Chapter 4
Local Area network

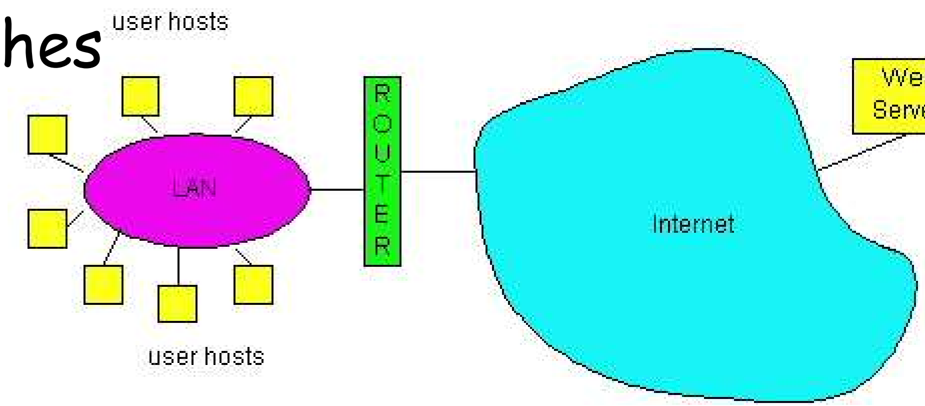
LAN technologies

Data link layer so far:

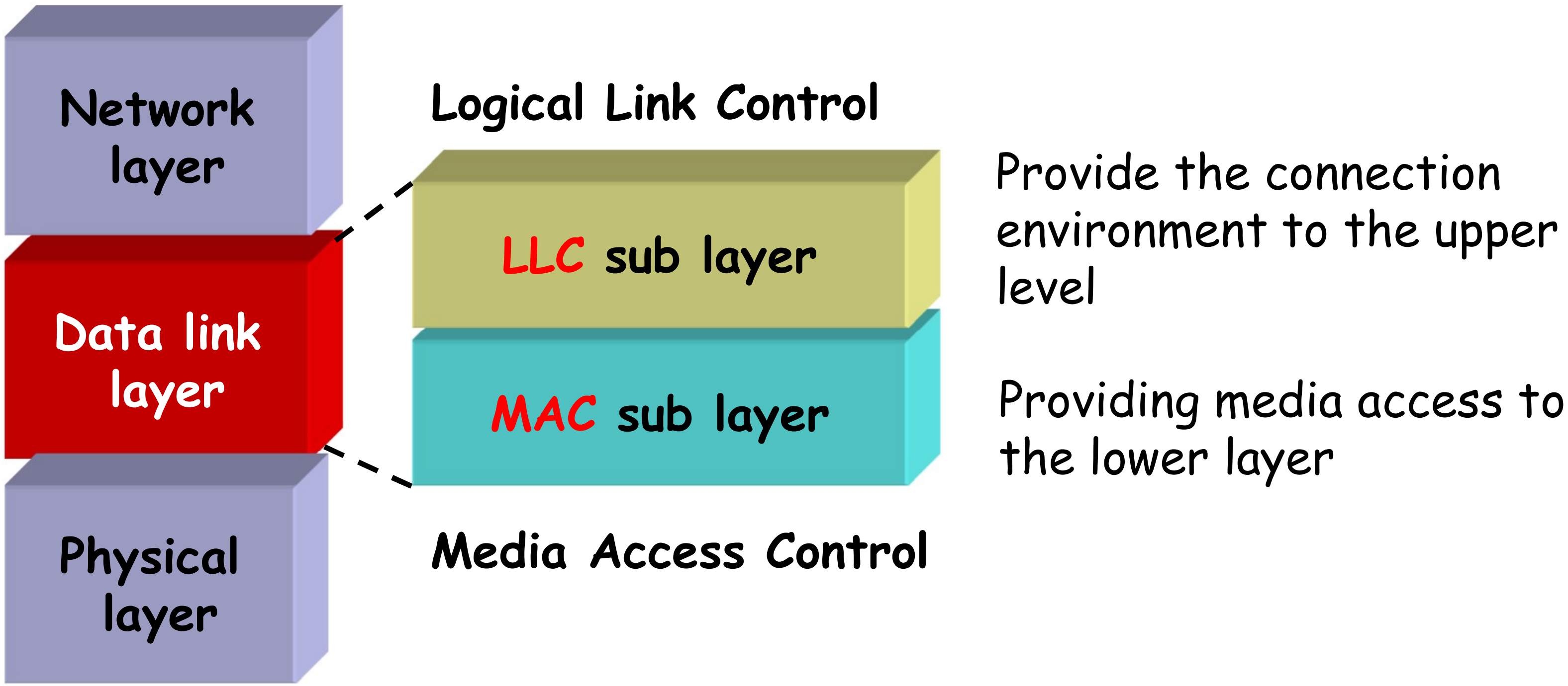
- services, framing, error detection/correction, reliable data transfer, multiple access

Next: LAN technologies

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

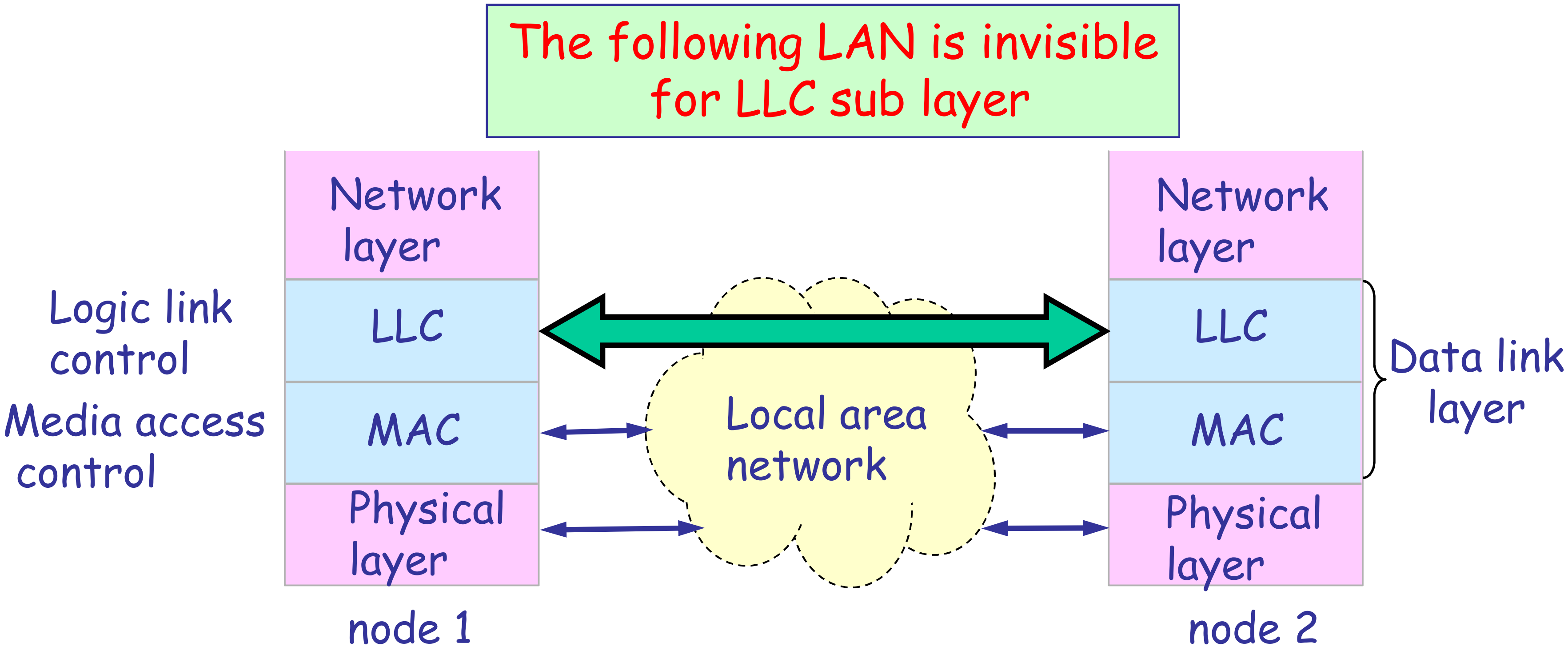


LAN model



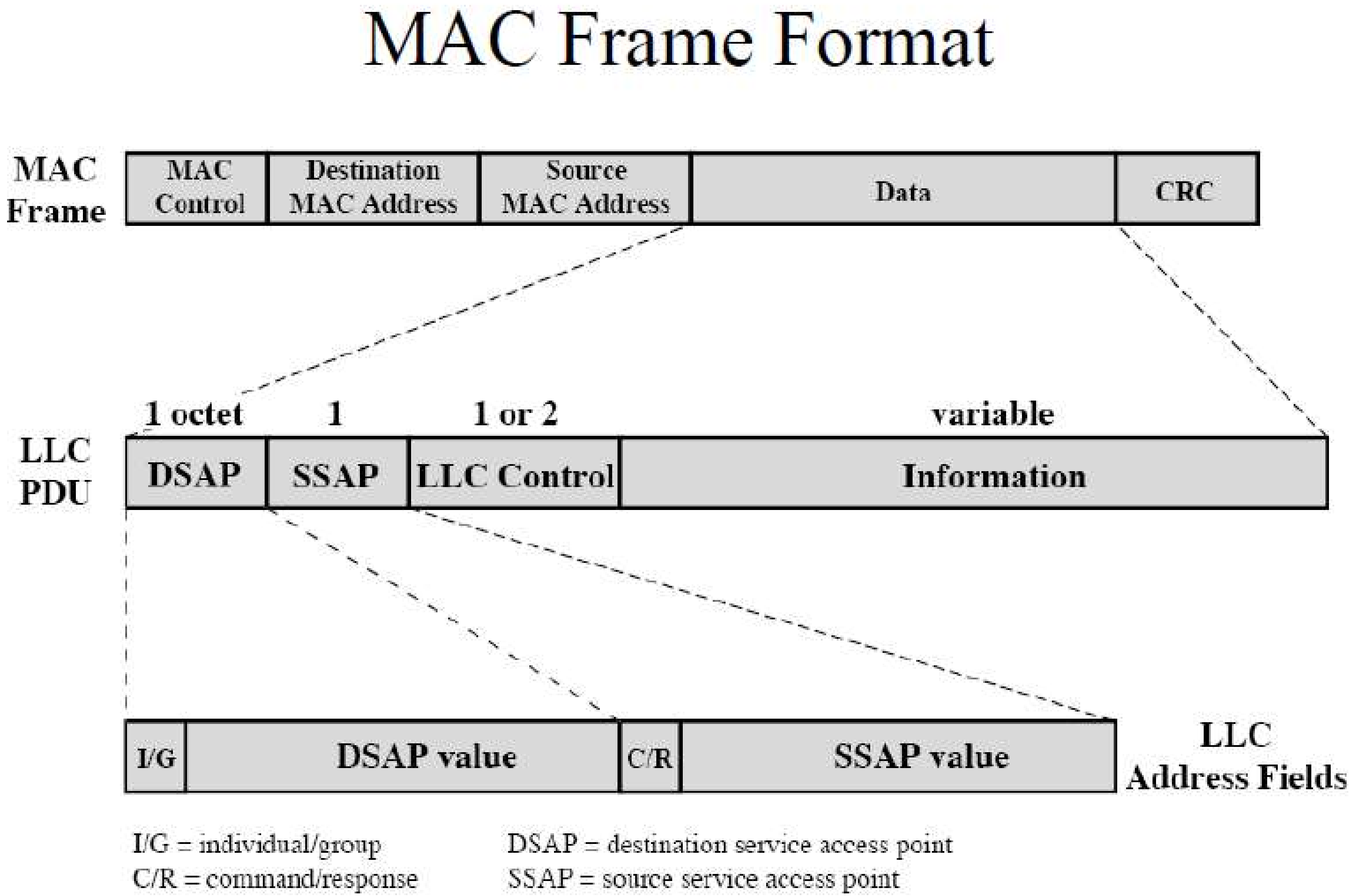
Network layer
Data link layer
Physical layer
Logical Link Control
LLC sub layer
MAC sub layer
Media Access Control
Provide the connection environment to the upper level
Providing media access to the lower layer

LAN model

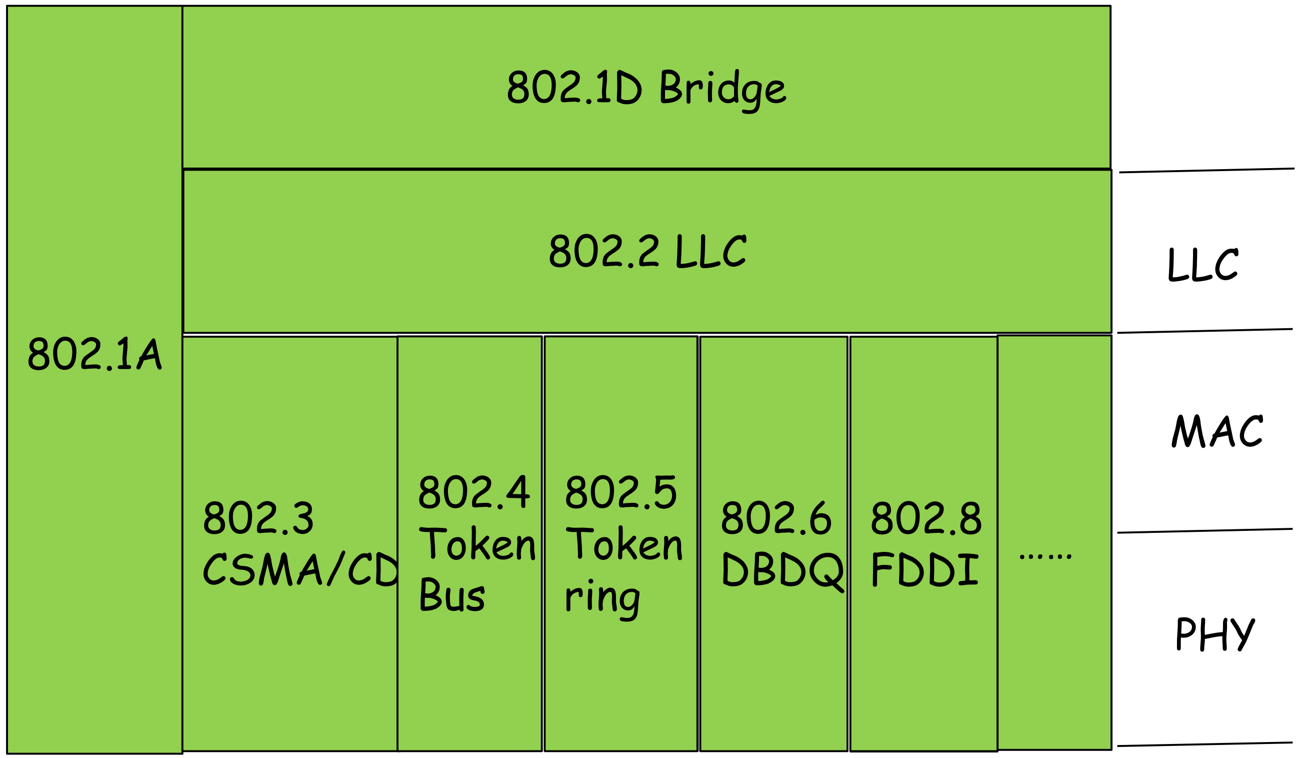


For the same LLC, several MAC options may be provided.

LLC and MAC


MAC Frame Format
MAC Frame
MAC Control
Destination MAC Address
Source MAC Address
Data
CRC
1 octet
1
1 or 2
variable
LLC PDU
DSAP
SSAP
LLC Control
Information
I/G
DSAP value
C/R
SSAP value
LLC Address Fields
I/G = individual/group
C/R = command/response
DSAP = destination service access point
SSAP = source service access point

IEEE 802 working group



LAN Addresses

32-bit IP address:

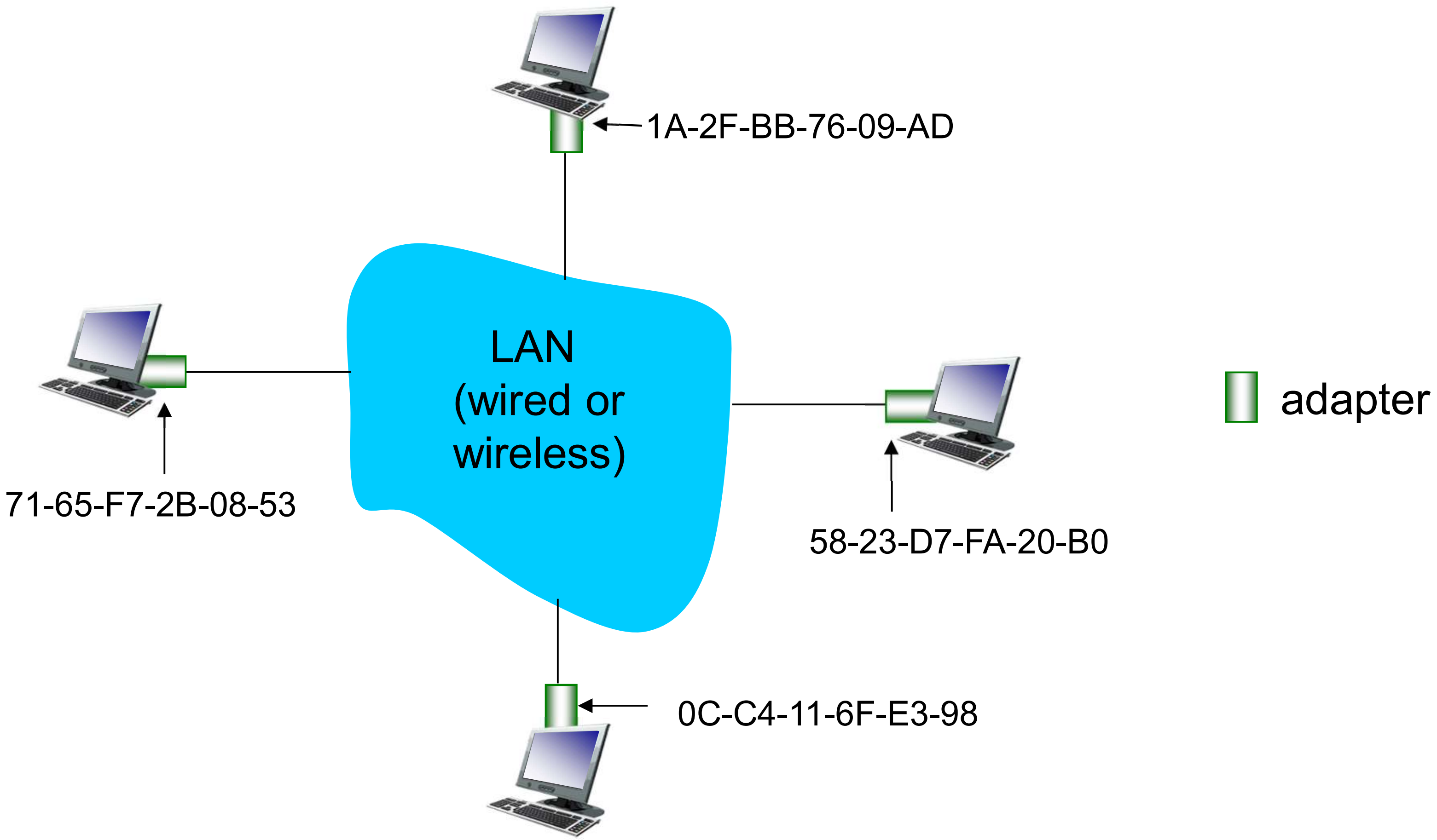
- *network-layer* address
- used to get datagram to destination network (recall IP network definition)

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 addresses

Each adapter on LAN has unique LAN address



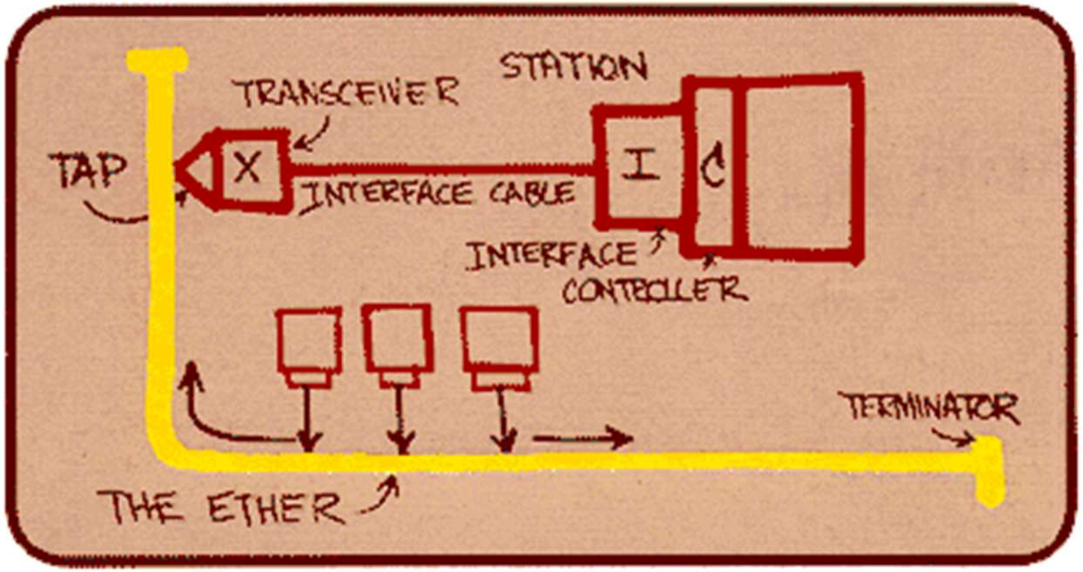
LAN Address (more)

- 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

Ethernet

"dominant" LAN technology:

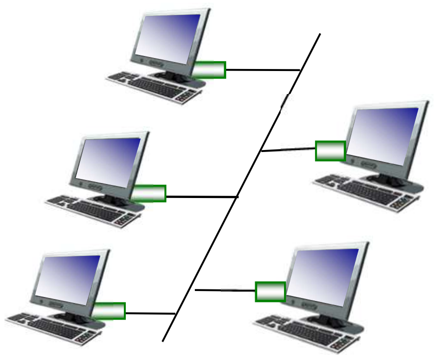
- cheap $20 for 100Mbs!
- first wildey used LAN technology
- Simpler, cheaper than token LANs and ATM
- Kept up with speed race: 10, 100, 1000 Mbps



