Wireless network technologies: WLAN, WPAN, ad hoc networks

Prof. Fabio Martignon

Summary (1)

- Introduction to wireless networks
  - Main differences with wired networks
  - Radio channel
  - Mobility management
- WLAN
  - 802.11 standards
  - Network architecture
  - MAC (legacy and QoS MAC 802.11e)

Summary (2)

- WPAN
  - Bluetooth
    - Network architecture
    - Medium access control
    - Network formation
  - ZigBee
    - Network architecture
    - Medium access control
- Ad Hoc
  - Definitions and basic networking issues
  - Routing schemes

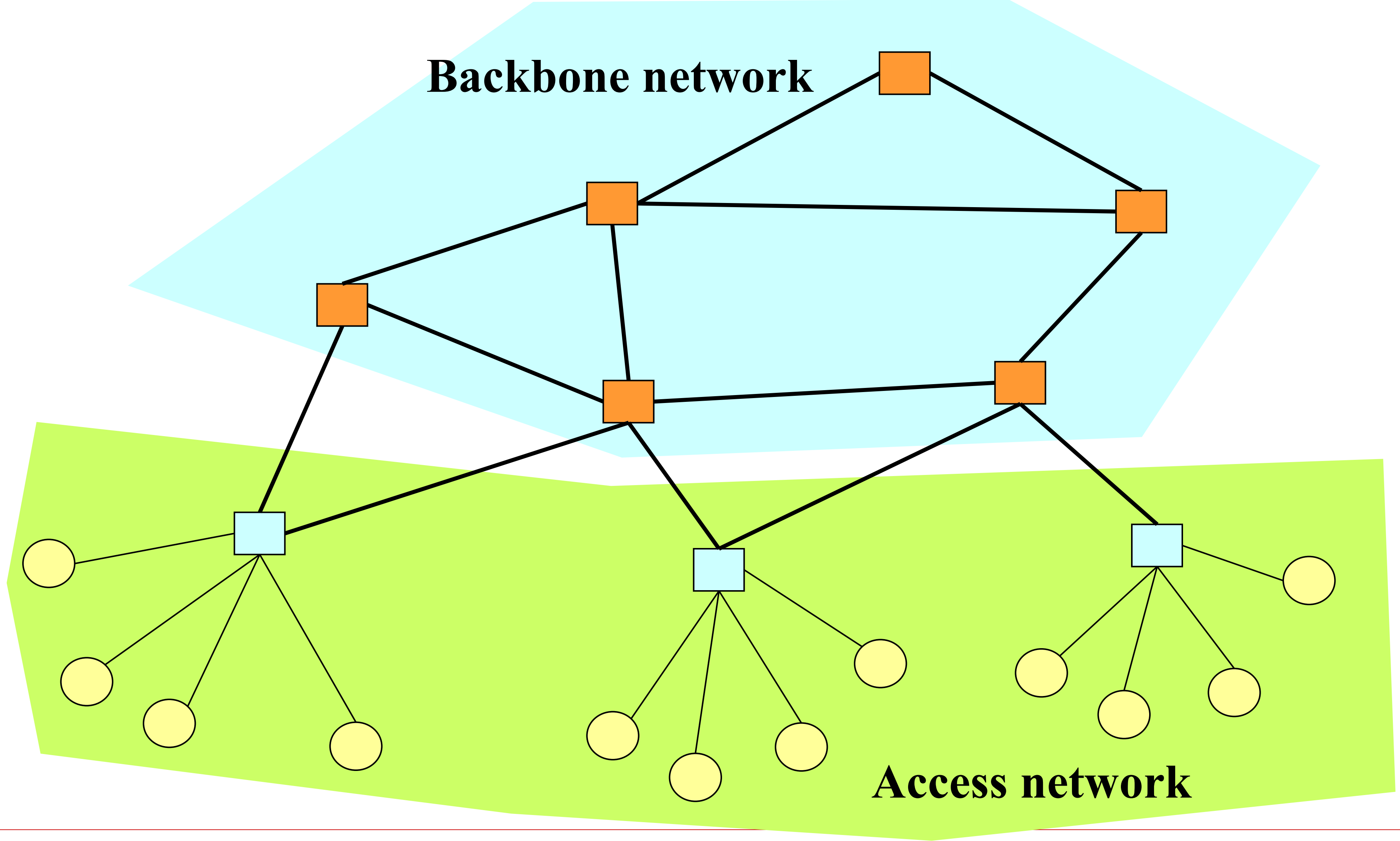
Wireless Networks

Wireless or wired, which is better?

Well, it depends on the situation!

- Is the transmission medium the only difference?
  - The peculiar medium characteristics have great impact on system characteristics
  - Wireless networks allow users to move and naturally manage mobility

Network architecture

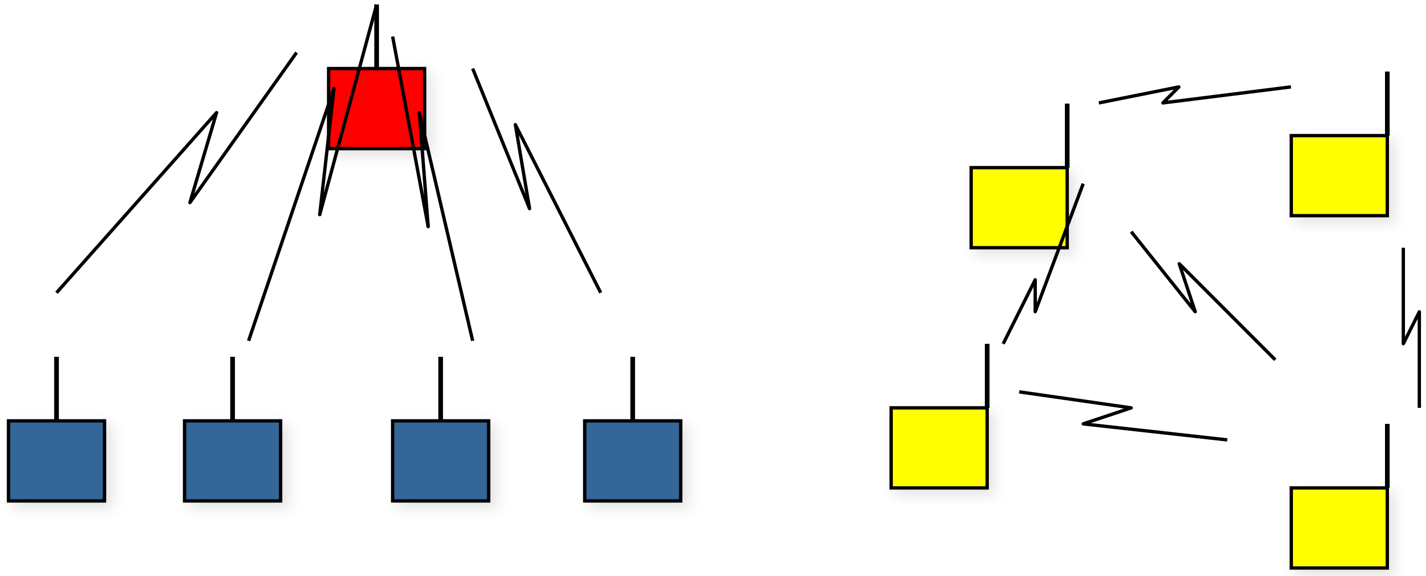


Wireless access networks

- Wireless networks are mainly access networks
- Backbone networks composed of radio point-to-point links are usually not considered wireless networks
- Wireless access networks are more challenging and have many fundamental differences with respect to wired access networks
- The first main difference is that the transmission medium is broadcast

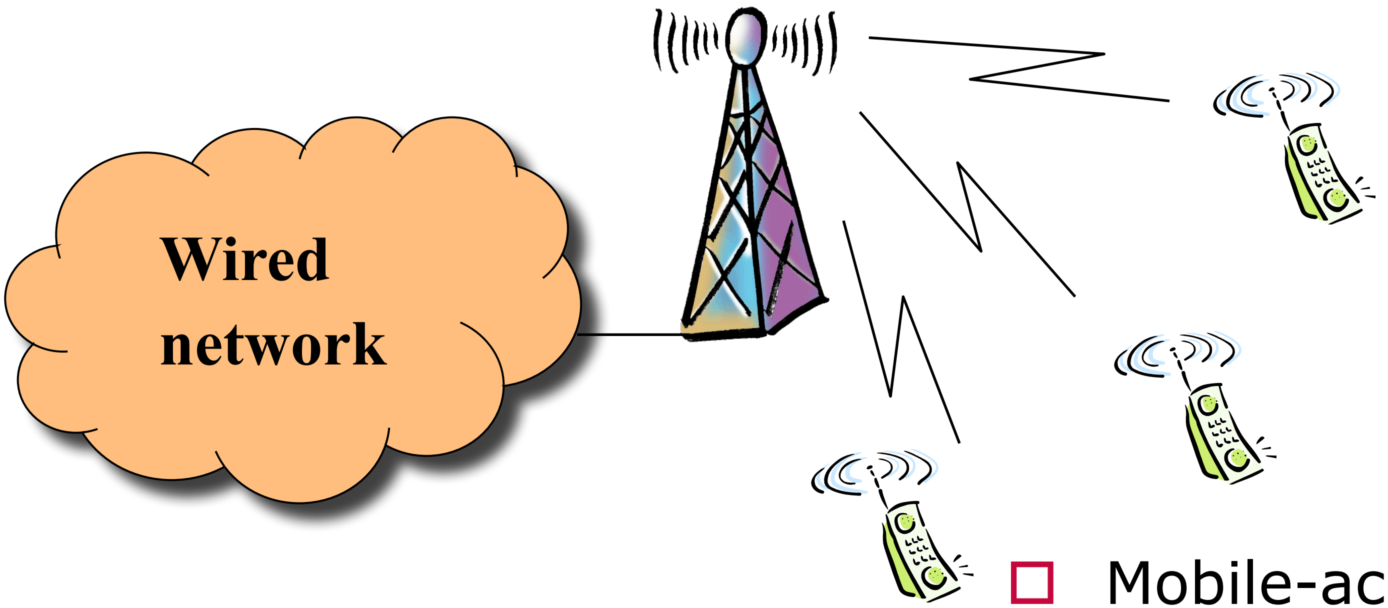
Broadcast channel

- Centralized broadcast channel
- Distributed broadcast channel



Centralized broadcast channel

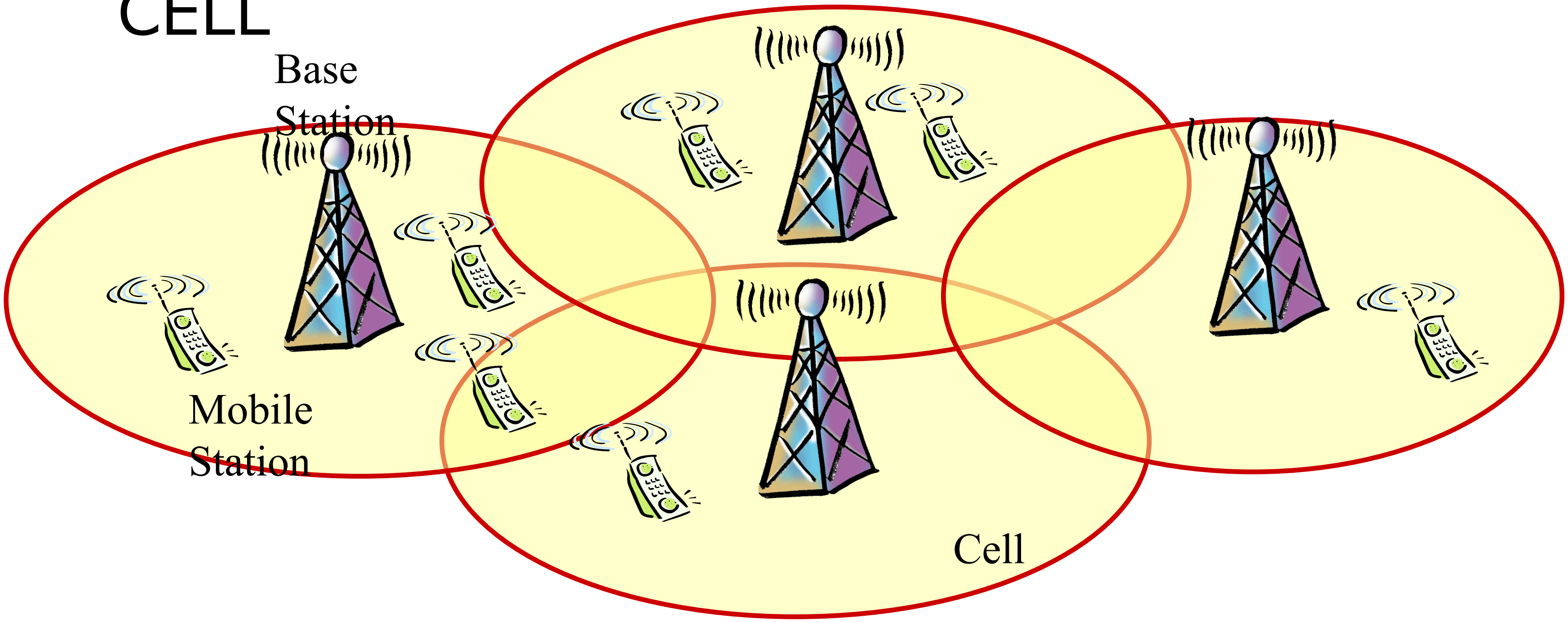
- Fixed access point (cellular systems, WLAN, WMAN)



- Mobile-access point connection

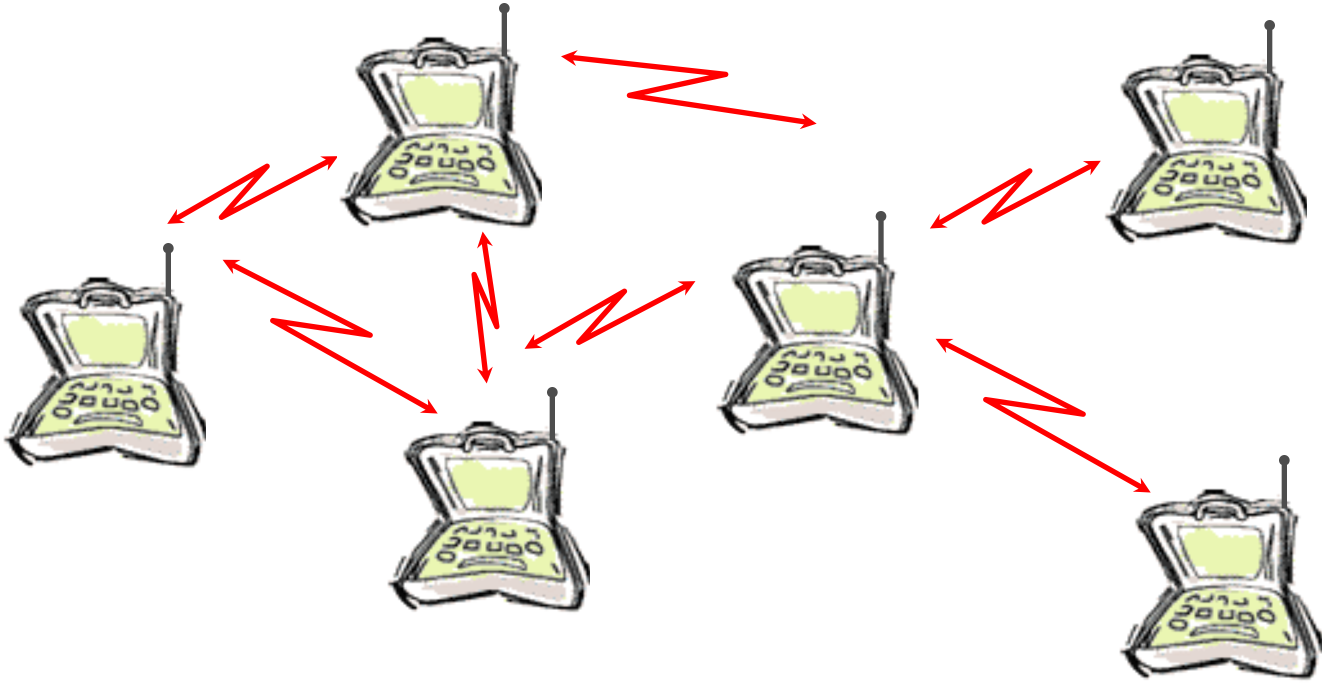
Centralized broadcast channel

- Cellular coverage: The territory coverage is obtained by Base Stations–BS (or Access Points) that provide radio access to Mobile Stations–MS within a service area called CELL



Distributed broadcast channel

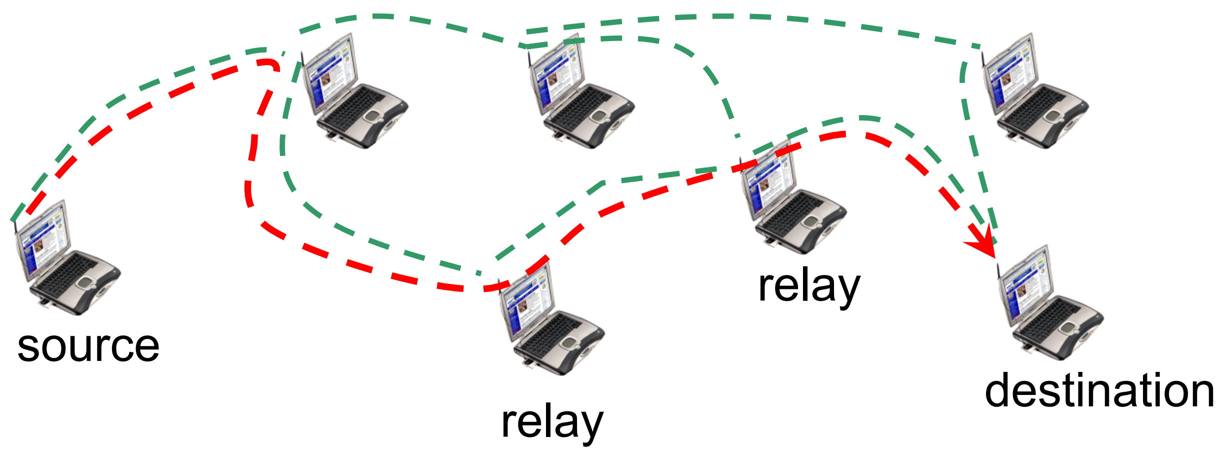
- Ad-hoc wireless networks (mesh networks, sensor networks)



- mobile - mobile connections

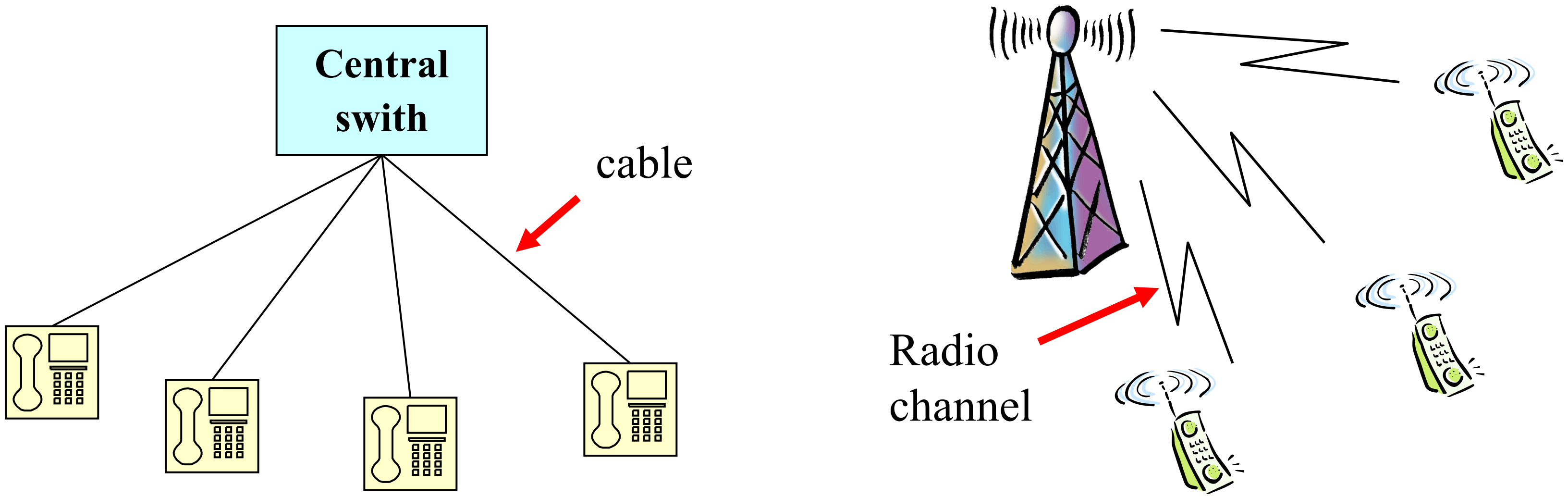
Distributed broadcast channel

- In multi-hop operation mobile stations can forward information



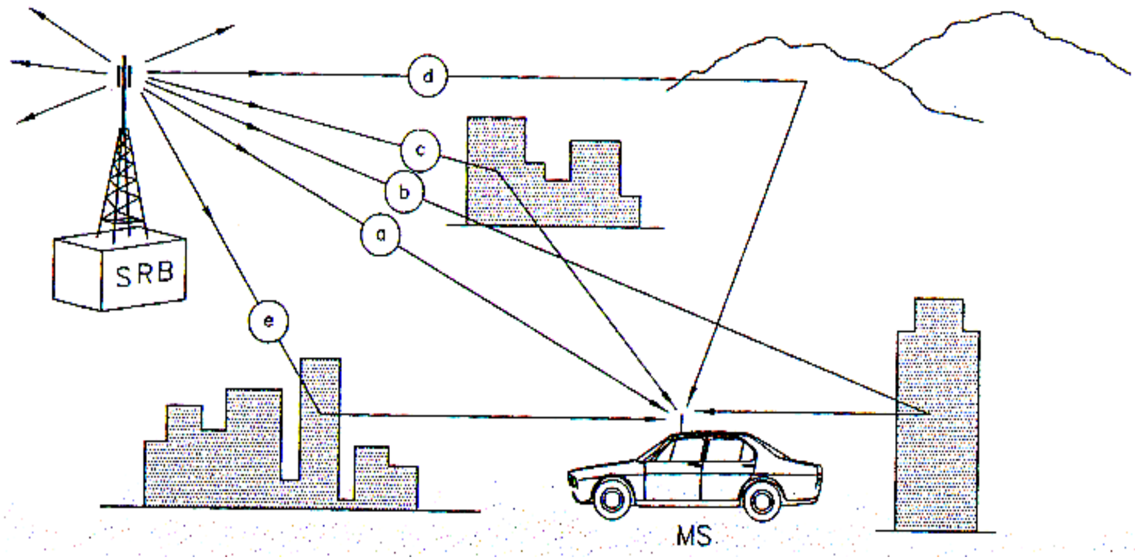
Wired-Wireless networks: Main differences

