other and think B is idle, then, they both send data to B. A collision appears at the destination, B.

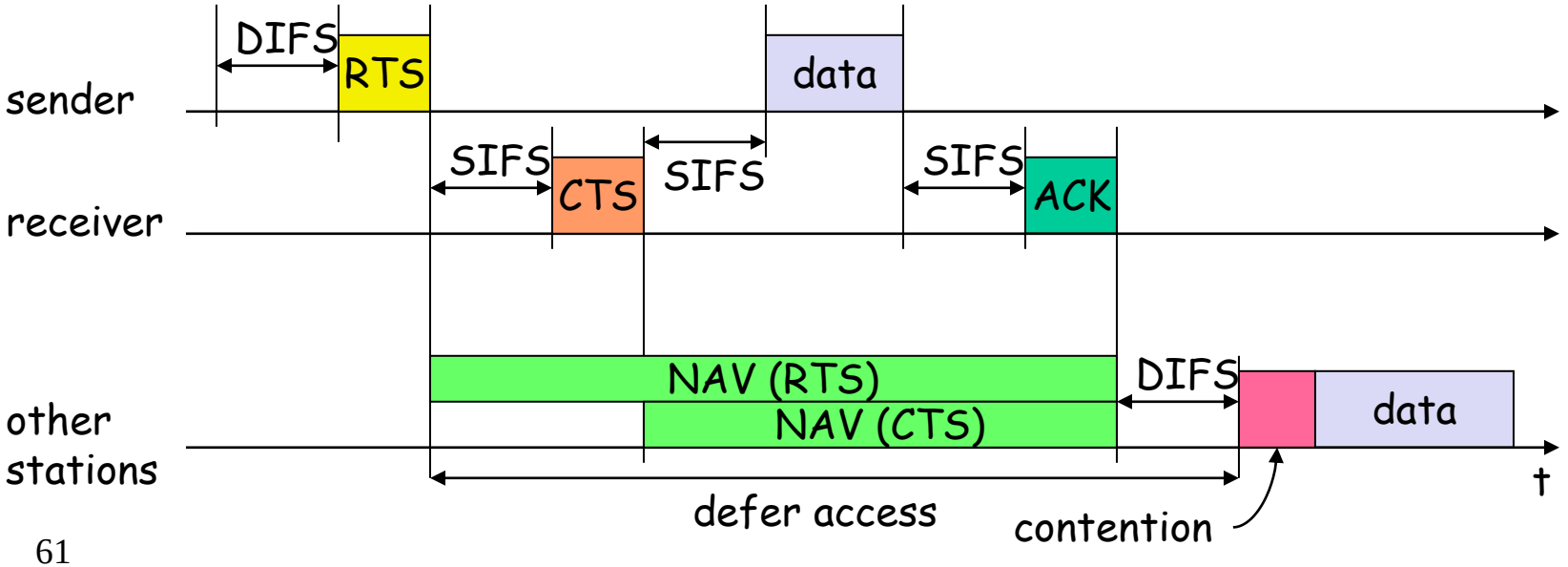
# LAN exposed terminal problem



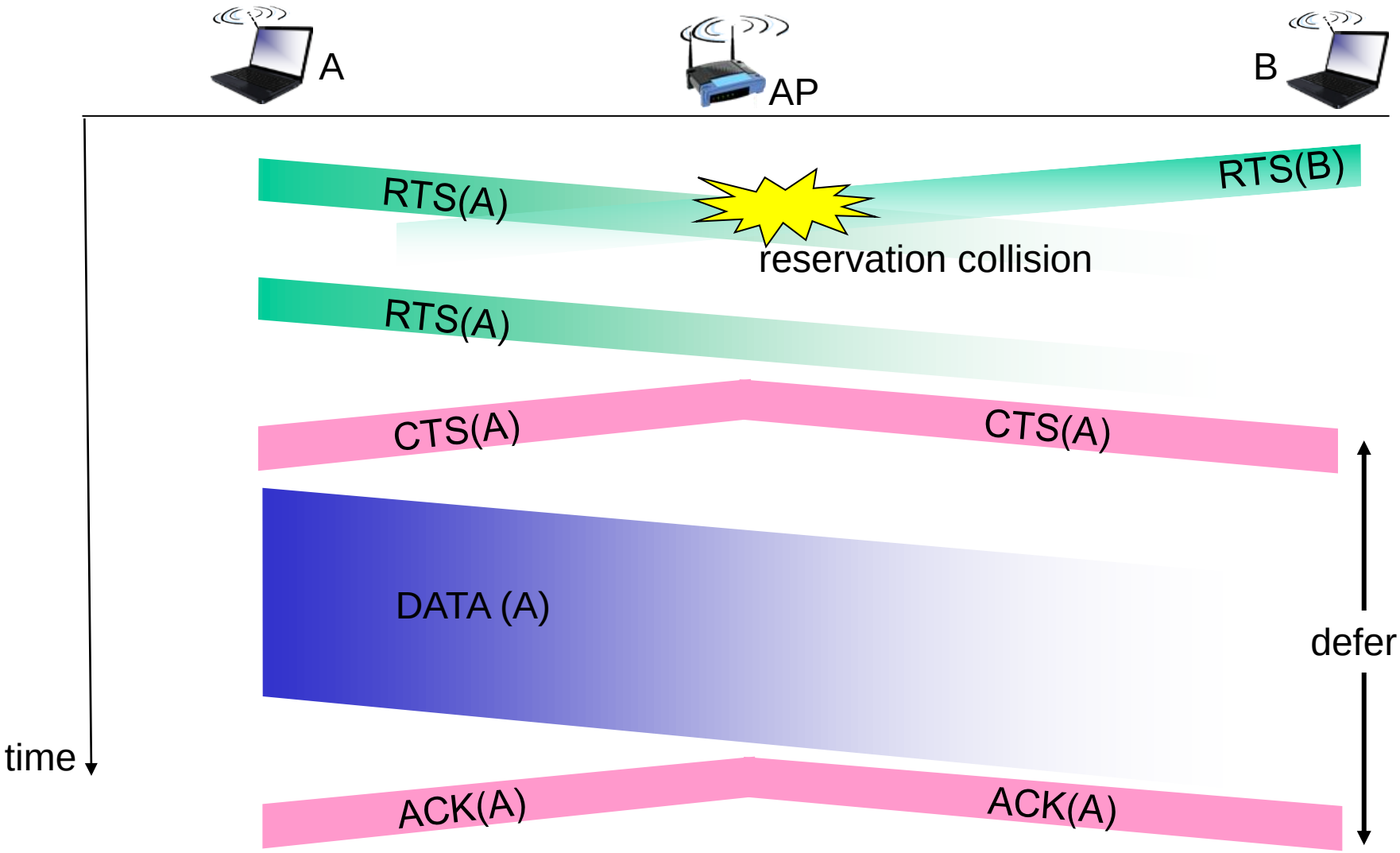

B is sending data to A. At the same time, C hopes to communication with D. But C senses a signal in the medium and dare not send the data.

# RTS/CTS

- Sending unicast packets
  - station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
  - acknowledgement via CTS after SIFS by receiver (if ready to receive)
  - other stations store medium reservations distributed via RTS and CTS
  - Two (potentially different) NAV groups