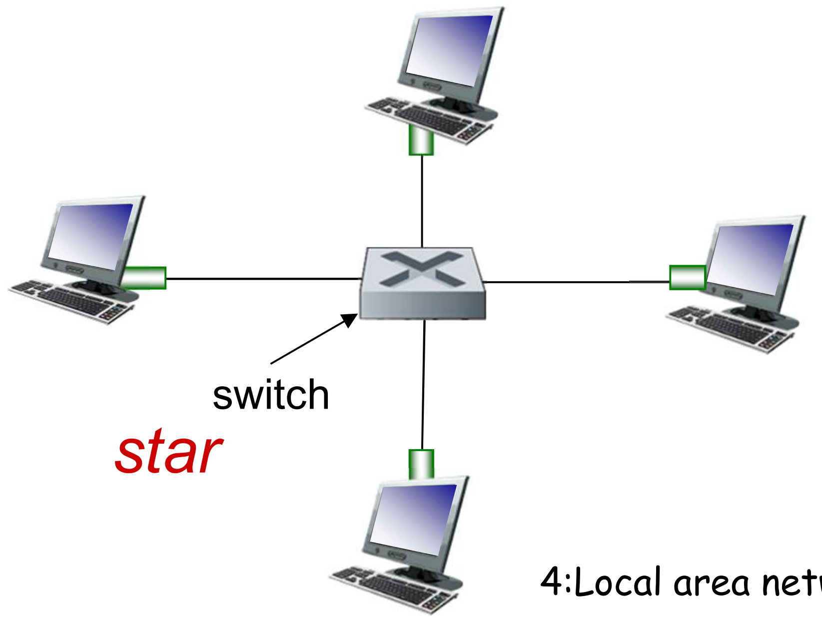
Metcalfe's Etheret sketch

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)

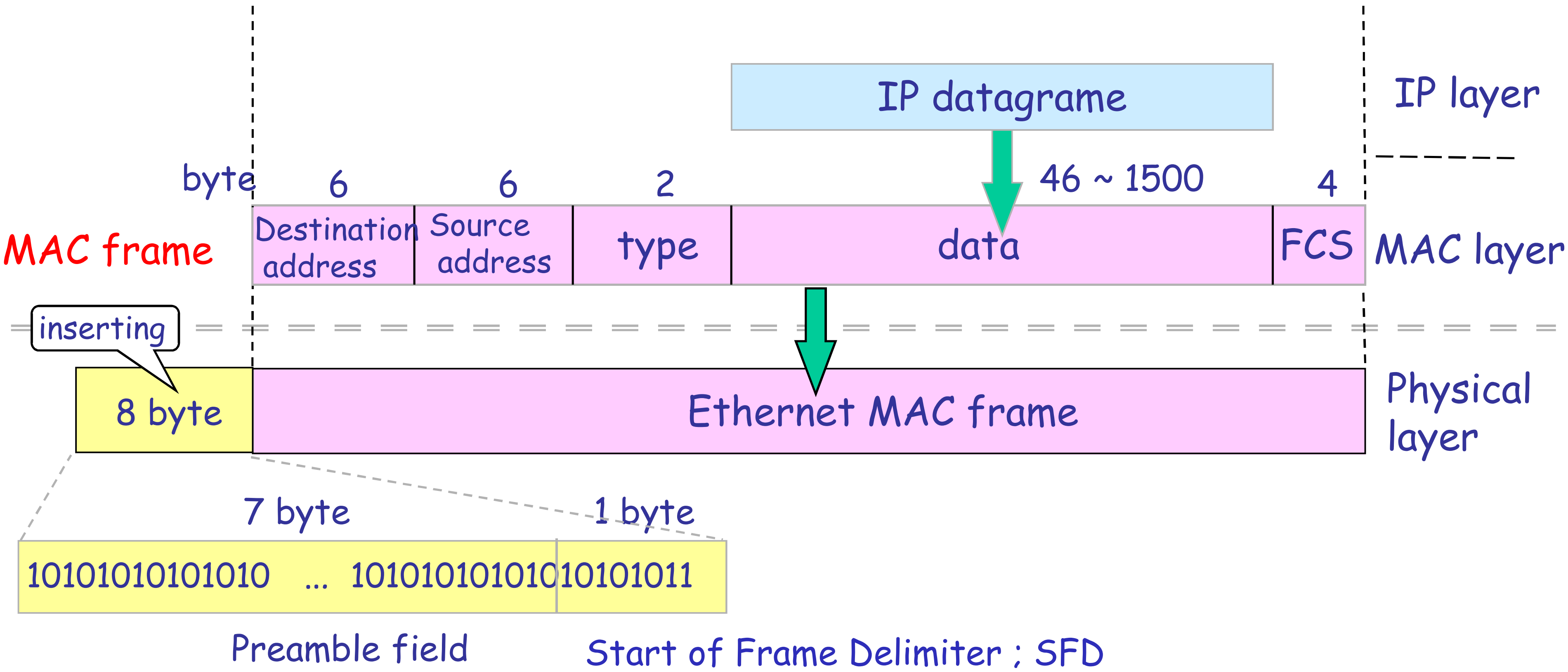


bus: coaxial cable



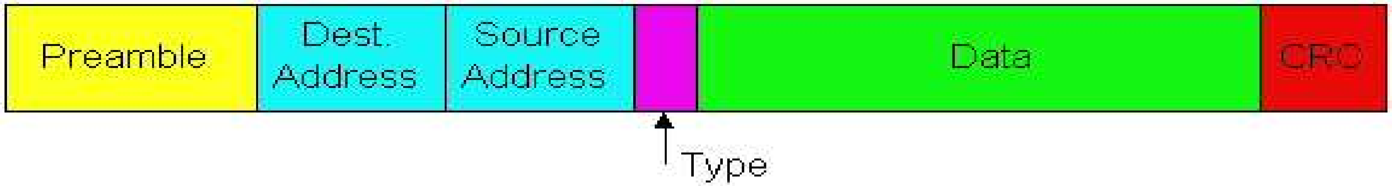
star

Ethernet Frame Structure



Ethernet Frame Structure

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

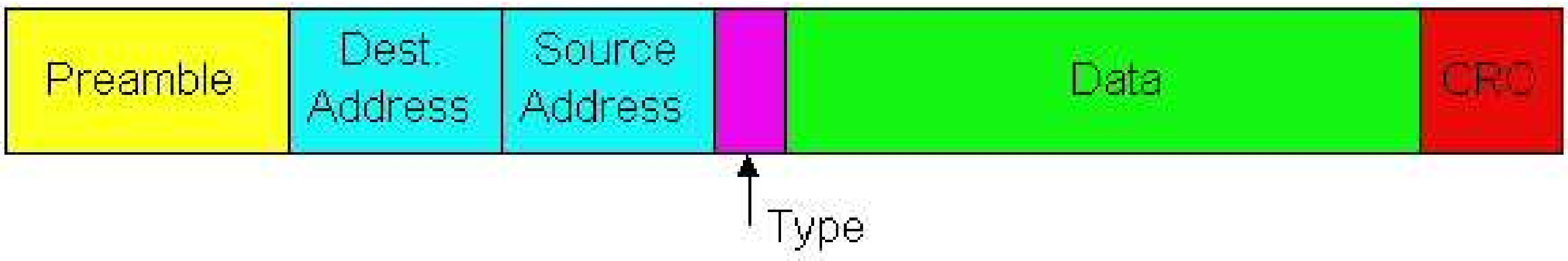


Preamble:

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

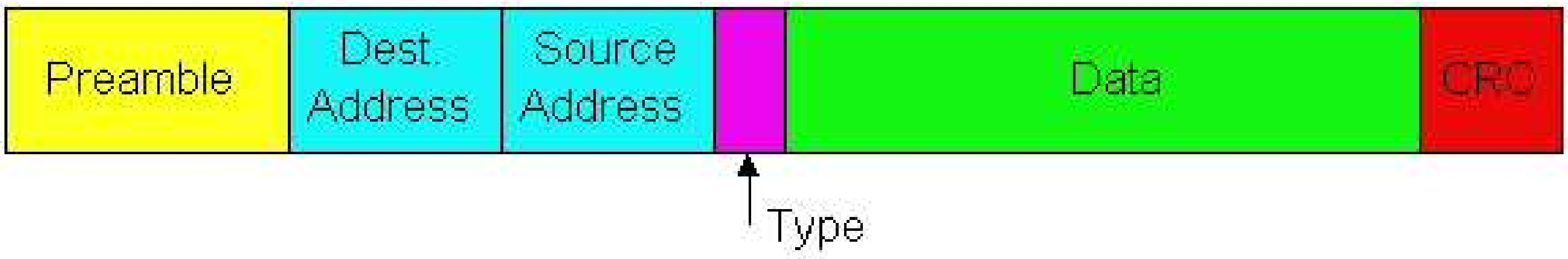
Ethernet Frame Structure (more)

- 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 2τ is 51.2 μs for IEEE 802.3, R=10Mbps)
- Maximum frame length: 1518 bytes, why?

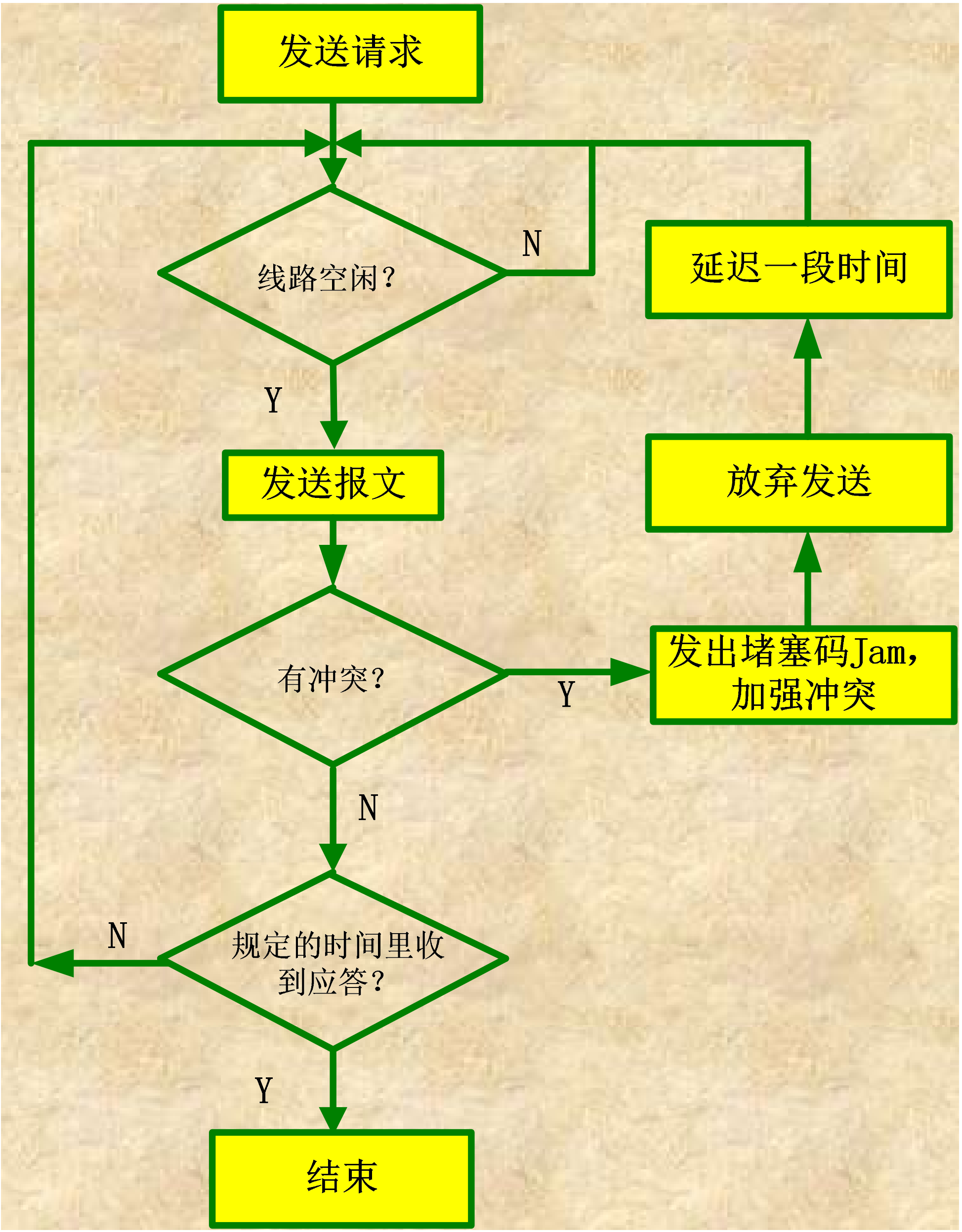


Ethernet: unreliable, connectionless

- *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*

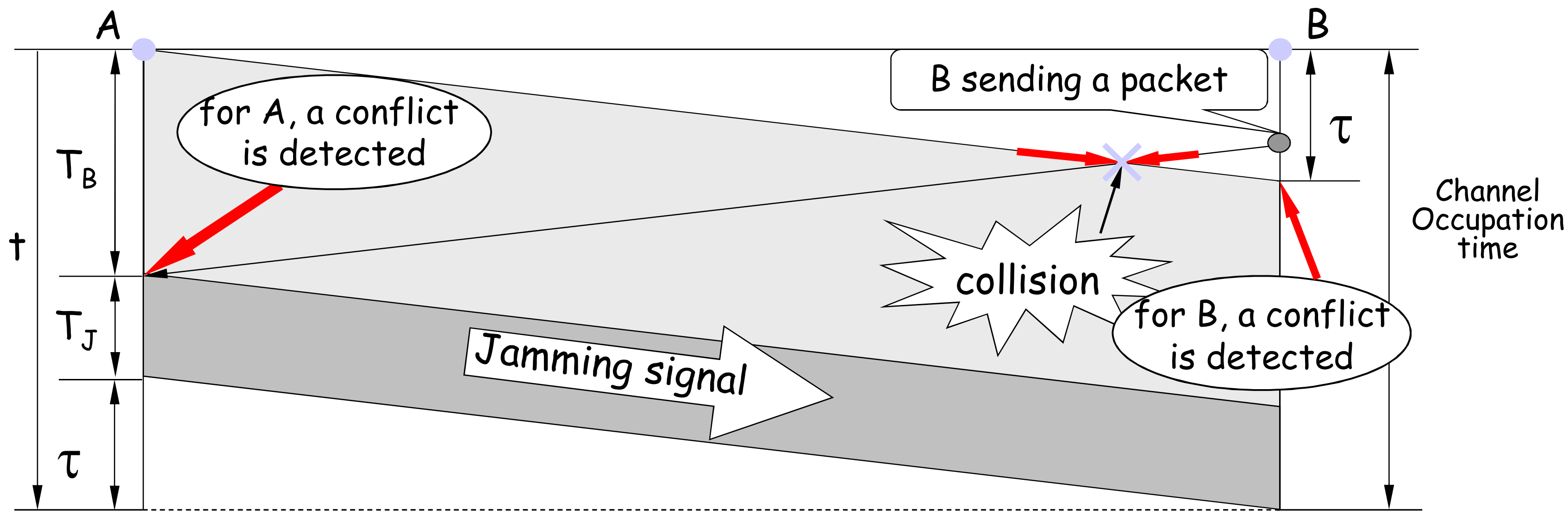
Ethernet: uses CSMA/CD

```
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}
```


发送请求
线路空闲?
N
Y
延迟一段时间
发送报文
放弃发送
有冲突?
Y
发出堵塞码Jam,
加强冲突
N
N
规定的时间里收
到应答?
Y
结束

Ethernet's CSMA/CD (more)

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



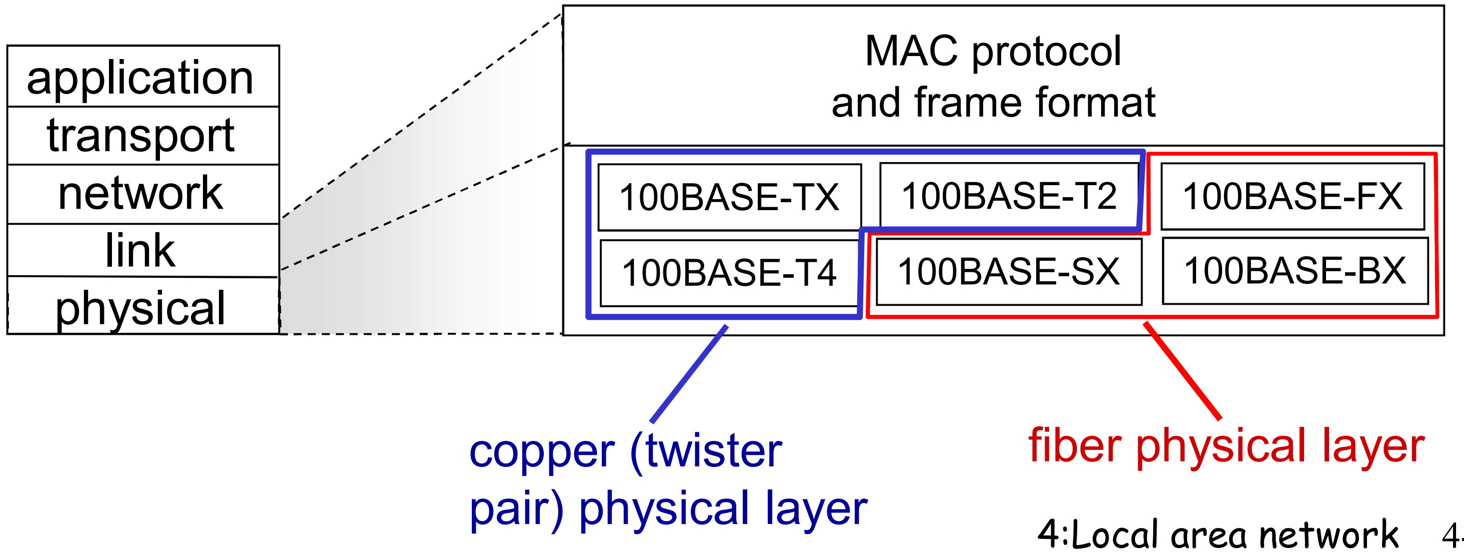
Ethernet's CSMA/CD (more)

Exponential Backoff:

- *Goal*: adapt retransmission attemtps to estimated current load
  - heavy load: random wait will be longer
- first collision: choose K from {0,1}; delay is K x 512 bit transmission times
- after second collision: choose K from {0,1,2,3}…
- after ten or more collisions, choose K from {0,1,2,3,4,…,1023}

802.3 Ethernet standards: link & physical layers

- *many* different Ethernet standards
  - common MAC protocol and frame format
  - different speeds: 2 Mbps, 10 Mbps, 100 Mbps, 1Gbps, 10 Gbps, 40 Gbps
  - different physical layer media: fiber, cable



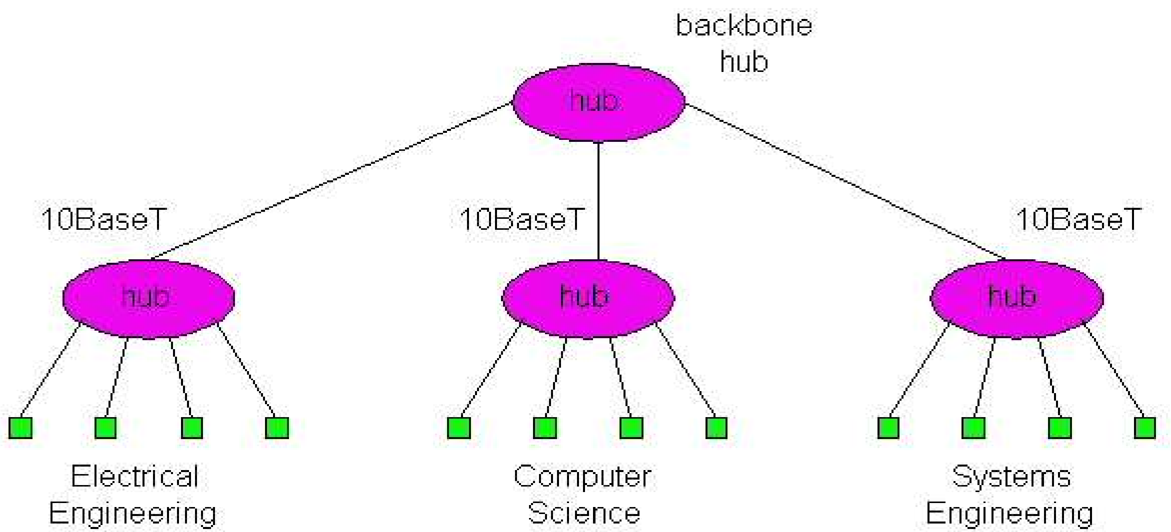
Interconnecting LANs

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)
- limited number of stations: 802.5 have token passing delays at each station

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

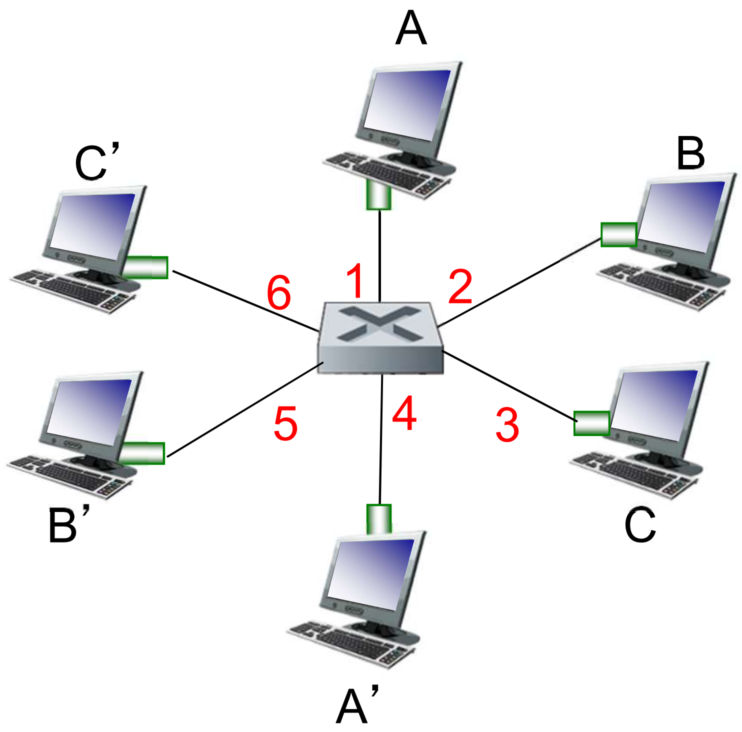
- single collision domain results in no increase in max throughput
  - multi-tier throughput same as single segment throughput
- individual LAN restrictions pose limits on number of nodes in same collision domain and on total allowed geographical coverage
- cannot connect different Ethernet types (e.g.,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



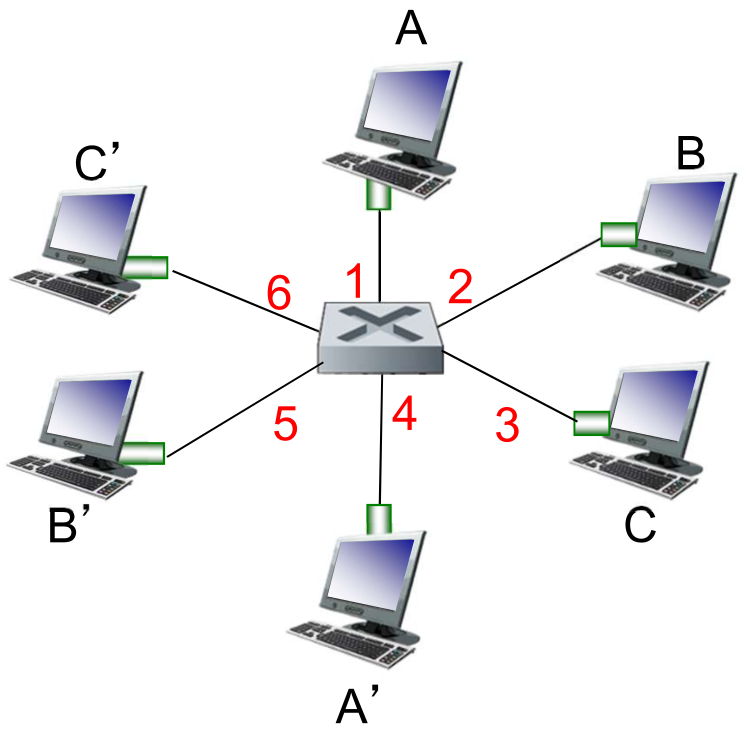
switch with six interfaces (1,2,3,4,5,6)

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!