- Shared transmission medium
  - Multiple access mechanisms
  - Radio resource reuse



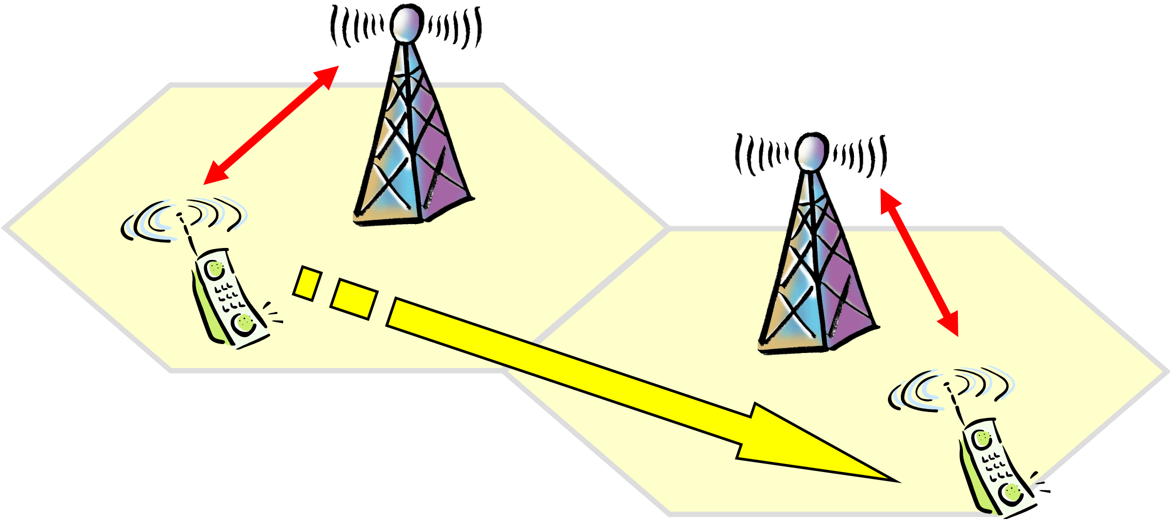
Wired-Wireless networks: Main differences

- Radio channel
  - Variable channel characteristics
  - Advanced modulation and coding schemes



Wired-Wireless networks: Main differences

- User mobility
  - Stand-by mobility
  - Active session (conversation) mobility



Wired-Wireless networks: Main differences

- In this course we'll focus on wireless technologies (how these problems are solved in practice):

- But first a few comments on:

- Wireless channels

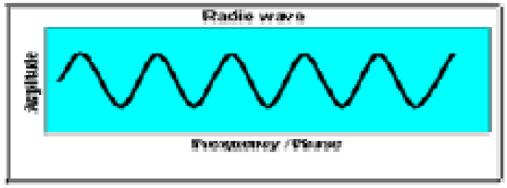
Wireless channel

- Generally speaking wireless channels have “worse” characteristics than wired ones (stronger attenuation, time-varying behavior, distortions, etc.)
- Signals propagating are affected by:
  - Attenuation due to TX-RX distance
  - Attenuation due to obstacles
  - Propagation over multiple paths

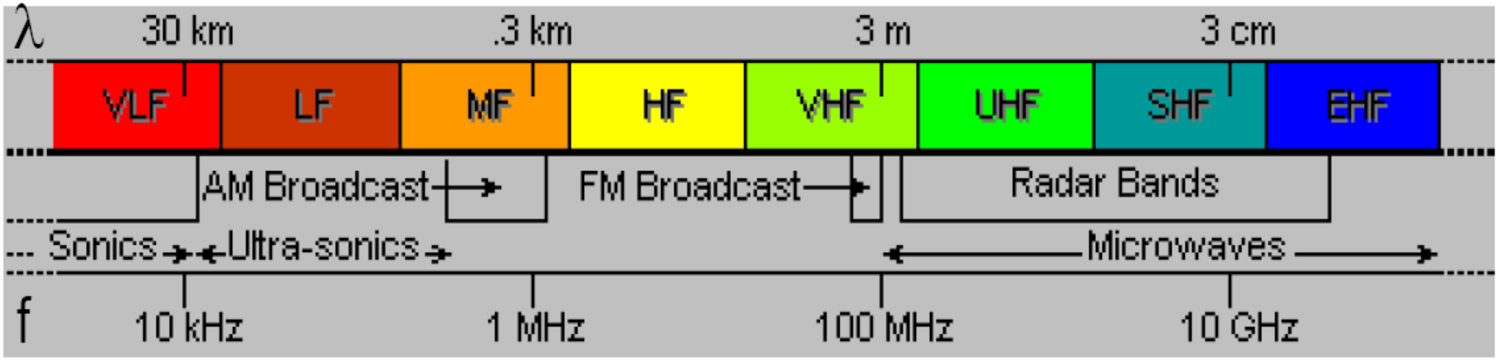
Wireless channel: radio spectrum

- Radio waves
  - Wave length $\lambda = \frac{c}{f}$
  - Light speed $c = 3 \cdot 10^8$ m/s
  - Frequency f

$$s(t) = \cos(2\pi f t + \varphi)$$



[V|U|S|E]HF = [Very|Ultra|Super|Extra] High Frequency



Wireless channel: radio spectrum

ELF	<3 KHz	Remote control, Voice, analog phone
VLF	3-30 KHz	Submarine, long-range
LF	30-300 KHz	Long-range, marine beacon
MF	300 KHz –3 MHz	AM radio, marine radio
HF	3-30 MHz	Amateur radio, military, long-distance aircraft/ships
VHF	30-300 MHZ	TV VHF, FM radio, AM x aircraft commun.
UHF	300 MHz - 3 GHz	Cellular, TV UHF, radar
SHF	3-30 GHz	Satellite, radar, terrestrial wireless links, WLL
EHF	30-300 GHz	Experimental, WLL
IR	300 GHz – 400 THz	LAN infrared, consumer electronics
Light	400-900 THz	Optical communications

The Spectrum

- Mobile radio networks
  - 900-2200 MHz (VHF-UHF)
  - Simple and small antennas (few cm)
  - With emitted powers around 1W we can cover up to few kilometers and penetrate building walls
- Point-to-point links and satellite links
  - 3-30 GHz (SHF)
  - Plenty of bandwidth available but strong attenuation due to meteorological effects (rain, fog, etc.)
- Data wireless networks (WLAN, WPAN, etc.)
  - 2.4 GHz e 5GHz (ISM band)
  - Interference with other systems (microwave ovens, remote controls, etc.)
  - In the 5 GHz attenuation due to rain and fog.

Wireless channel: radio spectrum

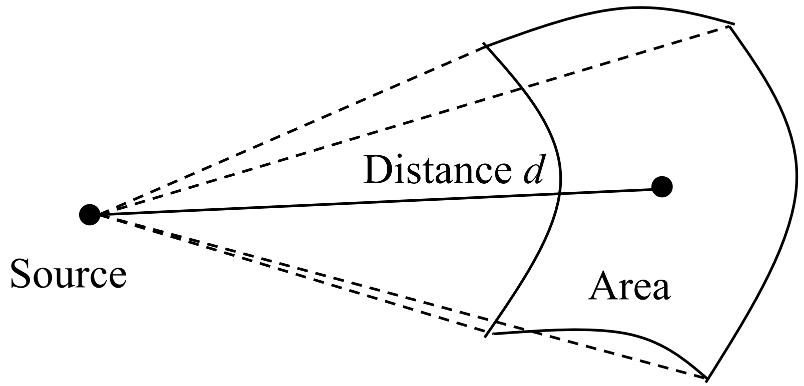
- High frequencies
  - High bandwidth availability
  - Spectrum is less crowded by other systems
  - Propagation is difficult due to low penetration of obstacles (which appear as opaque)
- Low frequencies
  - Low bandwidth availability
  - Big antennas
  - Many interference sources due to other human activities

Wireless channel: antennas

- Transmission and reception are achieved by means of an **antenna**
- An antenna is an electrical conductor or system of conductors
  - *Transmission* - radiates electromagnetic energy into space
  - *Reception* - collects electromagnetic energy from space
- In two-way communication, the same antenna can be used for transmission and reception
- Isotropic antenna (idealized)
  - Radiates power equally in all directions (3D)
  - Real antennas always have directive effects (vertically and/or horizontally)

Antennas

- A point source (isotropic radiator) transmitting a signal of power P_T irradiate it uniformly in all directions



- The power density on the surface of a sphere centered in the isotropic radiator and with radius d is given by:

$$F(d) = \frac{P_T}{4\pi d^2} \quad [\mathrm{W/m^2}]$$

Wireless channel: attenuation

- Directive characteristics of real antennas concentrate power in some directions
- This effect can be modeled using the gain $g(\theta)$ in the direction θ

$$g(\theta) = \frac{\text{power at distance } d \text{ in direction } \theta}{P_T / 4\pi d^2}$$

- The maximum gain g_T is conventionally in the direction $\theta = 0$.

Wireless channel: attenuation

- The power density in the maximum gain direction is given by:

$$F(d) = \frac{P_T g_T}{4\pi d^2} \quad [\mathrm{W/m^2}]$$

- The product $P_T\ g_T$ is called EIRP (Effective Isotropically Radiated Power) and it is the power required to reach the same power density with an isotropic radiator

Wireless channel: attenuation

- The *received power* depends on the power density at the receiver antenna and its equivalent area:

$$P_R = F(d)A_e$$

- For an isotropic antenna we have: $A_e = \dfrac{\lambda^2}{4\pi}$
- While for a directive antenna we can concentrate energy:

$$P_R = F(d)g_R A_e$$

  - where g_R is the receiver antenna gain
- Therefore:

$$P_R = P_T g_T g_R \left(\frac{\lambda}{4\pi d}\right)^2$$

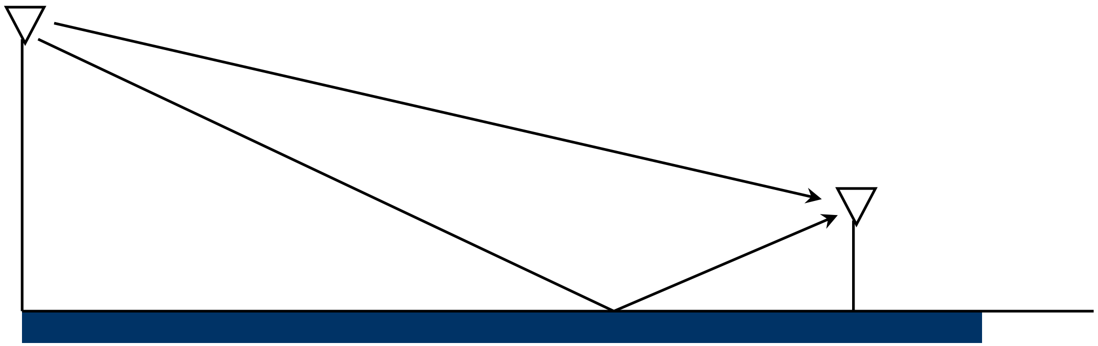
Wireless channel: free space model (Friis)

$$P_R = P_T g_T g_R \left(\frac{\lambda}{4\pi d} \right)^2 = P_T g_T g_R \left(\frac{c}{4\pi f d} \right)^2$$

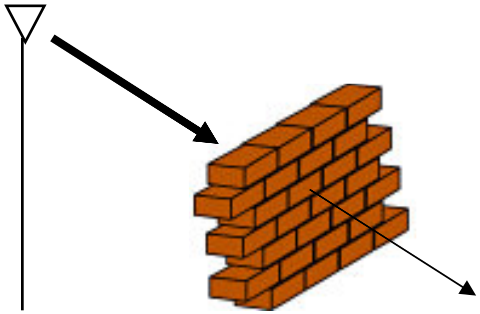
- The received power is $\propto d^{-2}$
- This is known as the *free space* propagation model
- It can be used for example with point-to-point radio links

Propagation effects

- Reflections



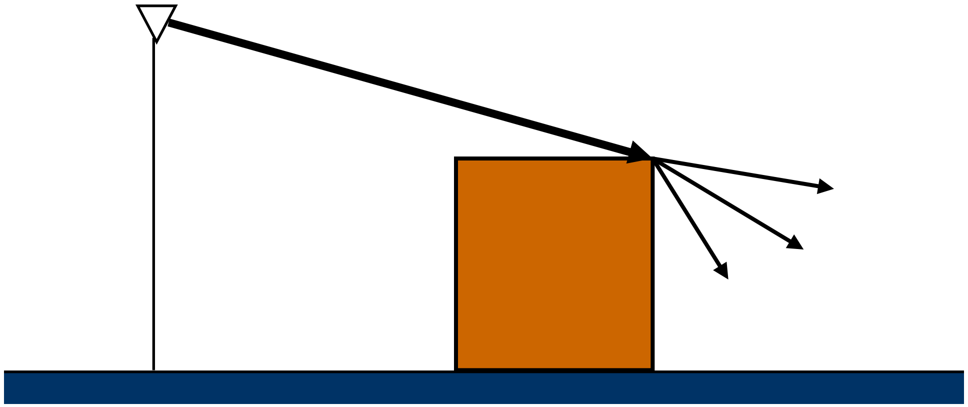
- Shadowing



Propagation effects

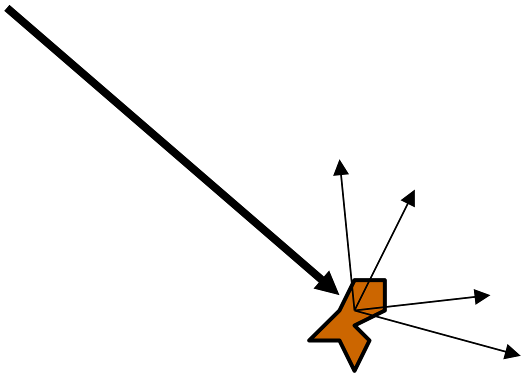
- Diffraction

When wave meets a sharp edge of an obstacle, the edge acts as a linear emitter



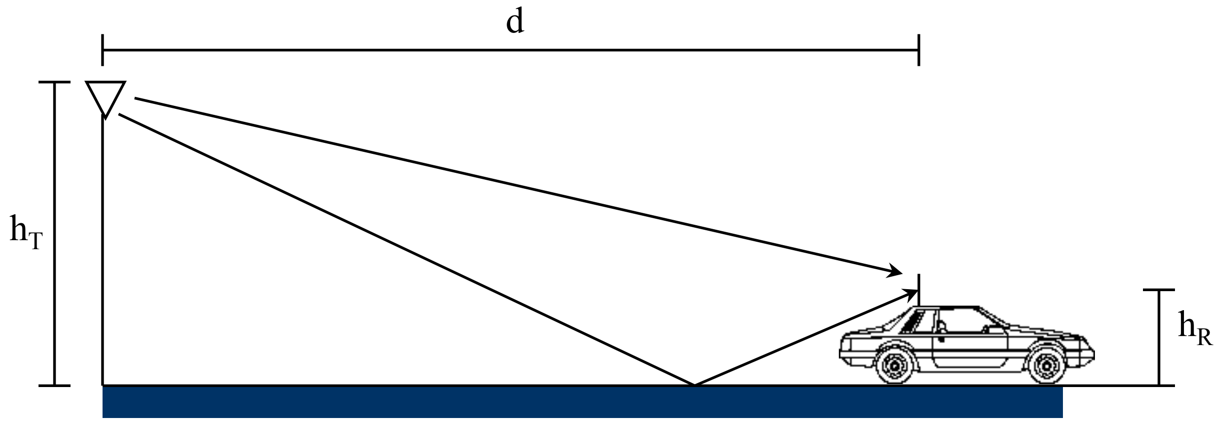
- Scattering

When wave meets a small object with respect to wave length, the object acts like a point emitter



Two-ray model

- If due to reflections, diffraction and scattering more copies of the same signal arrive to the receiver, they combines vectorially
- In the case of propagation with two rays, a direct ray and a completely reflected one, it is possible to calculate the attenuation of the received signal in closed form



Two-ray model

- Then:

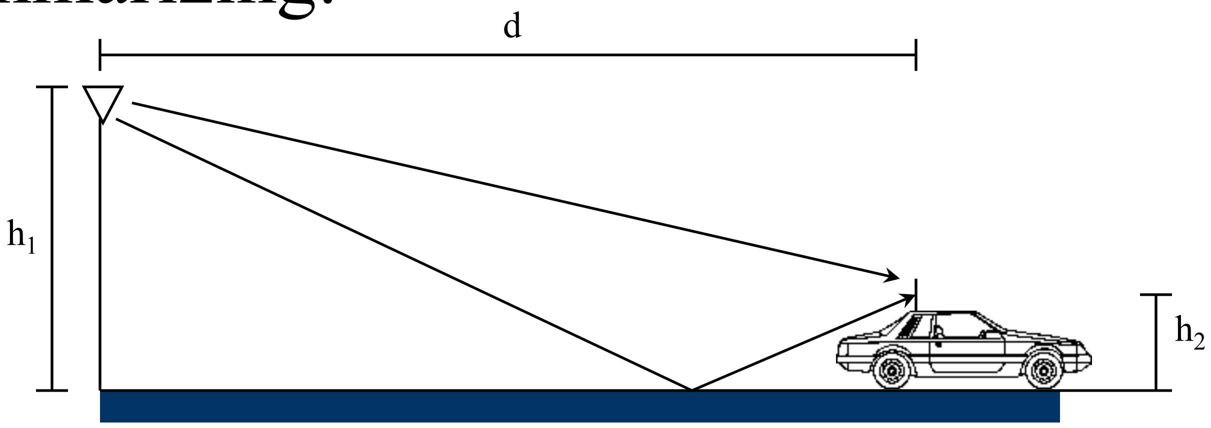
$$P_R(d) \approx 4 P_T g_T g_R \left(\frac{\lambda}{4\pi d}\right)^2 \left(\frac{2\pi h_T h_R}{\lambda d}\right)^2 = P_T g_T g_R \frac{h_T^2 h_R^2}{d^4}$$

- Therefore in the two-ray model we have:

$$P_R(d) \propto d^{-4}$$

Two-ray model

- Summarizing:



- The ratio between received power and transmitted power is given by:

$$\frac{P_R}{P_T} = g_R g_T \left(\frac{h_1 h_2}{d^2} \right)^2$$

Attenuation due to distance

- Assuming a two-ray propagation, the received power decreases due to distance much faster ($\sim 1/d^4$) than in the case of free space propagation ($\sim 1/d^2$)
- Actually, the typical propagation in wireless systems is often different and more complex than in these two cases
- Nevertheless, a common approach to propagation modeling in wireless systems assumes propagation is given by a formula similar to the above two cases where however the exponent of the distance is different (propagation coefficient η) that can get values between 2 (free-space) and 5 (strong attenuation in urban environment):

$$P_R = P_T g_T g_R \left(\frac{\lambda}{4\pi}\right)^2 \frac{1}{d^\eta}$$

Empirical models

- There are several more sophisticated techniques for the estimation of the received power that are based on the detailed modeling of the characteristics of the area in which signal propagates and propagation simulation (*ray tracing techniques*)
- These technique are usually very complex in terms of computation and difficult to use because of non accurate modeling of propagation environment
- For this reason, quite often empirical models are adopted that calculate attenuation due to distance with approximate formulas just capturing general characteristics of the propagation area

Empirical models

- The most famous empirical model modeling distance attenuation is the Okumura-Hata (1980)
- It provides the attenuation formulas in several reference scenarios
  - Big cities; medium-small cities; rural areas
  - Distances > 1 km