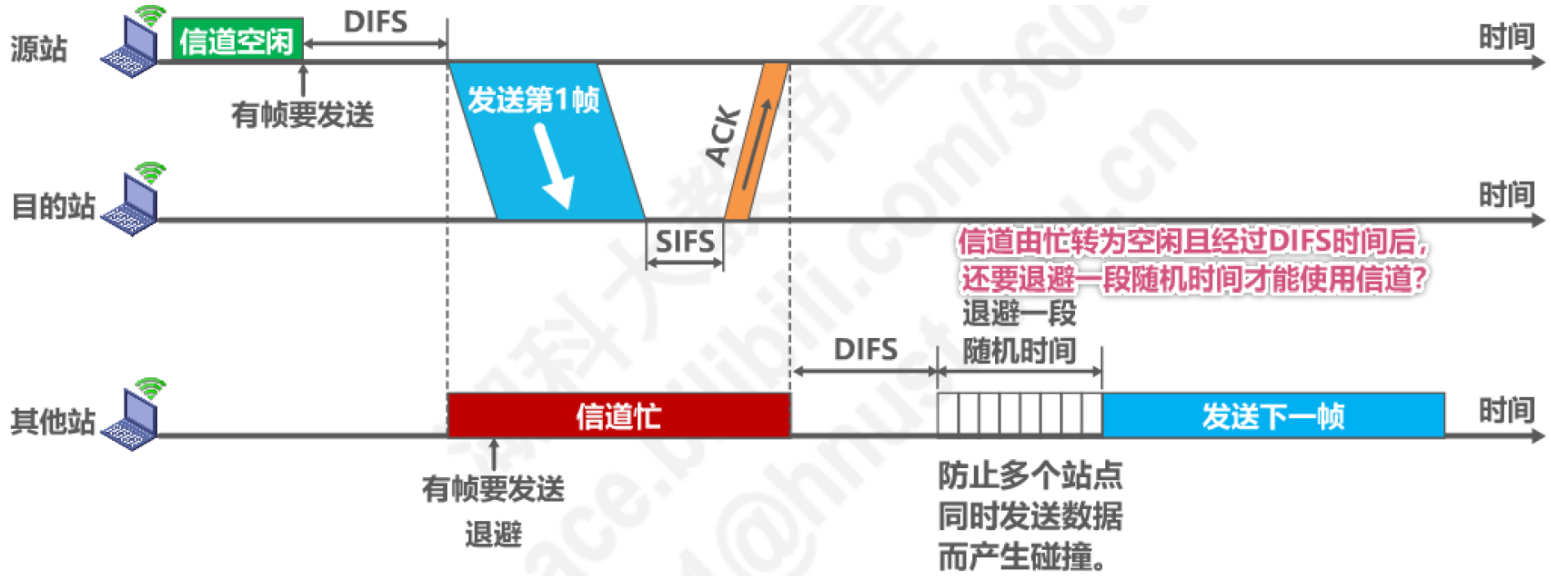
# Collision Avoidance: RTS-CTS exchange

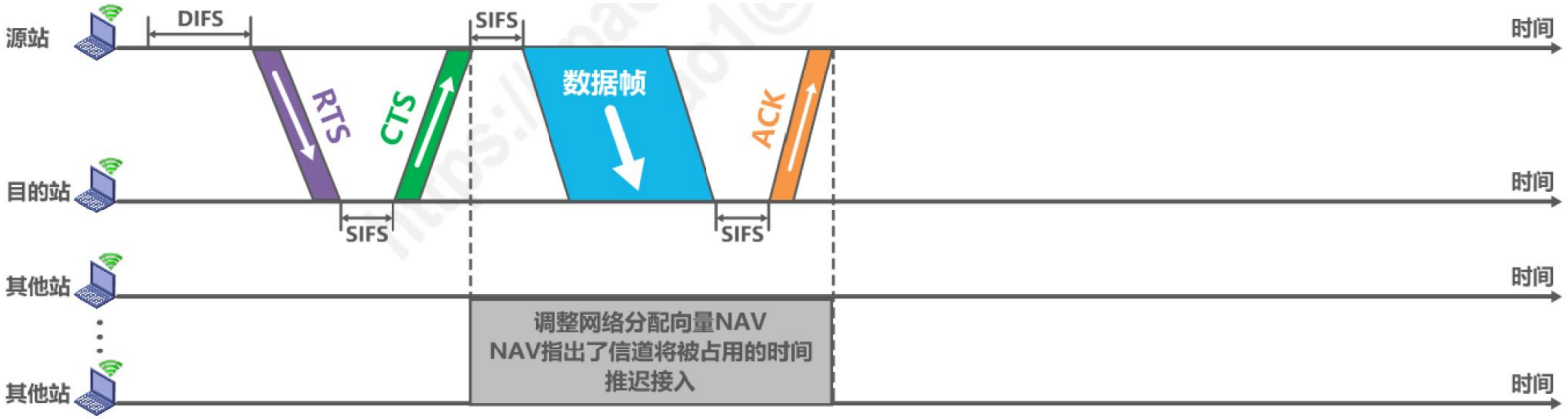


# RTS/CTS (Continued)

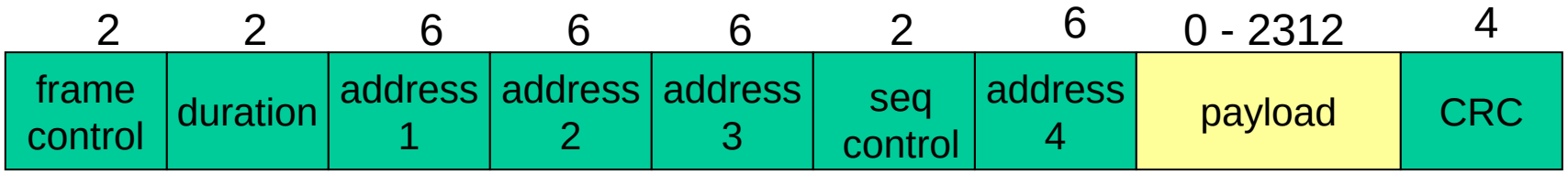
- Avoid hidden terminal problems
- Also, reduce bandwidth waste by collisions
  - Data frame can be as large as 2300bytes
  - RTS = 20bytes, CTS = 14bytes
  - The bigger is the data frame, the more advantageous
- Price : extended delay and more resource consumption!
- RTS threshold
  - Enable RTS/CTS for frames which are bigger than RTS threshold
  - Each node's decision