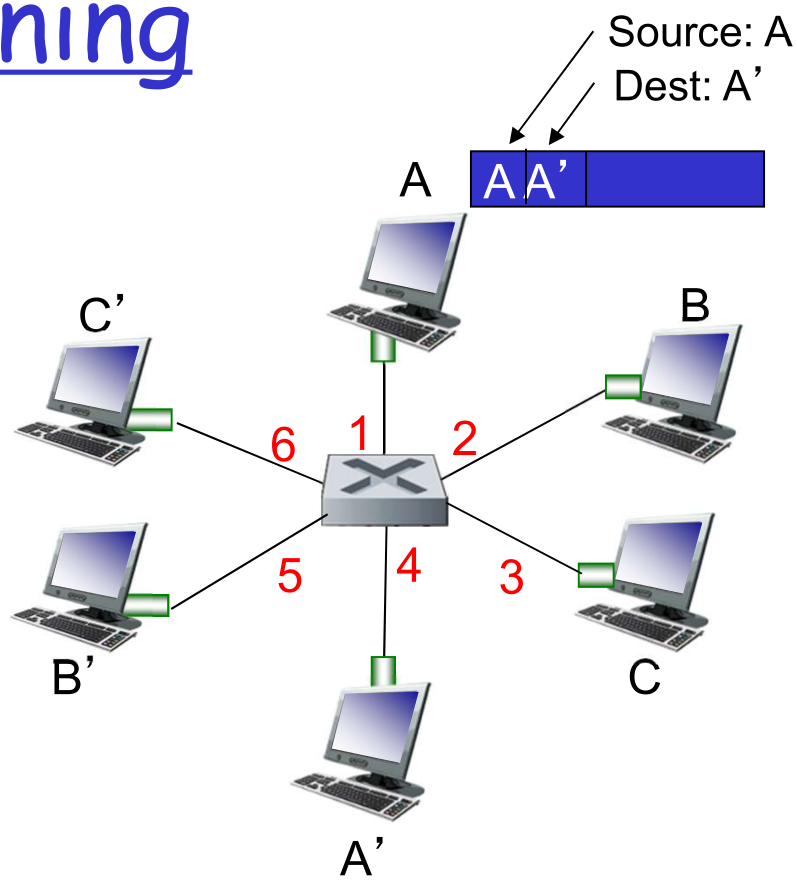
Q: how are entries created, maintained in switch table?
  - something like a routing protocol?



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:

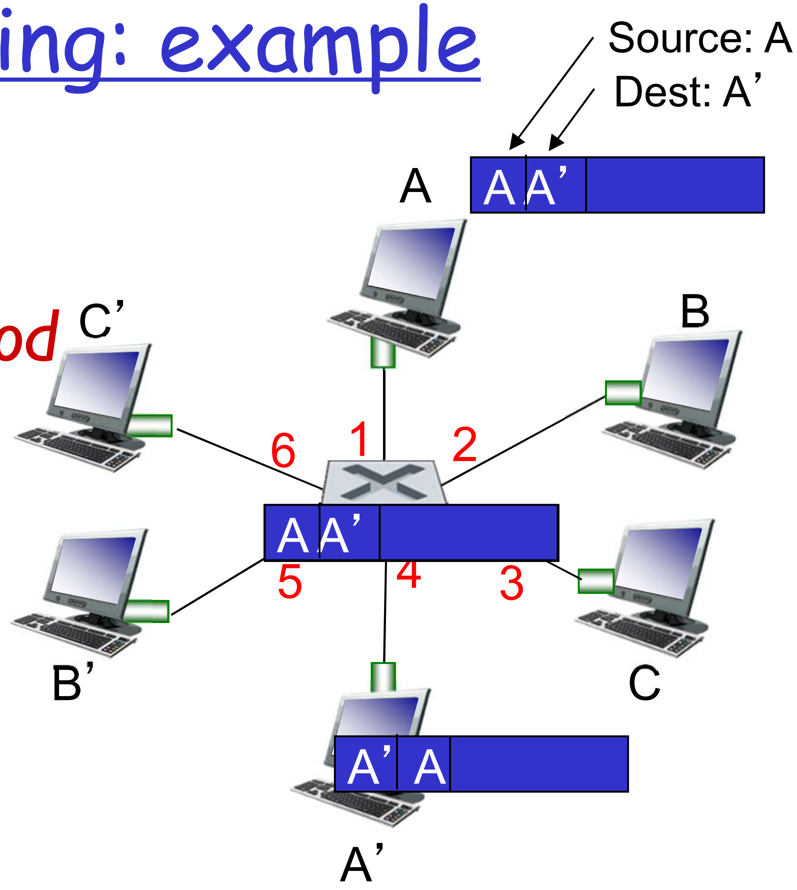
1. record incoming link, MAC address of sending host
2. index switch table using MAC destination address
3. if entry found for destination

```
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

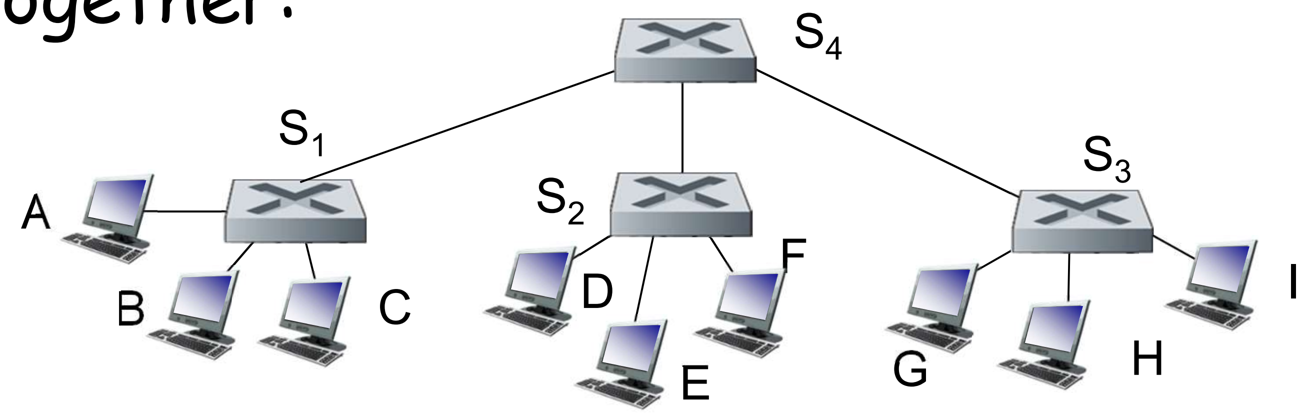


MAC addr	interface	TTL
A	*1*	*60*
A'	*4*	*60*

switch table (initially empty)

Interconnecting switches

self-learning switches can be connected together:

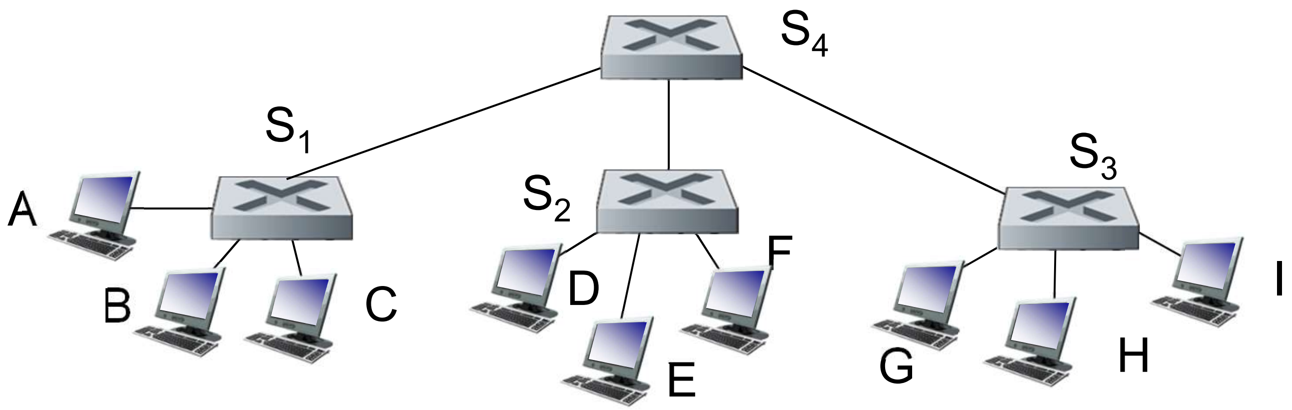


Q: sending from A to G - how does S_1 know to forward frame destined to G via S_4 and S_3?

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

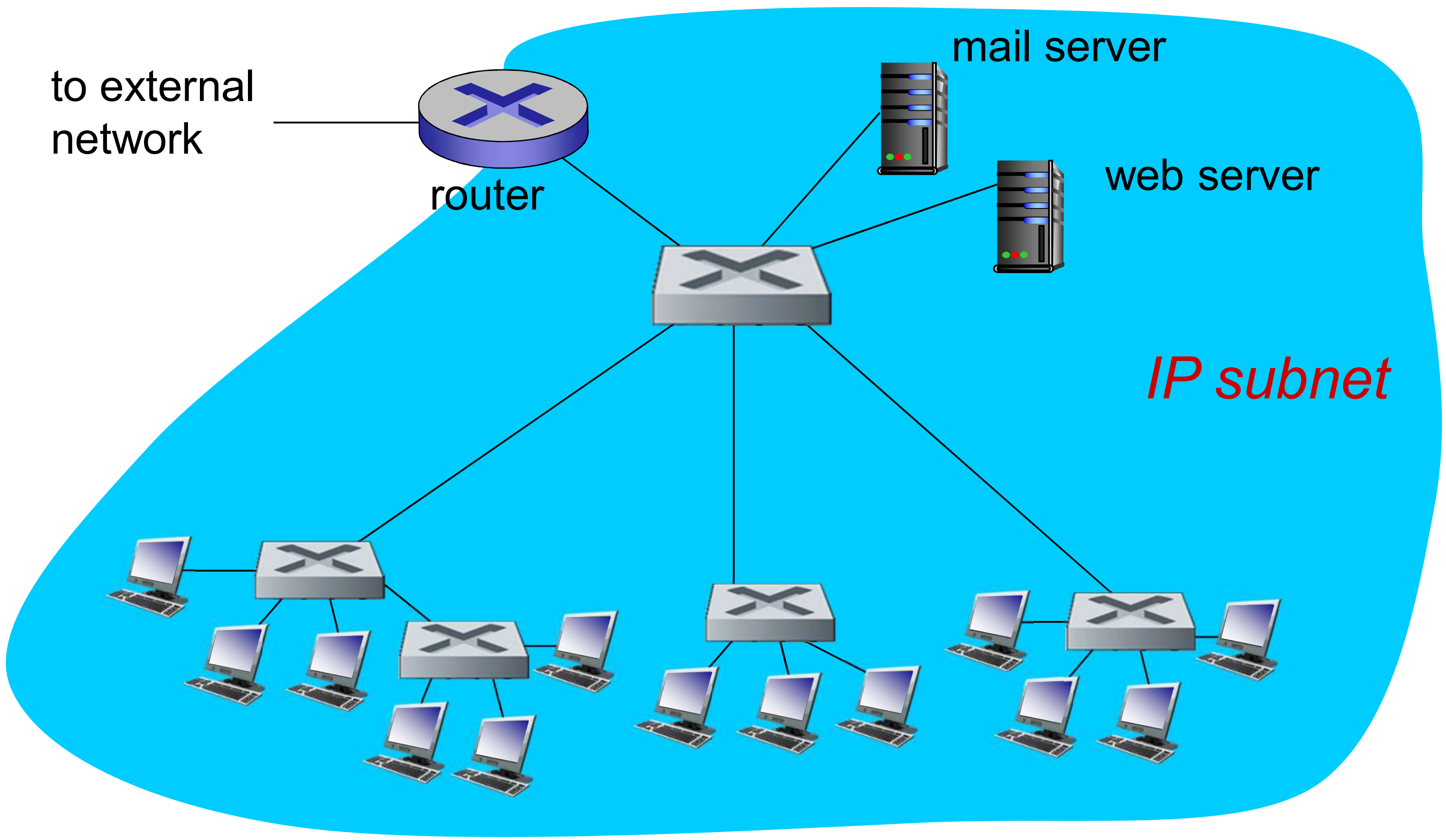
Self-learning multi-switch example

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



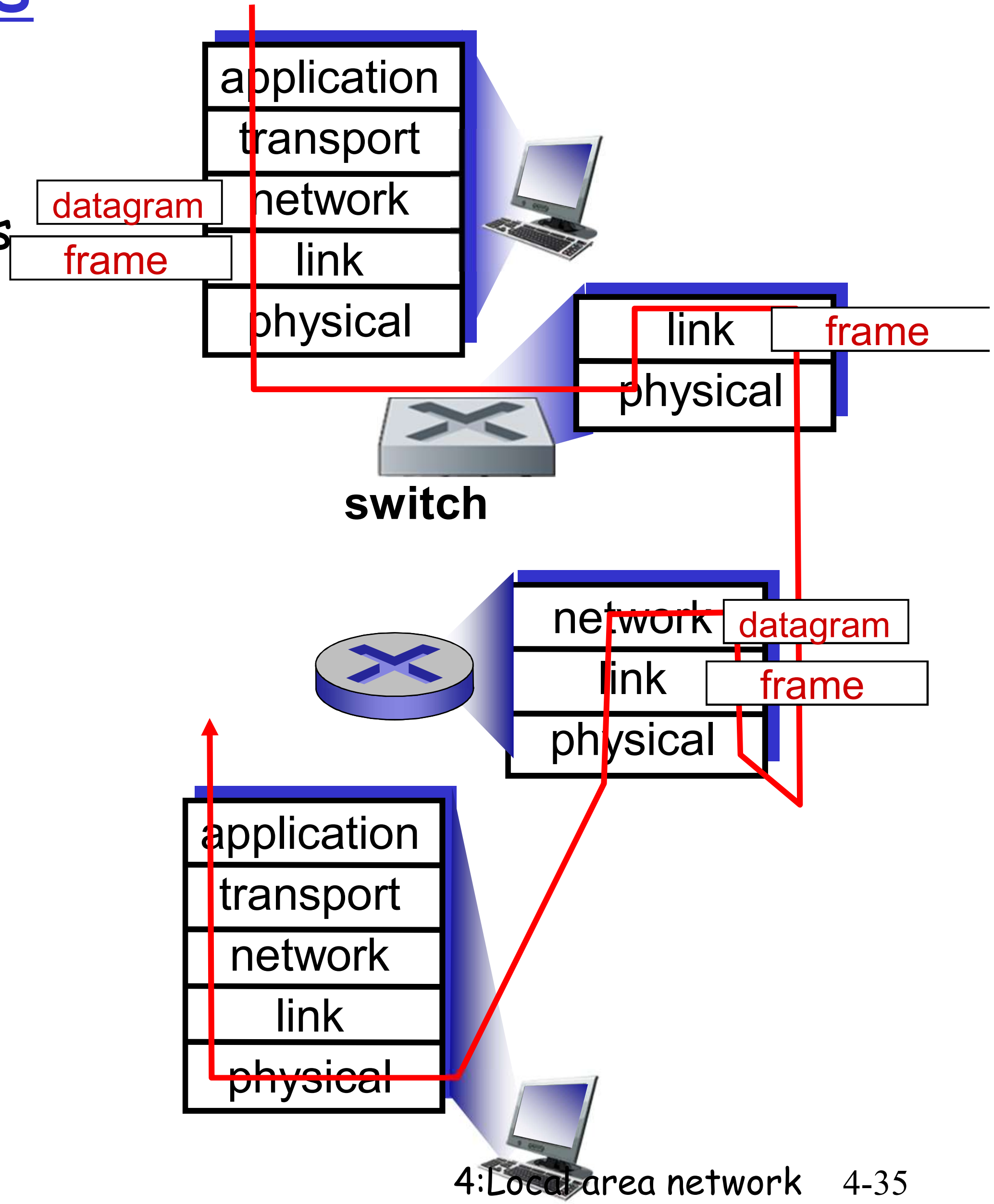
Switches vs. routers

both are store-and-forward:

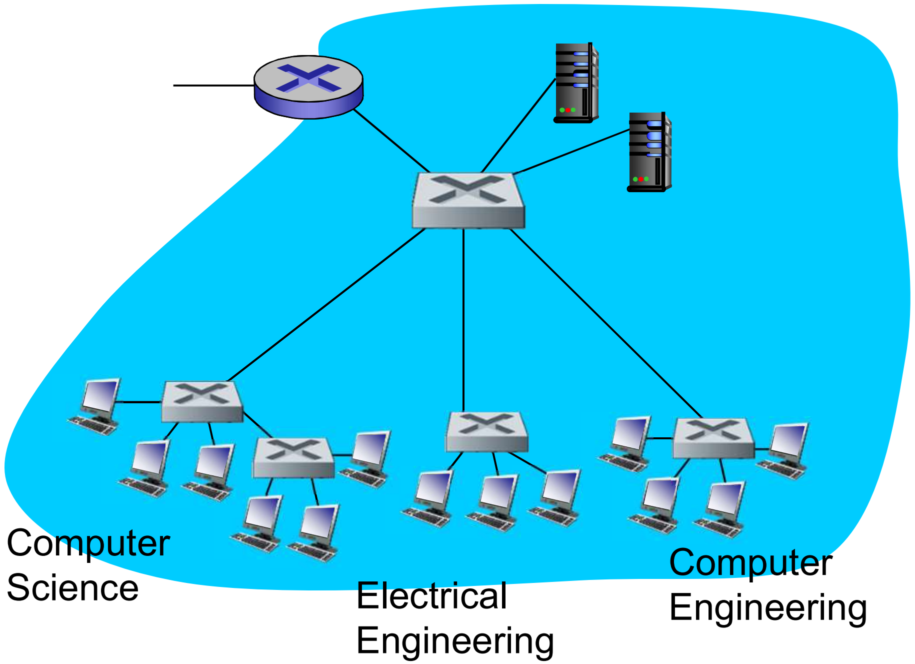
- *routers:* network-layer devices (examine network-layer headers)
- *switches*: link-layer devices (examine link-layer headers)

both have forwarding tables:

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



VLANs: motivation

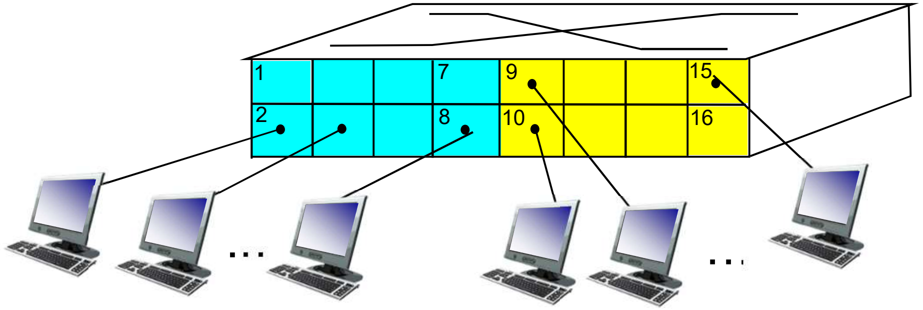


consider:

- 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

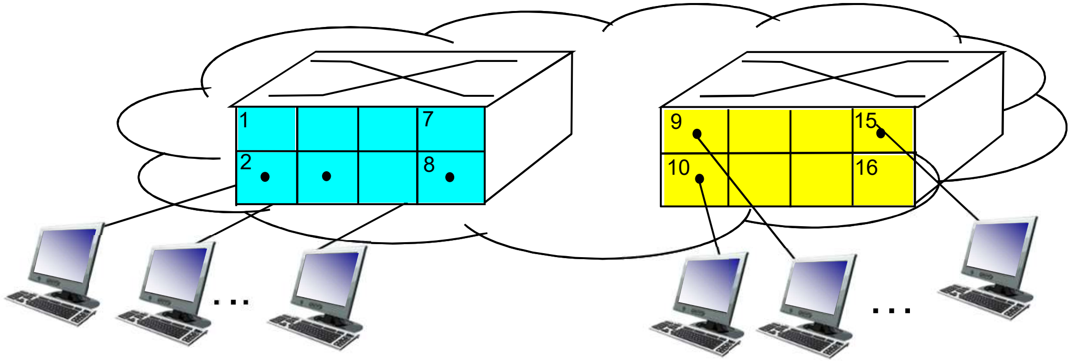
port-based VLAN: switch ports grouped (by switch management software) so that *single* physical switch ……



Electrical Engineering
(VLAN ports 1-8)

Computer Science
(VLAN ports 9-15)

… operates as multiple virtual switches



Electrical Engineering
(VLAN ports 1-8)

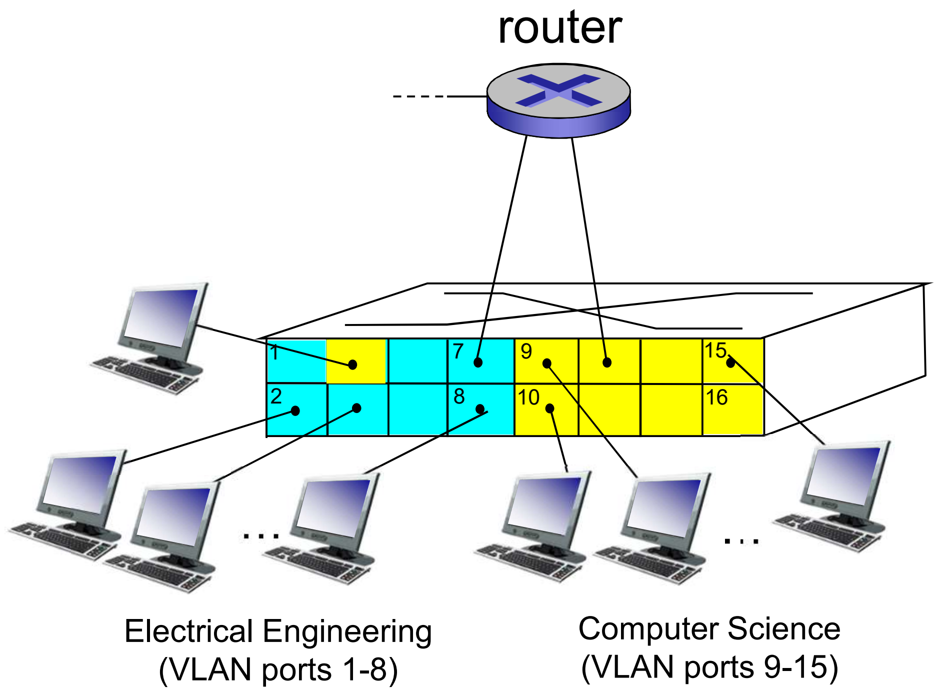
Computer Science
(VLAN ports 9-16)

Virtual Local Area Network

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

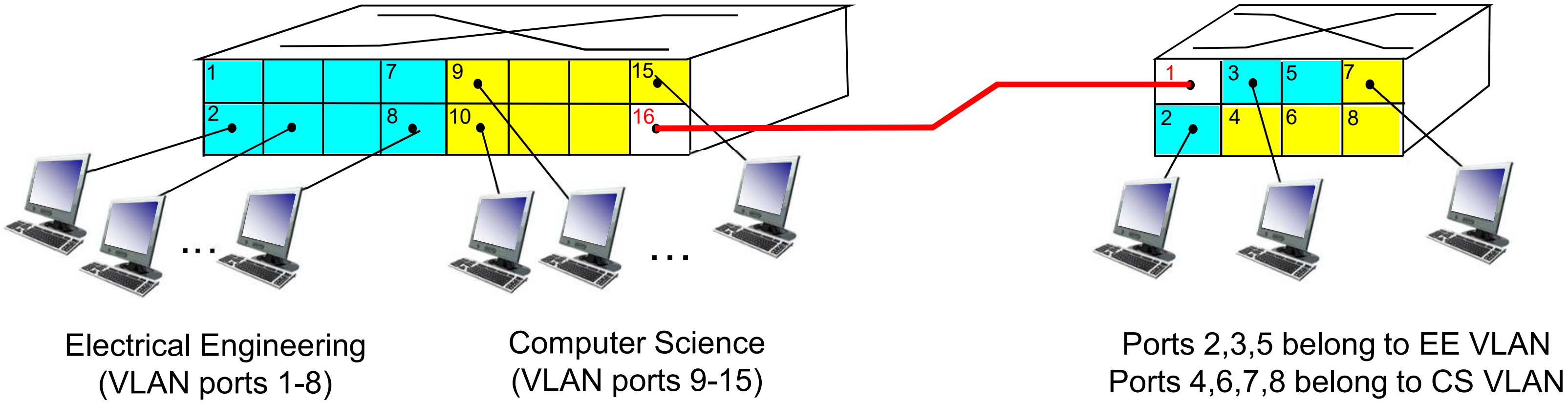
Port-based VLAN

- *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



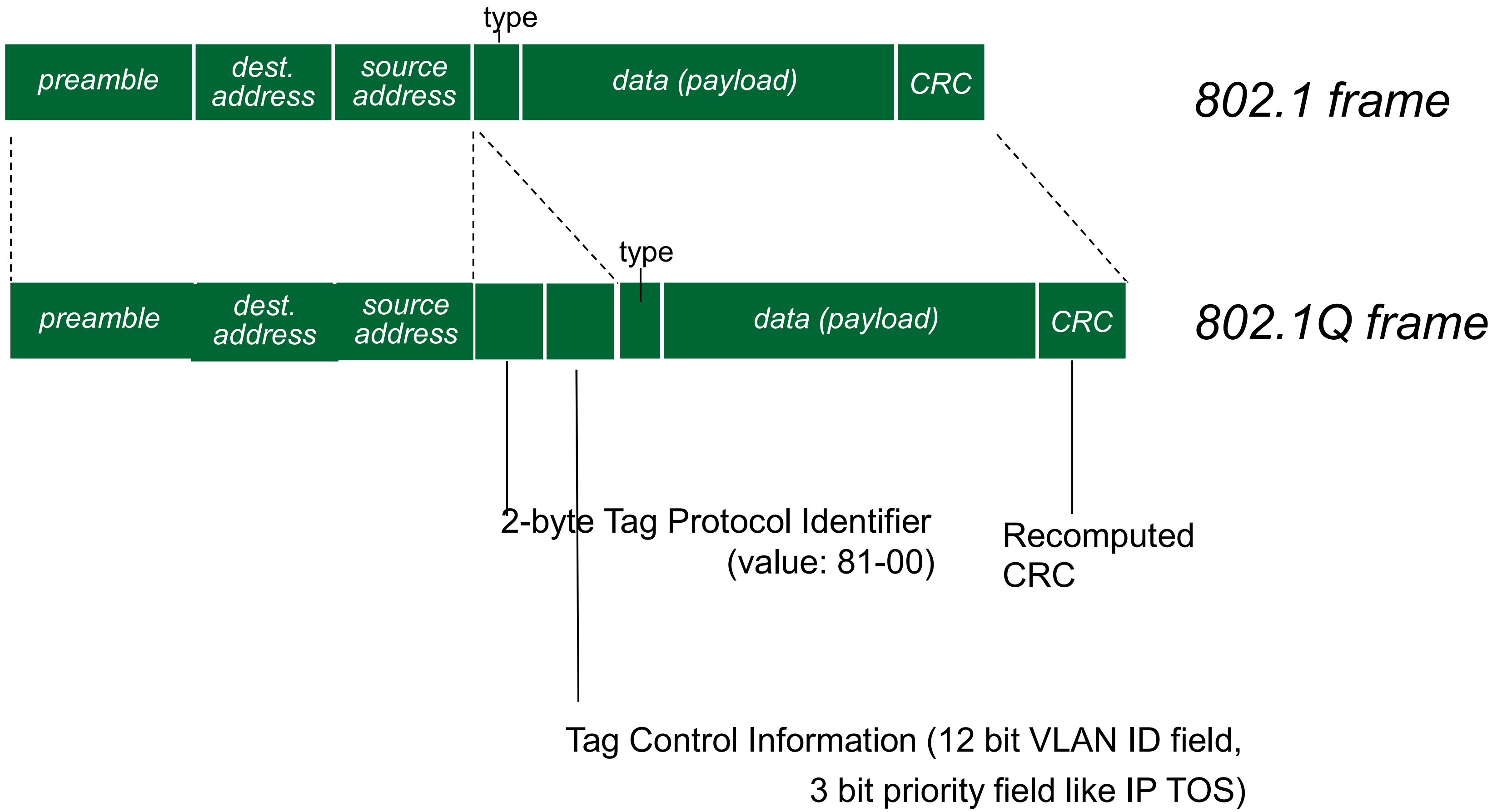
- forwarding between VLANS: done via routing (just as with separate switches)
  - in practice vendors sell combined switches plus routers

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

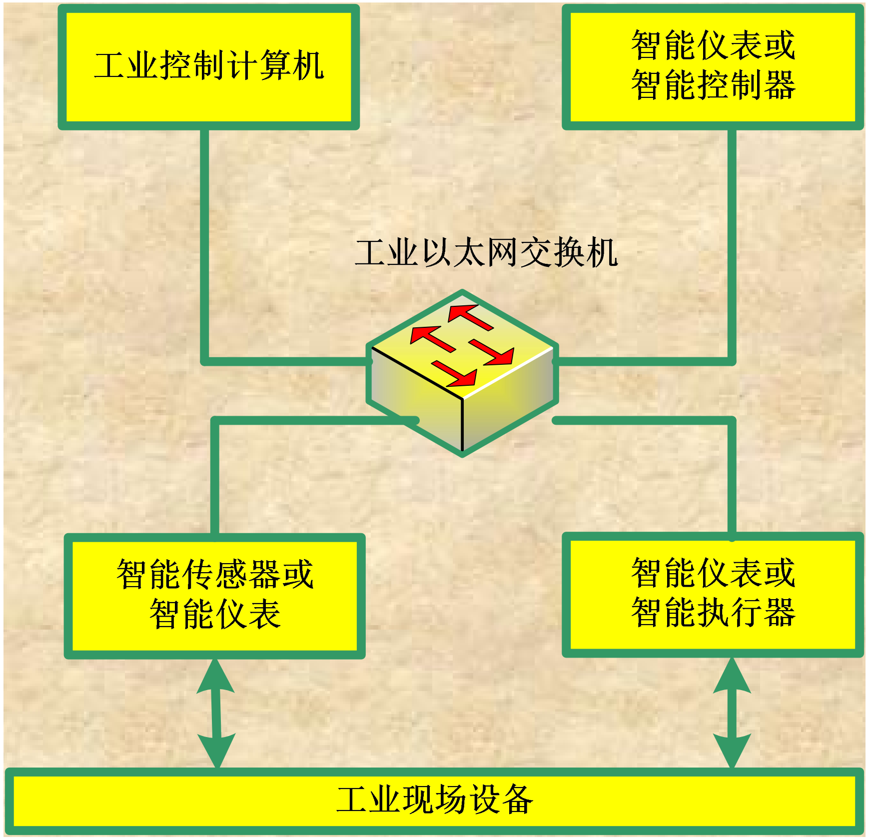
802.1Q VLAN frame format



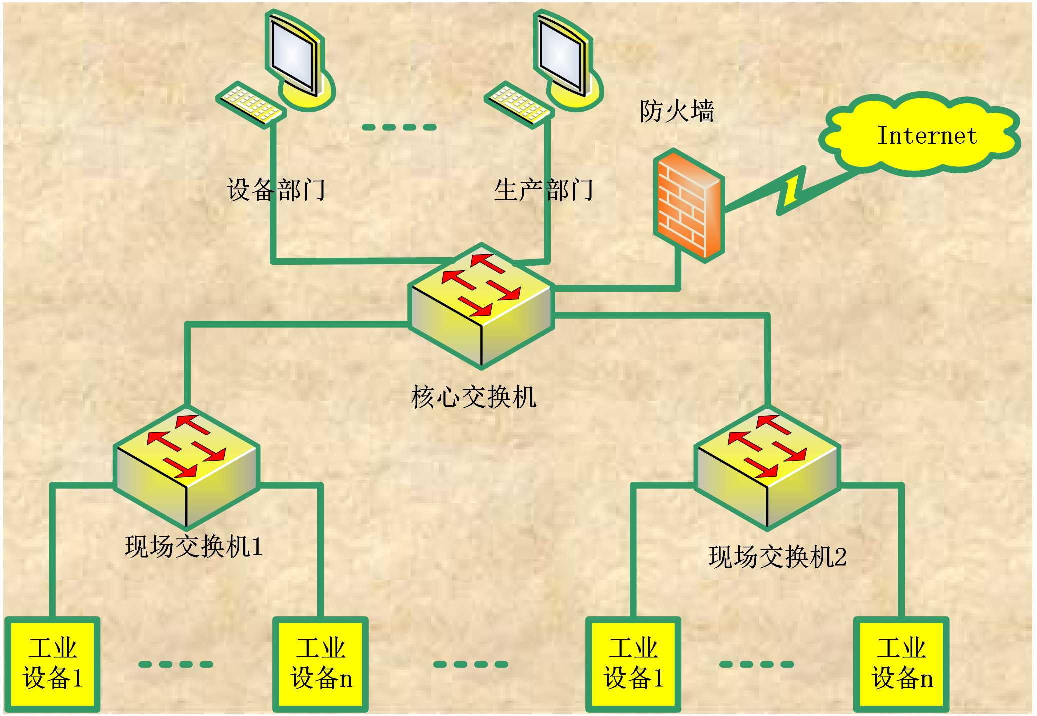
Industrial Ethernet

项目	工业以太网设备	商用以太网设备
元器件	工业级	商用级
接插件	耐腐蚀、防尘、防水、加固型**RJ45/DB-9**等	一般**RJ45**
工作电压	**DC 24V**	**AC 220V**
电源冗余	双电源	一般没有
安装方式	**DIN**导轨或其他固定安装	桌面或机架
工作温度	**－40C^0～85 C^0**	**5C^0～40 C^0**
电磁兼容性标准	**EN 50081-1**、**EN 50081-2**（工业级**EMC**）	办公室用**EMC**
MTBF值	至少**10**年	**3**～**5**年

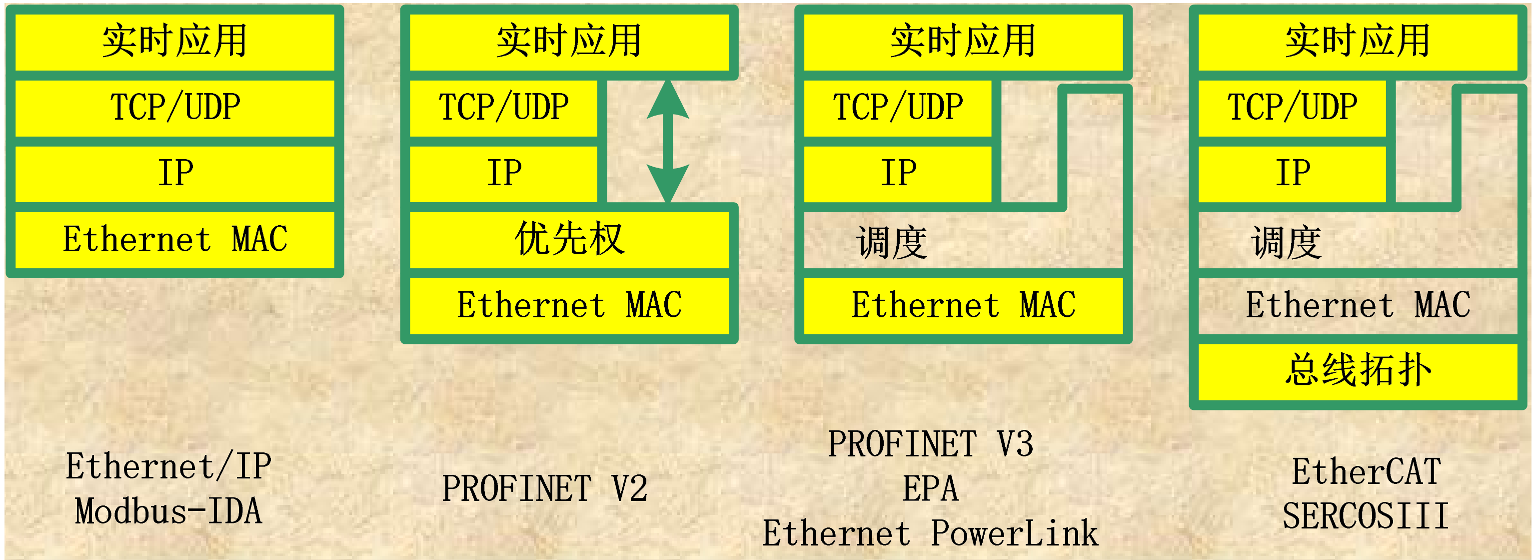
Industrial Ethernet



Industrial Ethernet



Industrial real time Ethernet