Empirical models

- Okumura-Hata: urban area

$$L_P = 69.55 + 26.16\log f - 13.82\log h_T - a(h_R) +$$
$$+ \left(44.9 - 6.55\log h_T\right)\log d \quad [\text{dB}]$$

- where
  - f is the frequency in MHz (valid from 150 to 1500 MHz)
  - h_T is the height of the base station (in m)
  - h_R is the height of the mobile terminal (in m)
  - $a(h_R)$ correction parameter due to area type
  - d is the distance(in km)
- Big cities: $a(h_R) = 3.2\left[\log_{10}\left(11.75 \cdot h_R\right)\right]^2 - 4.97$
- Small-medium cities:

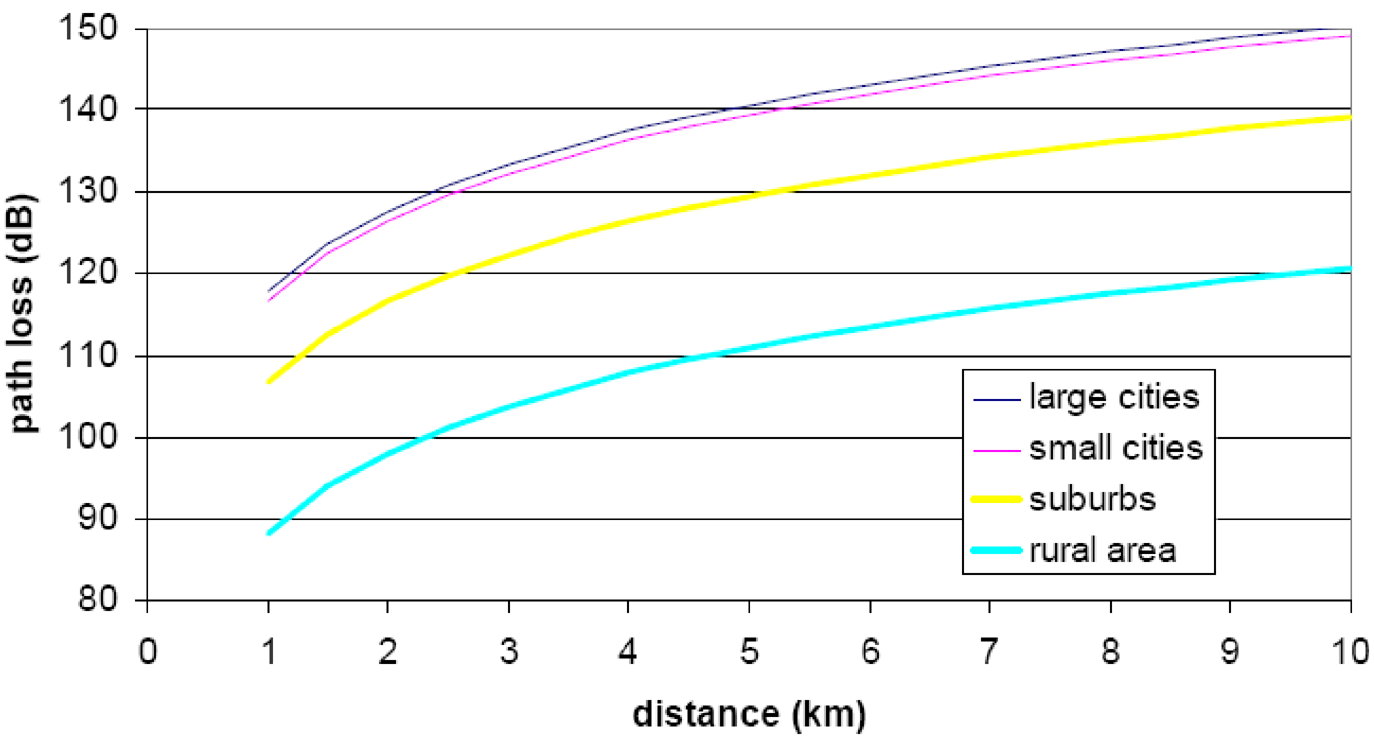
$$a(h_R) = \left[1.1\log_{10} f - 0.7\right]h_R - \left[1.56\log_{10} f - 0.8\right]$$

Empirical models

- Okumura-Hata: sub-urban & rural areas
- Calculated starting from that of urban areas (L_P)
- Sub-urban: $$L_{path} = L_P - 2\left[\log_{10}\frac{f}{28}\right]^2 - 5.4$$
- Rural: $$L_{path} = L_P - 4.78\left[\log_{10} f\right]^2 + 18.33\log_{10} f - 40.94$$

Empirical models

- Okumura-Hata: numerical example



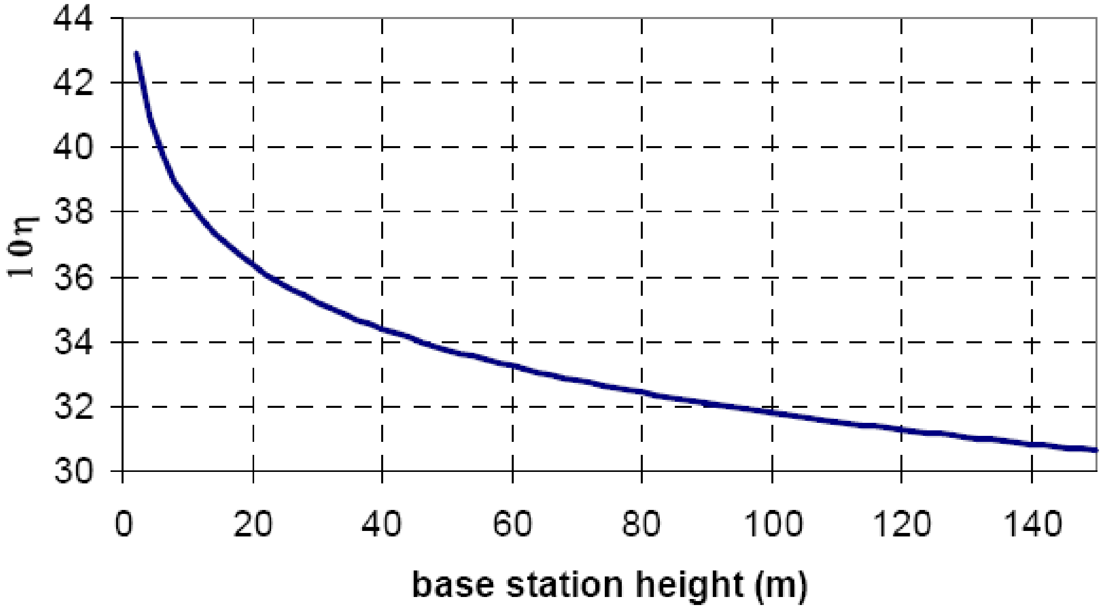
F=900MHz, h_{bs}=80m, h_{ms}=3m

Empirical models

- Okumura-Hata: propagation factor η
  - Propagation factor depends only on the height of the base stations:

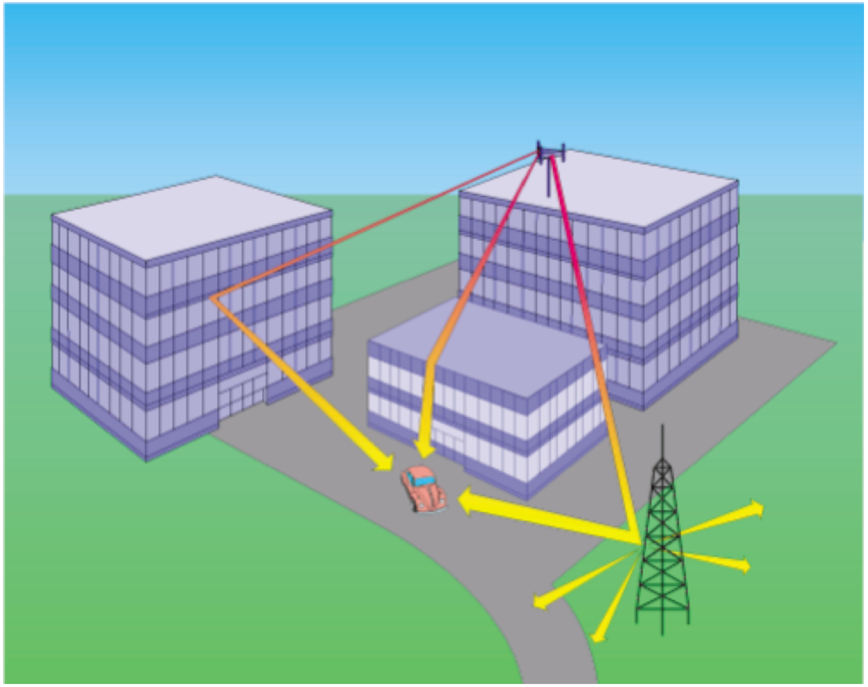
$$\left(44.9 - 6.55\log h_T\right)\log d \Rightarrow$$

$$\left(44.9 - 6.55\log h_T\right) = 10\eta$$

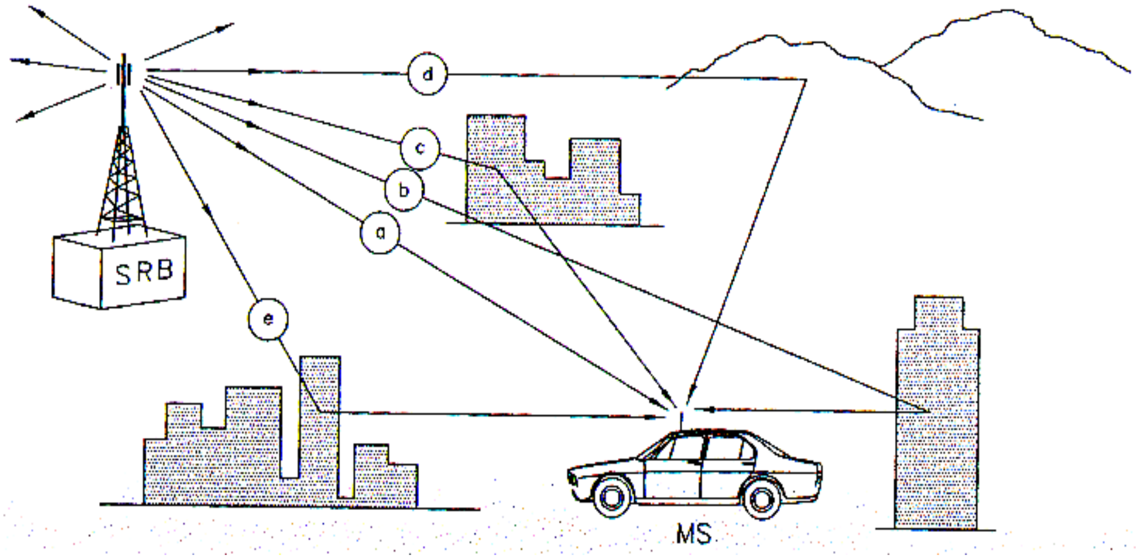


Multi-path Fading

- In the propagation between transmitter and receiver, signal can follow different paths due to total or partial reflection over obstacles
- The behavior of the waves when interacting with objects depends on their frequency and the characteristics and size of the objects
- Generally speaking, signals at low frequency can cross many objects (that appear as transparent) with small attenuation, while as frequency increases signals tend to be absorbed or reflected by obstacles (at very high frequencies – over 5 GHz – it is possible basically only direct propagation).



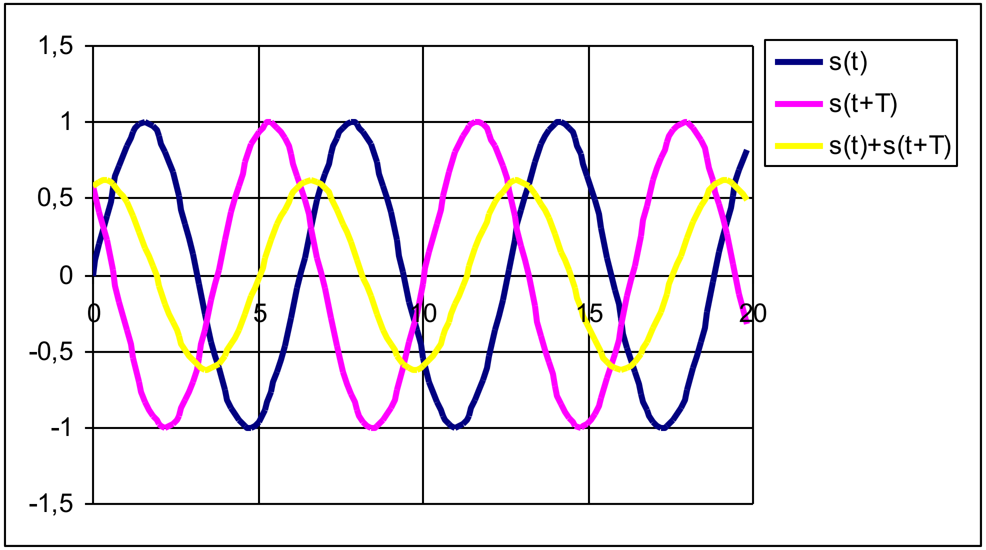
Multi-path Fading

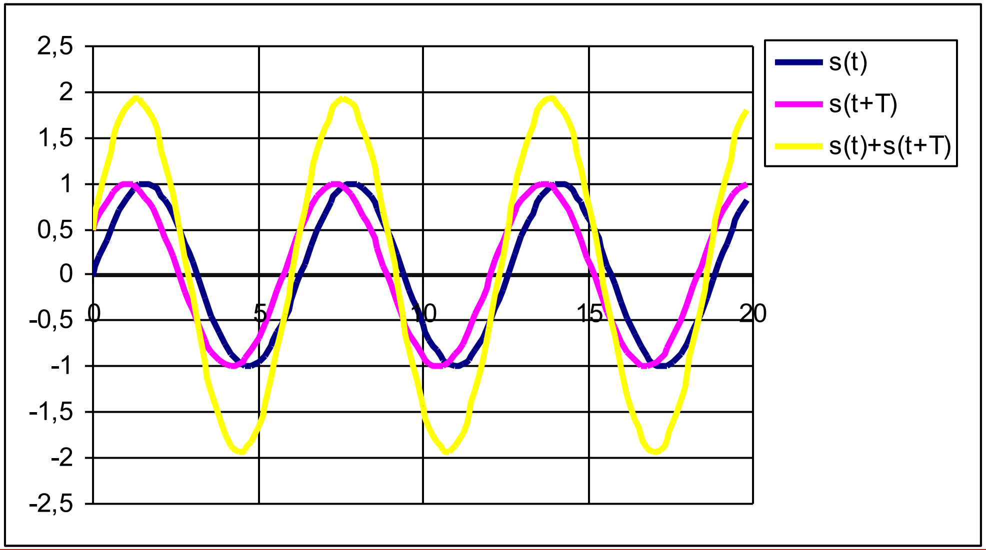


- As we already know from two-ray model, replicas combines at the received
- The resulting signal depends on:
  - Number of replicas (N)
  - Relative phases (φ_k)
  - Amplitudes (a_k)
  - Frequency (f_0)

$$e_R(t) = \sum_{k=1}^{N} a_k \cos(2\pi f_0 t + \varphi_k)$$

Multi-path Fading





- Signal can be attenuated

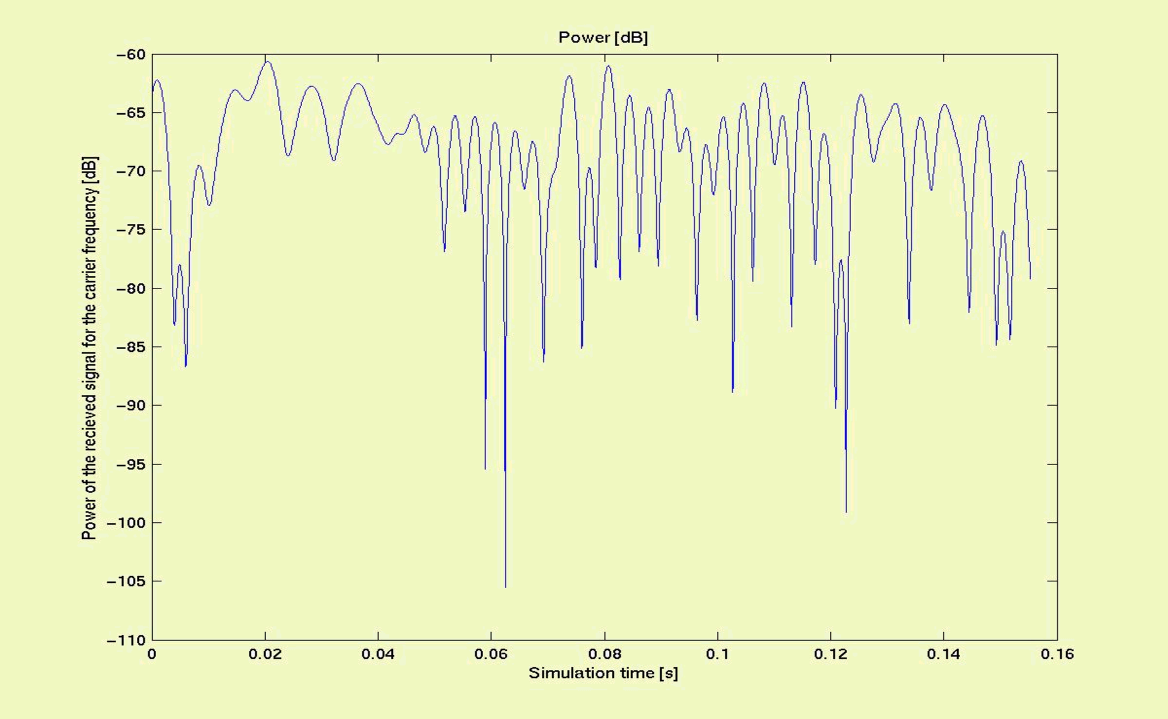
T=4/5π

- Or even amplified

T= π /6

Multi-path Fading

- If terminal moves, the characteristics of the composed signal change with time



- Fading notches tend to occur regularly at intervals corresponding to the time necessary for covering half of the wave length

Multi-path Fading

- In some simplified scenarios it is possible to give a statistical representation of the multi-path fading:

$$e_R(t) = \sum_{k=1}^{N} a_k \cos(2\pi f_0 t + \varphi_k) =$$

$$= \cos(2\pi f_0 t) \sum_{k=1}^{N} a_k \cos\varphi_k - \sin(2\pi f_0 t) \sum_{k=1}^{N} a_k \sin\varphi_k =$$

$$= X\cos(2\pi f_0 t) - Y\sin(2\pi f_0 t)$$

Multi-path Fading

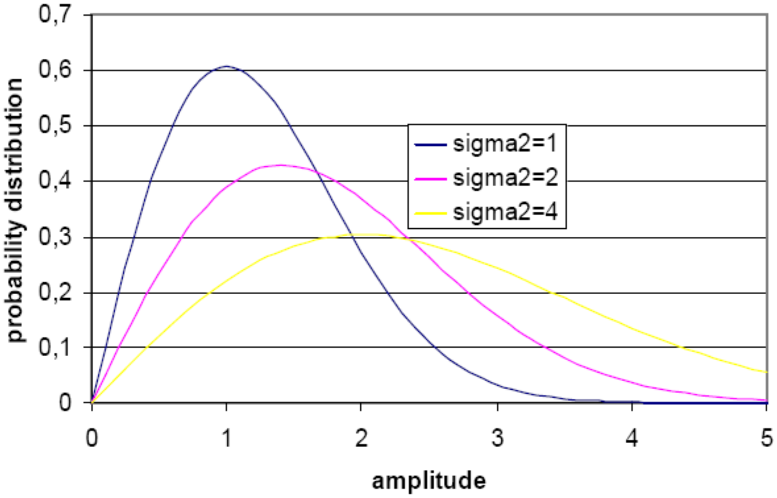
- Rayleigh Fading
  - If we assume
    - An infinite number of paths
    - No dominating component (a_k comparable) [usually verified when there are only reflected paths]
    - Random phases uniform in $[0,2\pi]$
  - The two signal components X and Y are independent Gaussian variables

$$f_X(x) = f_Y(x)\frac{1}{\sqrt{2\pi}\sigma}e^{-\frac{(x-m)^2}{2\sigma^2}}$$

Multi-path Fading

- The amplitude of the vector: $R = \sqrt{X^2 + Y^2}$
- With Gaussian components has a Rayleigh distribution:

$$f_R(x) = \frac{x}{\sigma^2} e^{-\frac{x^2}{2\sigma^2}}, \quad x \geq 0$$



- with $E_R(x) = \sigma\sqrt{\frac{\pi}{2}}$,

$$E_R(x^2) = 2\sigma^2, \qquad \sigma_R^2 = \sigma^2\left(\frac{4-\pi}{2}\right).$$