# CSMA/CA access method



# 802.11 frame: addressing



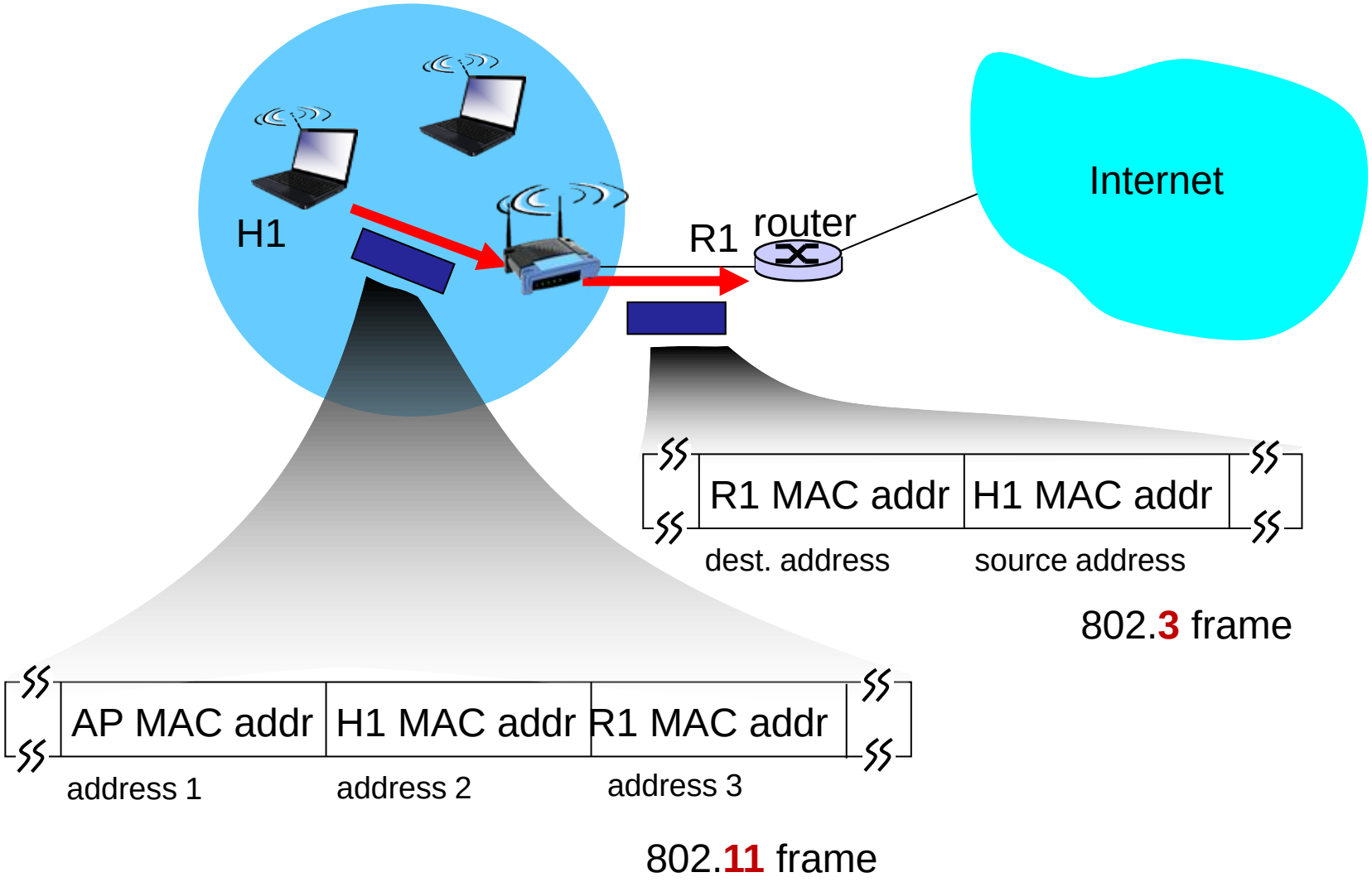

Address 1: MAC address of wireless host or AP to receive this frame