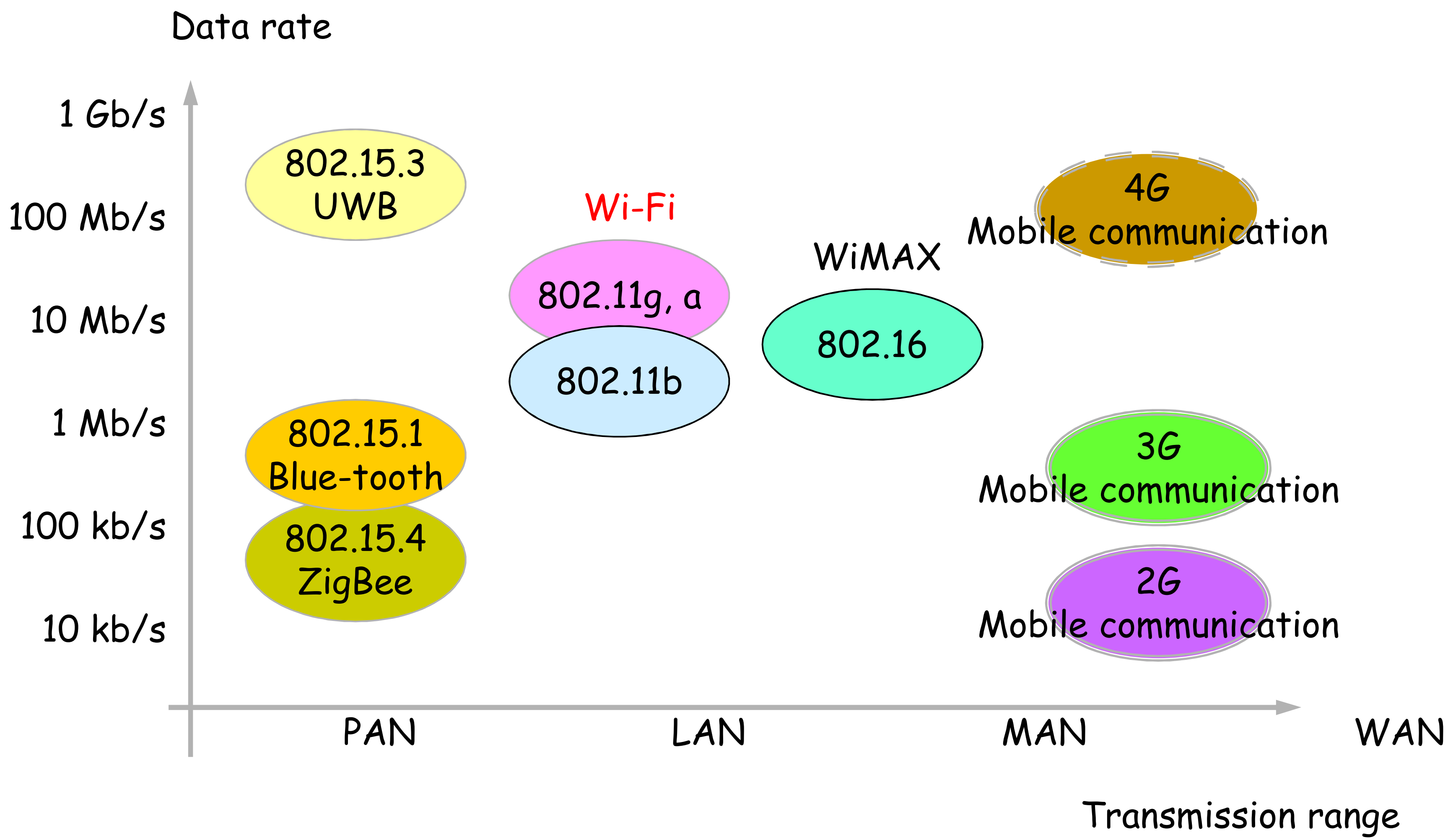


Wireless Networks

Background:

- # wireless (mobile) phone subscribers now exceeds # wired phone subscribers (5-to-1)!
- # wireless Internet-connected devices equals # wireline Internet-connected devices
  - laptops, Internet-enabled phones promise anytime untethered Internet access
- two important (but different) challenges
  - *wireless:* communication over wireless link
  - *mobility:* handling the mobile user who changes point of attachment to network

Wireless communication technology



IEEE Wireless Technology

Local wireless networks
WLAN 802.11

802.11a **WiFi5**

802.11b → 802.11g
WiFi

802.11i/e/f/n/s…

Personal wireless networks
WPAN 802.15

ZigBee
802.15.4

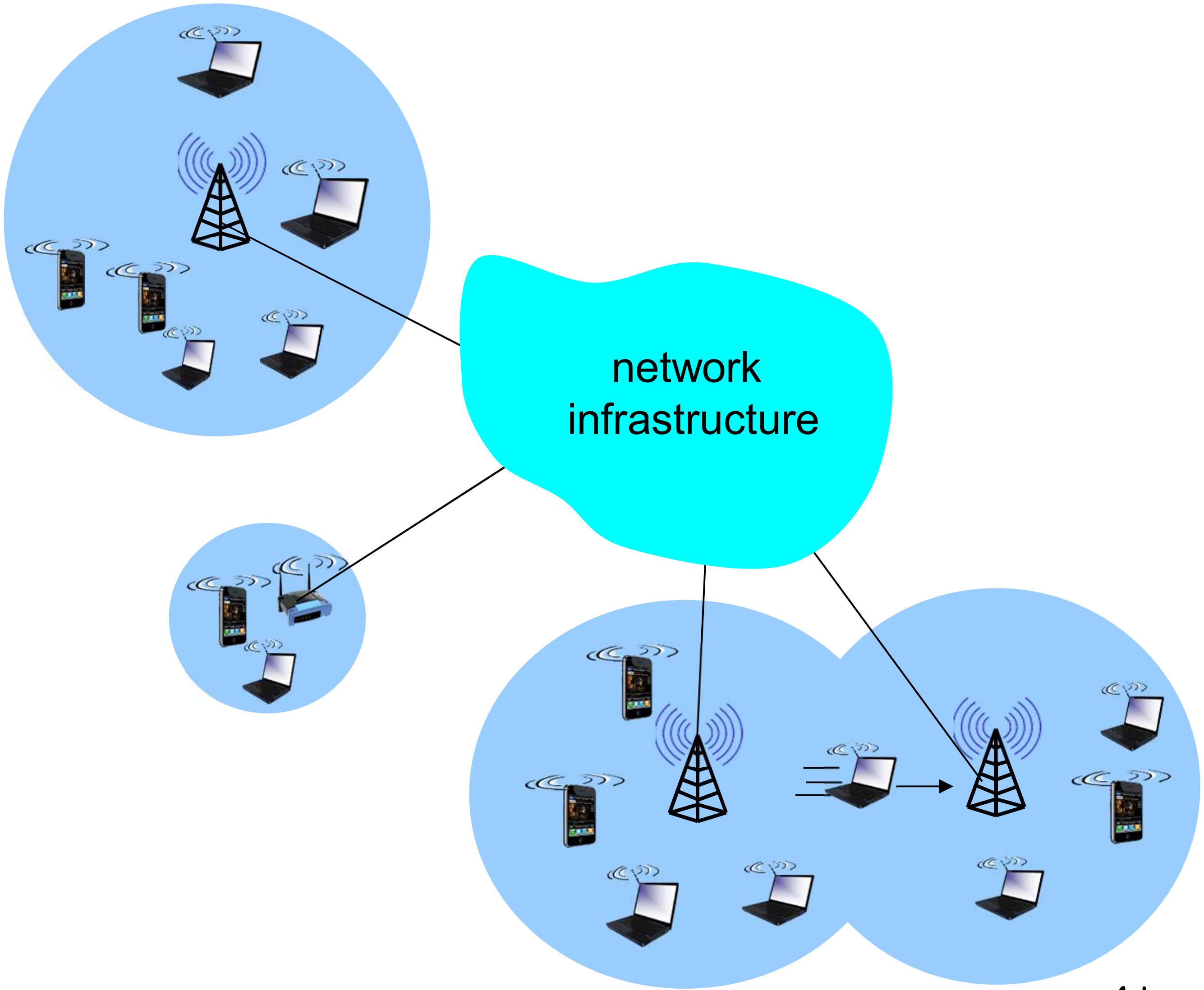
802.15.3
UWB

802.15.1
Bluetooth

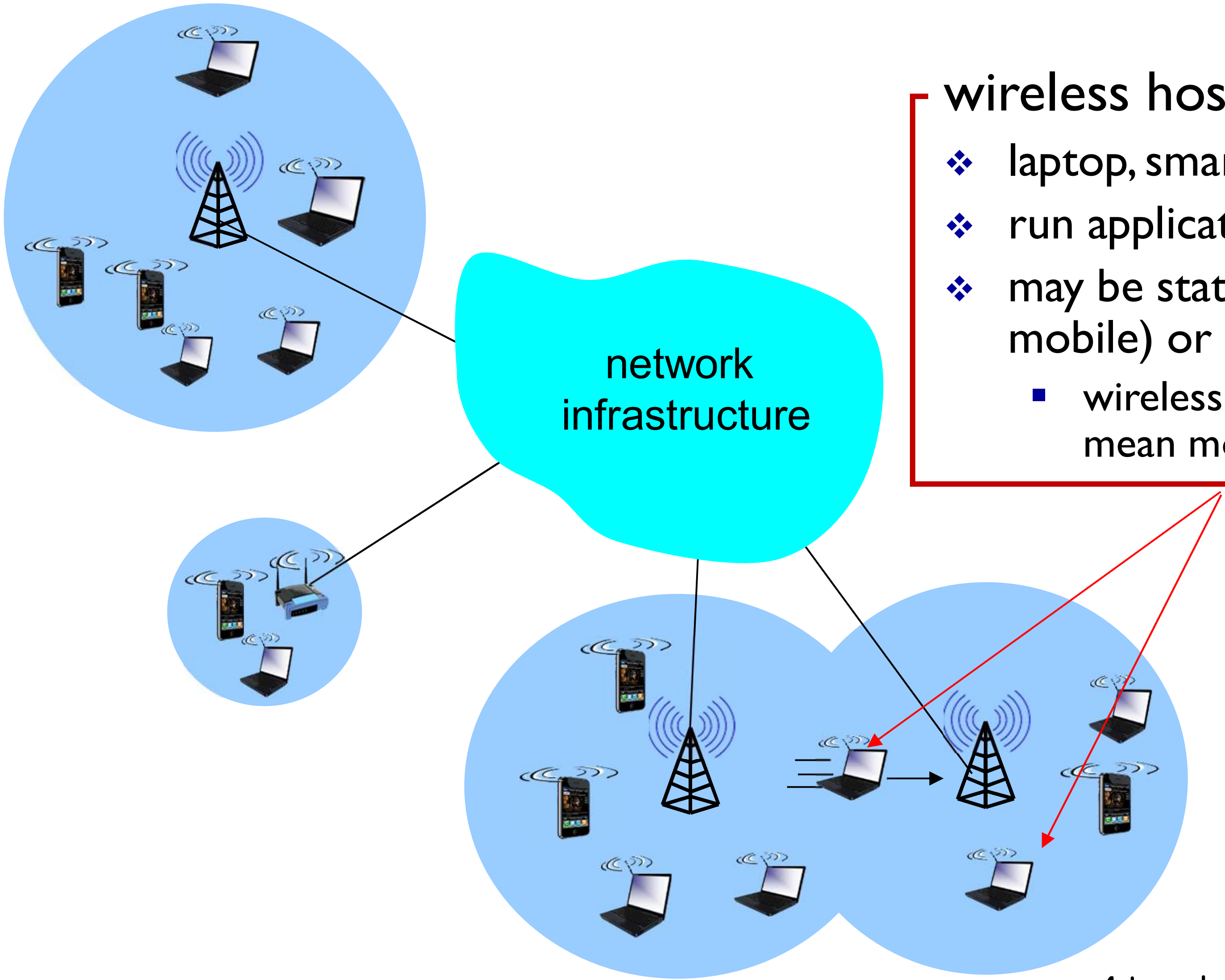
WMAN 802.16 (Broadband Wireless Access) **WiMAX**

+ Mobility
WiBro, 802.20

Elements of a wireless network



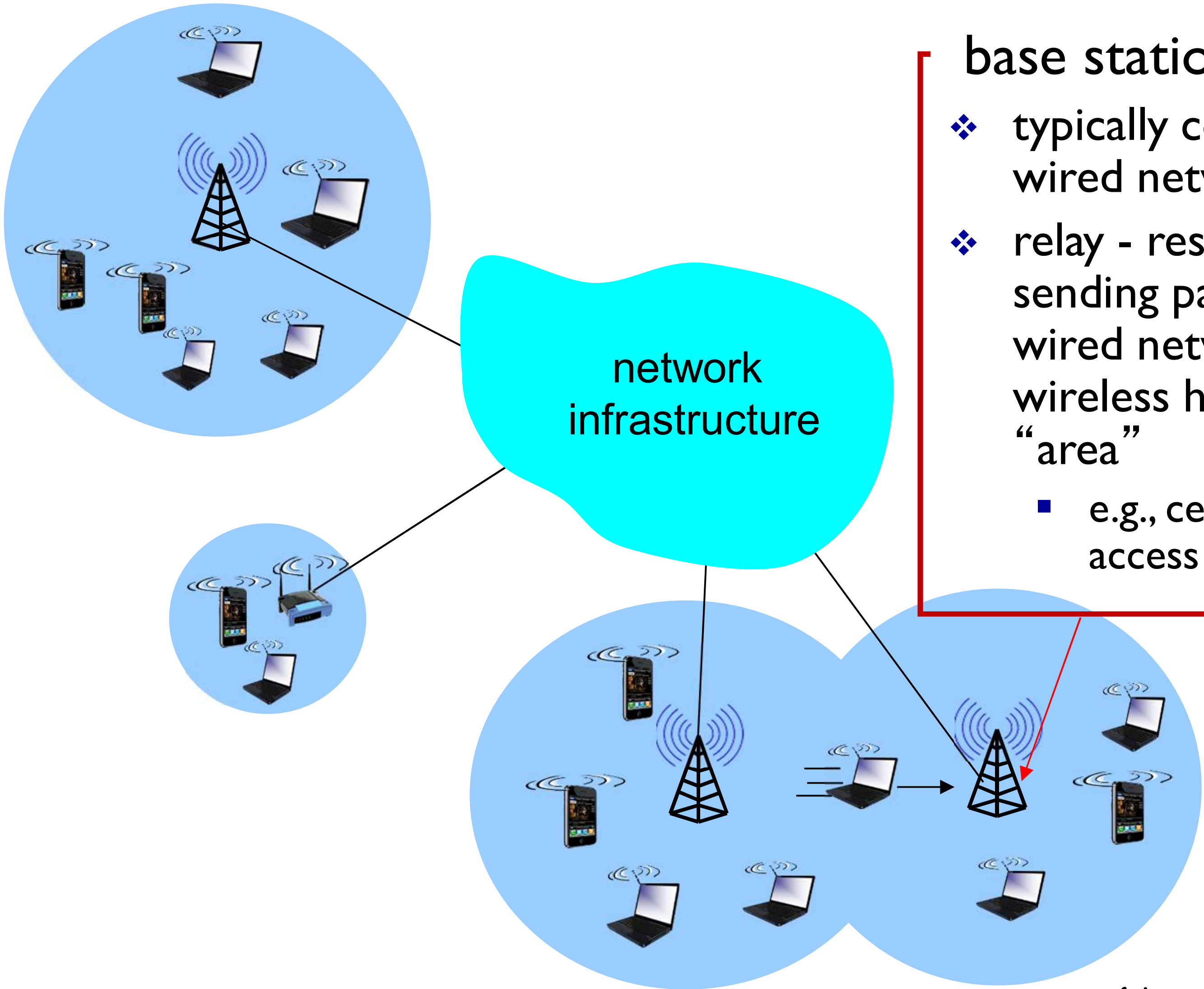
Elements of a wireless network



wireless hosts

- laptop, smartphone
- run applications
- may be stationary (non-mobile) or mobile
  - wireless does *not* always mean mobility

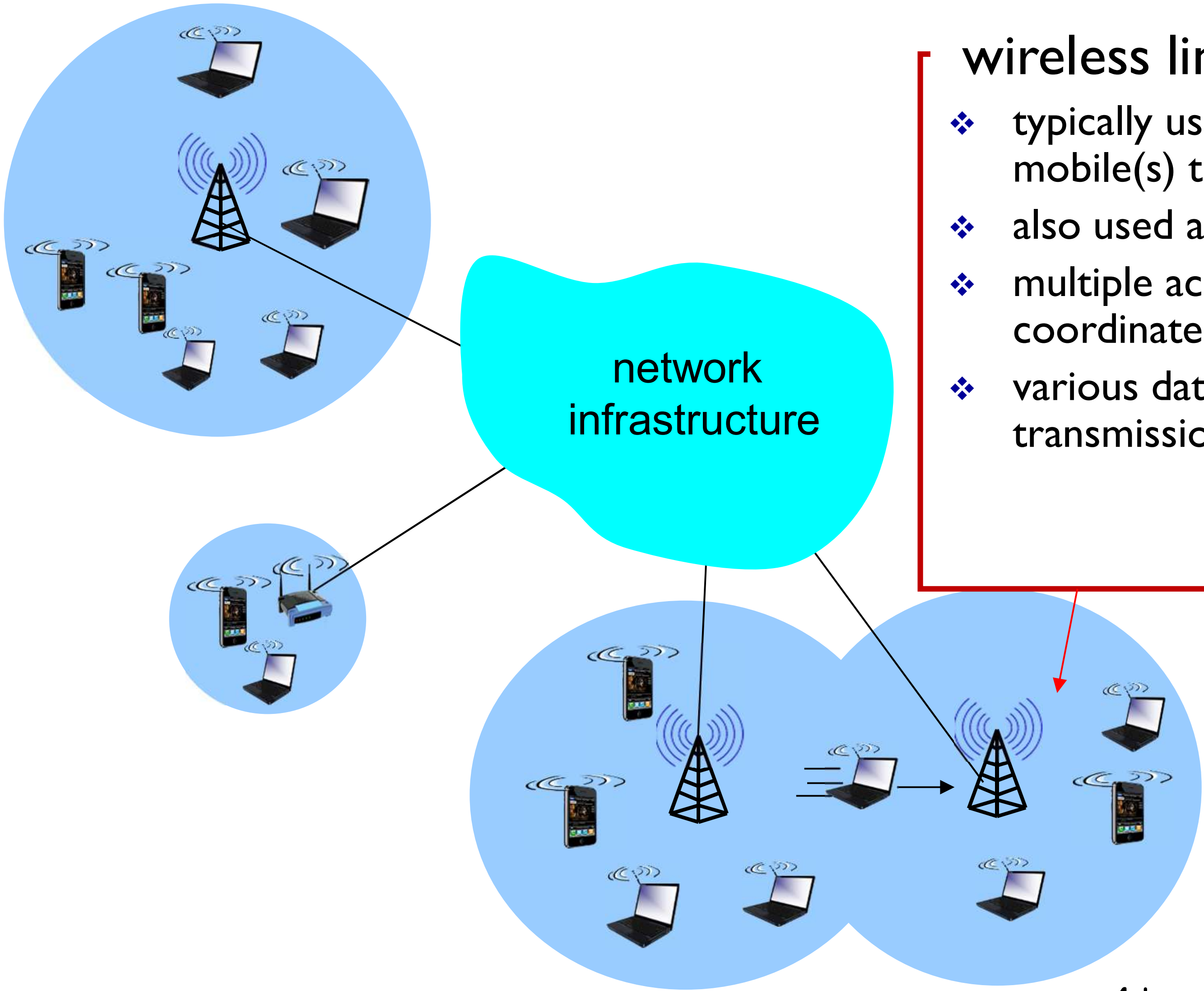
Elements of a wireless network



base station

- typically connected to wired network
- relay - responsible for sending packets between wired network and wireless host(s) in its "area"
  - e.g., cell towers, 802.11 access points

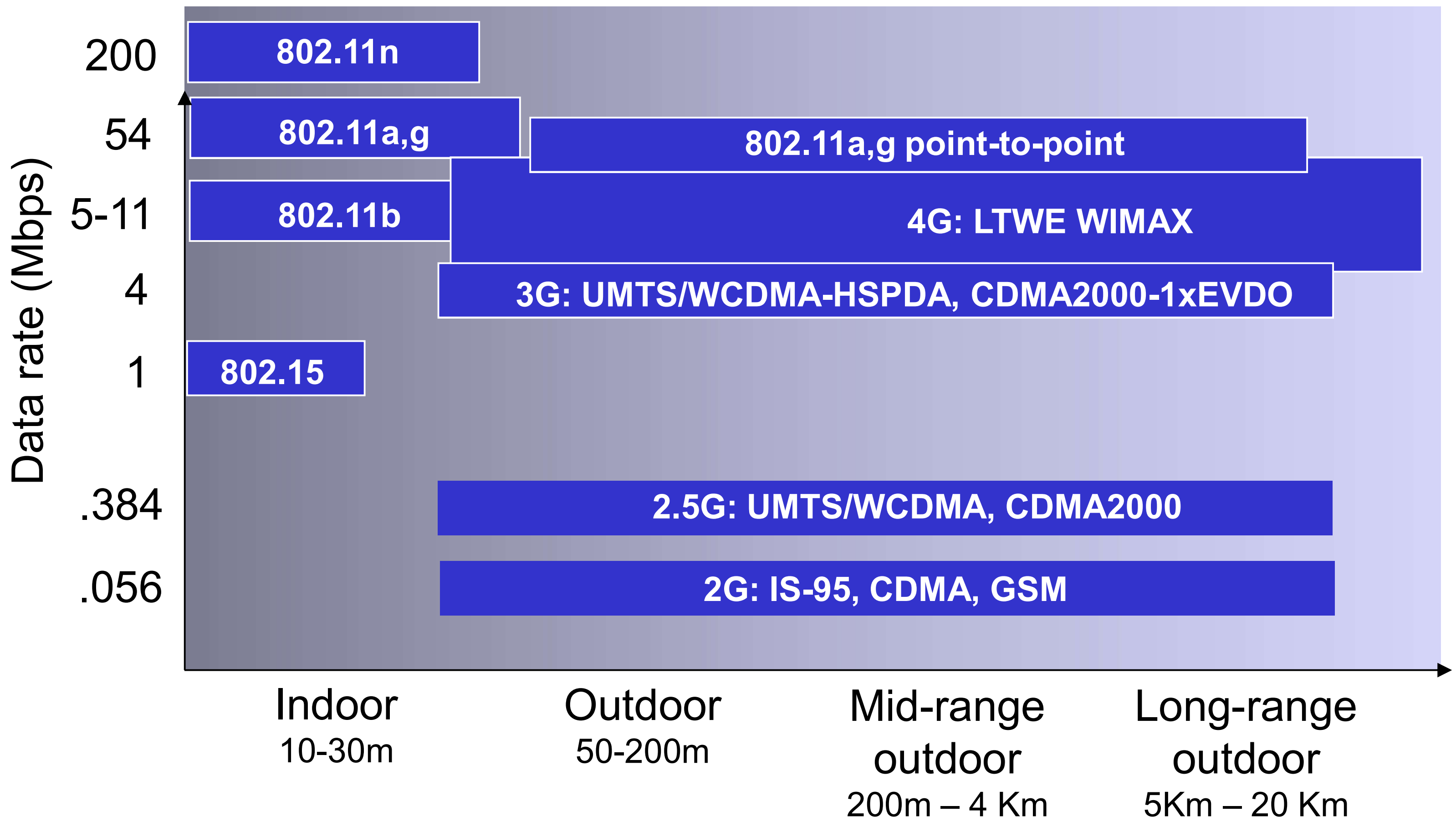
Elements of a wireless network



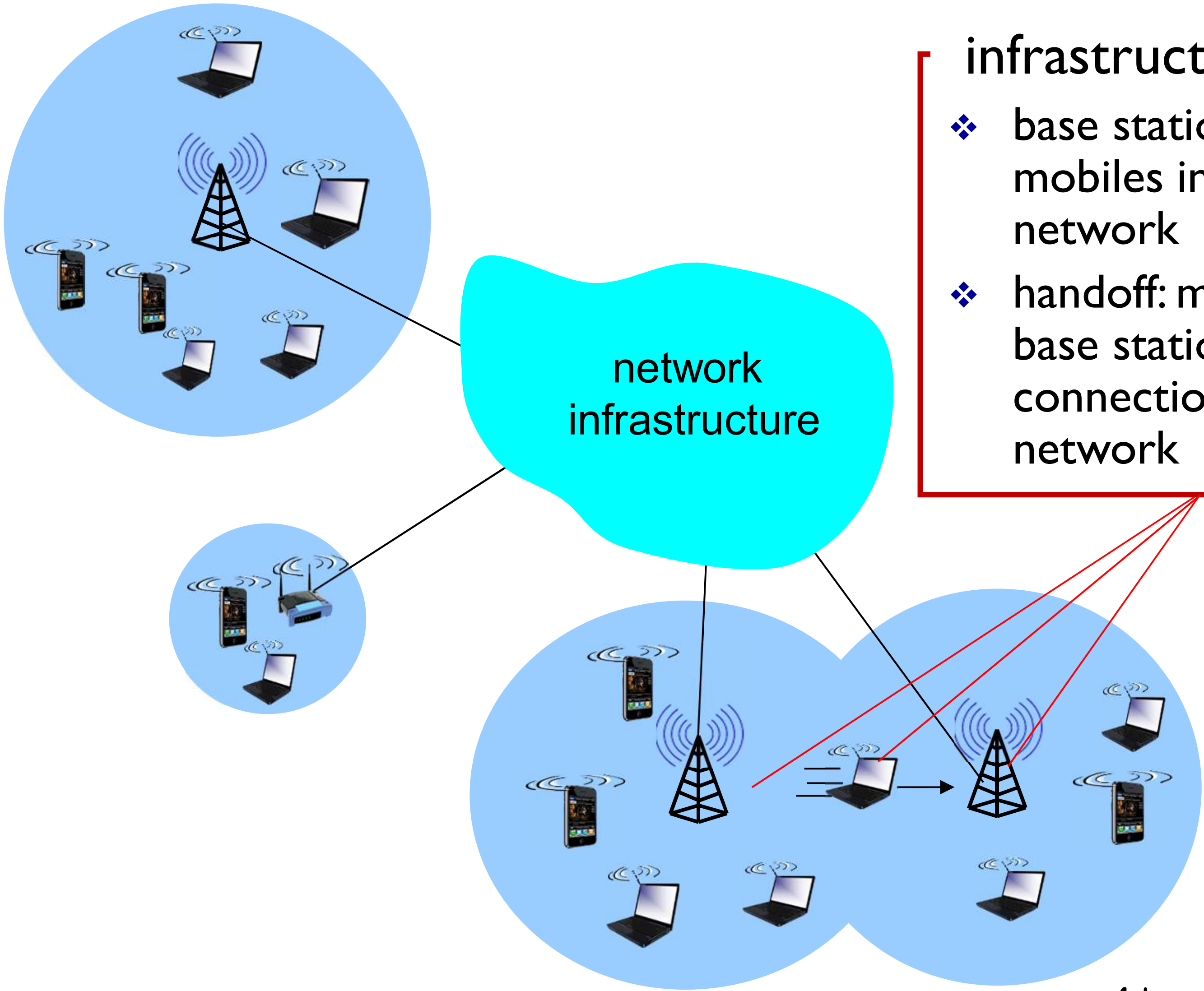
wireless link

- typically used to connect mobile(s) to base station
- also used as backbone link
- multiple access protocol coordinates link access
- various data rates, transmission distance

Characteristics of selected wireless links



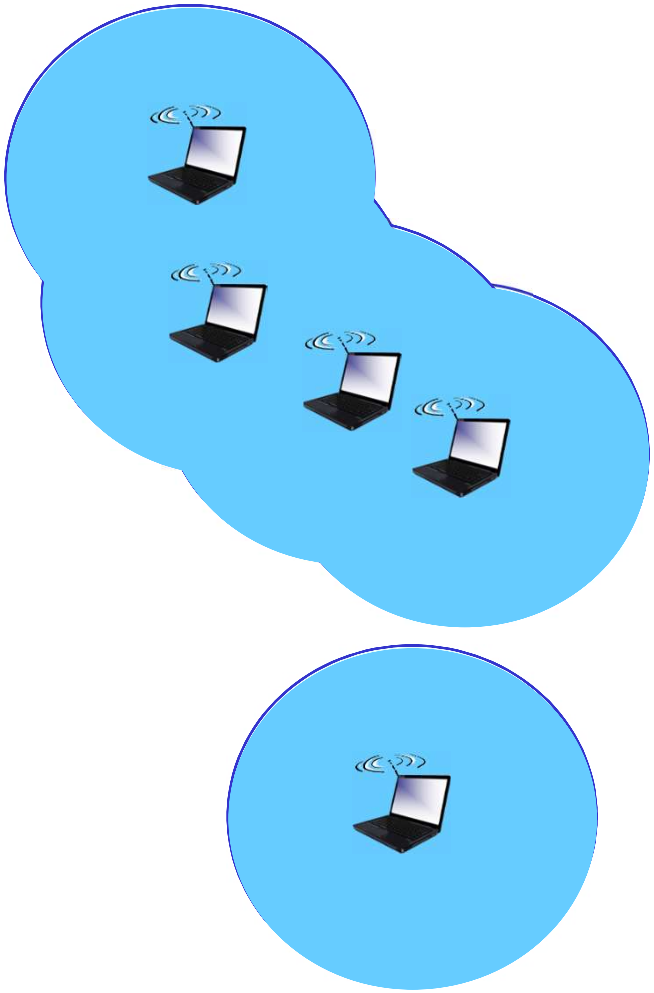
Elements of a wireless network



infrastructure mode

- base station connects mobiles into wired network
- handoff: mobile changes base station providing connection into wired network

Elements of a wireless network



ad hoc mode

- no base stations
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves

Wireless network taxonomy

	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet: *mesh net*
no infrastructure	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	no base station, no connection to larger Internet. May have to relay to reach other a given wireless node MANET, VANET

Wireless Link Characteristics (1)

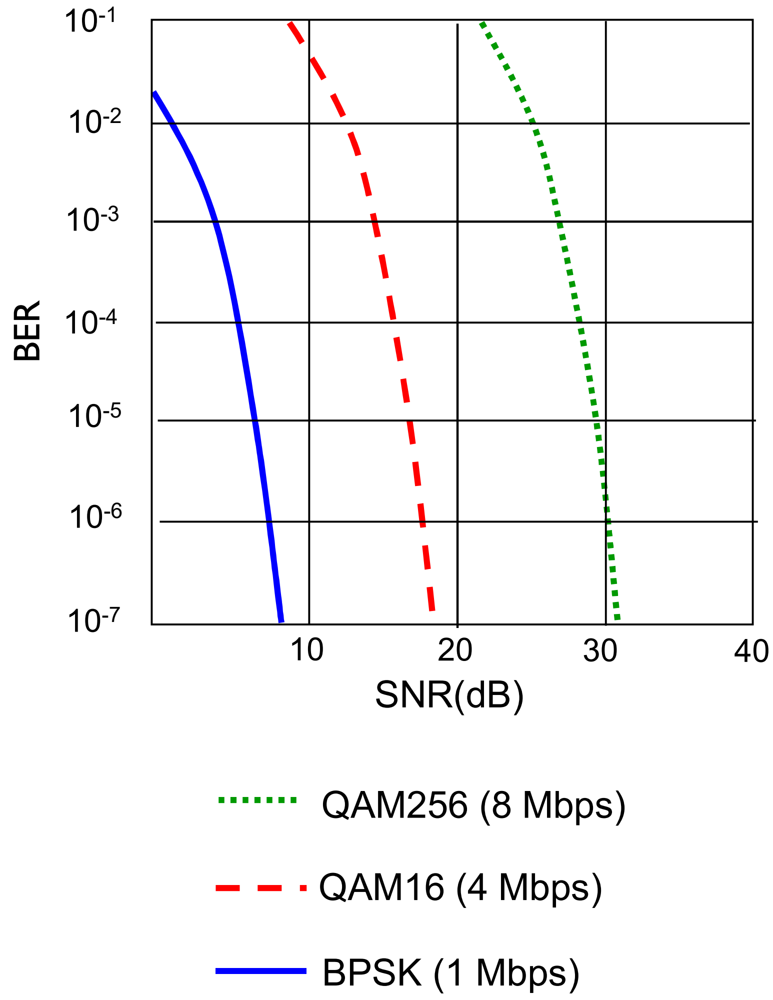
important differences from wired link ….

- *decreased signal strength:* radio signal attenuates as it propagates through matter (path loss)