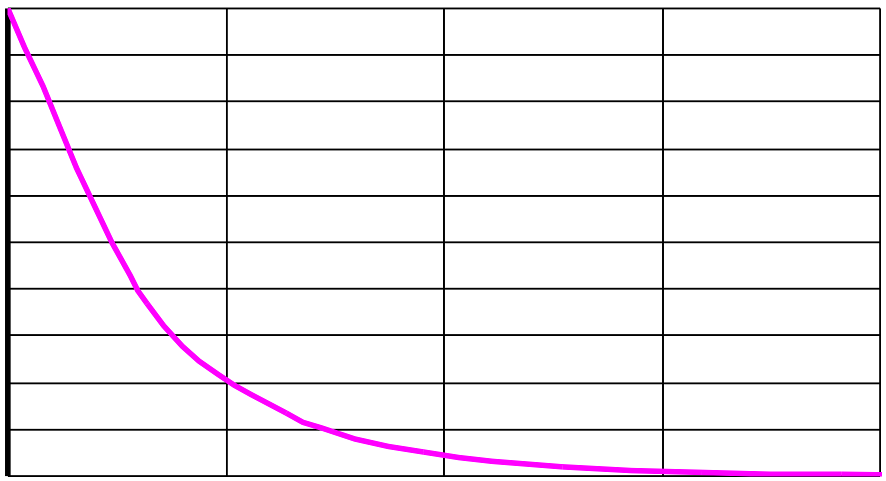
- Usually a normalized distribution is considered $E_R(x^2) = 1$

Multi-path Fading

- The power P of a signal with Rayleigh distributed amplitude has an exponential distribution

$$f_P(x) = \frac{1}{2\sigma^2} e^{-x/2\sigma^2}, \quad F_P(x) = 1 - e^{-x/2\sigma^2}$$

Average power: $2\sigma^2$



Multi-path Fading

- Outage probability
  - Probability that the signal power is below a given receiver threshold
  - Average power P_0
  - Threshold γ

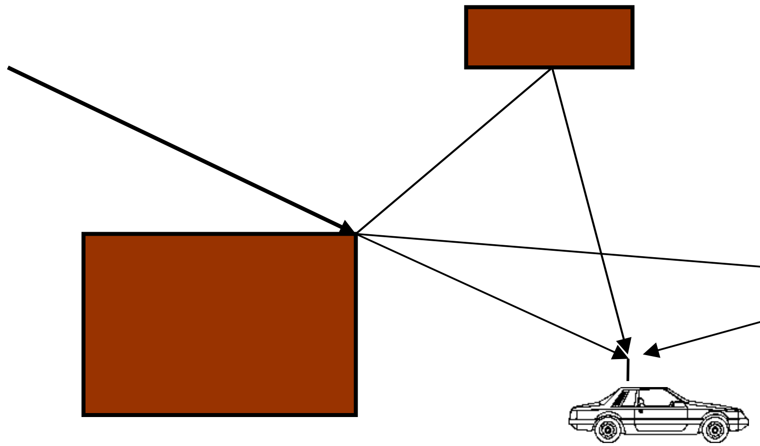
$$F_P(\gamma) = 1 - e^{-\gamma / P_0}$$

Example 1:
Average power = 100 μW
Threshold = 5 μW
Outage prob. = 4.9%

Example 2:
Average power = -75 dBm
Threshold = -90 dBm
Outage prob. = 3.1%

Shadowing

- In the propagation the signal crosses or is partially reflected and diffracted by obstacles
- This generates a further attenuation that is usually indicated with the name of *shadowing*
- This is a slowly varying fading that changes only when the move is big enough to modify the components of the signal
- In practice shadowing is used to model all the other effects not captured by distance based models and multi-path



Shadowing

- Shadowing is usually modeled as a log-normal random variable *x*,
- So the power in dB (average value P_{dB}) has an attenuation component Z=log (x) which is a Guassian variable with standard deviation σ_{dB} that usually gets values between 0 and 12 dB

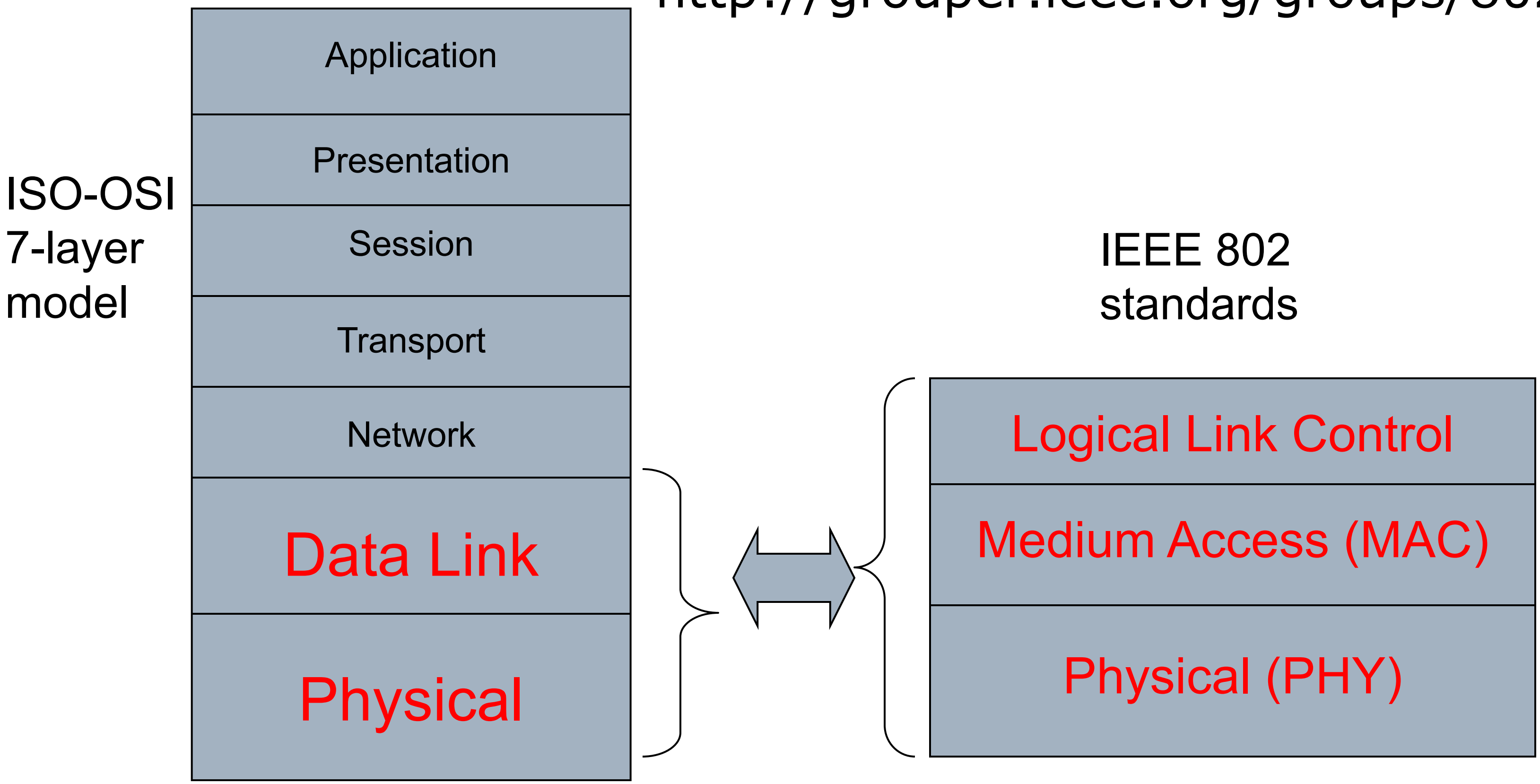
$$f_Z(x) = \frac{1}{\sqrt{2\pi} \cdot \sigma_{dB}} e^{-(x-P_{dB})^2/2\sigma_{dB}^2}$$

Part 1
WLAN

Standardization of Wireless Networks

- Wireless networks are standardized by IEEE (Institute of Electrical and Electronics Engineers)
- under 802 LAN/MAN standards committee.

http://grouper.ieee.org/groups/802/11/



802.11 History

Wireless Evolution of LAN

- **802.11-legacy** standard first ratified in July **1997**
  - 802.3 LAN emulation
  - 3 PHY's were specified for 1 & 2 Mbps (FHSS, DSSS, Infrared)
- Two High Rate PHY's ratified in Sep **1999**
  - **802.11a** 6 to 54Mbps in the 5GHz band (OFDM)
  - **802.11b** 5.5 and 11Mbps in the 2.4GHz band
- PHY up to 54 Mbit/s in 2.4 GHz band ratified in **2003**
  - **802.11g**
- 802.11a compatible with European spectrum regulation in 5GHz band ratified in **2004**
  - **802.11h** (Transmit Power control to avoid interference with satellites, radars, etc …)

802.11 History

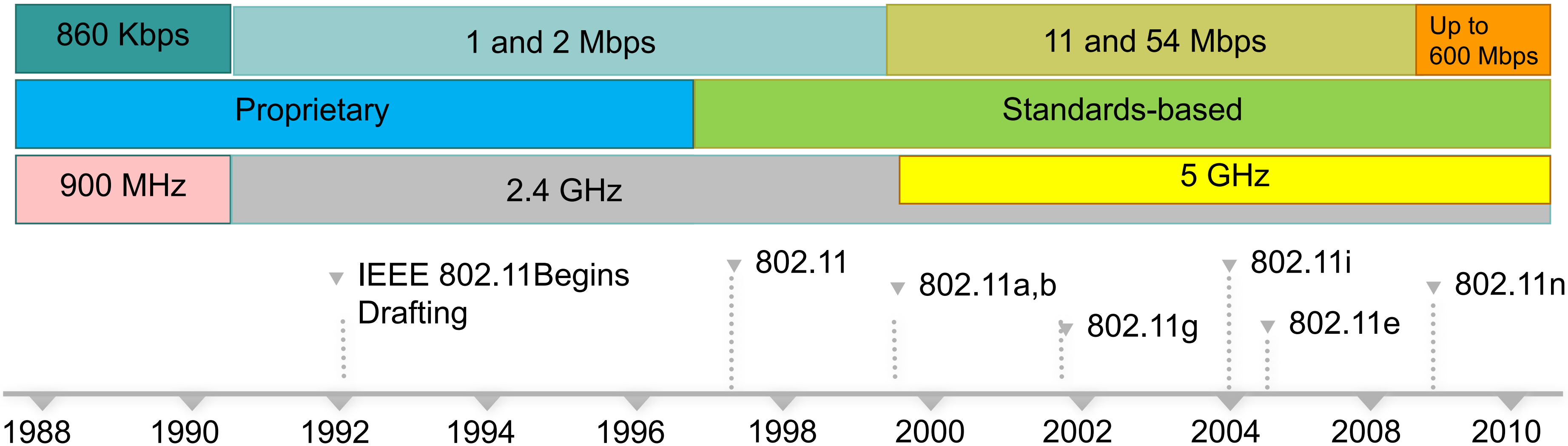
- Enhanced security framework ratified in **2004**
  - **802.11i**
- Enhanced MAC with QoS support ratified in **2005**
  - **802.11e**
- High rate standard (PHY and also MAC) ratified in **2009** (draft 2007 with WiFi pre-standard products)
  - **802.11n**

And more to come:

- **802.11s:** mesh networking
- **802.11p:** WAVE—Wireless Access for the Vehicular Environment
- **802.11v:** Wireless network management
- **802.11ac:** Very High Throughput (0.5 – 1 Gbit/s)
- **802.11af:** White-Fi (CRN, using TV Whitespace …)

802.11 History

- WLAN Timeline

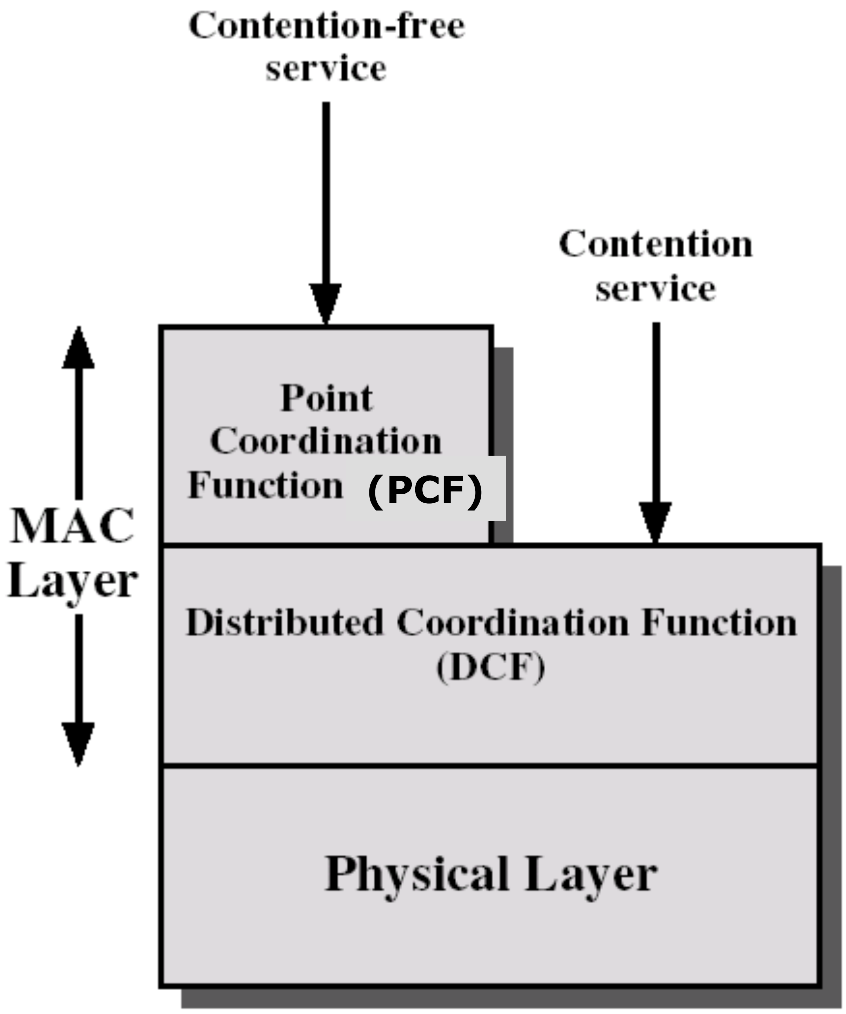


Wi-Fi

- Wi-Fi™ Alliance
  - Wireless Fidelity Alliance
  - 500+ members
  - Over 350 products certified
- Wi-Fi's™ Mission
  - Certify interoperability of WLAN products (802.11)
  - Wi-Fi™ is the "stamp of approval"
  - Promote Wi-Fi™ as the global standard

802.11 Protocol Architecture

- The standard provides two modes of operation which are:
- **DCF** (mandatory) – best effort contention service – uses CSMA with Collision Avoidance (CSMA/CA)
- **PCF** (optional) – base station controls access to the medium – uses a *polling* mechanism with higher priority access to the medium, plus three types of frames: data, control and management



WLAN:
Network architecture

Components

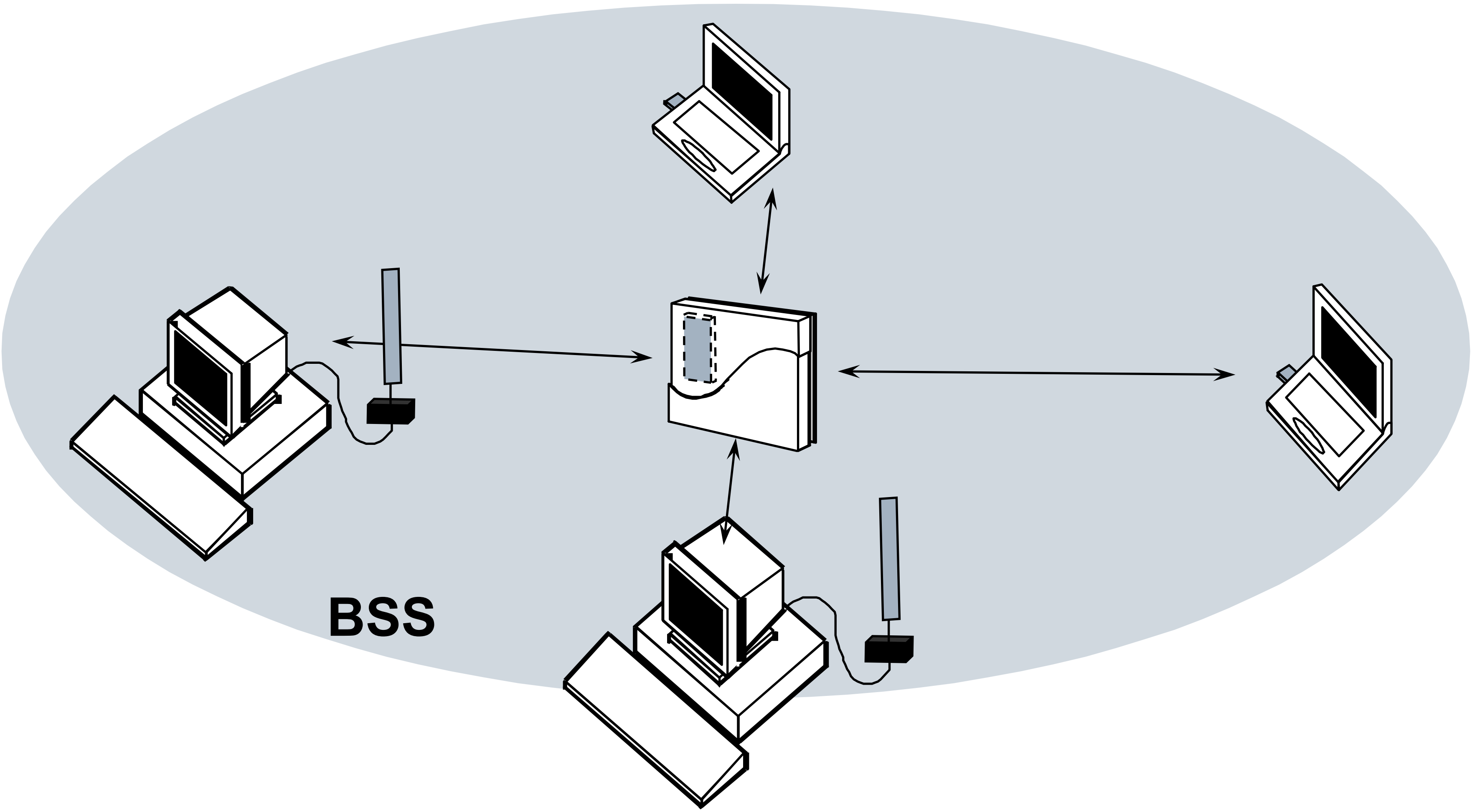
- Station (**STA**)
- *Access Point* (**AP**)
  - *bridging wired/wireless*
- **BSS** - *Basic Service Set*
  - *Infrastructure* BSS: infrastructure based
  - *Independent* BSS (IBSS): *ad hoc*
- **ESS** - *Extended Service Set*
  - Set of *Infrastructure* BSS
  - A set of *access points* connected through a:
- **DS** – *Distribution System* (not directly addressed in the standard)
  - Wired
  - Wireless (WDS)

Basic Service Set (BSS)

- Set of stations (STAs) controlled by the same "*Coordination Function*" (logic function that manages the access to the shared channel)
- Similar to the concept of "cell" in mobile radio networks
- Two types of BSS:
  - *Infrastructure* BSS
  - *Independent* BSS (IBSS)