Address 2: MAC address of wireless host or AP transmitting this frame

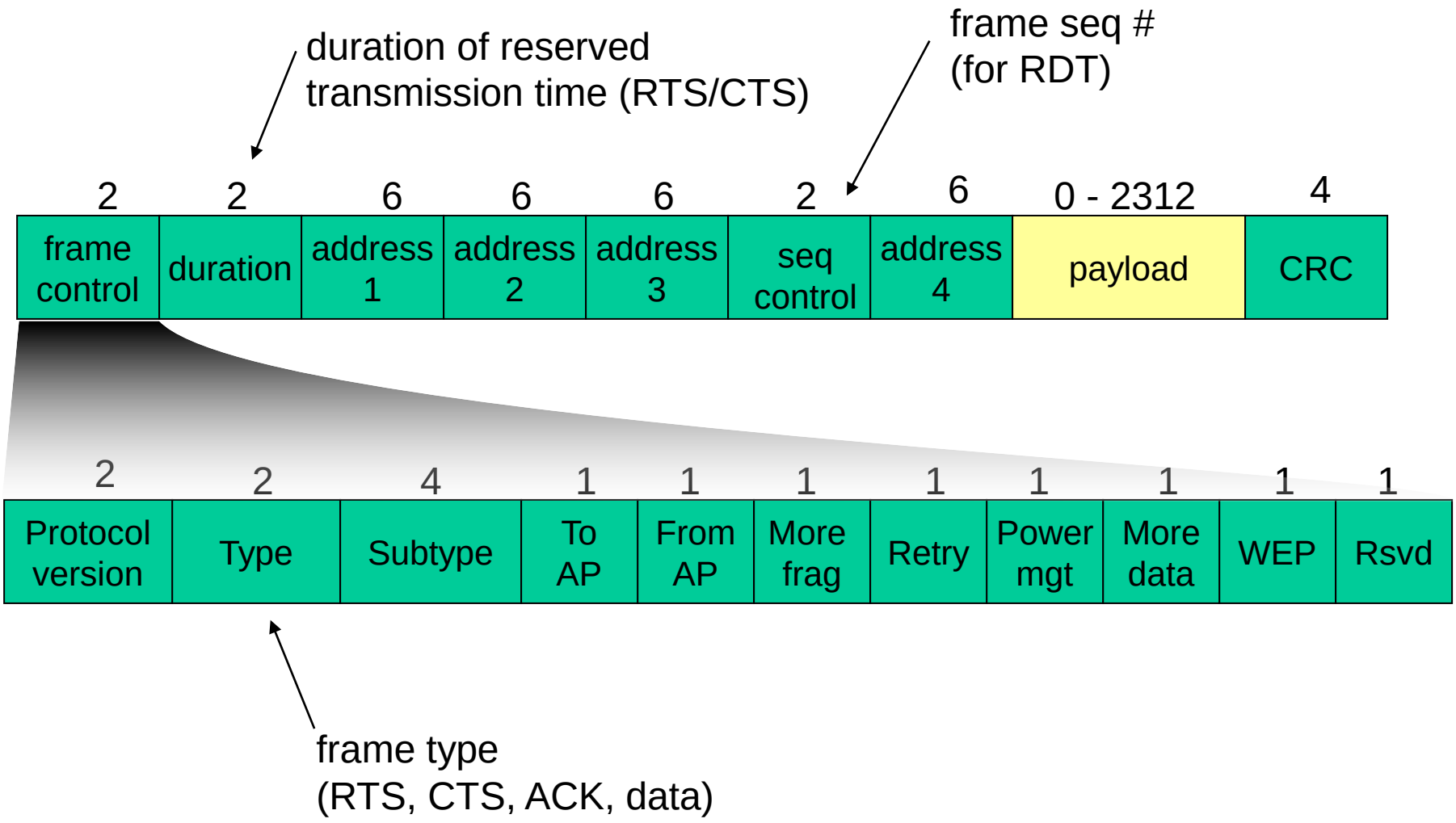
Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