- *interference from other sources:* standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- *multipath propagation:* radio signal reflects off objects ground, arriving ad destination at slightly different times

…. make communication across (even a point to point) wireless link much more "difficult"

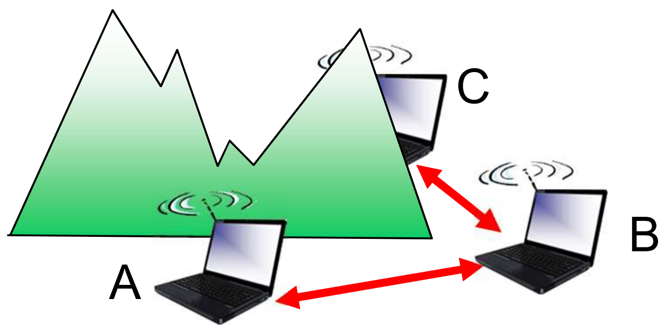
Wireless Link Characteristics (2)

- SNR: signal-to-noise ratio
  - larger SNR – easier to extract signal from noise (a "good thing")
- *SNR versus BER tradeoffs*
  - *given physical layer:* increase power -> increase SNR->decrease BER
  - *given SNR:* choose physical layer that meets BER requirement, giving highest thruput
    - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)



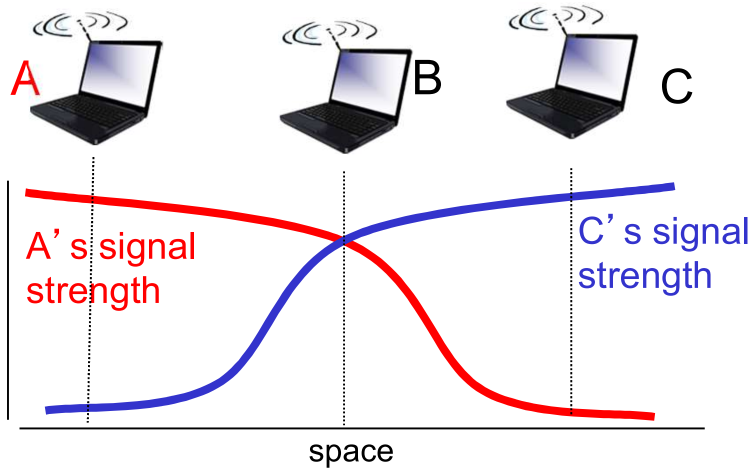
Wireless network characteristics

Multiple wireless senders and receivers create additional problems (beyond multiple access):



Hidden terminal problem

- B, A hear each other
- B, C hear each other
- A, C can not hear each other means A, C unaware of their interference at B



Signal attenuation:

- B, A hear each other
- B, C hear each other
- A, C can not hear each other interfering at B

IEEE 802.11 Wireless LAN

802.11b

- 2.4-5 GHz unlicensed spectrum
- up to 11 Mbps
- direct sequence spread spectrum (DSSS) in physical layer
  - all hosts use same chipping code

802.11a

- 5-6 GHz range
- up to 54 Mbps

802.11g

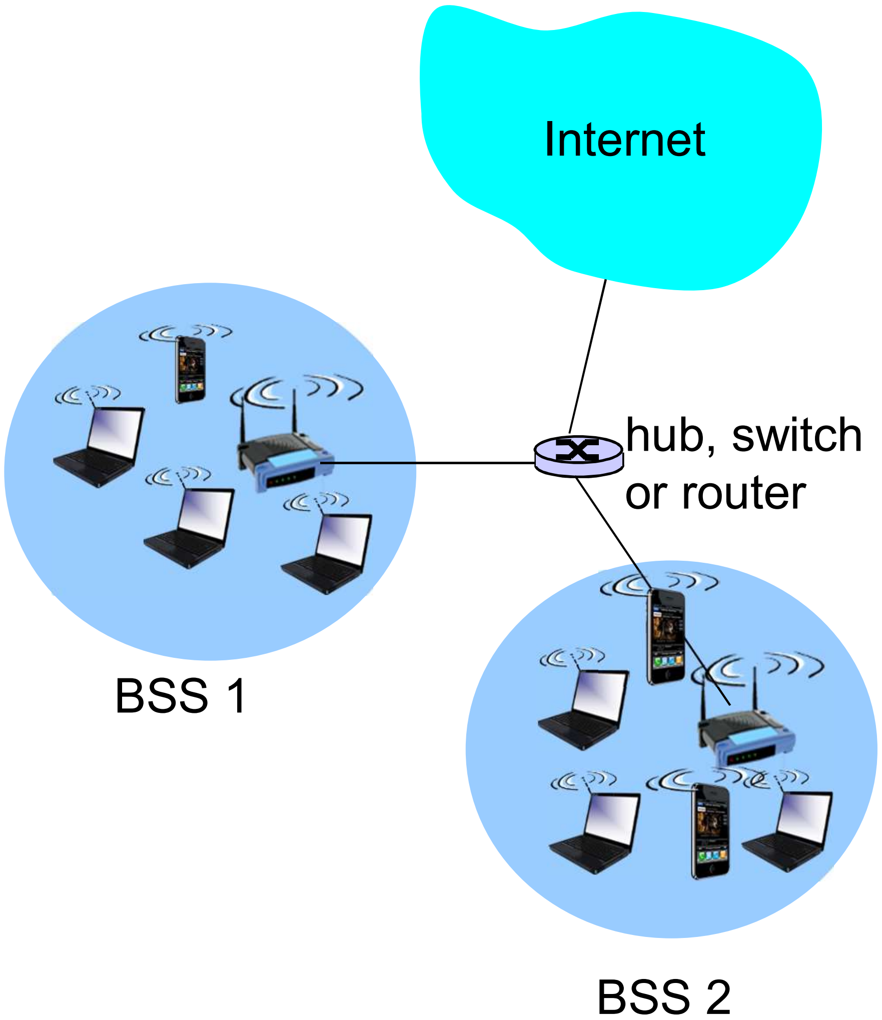
- 2.4-5 GHz range
- up to 54 Mbps

802.11n: multiple antennae

- 2.4-5 GHz range
- up to 200 Mbps

- all use CSMA/CA for multiple access
- all have base-station and ad-hoc network versions

802.11 LAN architecture

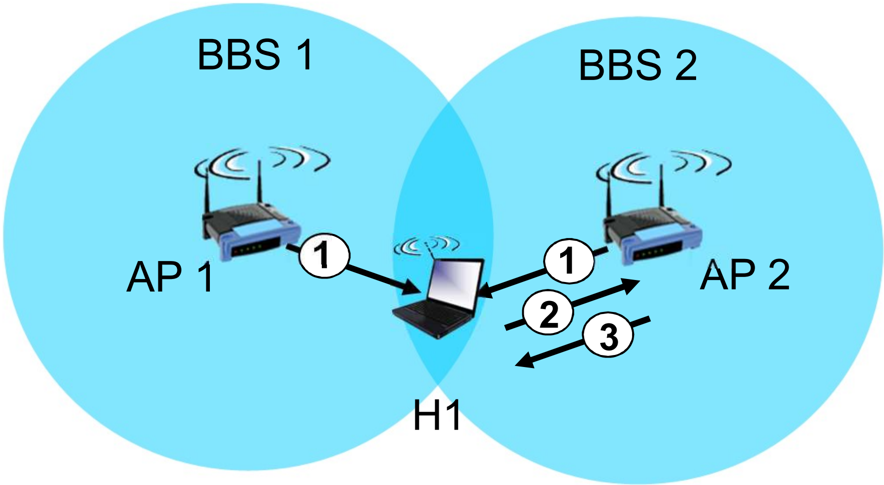


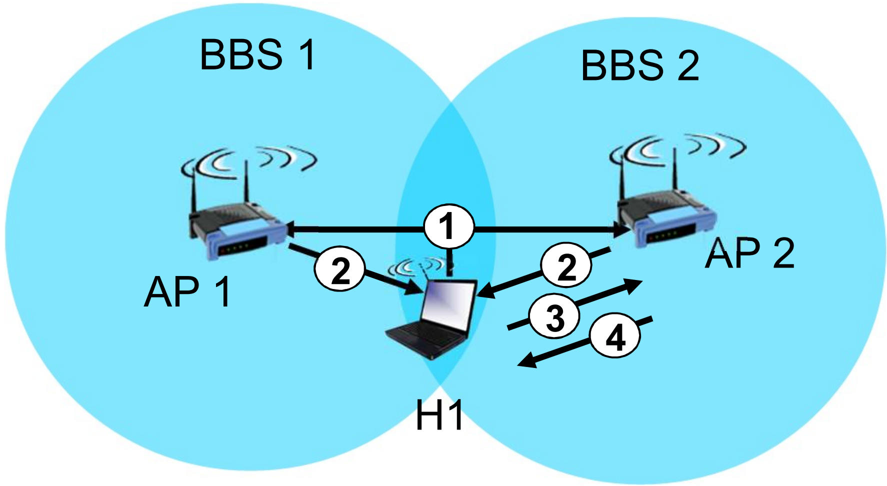
- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

802.11: Channels, association

- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  - AP admin chooses frequency for AP
  - interference possible: channel can be same as that chosen by neighboring AP!
- host: must *associate* with an AP
  - scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
  - selects AP to associate with
  - may perform authentication [Chapter 8]
  - will typically run DHCP to get IP address in AP's subnet

802.11: passive/active scanning





passive scanning:

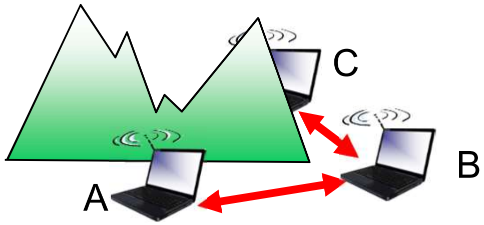
(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent from selected AP to H1

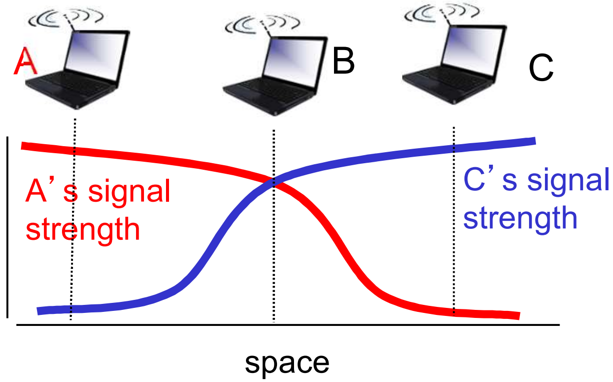
active scanning:

(1) Probe Request frame broadcast from H1
(2) Probe Response frames sent from APs