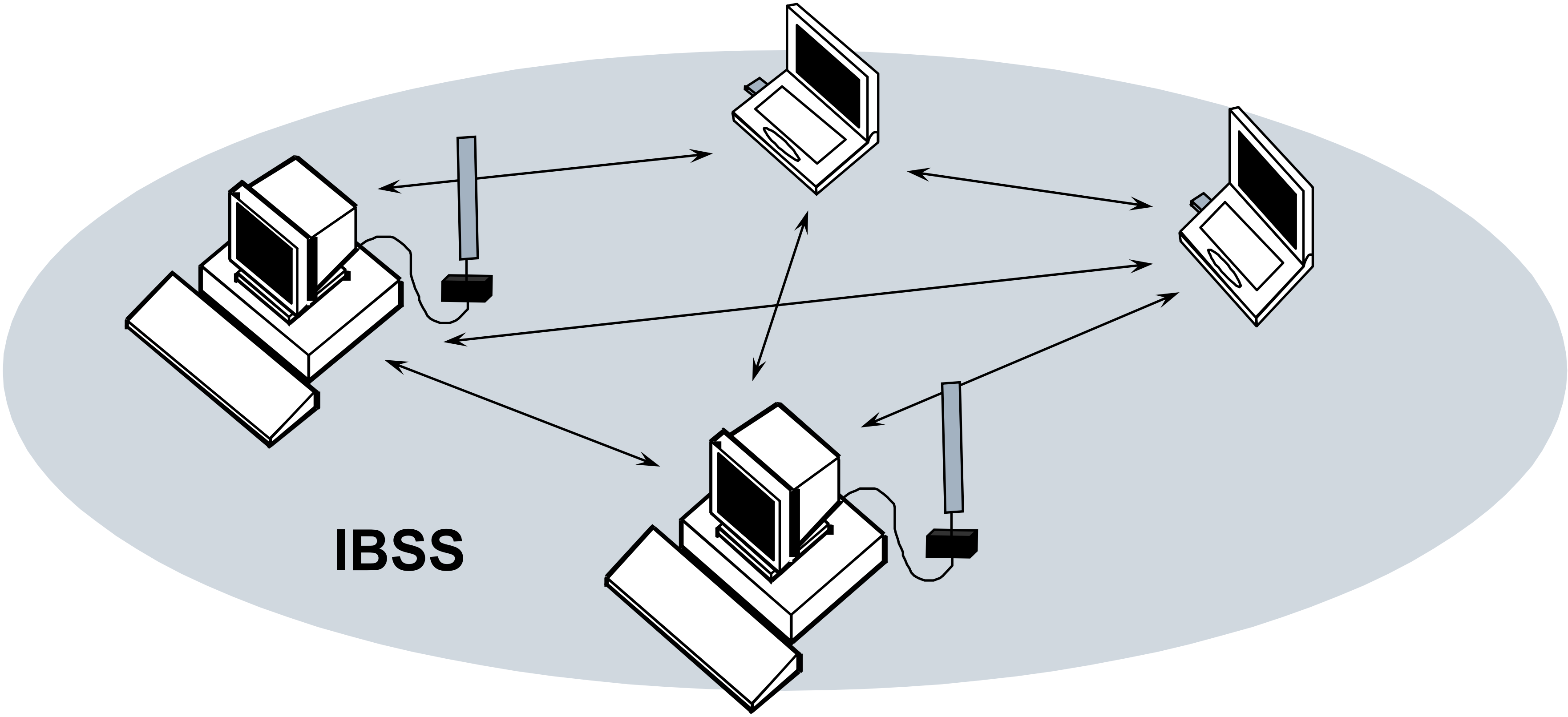
Infrastructure BSS

Centralized architecture



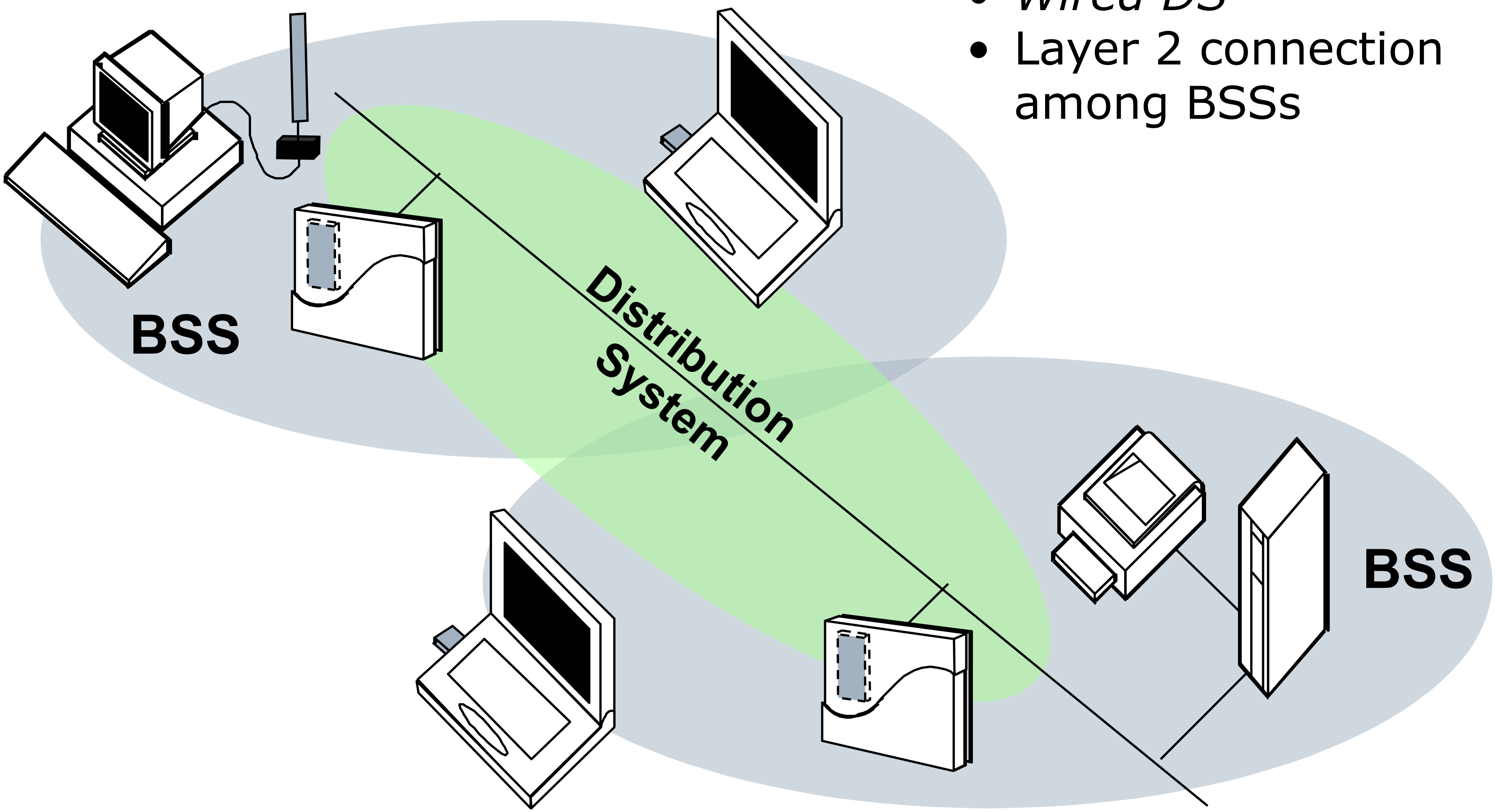
Independent Basic Service Set (IBSS)

Ad hoc architecture

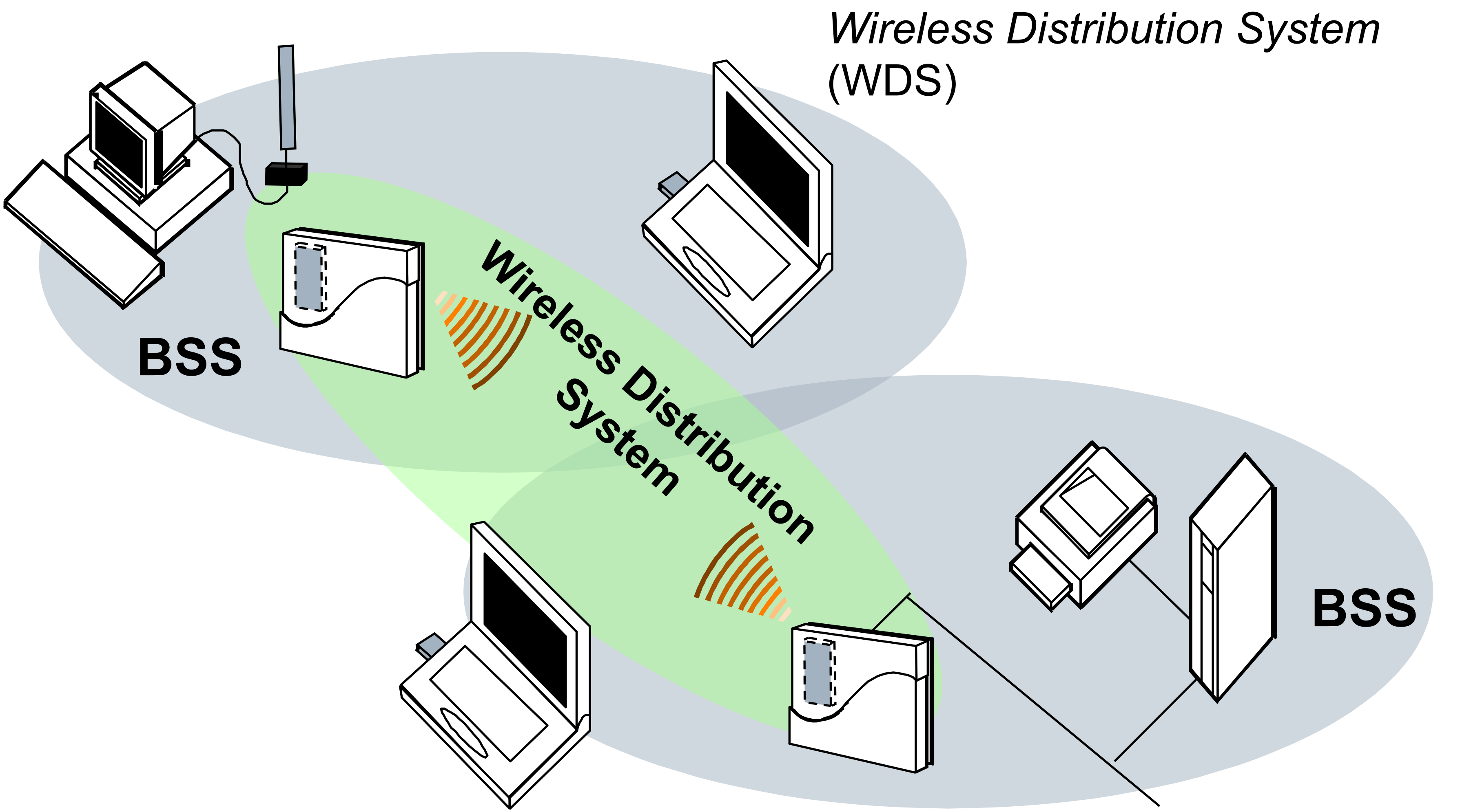


Extended Service Set (ESS)

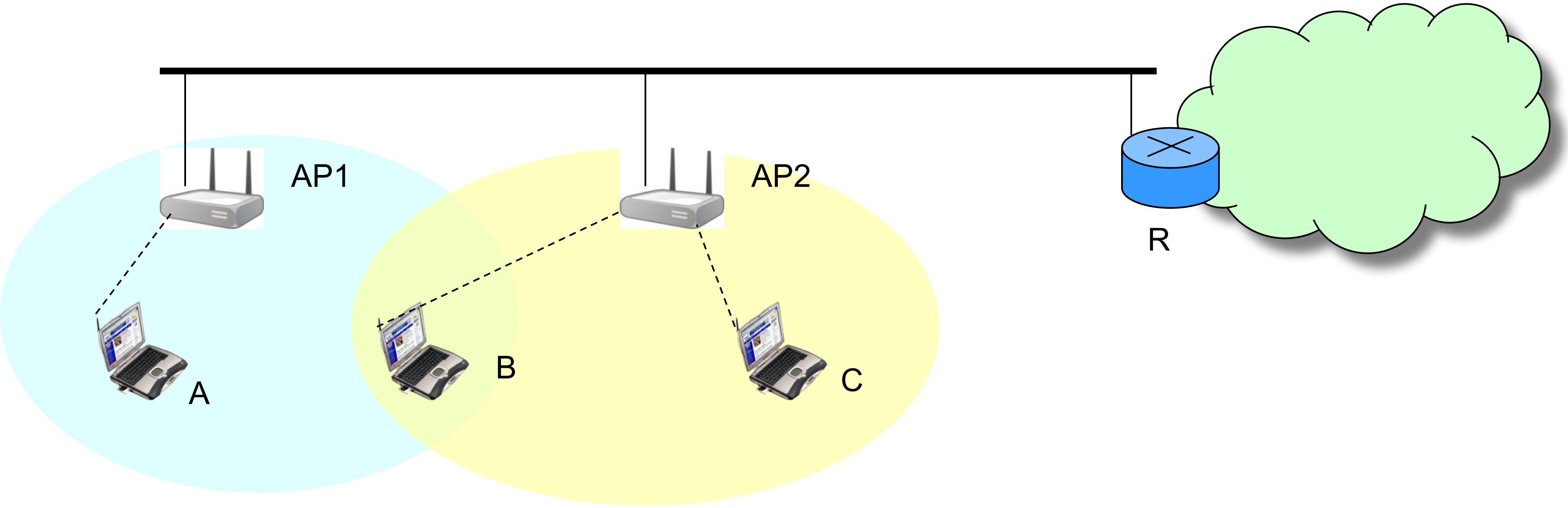
- *Wired DS*
- Layer 2 connection among BSSs



Extended Service Set (ESS)

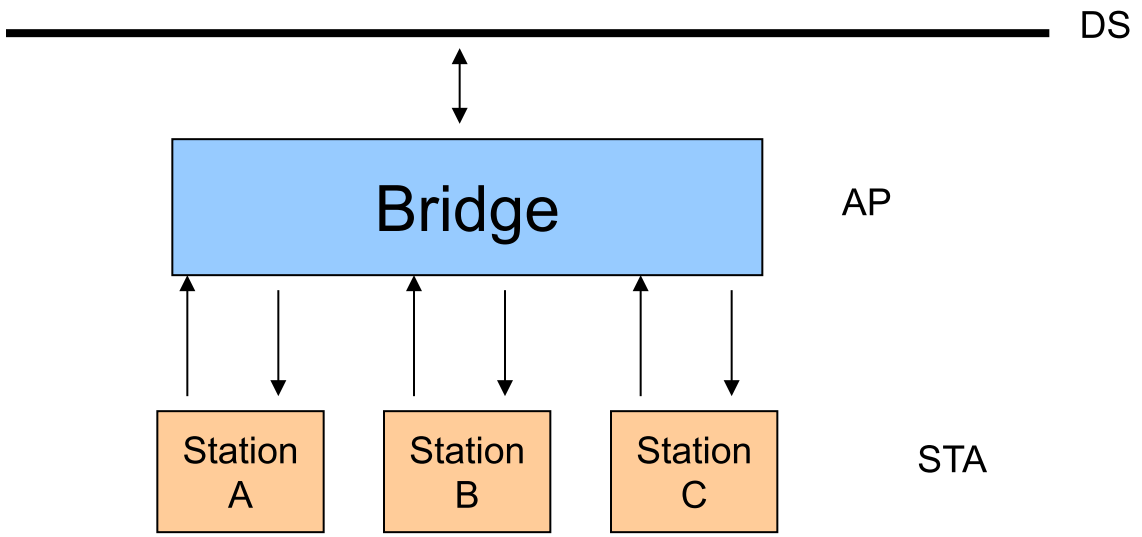


Distribution System



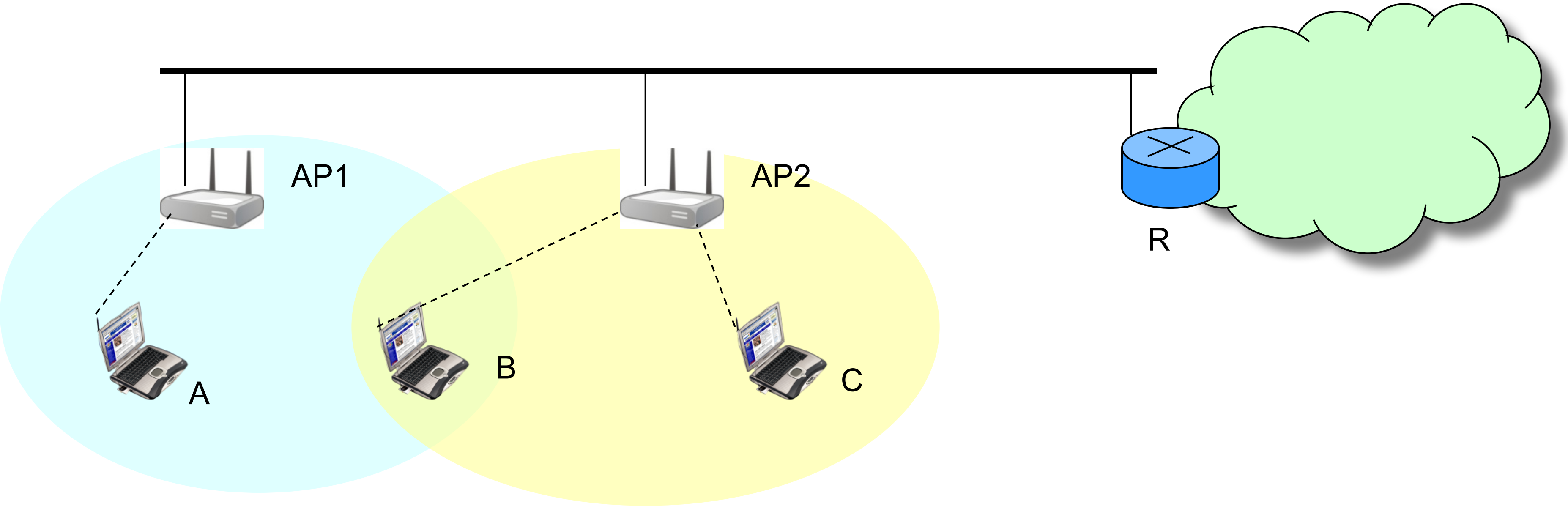
- STA associates to one, and *only one*, AP through an association procedure
- Association procedure is "equivalent" to plugging the ethernet cable
- An ESS is a layer-2 network, and therefore a single IP subnet with its own addressing space

Distribution System



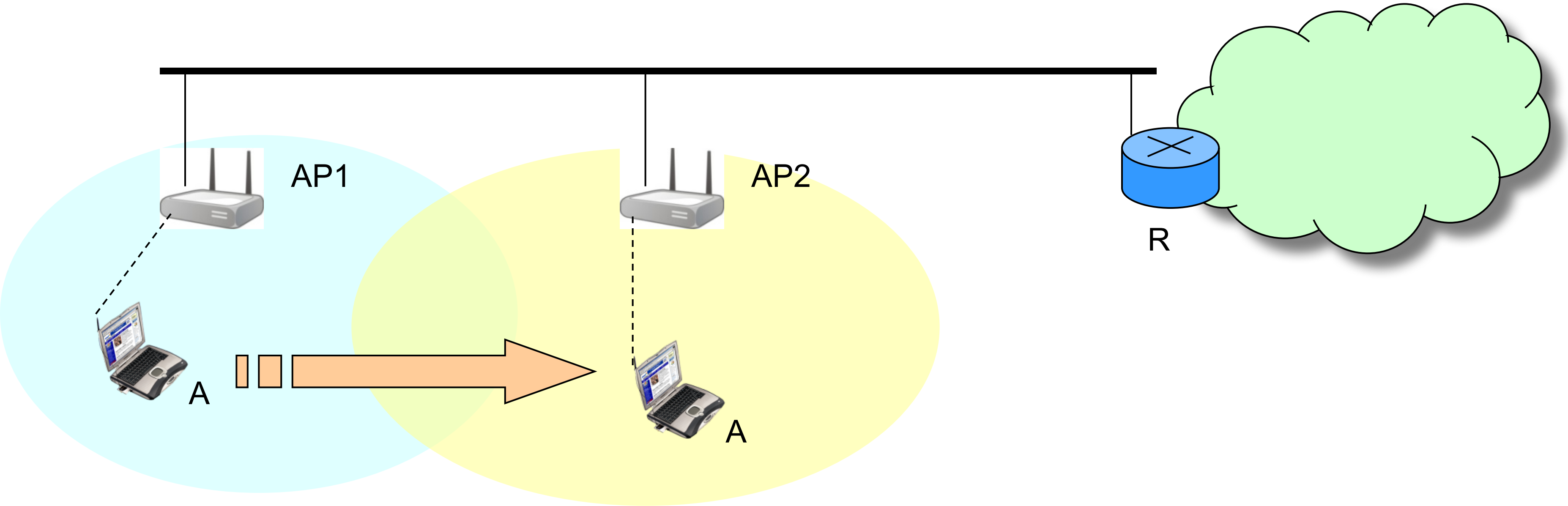
- APs behave like an *Ethernet bridge* (layer-2 switch)
- Association tables are used for the bridging process
- For example, frames received via the DS and indicating as destination a wireless STA are forwarded to the wireless interface once converted to 802.11 format

Distribution System



- **Question**: How exactly can an IP packet go from router R to STA B (assume ARP tables empty)?