# 802.11 frame: addressing

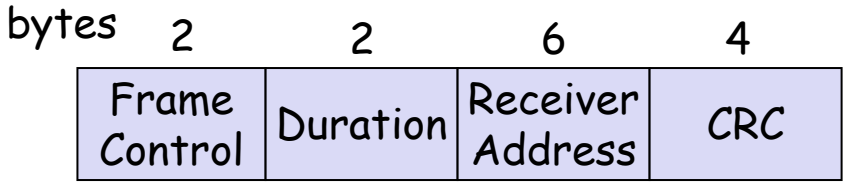


# 802.11 frame: more

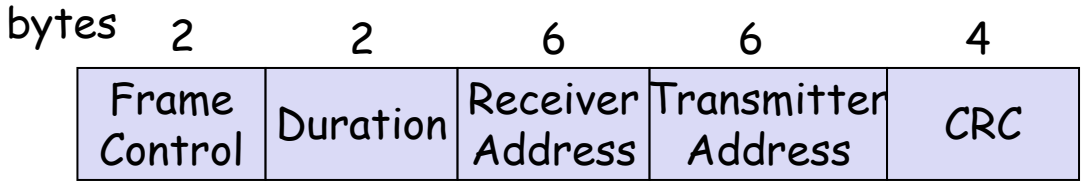


# Special Frames: ACK, RTS, CTS

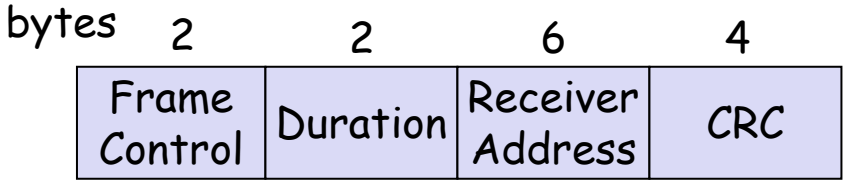
- Acknowledgement ACK



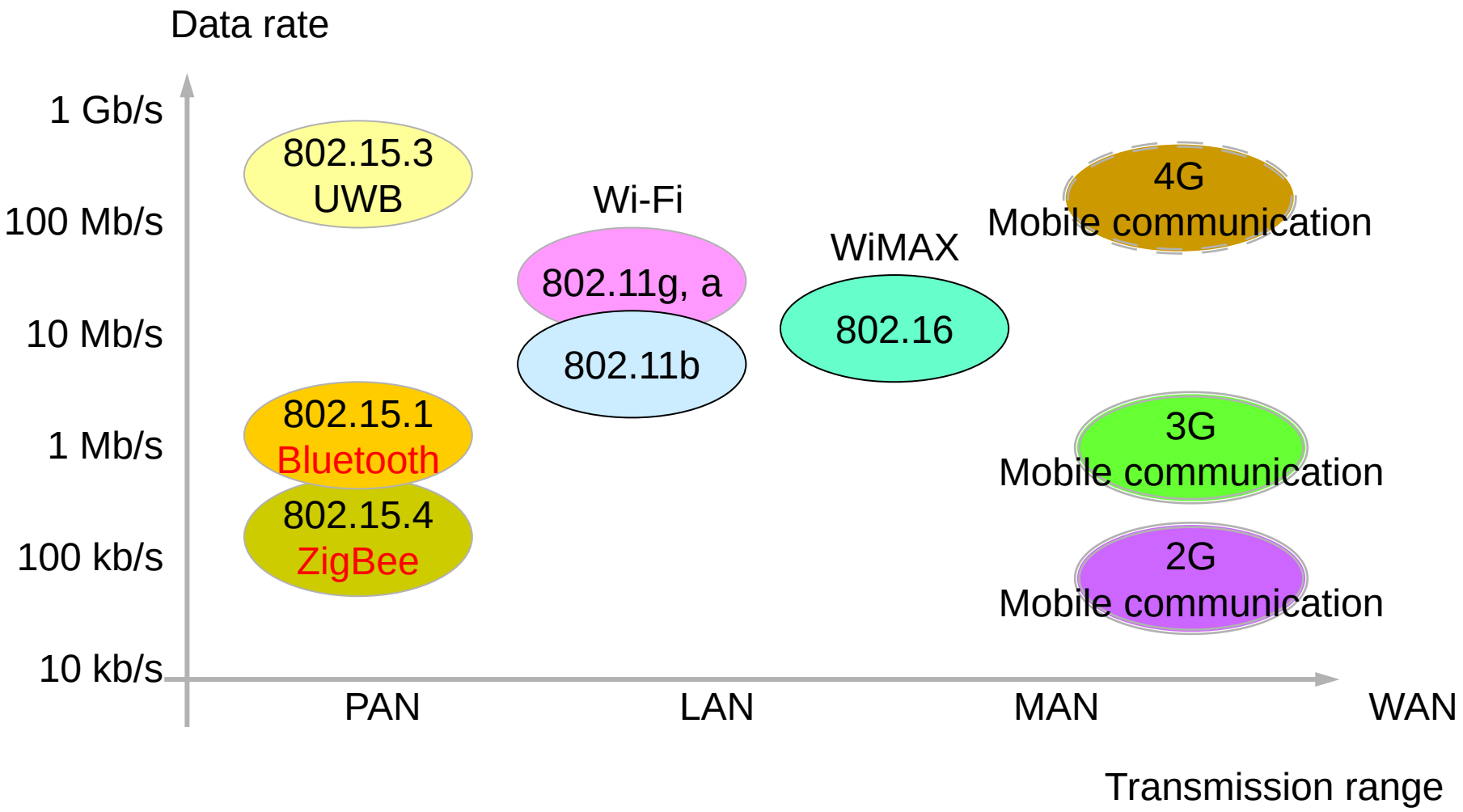

- Request To Send RTS




- Clear To Send CTS



# Wireless communication technology



# Wireless standards

| Market Name | ZigBee® | --- | Wi-Fi™ | Bluetooth™ |
|---|---|---|---|---|
| Standard | 802.15.4 | GSM/GPRS CDMA/1xRTT | 802.11b | 802.15.1 |
| Application Focus | Monitoring & Control | Wide Area Voice & Data | Web, Email, Video | Cable Replacement |
| System Resources | 4KB - 32KB | 16MB+ | 1MB+ | 250KB+ |
| Battery Life (days) | 100 - 1,000+ | 1-7 | .5 - 5 | 1 - 7 |
| Network Size | Unlimited ($2^{64}$) | 1 | 32 | 7 |
| Bandwidth (KB/s) | 20 - 250 | 64 - 128+ | 11,000+ | 720 |
| Transmission Range (meters) | 1 - 100+ | 1,000+ | 1 - 100 | 1 - 10+ |
| Success Metrics | Reliability, Power, Cost | Reach, Quality | Speed, Flexibility | Cost, Convenience |