(3) Association Request frame sent: H1 to selected AP
(4) Association Response frame sent from selected AP to H1

IEEE 802.11: multiple access

- avoid collisions: 2+ nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
  - don't collide with ongoing transmission by other node
- 802.11: *no* collision detection!
  - difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
  - can't sense all collisions in any case: hidden terminal, fading
  - goal: *avoid collisions:* CSMA/C(ollision)A(voidance)





IEEE 802.11 MAC Protocol: CSMA/CA

802.11 sender

1 if sense channel idle for **DIFS** then

transmit entire frame (no CD)

2 if sense channel busy then

start random backoff time

timer counts down while channel idle

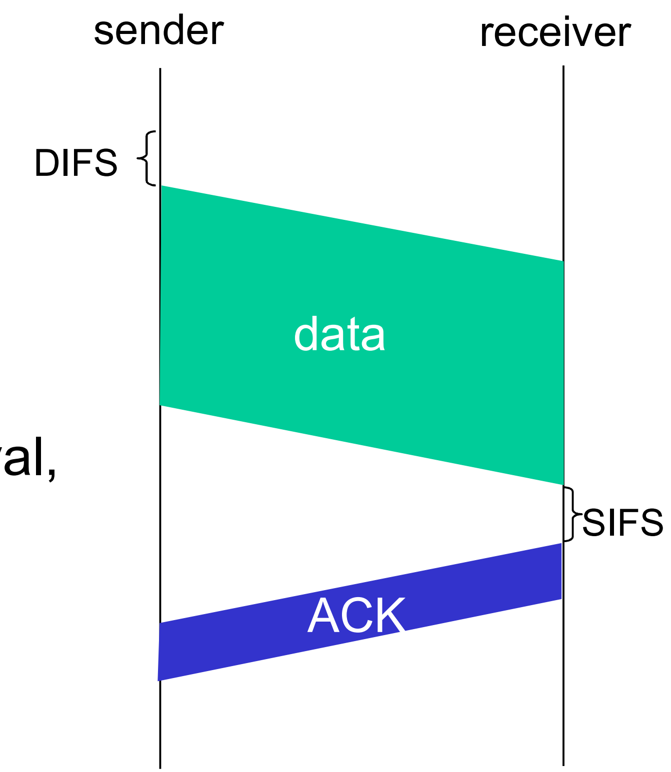
transmit when timer expires

if no ACK, increase random backoff interval, repeat 2

802.11 receiver

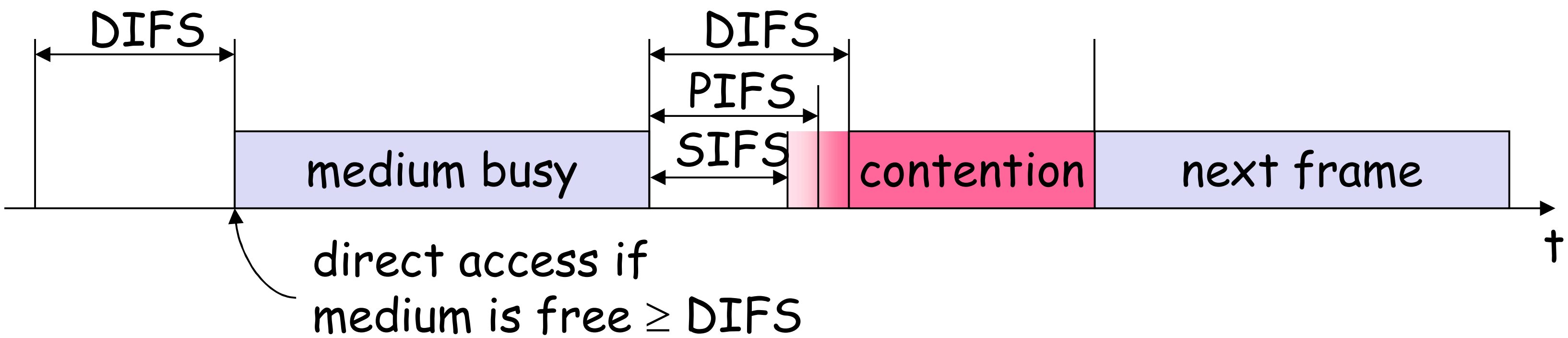
- if frame received OK

return ACK after **SIFS** (ACK needed due to hidden terminal problem)

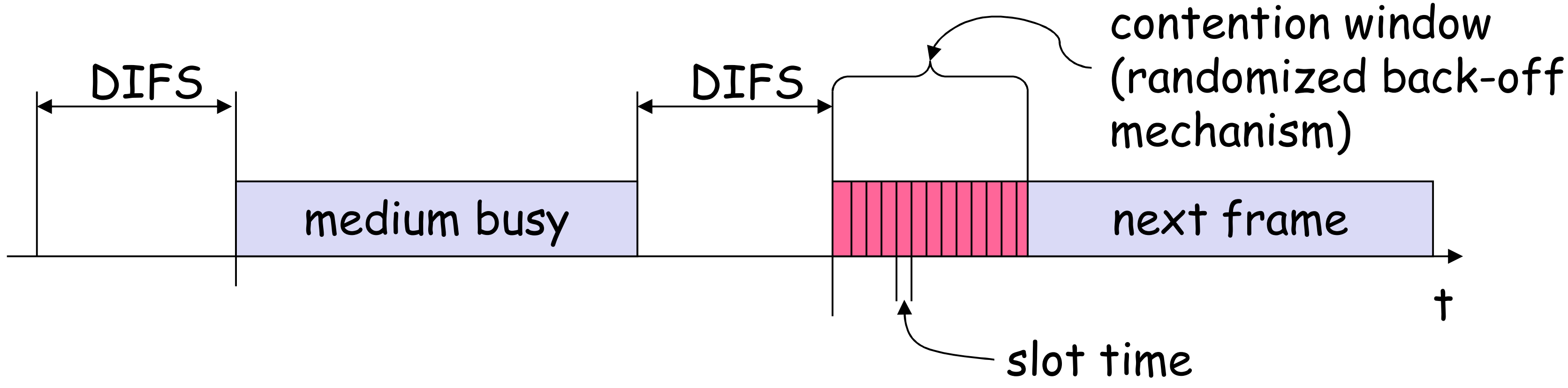


802.11 - MAC

- 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

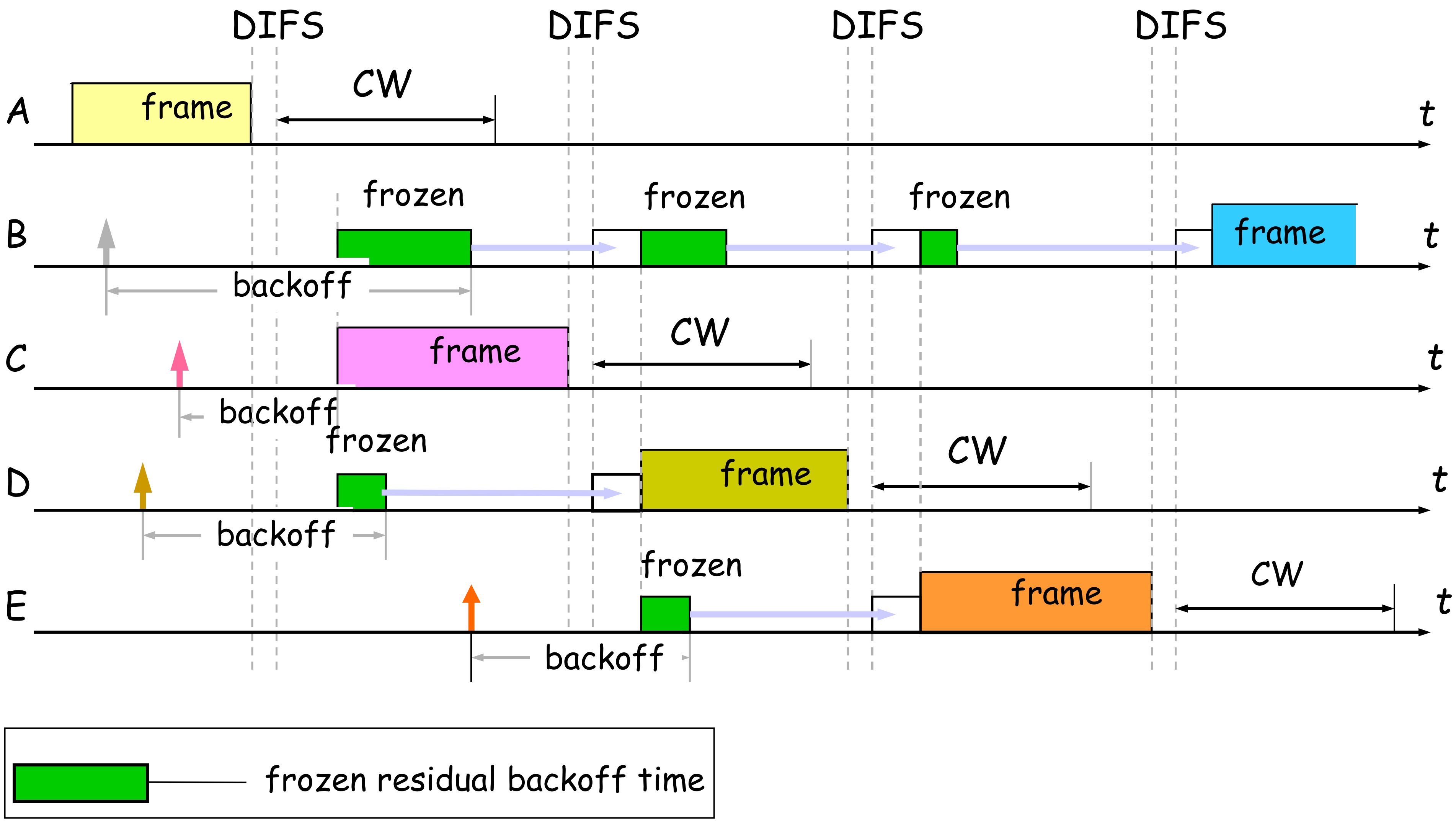


CSMA/CA access method



- 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

A simplified example



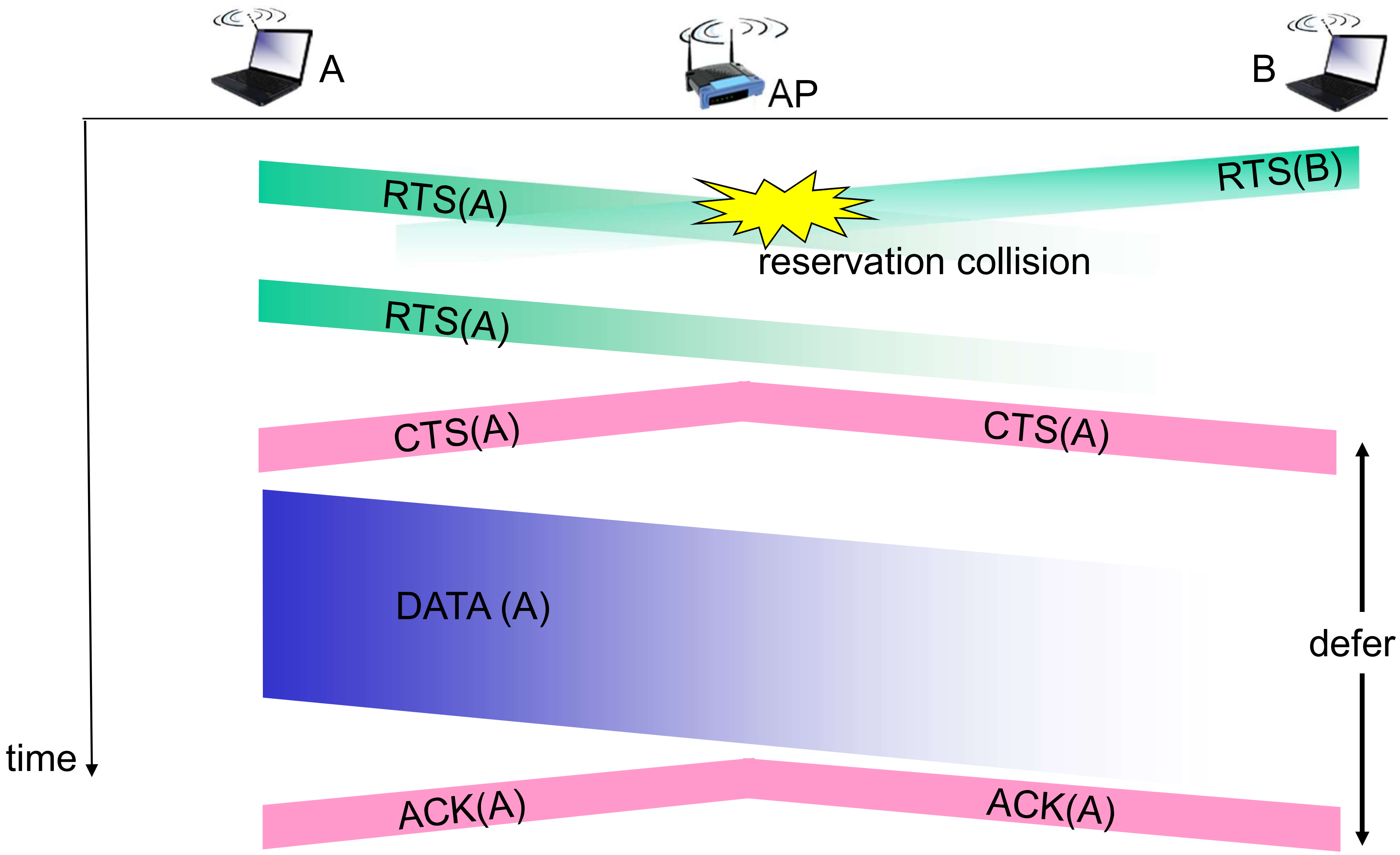
Avoiding collisions (more)

idea: allow sender to "reserve" channel rather than random access of data frames: avoid collisions of long data frames

- sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
  - RTSs may still collide with each other (but they're short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

avoid data frame collisions completely using small reservation packets!

Collision Avoidance: RTS-CTS exchange



802.11 frame: addressing

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

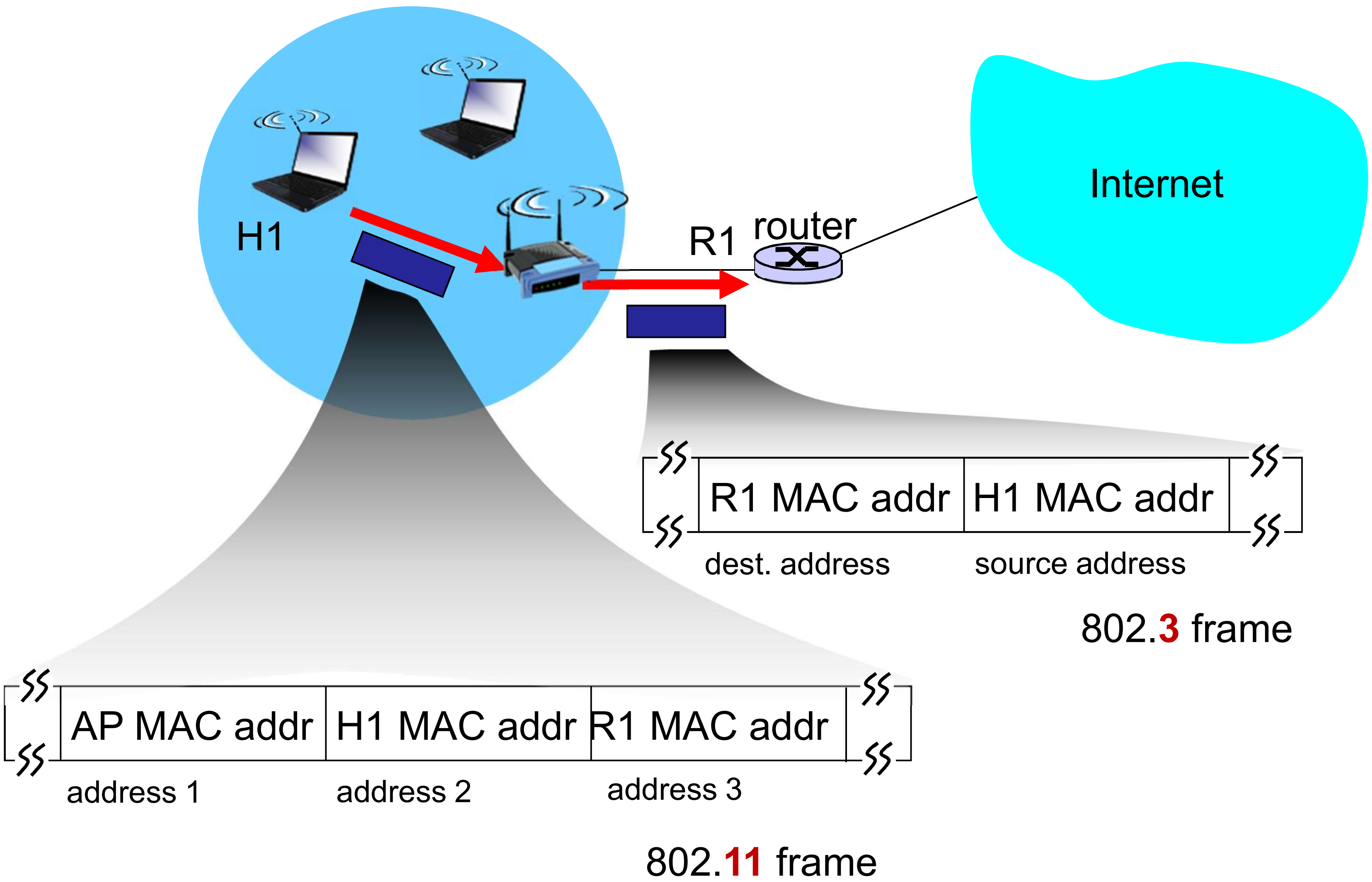
Address 1: MAC address of wireless host or AP to receive this frame

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

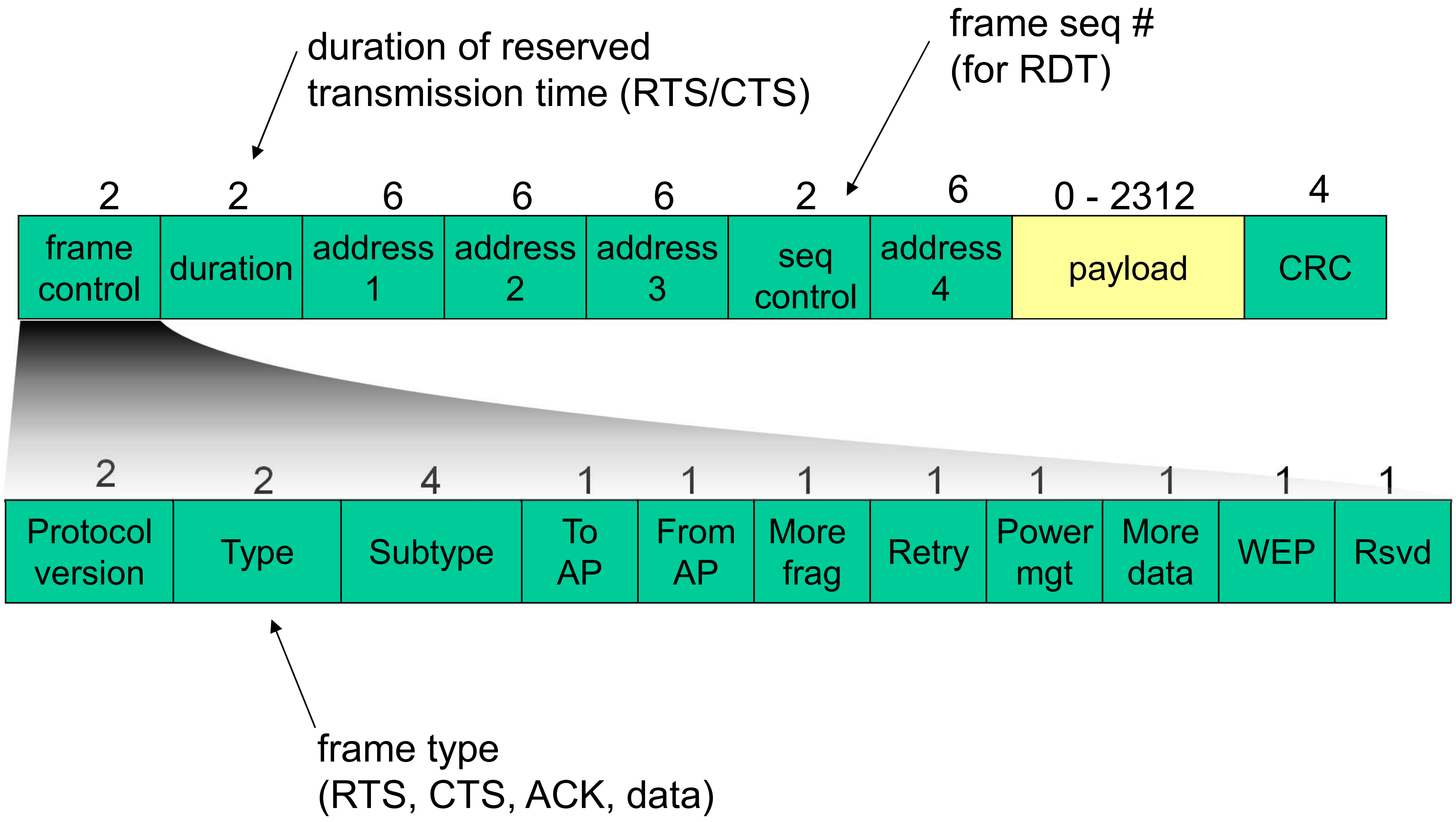
Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

802.11 frame: addressing



802.11 frame: more



Special Frames: ACK, RTS, CTS

- Acknowledgement

ACK

bytes 2	2	6	4
Frame Control	Duration	Receiver Address	CRC

- Request To Send

RTS

bytes 2	2	6	6	4
Frame Control	Duration	Receiver Address	Transmitter Address	CRC

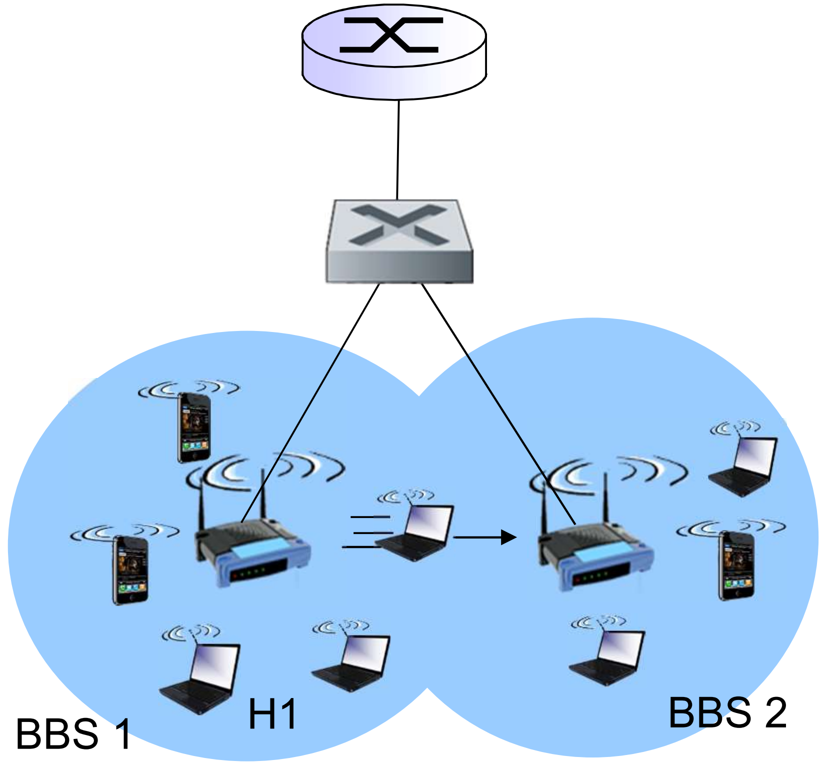
- Clear To Send

CTS

bytes 2	2	6	4
Frame Control	Duration	Receiver Address	CRC

802.11: mobility within same subnet

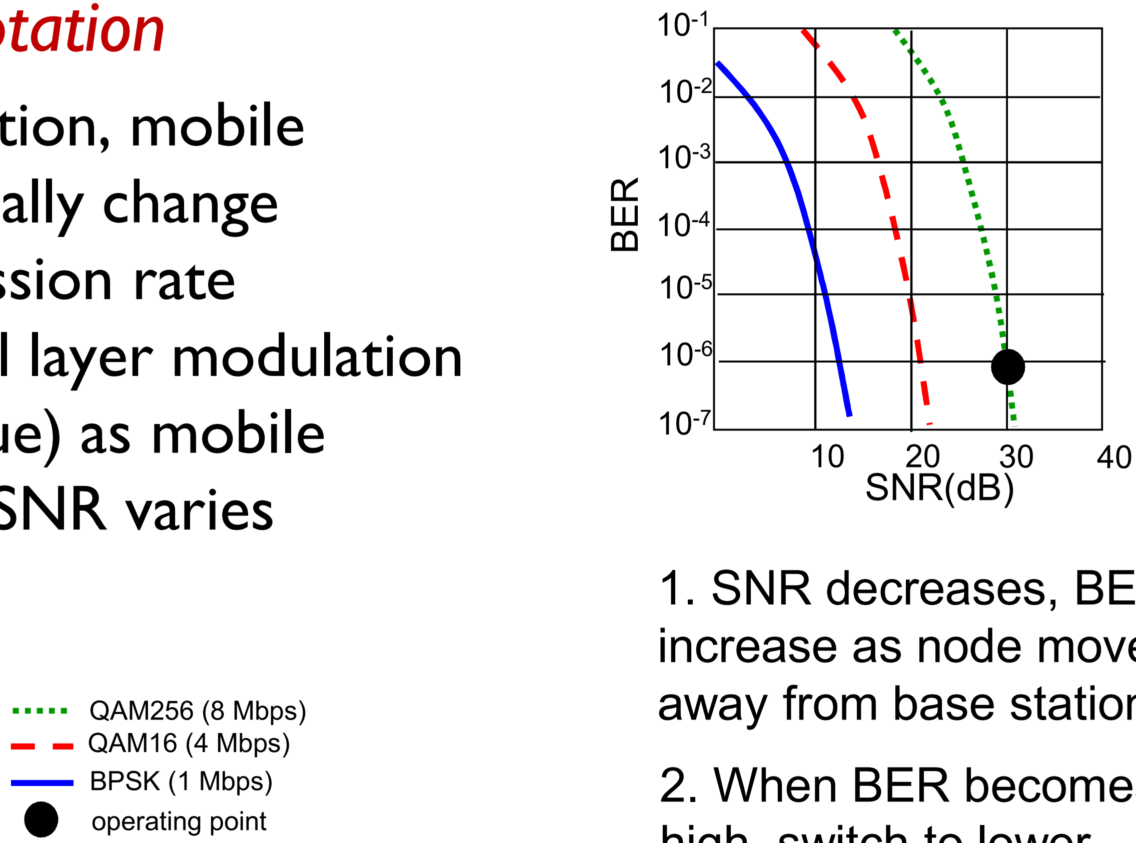
- H1 remains in same IP subnet: IP address can remain same