Distribution System



- What happens when a station moves from AP1 to AP2? (*handover* or *handoff*)

WLAN:
Medium Access Control

MAC services and functionalities

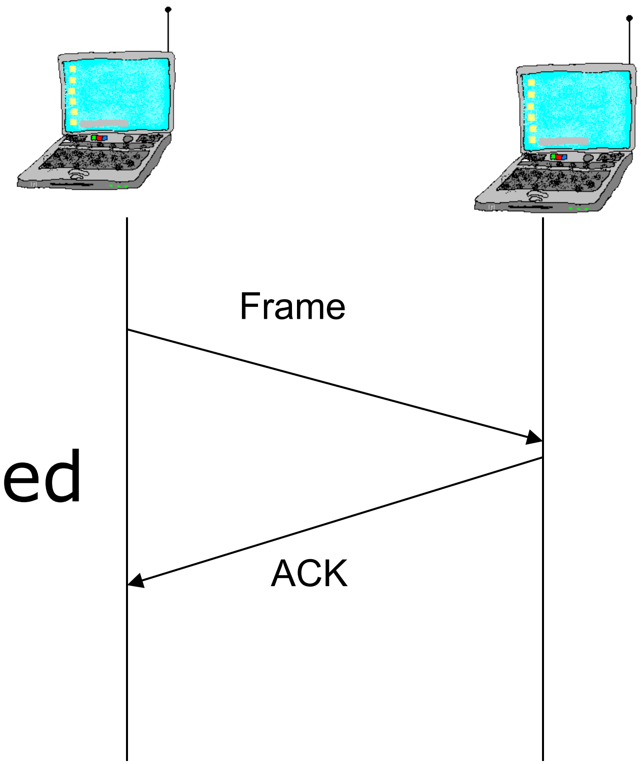
- Channel access
- Error recovery
- Fragmentation and reassembly
- Power saving
- Addressing
- Framing

Channel access

- The access to the transmission medium is regulated by the so called "*coordination functions*"
- Two coordination functions are defined
  - *Distributed Coordination Function* (DCF)
    - Based on CSMA with *backoff*
  - *Point Coordination Function* (PCF)
    - *Collision free* access based on polling
    - Several BUGS in the standard – never implemented in commercial devices

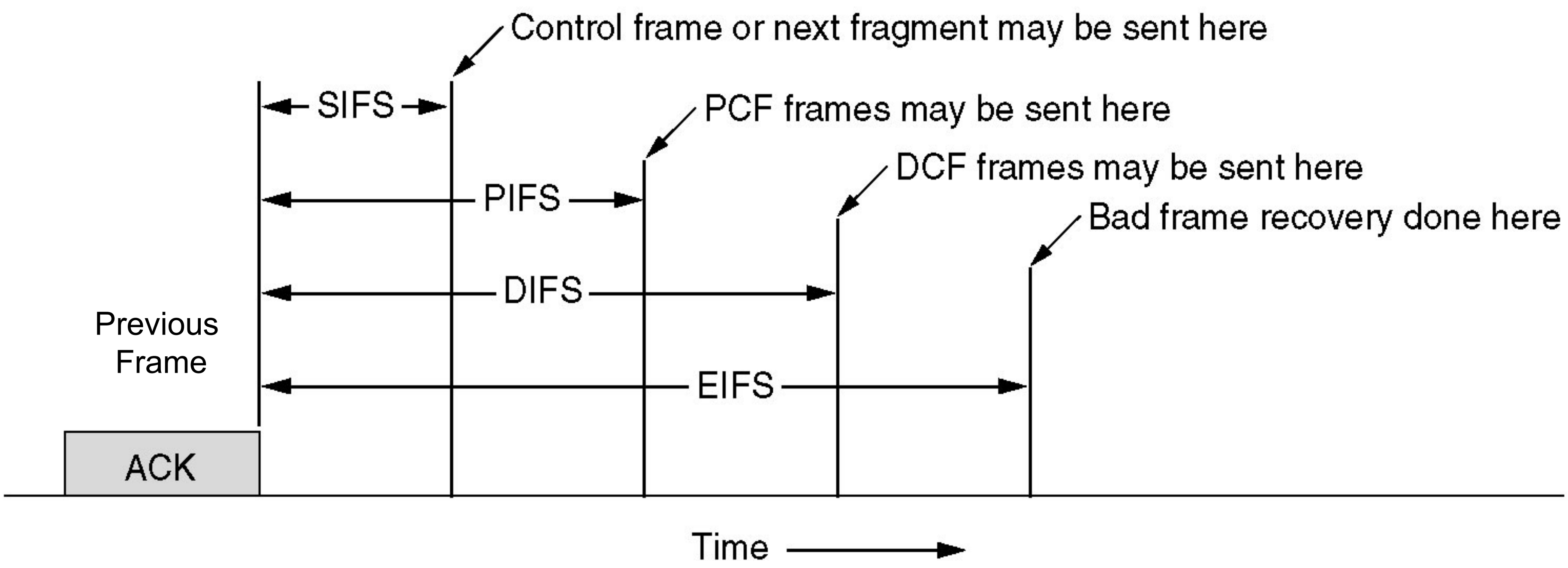
Error recovery

- Absolutely necessary on a "noisy" (wireless) channel
- Only for *unicast transmissions* (broadcast service is *unreliable*)
- Based on a positive acknowledgment per received frame ("*stop & wait*")
- Requires to use retransmission timers



Question: Do we have ACKs in Ethernet? Why?

Interframe spacing



- Several time intervals regulate the channel access
- These are *minimum* waiting intervals after last and are based on the physical *carrier sensing* mechanism

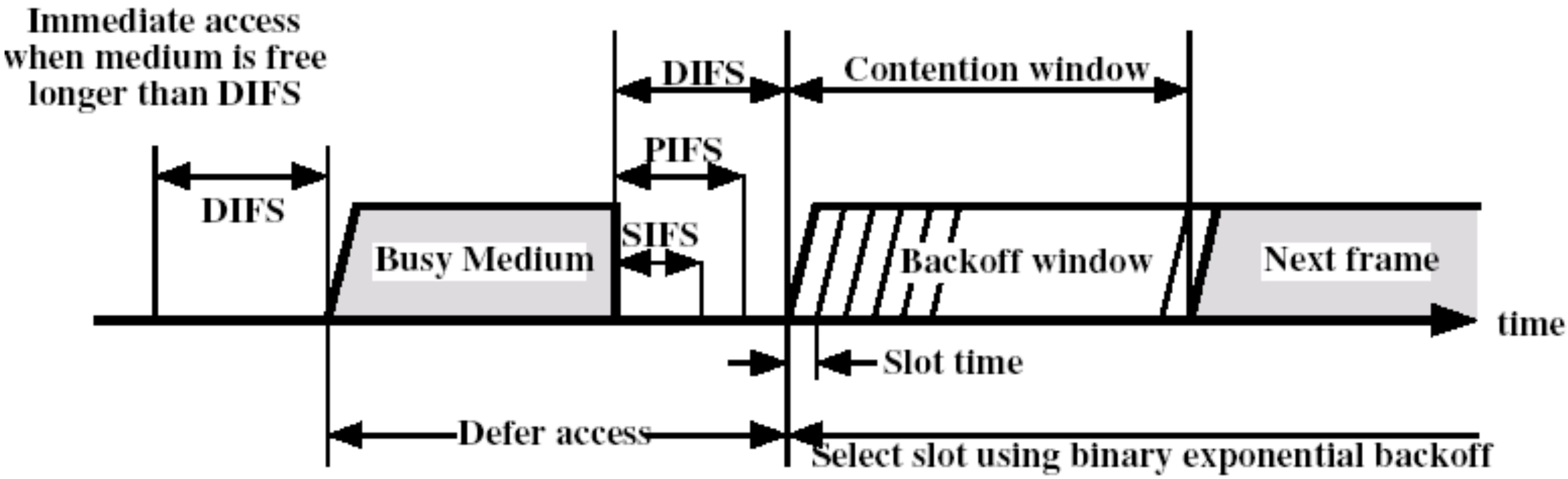
Interframe spacing

- *Short Inter Frame Spacing* (SIFS):
  - High priority transmissions can start after a SIFS after previous transmission
- *PCF Inter Frame Spacing* (PIFS):
  - Interframe space used to issue polling frames in PCF mode
- *DCF Inter Frame Spacing* (DIFS):
  - Regular data transmission in DCF mode can start after a DIFS
- *Extended Inter Frame Spacing (EIFS)*:
  - Used in special cases when previous transmission cannot be decoded

Distributed Coordination Function

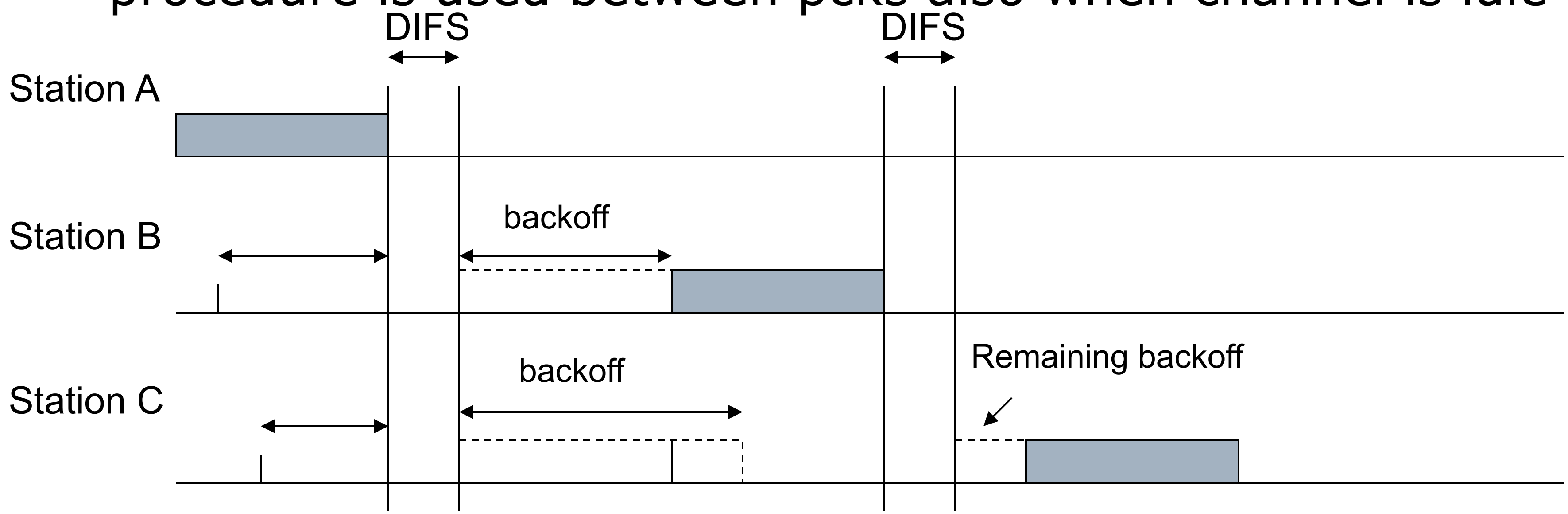
- DCF allows the coordination among stations without the need of a central controlling entity
- It can be used either in a IBSS and in a *infrastructure* BSS
- It is based on *Carrier Sense Multiple Access* with *Collision Avoidance* (CSMA/CA)
  - Before starting a transmission, the station listens to the channel:
    - If the Channel is idle (for *at least* a DIFS): start transmitting
    - If the Channel is busy: wait and start *backoff*

Distributed Coordination Function



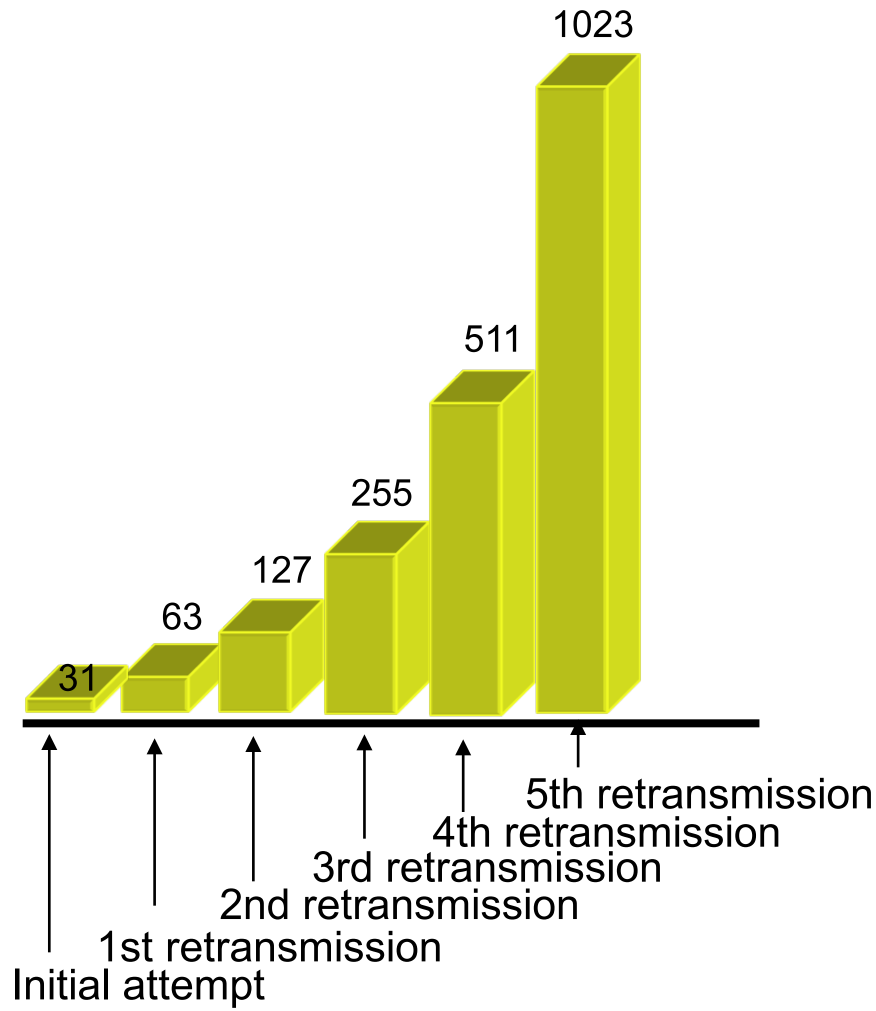
Collision Avoidance through the *Backoff* procedure

- Before transmitting, a station waits for a time period equal to a random number of slots (backoff) + DIFS
- The random number is uniform between 0 and CW (*Contention Window*)
- If during backoff the channel becomes busy, the counting down of slots is *stopped,* and it is then resumed when the channel is idle again
- If consecutive packets need to be transmitted, the backoff procedure is used between pcks also when channel is idle



Backoff Mechanism – the CW parameter

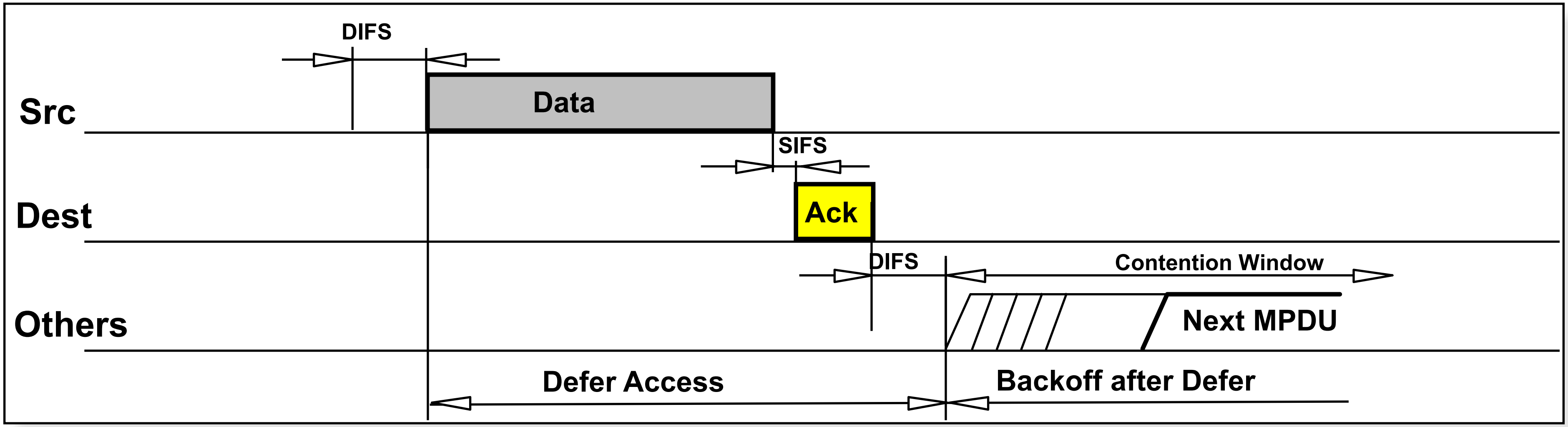
- *backoff* is uniform in [0, CW]
- CW is set dynamically:
  - If an error/collision occurs, (almost) double CW (up to CWmax=1023 slots)
  - If transmission is correct, set CW=CWmin=31



Error recovery in DCF

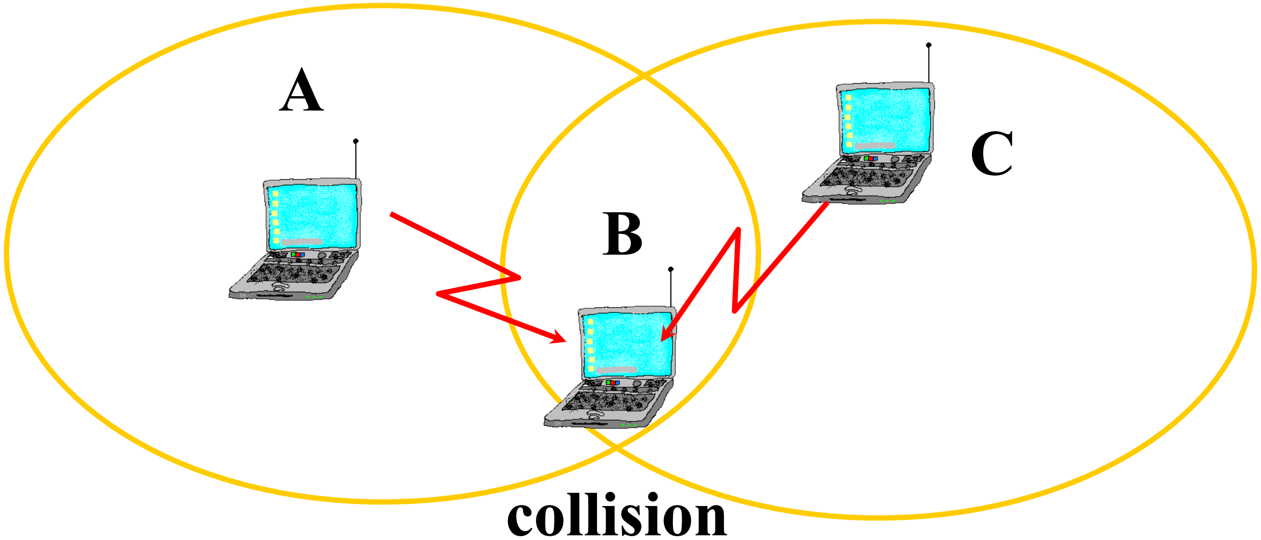
- Transmitting station can recover corrupted frames through retransmission
- Transmission feedback from receiver is based on a "*positive acknowledgement*"
  - Reception of *unicast* frames needs to be acknowledged
  - If acknowledgement is not received, the frame is considered lost and retransmitted
  - There is a maximum number of retransmissions per frame
- Retry Counters
  - *Short Retry counter (for "short" frames)*
  - *Long Retry counter (for "long" frames)*

Transmission example



- SIFS < DIFS, therefore ACKs have priority over data frames

Hidden Terminal

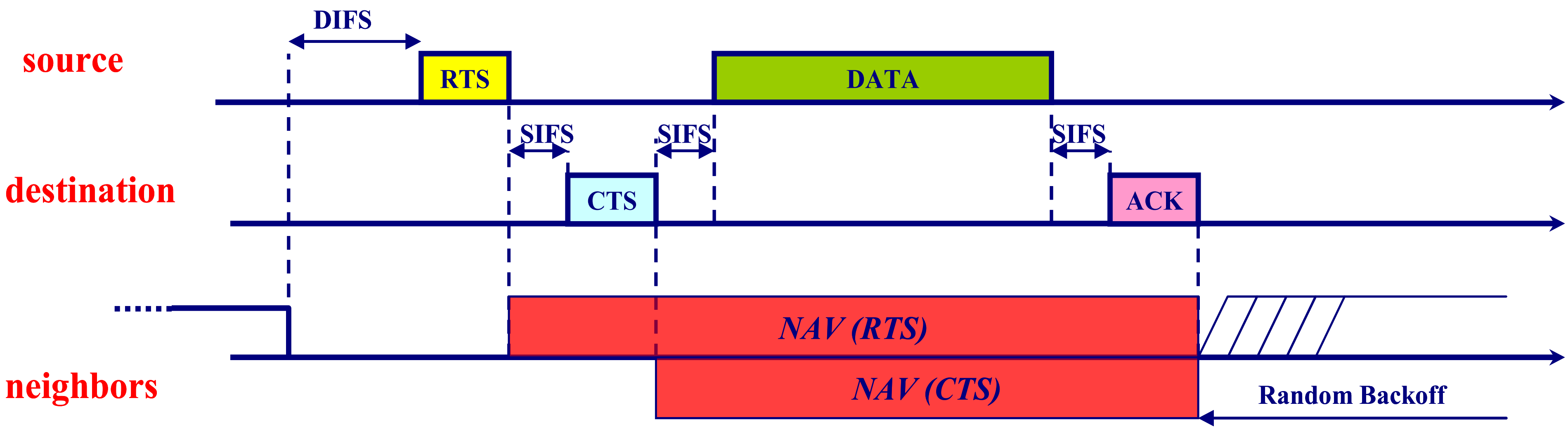


- Station A is "hidden" to station C
- Since B is in range of both A and C, a <u>collision</u> occurs (i.e., two (or more) signals arrive at the same time in the same place, namely station B)