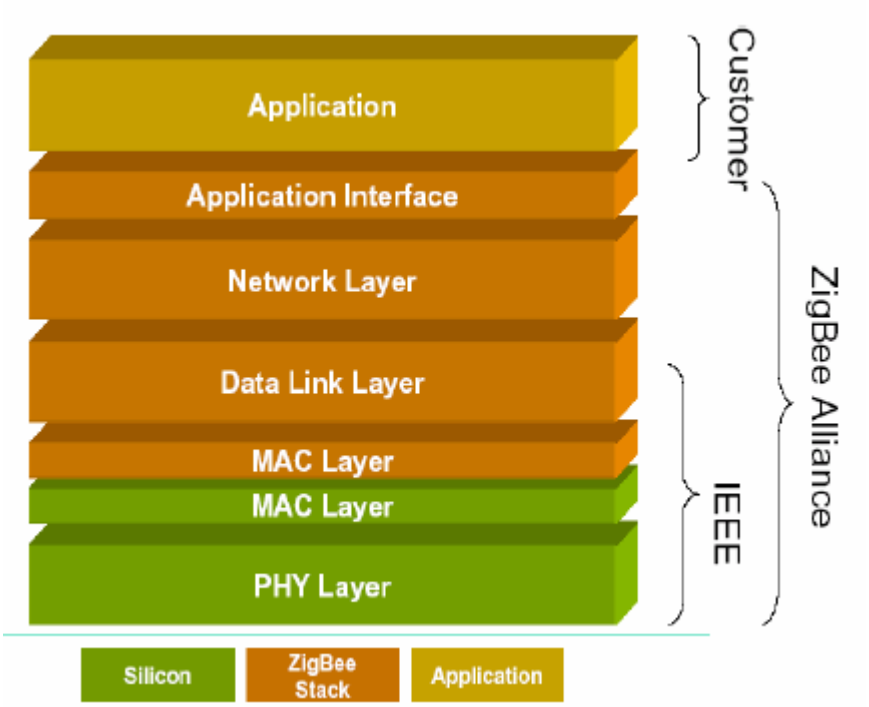
# IEEE 802.15.4 and ZigBee

- IEEE 802.15.4 Working Group

  Defining lower layers of protocol stack: MAC and PHY

- ZigBee Alliance

  Defining upper layers of protocol stack from network to application

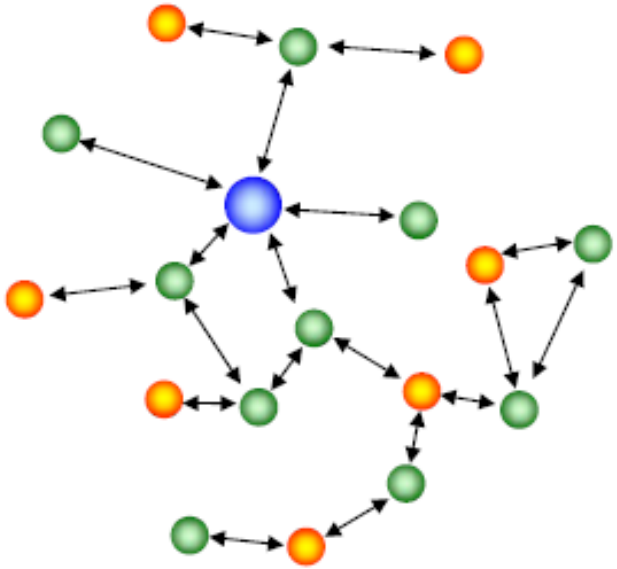


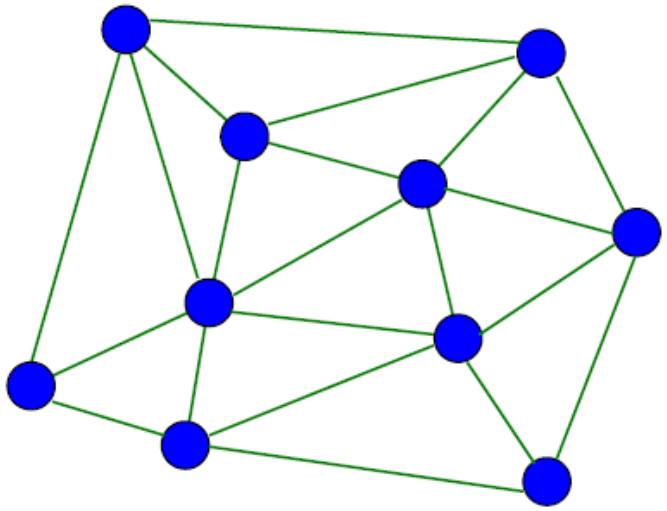
# ZigBee overview

- ZigBee was created to address the market need for a cost-effective, standards based wireless networking solution that supports low data-rates, low-power consumption, security, and reliability.
- ZigBee is the only standards-based technology that addresses the unique needs of most remote monitoring and control and sensory network applications.
- The initial markets for the ZigBee Alliance include Home Automation, Building Automation and Industrial Automation.