- switch: which AP is associated with H1?
  - self-learning (Ch. 5): switch will see frame from H1 and "remember" which switch port can be used to reach H1



802.11: advanced capabilities

Rate adaptation

- base station, mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies



1. SNR decreases, BER increase as node moves away from base station

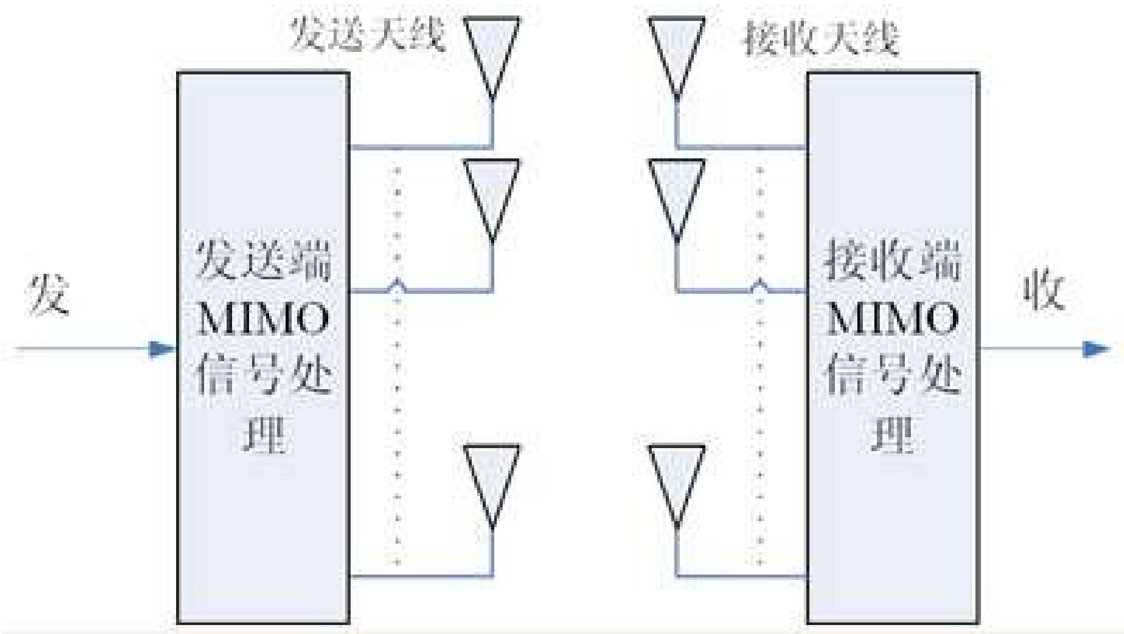
2. When BER becomes too high, switch to lower transmission rate but with lower BER

802.11: advanced capabilities

power management

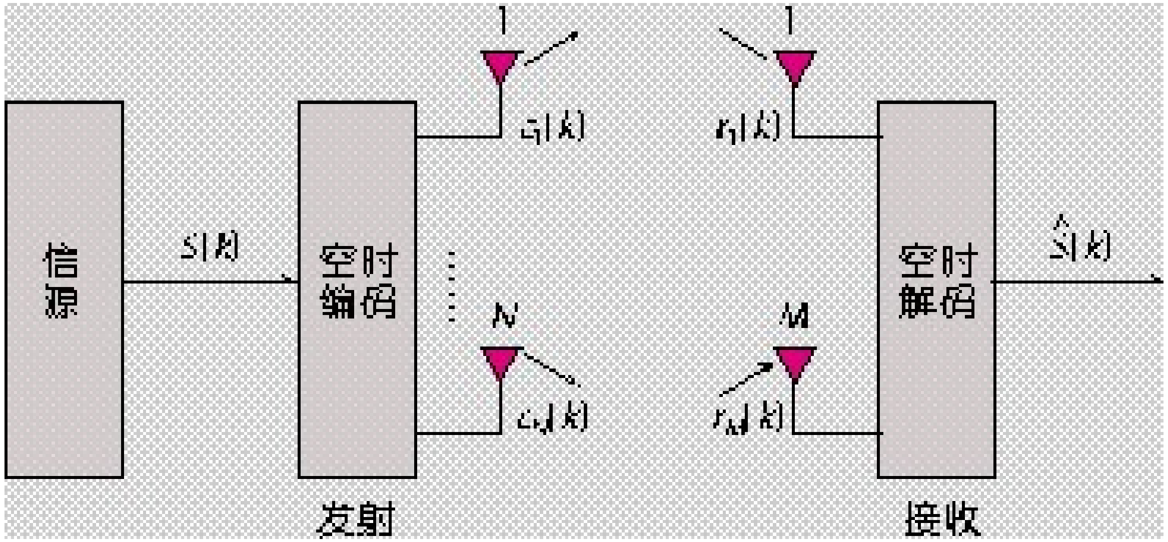
- node-to-AP: "I am going to sleep until next beacon frame"
  - AP knows not to transmit frames to this node
  - node wakes up before next beacon frame
- beacon frame: contains list of mobiles with AP-to-mobile frames waiting to be sent
  - node will stay awake if AP-to-mobile frames to be sent; otherwise sleep again until next beacon frame

Basic Principles of MIMO



$$C = [min(M, N)]B\log_2(\rho/2)$$

Basic Principles of MIMO

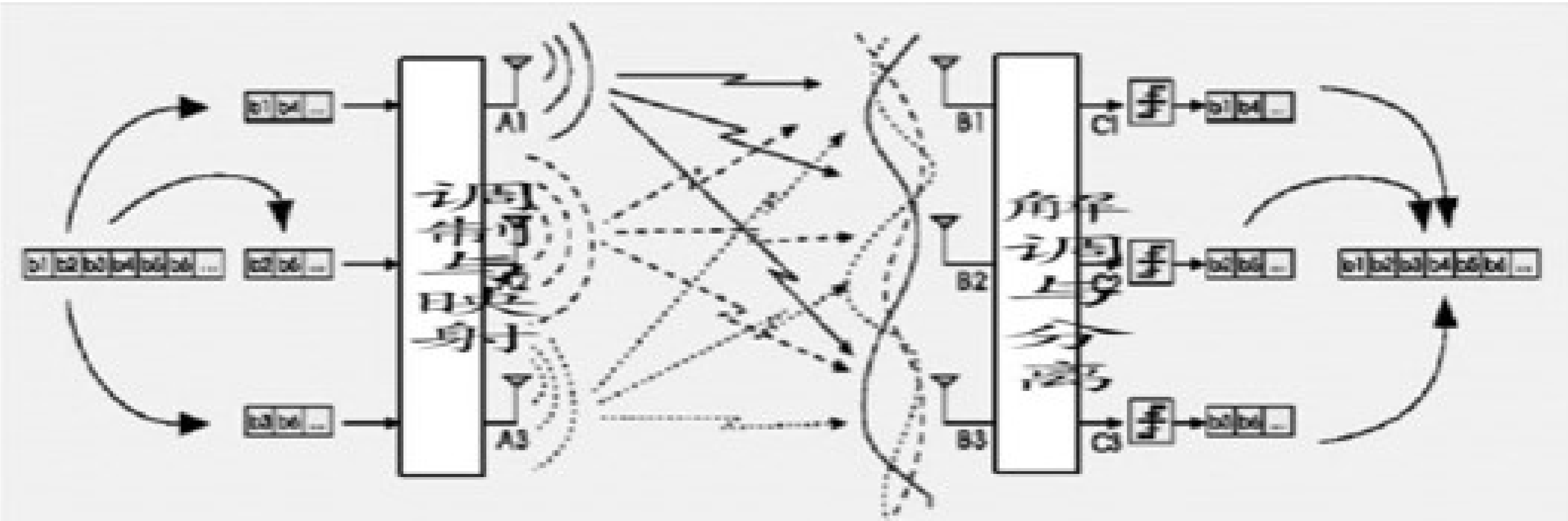


Main technology:

- Spatial Multiplexing
- Space Time Coding
- Beam Forming

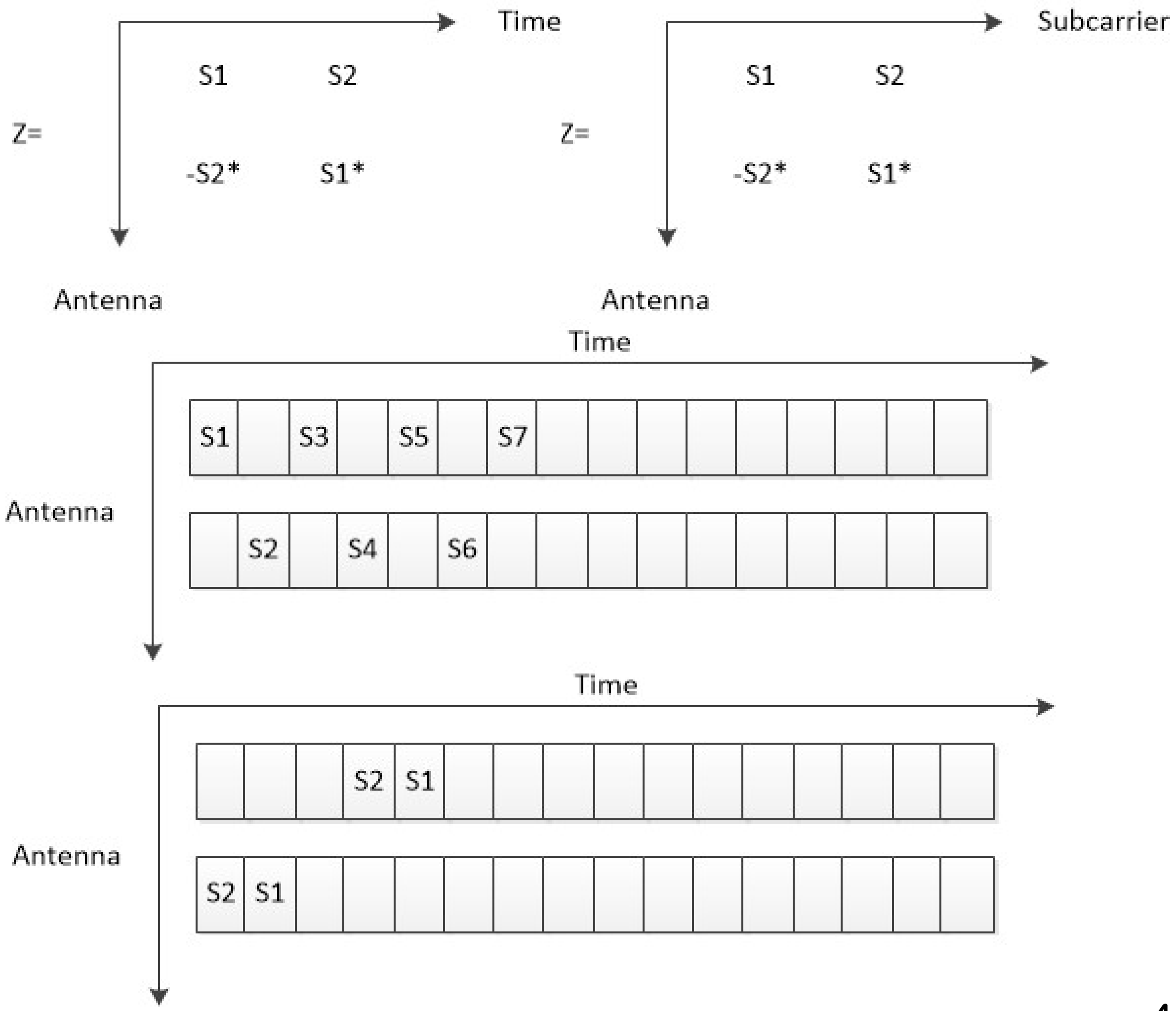
Basic Principles of MIMO

Spatial Multiplexing



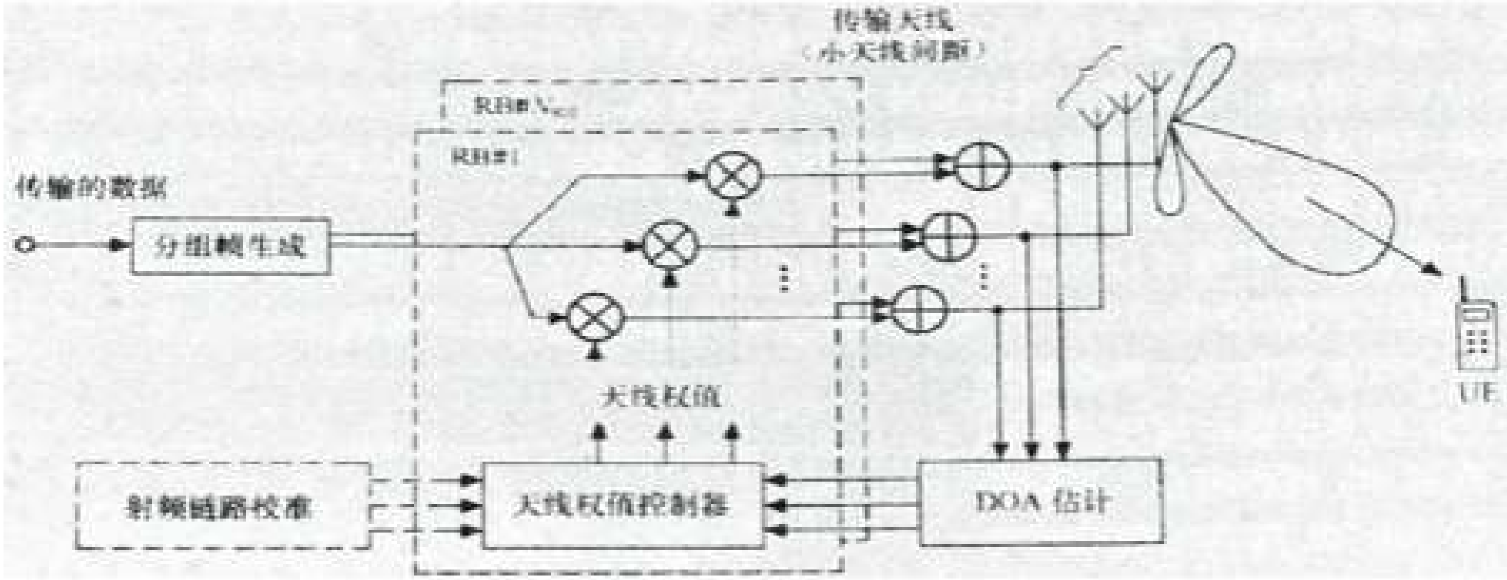
Basic Principles of MIMO

Space Time Coding



Basic Principles of MIMO

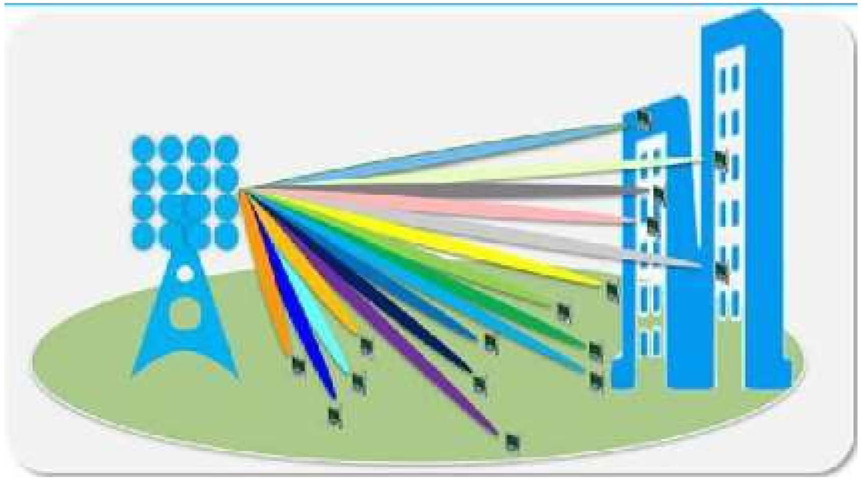
Beam Forming



波束赋形示意图

5G technology

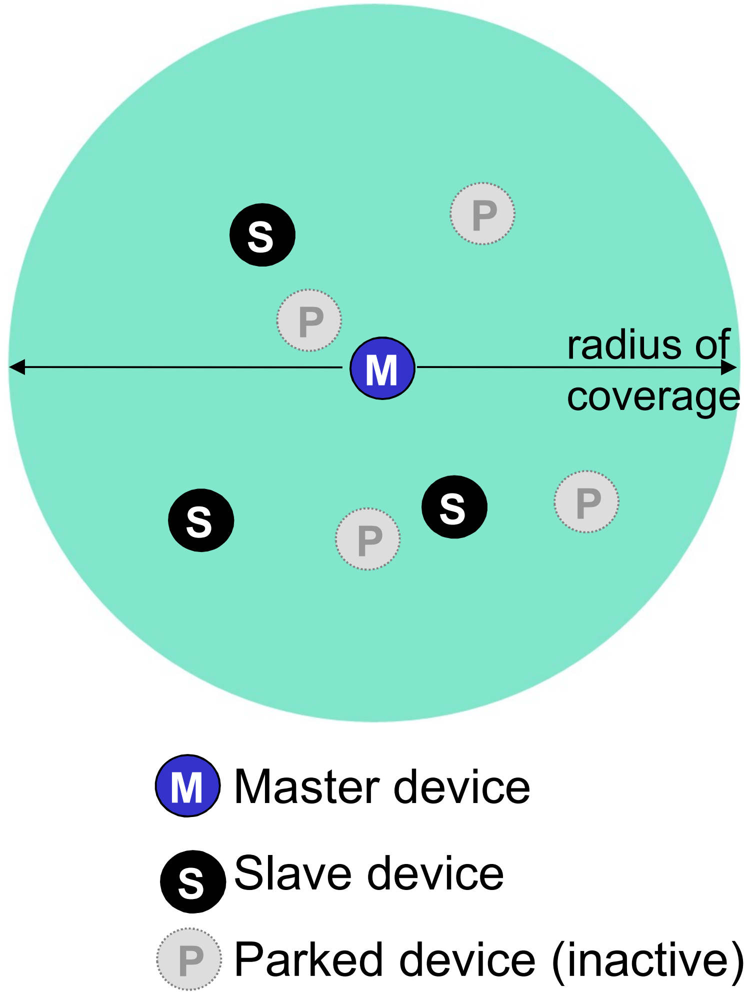
5G Main technology
- Massive MIMO
- NOMA



$$C_{sum} <=> \sum_{Cells} \sum_{Channels} B_i \log_2 \left(1 + \frac{P_i}{I_i + N_i}\right)$$

802.15: personal area network

- less than 10 m diameter
- replacement for cables (mouse, keyboard, headphones)
- ad hoc: no infrastructure
- master/slaves:
  - slaves request permission to send (to master)
  - master grants requests
- 802.15: evolved from Bluetooth specification
  - 2.4-2.5 GHz radio band
  - up to 721 kbps

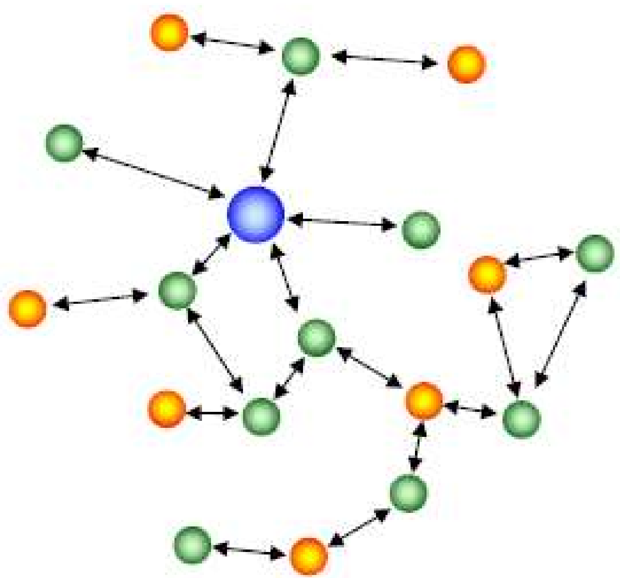


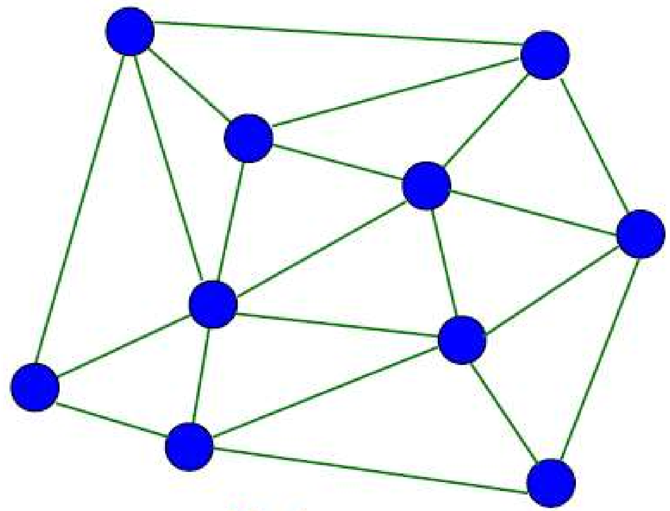
ZigBee overview

- 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.

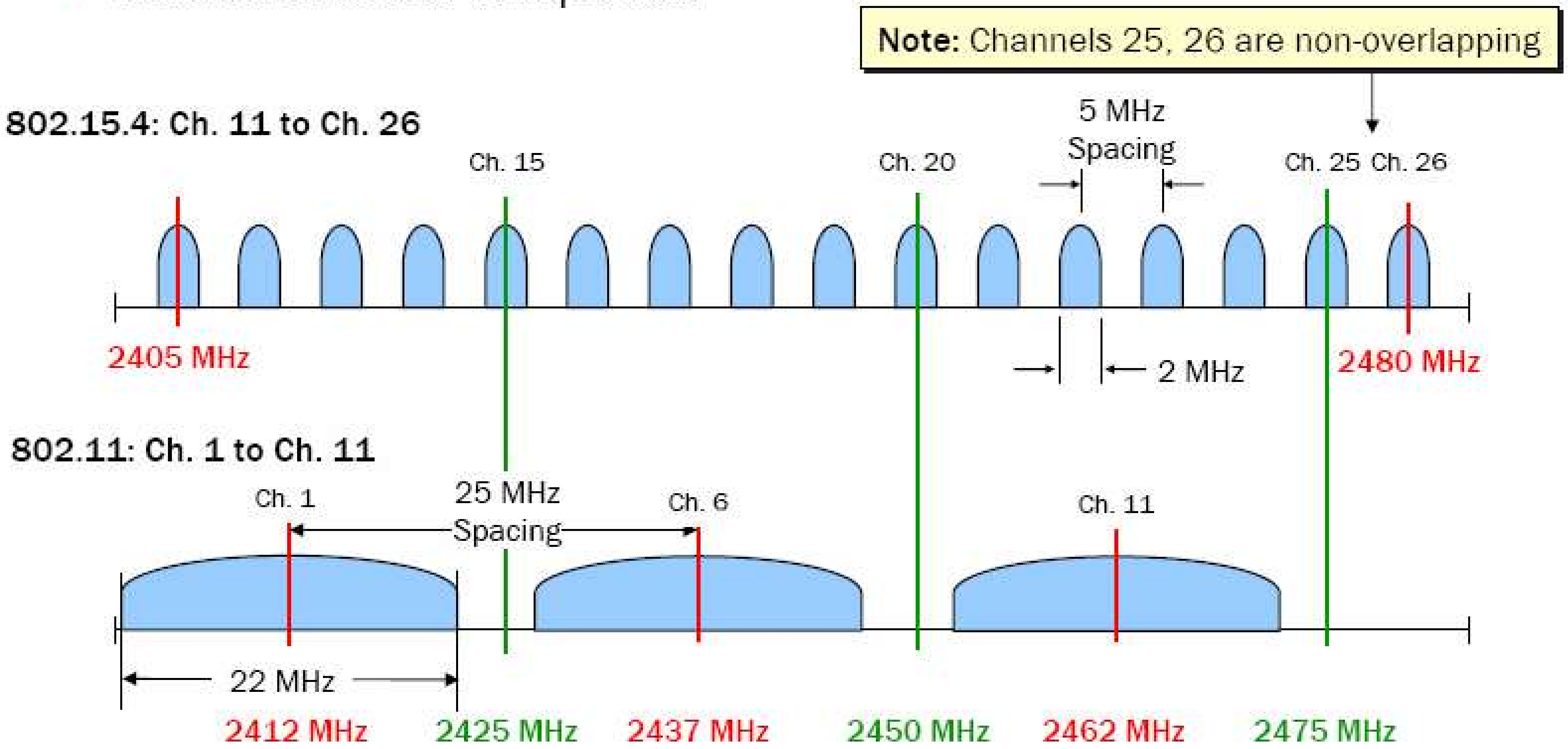




Interference and Coexistence in the 2.4GHz Band

802.15.4 and 802.11b Spectrum Relationship

Co-exists with WiFi, Bluetooth
- Channel selection is important



Chapter 4:Local area network Summary

- principles behind data link layer services:
  - framing
  - error detection, correction
  - reliable data transfer
  - sharing a broadcast channel: multiple access
- various link layer technologies
  - LAN model
  - Ethernet
  - hubs, bridges, switches
  - IEEE 802.11
  - IEEE 802.15