Solution to the *Hidden Terminal*

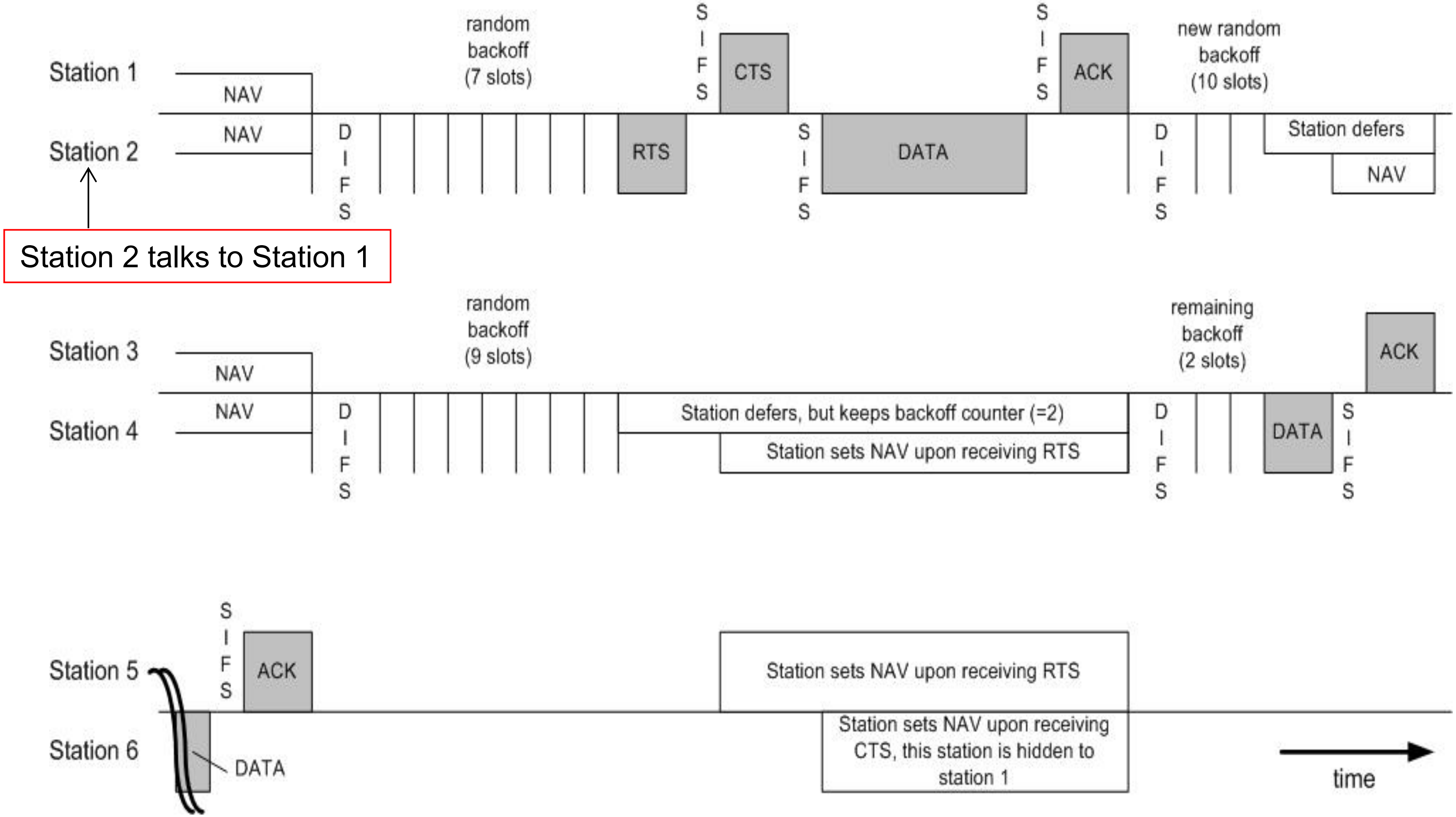
- The standard adds a procedure of logical (virtual) *carrier sensing* to the physical one
- Control frames are used, in which it is coded the so called *Network Allocation Vector (NAV)*
- The NAV contains the *duration* of the communication which is currently occupying the channel
- Mobile stations that receive such control frames do not try to access the channel during the time specified in the NAV

Virtual Carrier Sense

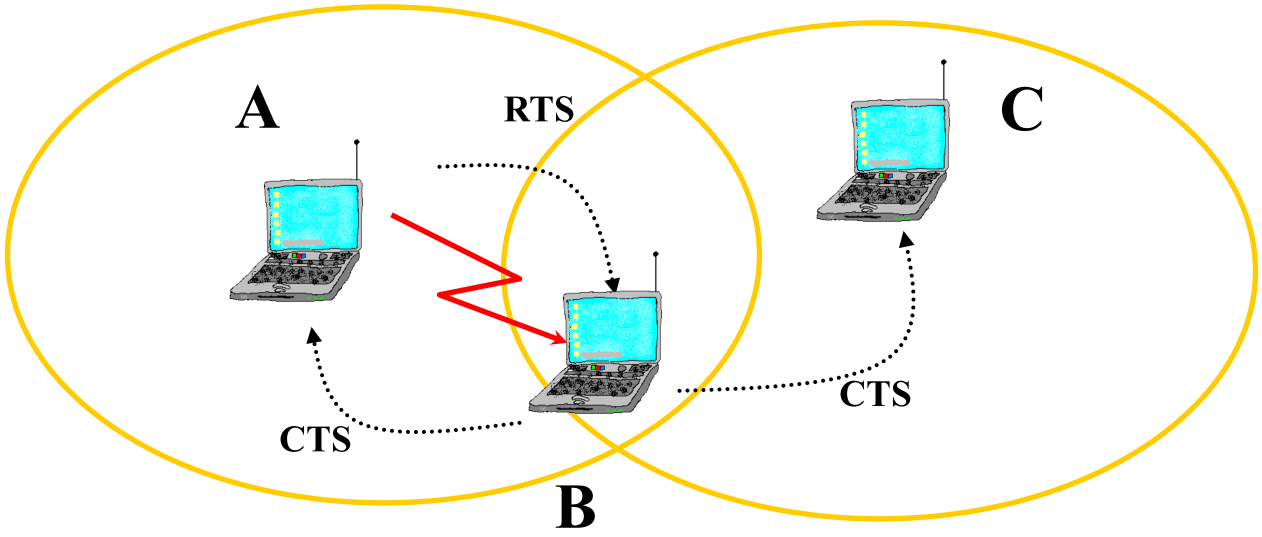


- Ingredients
  - Control frames:
    - *Request To Send (RTS)*
    - *Clear To Send* (CTS)
  - Network Allocation Vector (NAV)

Example

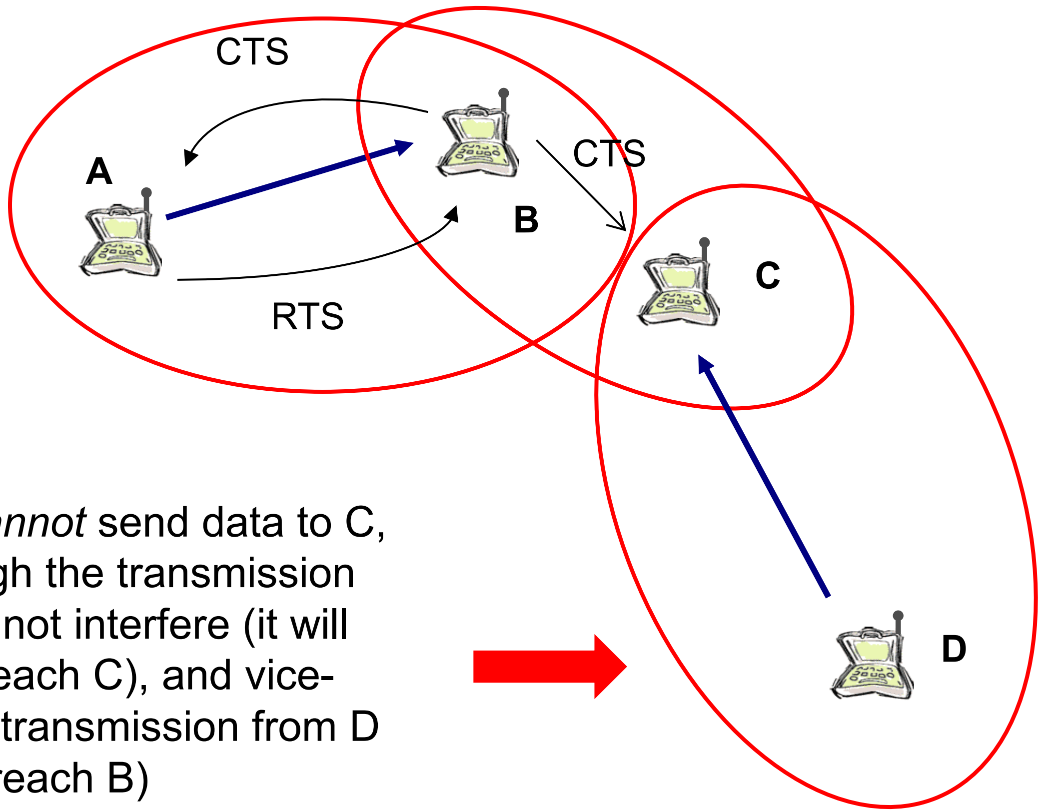

Station 1
Station 2
Station 3
Station 4
Station 5
Station 6
NAV
NAV
DIFS
random backoff (7 slots)
RTS
SIFS
CTS
SIFS
DATA
SIFS
ACK
DIFS
new random backoff (10 slots)
Station defers
NAV
Station 2 talks to Station 1
random backoff (9 slots)
Station defers, but keeps backoff counter (=2)
Station sets NAV upon receiving RTS
remaining backoff (2 slots)
DATA
SIFS
ACK
SIFS
ACK
DATA
Station sets NAV upon receiving RTS
Station sets NAV upon receiving CTS, this station is hidden to station 1
time

Hidden terminal solved



Exposed terminal

- … but another problem is created



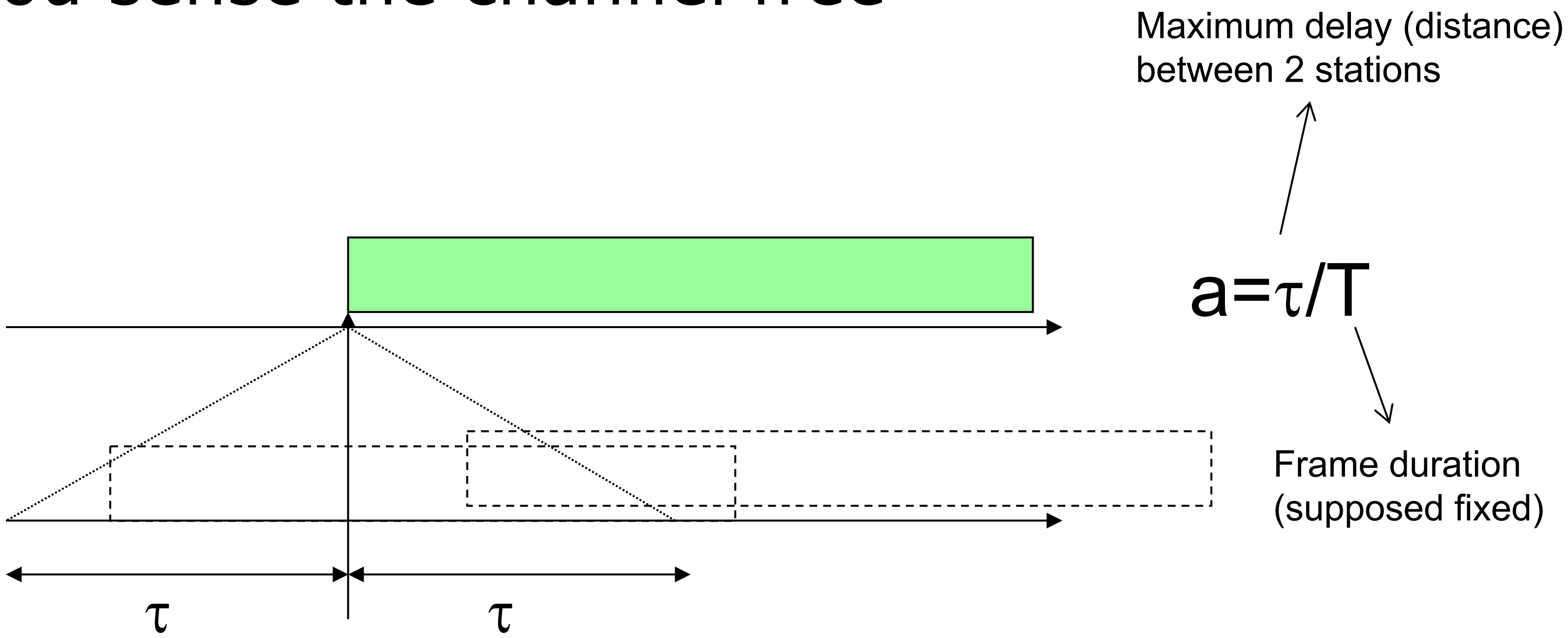
Here, D *cannot* send data to C, even though the transmission from A will not interfere (it will not even reach C), and vice-versa (the transmission from D will never reach B)

Overhead

- The exchange of control frames *reduces* channel capacity
- Transmission efficiency depends on:
  - Channel quality
  - Data frame size
- 802.11 standard defines a threshold (*RTSThreshold*) on the size (D) of data frames:
  - If D < *RTSThreshold,* RTS/CTS exchange is <u>*NOT*</u> used
  - If D > *RTSThreshold*, RTS/CTS exchange is used

Throughput analysis of CSMA

- Simplified model
- No hidden terminals
- CSMA: like Aloha but transmit only when you sense the channel free



Throughput analysis of CSMA

- On the channel we have cycles of *Busy* (at least one station senses the channel as busy) and *Idle* (all stations sense the channel free) periods
- The throughput S can be given by:

$$S = \frac{\alpha}{B + I}$$

- where B and I are the *average busy* and *idle periods,* and α is the probability that there is a successful transmission in a busy period

Throughput analysis of CSMA

- Making the same assumptions of the Aloha infinite population model we have: $\alpha = e^{-aG}$

$$I = \frac{1}{G}$$

$$B = e^{-aG}(1+a) + (1-e^{-aG})(1+a+Z)$$

- where *Z* is the time when colliding transmissions partially overlap

Throughput analysis of CSMA

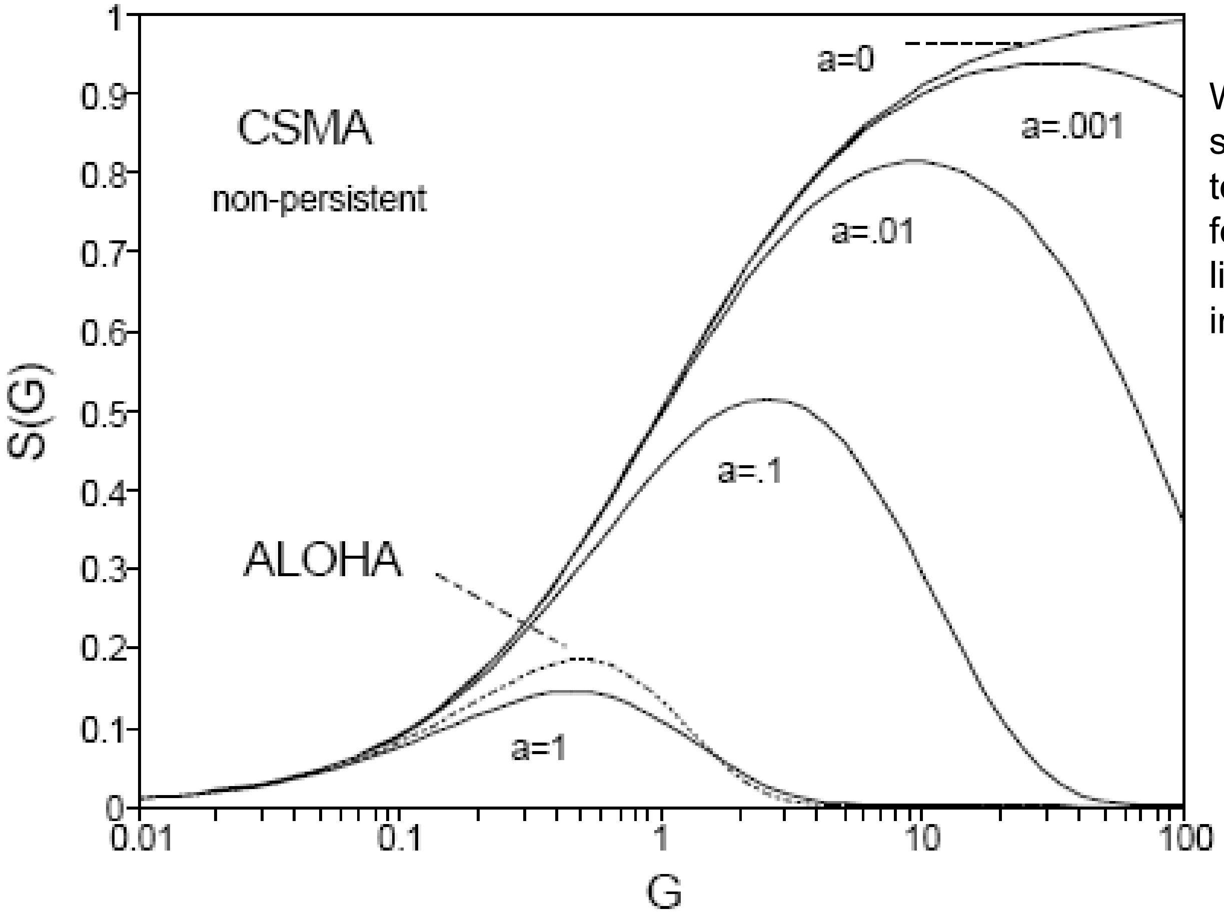
- It can be shown that:

$$Z = a + \frac{ae^{-aG}}{1-e^{-aG}} - \frac{1}{G}$$

- Therefore we get:

$$S = \frac{Ge^{-aG}}{G(1+2a)+e^{-aG}}$$

Throughput analysis of CSMA



When a is small, all stations are *very close* to each other (the feedback from channel listening is almost immediate)

Throughput analysis of CSMA/CA

- Similarly to the general model we can derive a model for 802.11 DCF

$$\alpha = e^{-aG}$$

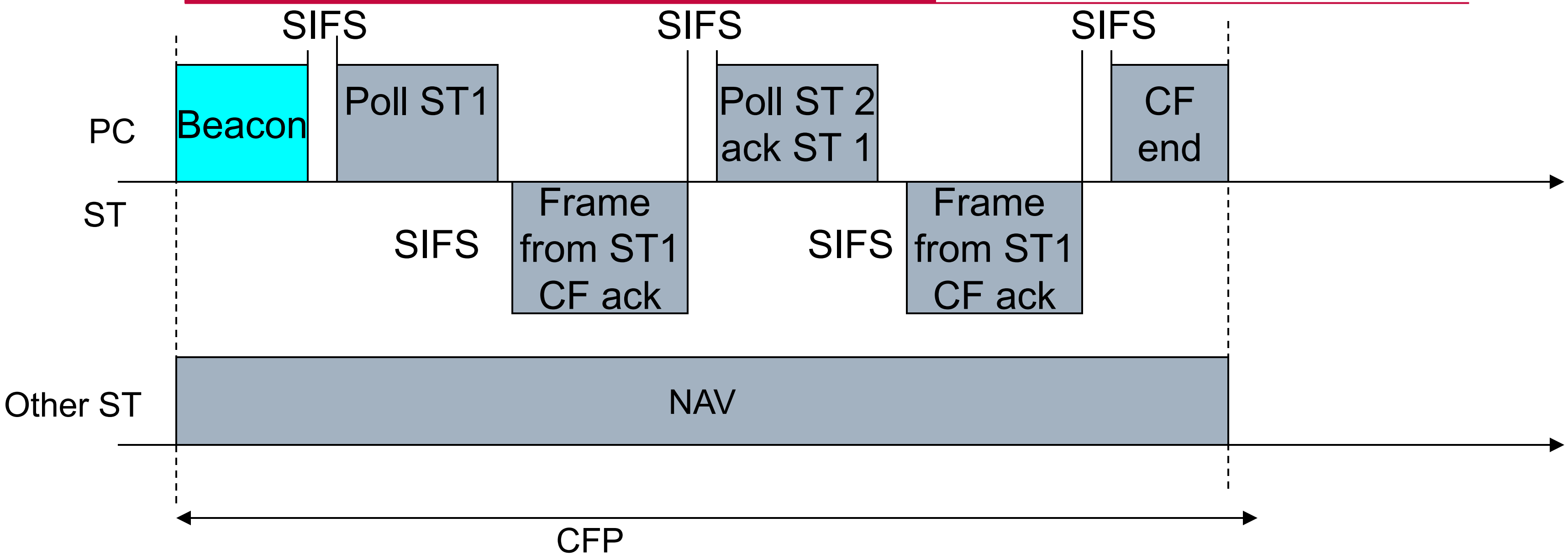
a = interframe space
b = duration of RTS and CTS

$$I = \frac{1}{G}$$

$$B = e^{-aG}(1+3a+2b)+(1-e^{-aG})(b+a+Z)$$

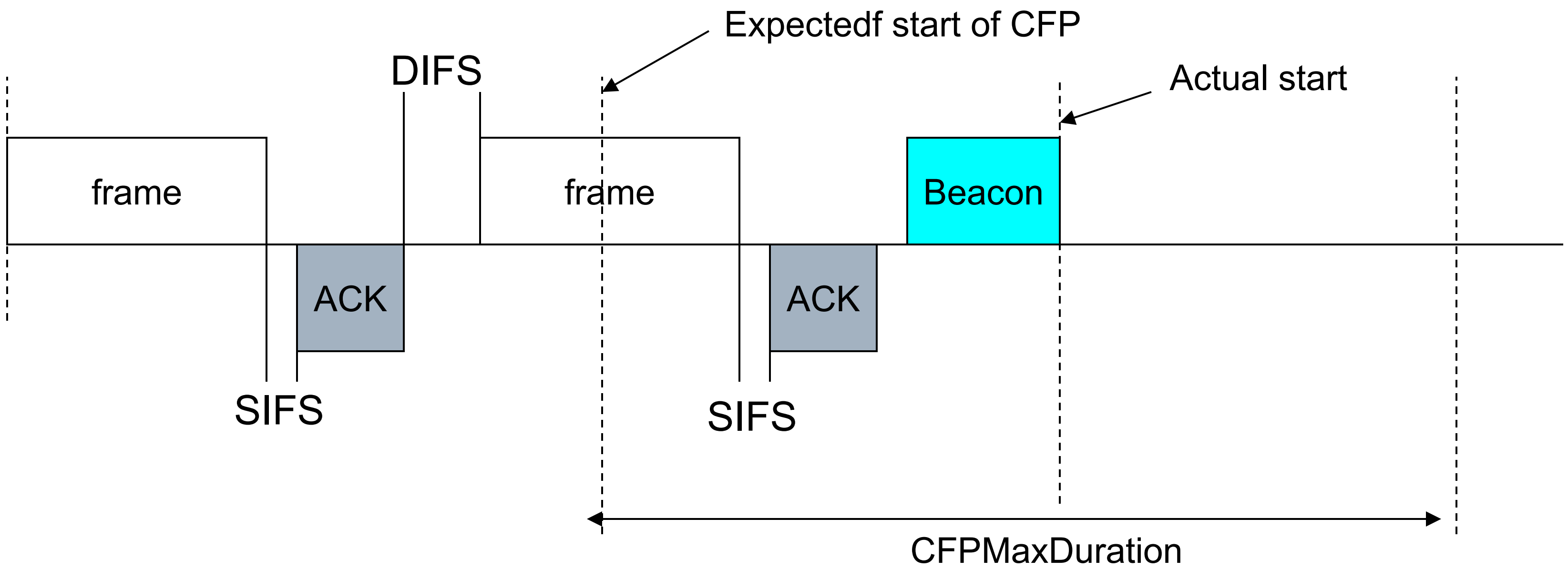
$$S = \frac{Ge^{-aG}}{G(1+2a)+e^{-aG}-G(1-b)(1-e^{-aG})+(2a+2b)Ge^{-aG}}$$