# How to achieve low power consumption?

- The duty cycle of battery is designed to be very low, resulting in very low average power consumption.
- Once associated with a network, a ZigBee node can wake up and communicate with other devices and return to sleep.
- Short range operation.
- Simple but flexible protocol.





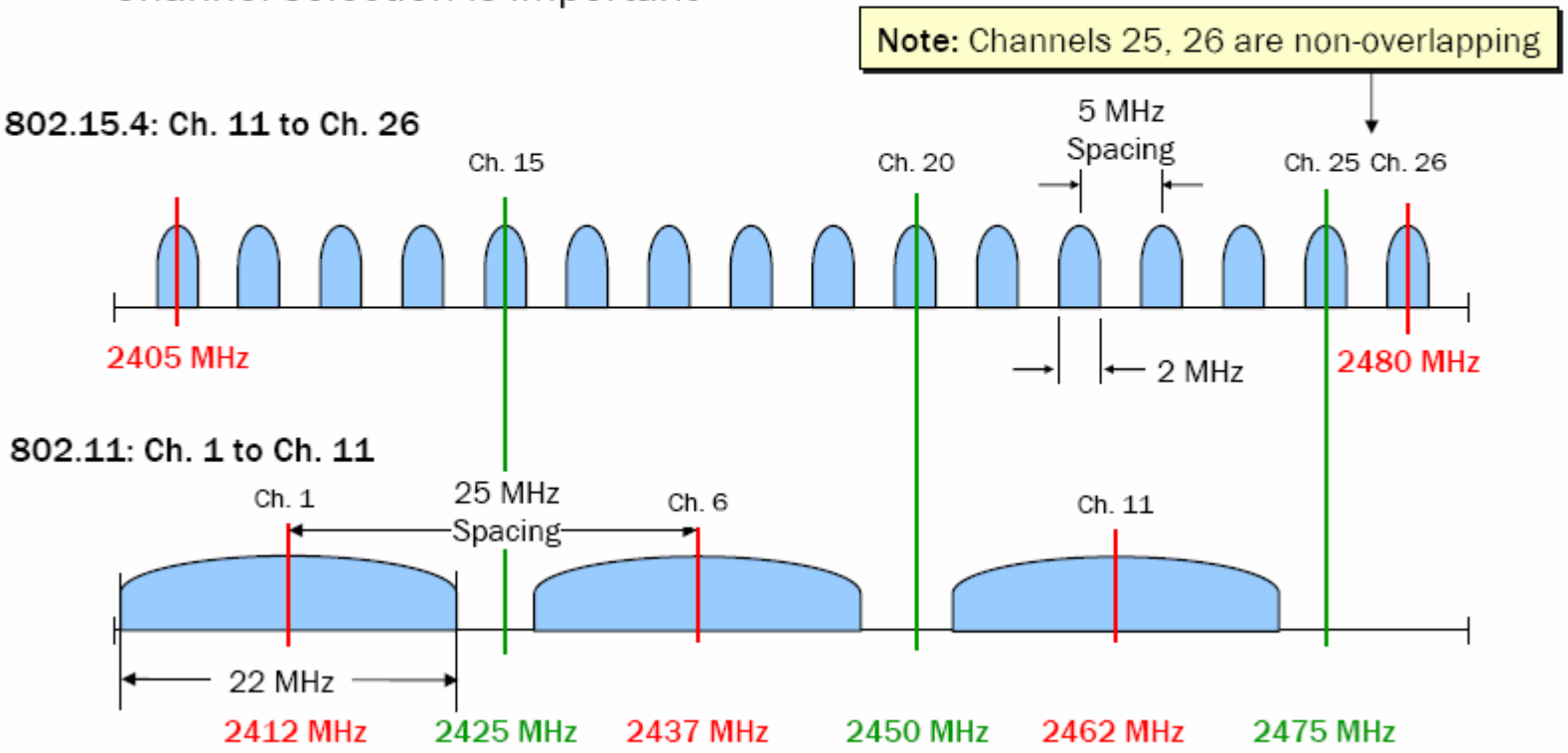
Mesh

# Interference and Coexistence in the 2.4GHz Band

## 802.15.4 and 802.11b Spectrum Relationship

Co-exists with WiFi, Bluetooth

- Channel selection is important



# Chapter 4:Local area network Summary

- various link layer technologies
  - LAN model
  - Ethernet
  - hubs, switches
  - VLAN
  - IEEE 802.11
  - IEEE 802.15