Point Coordination Function (PCF)



- PCF has never been used in commercial devices
- PCF cannot guarantee QoS due to a couple of "mistakes"

Point Coordination Function (PCF)



- Unpredictable inter-beacon interval
- No constraint on frame transmission duration

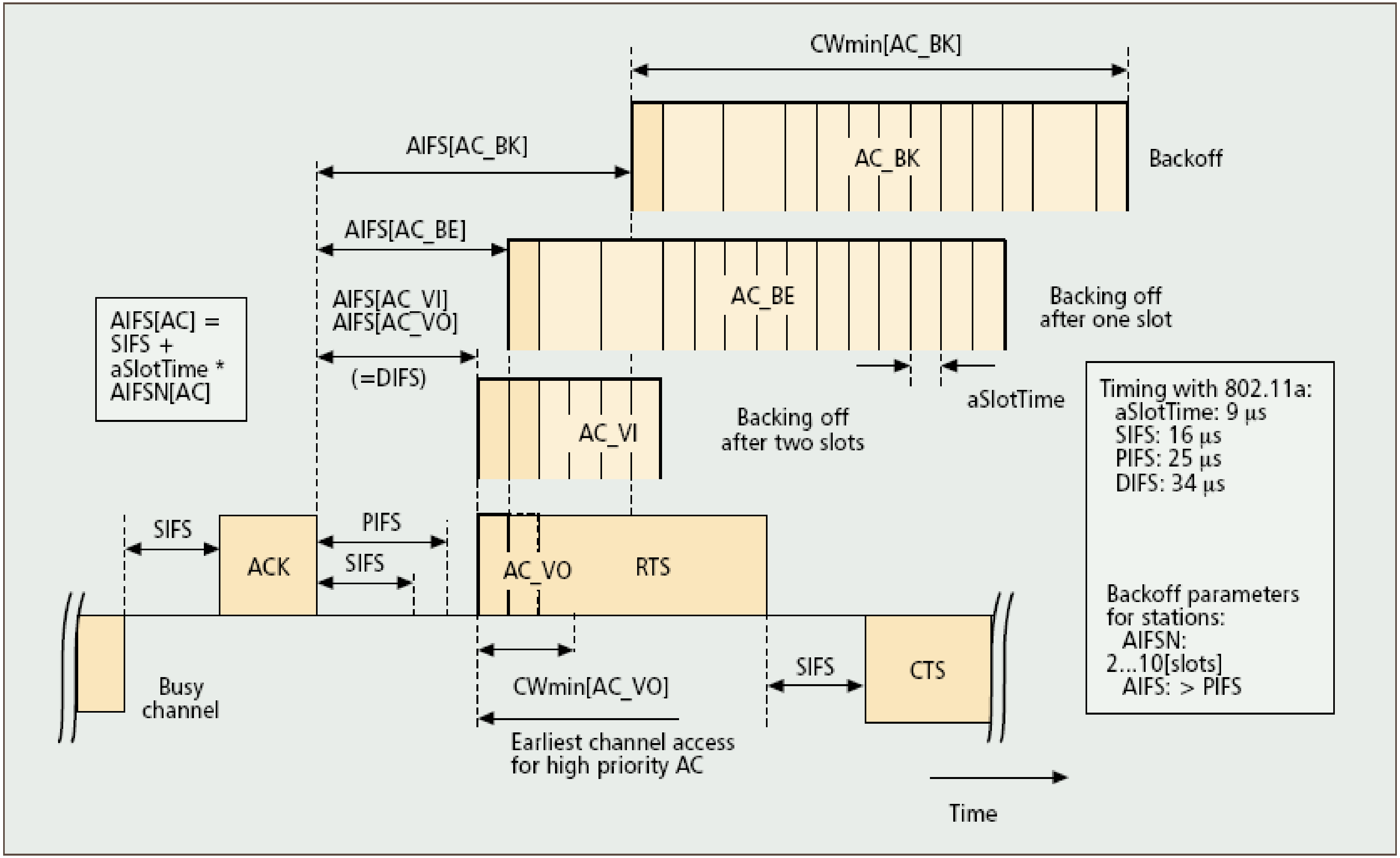
802.11e

- Flow differentiation
  - 4 queues for 4 traffic classes
- *Transmission Opportunities* (TXOP)
  - Defined as the Maximum transmission time per transmission
- Direct transmission
- *Block ACK (*single ACK for a "train" of frames*)*
- *Hybrid Coordination Function (HCF) with two access modes*
  - Contention based (EDCA, *Enhanced Distributed Channel Access*)
  - Contention free (HCCA, *HCF Controlled Channel Access*)

EDCA

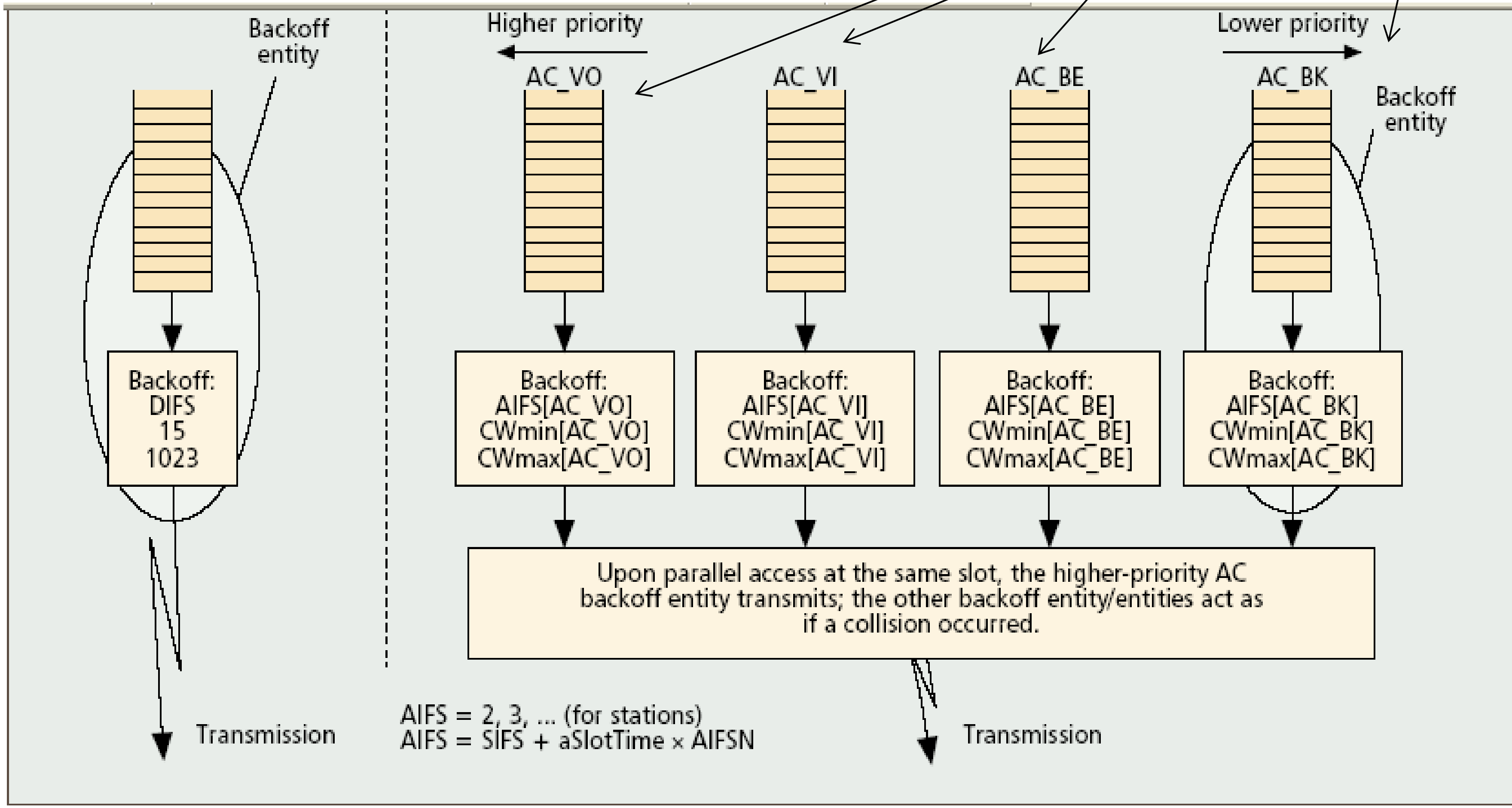
- 4 Access Categories (AC)
  - AC_VO: voice
  - AC_VI: video
  - AC_BE: best effort
  - AC_BK: background
- Each AC is characterized by different *backoff* parameters:
  - *AIFS[AC]: inter-frame space*
  - *CWMin[AC]: minimum backoff window*
  - *CWMax[AC]: maximum backoff window*
  - *TXOPlimit[AC]: maximum transmission duration*

Example: access with EDCA



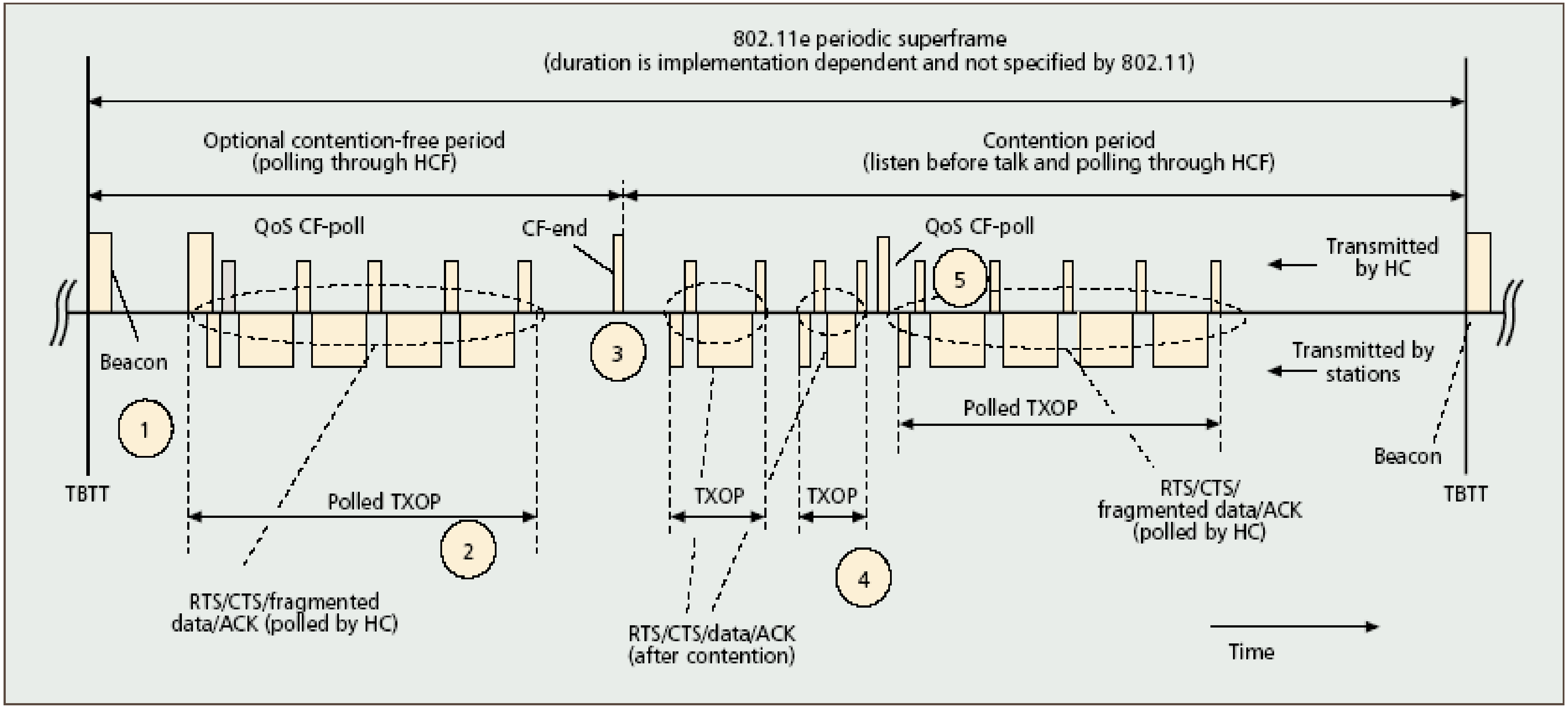
802.11e

Each queue behaves as a single DCF contending entity



- Several *backoff entities* inside the same station (*Virtual collision* handler)

HCCA



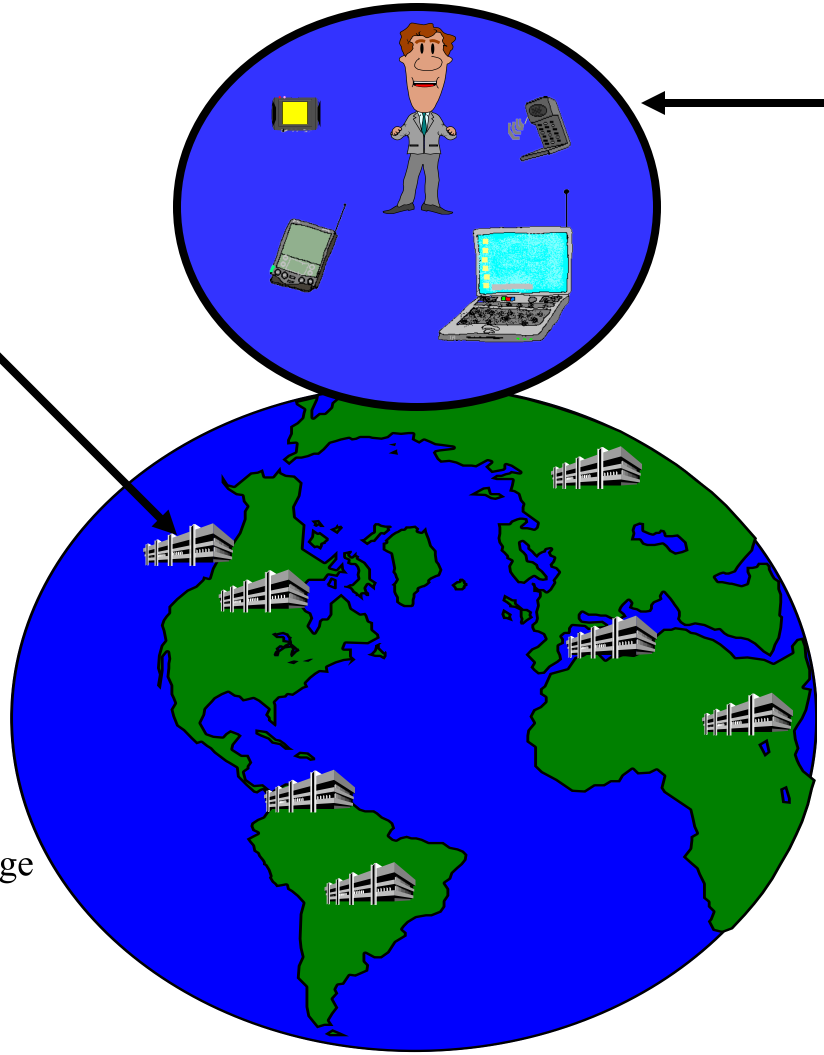
- Contention-free and contention-based transmissions can be mixed together

Part B
WPAN

Personal Area

WLAN

On-campus: Office, School, Airport, Hotel, Home



WPAN

Person Space: Office, Room, Briefcase, Pocket, Car

Short Range/Low Power

Voice AND Data

Low-cost

Small form factor

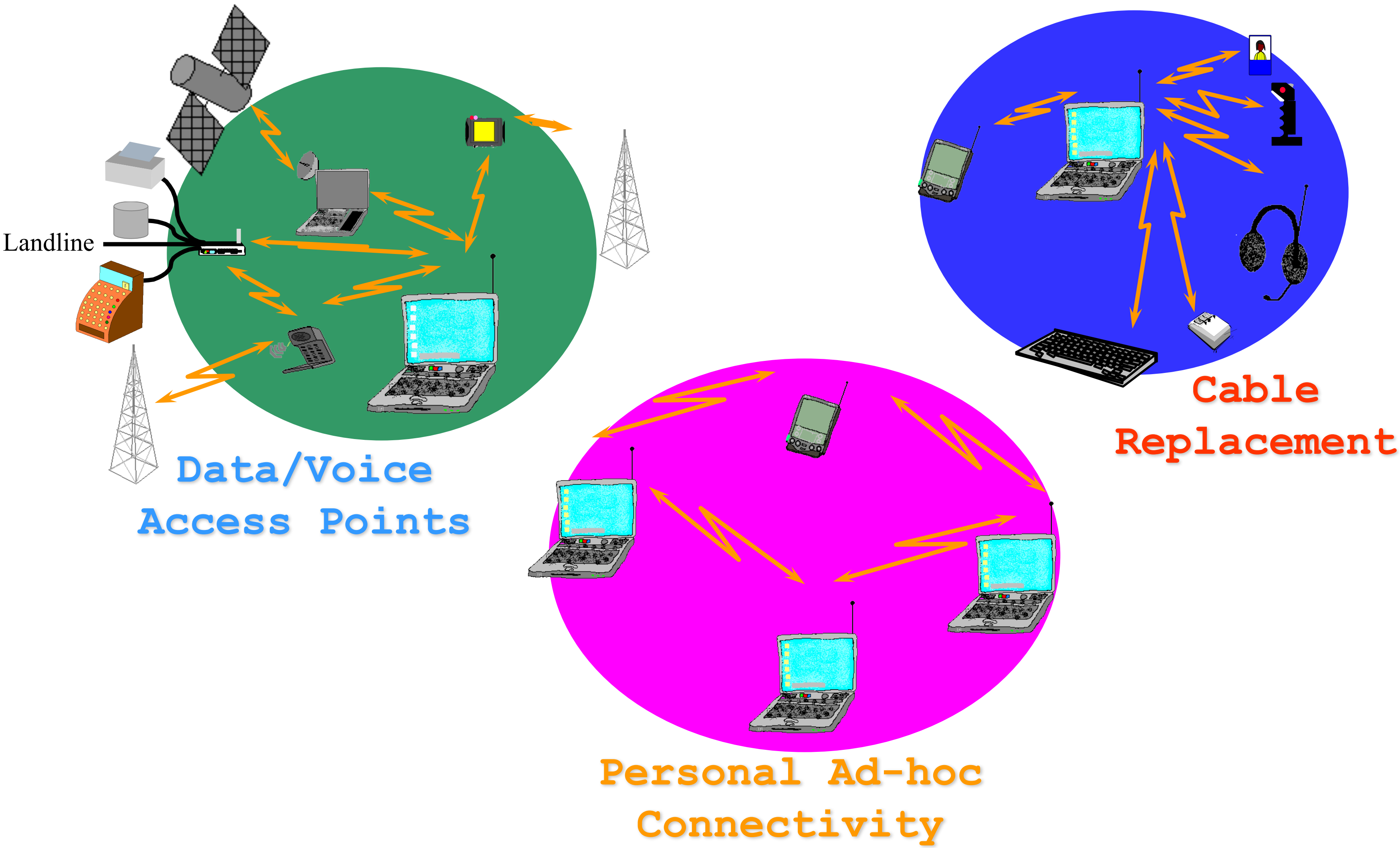
Many Co-located Nets

Universal Bridge

Cellular

Off-Campus Global Coverage

Personal Area



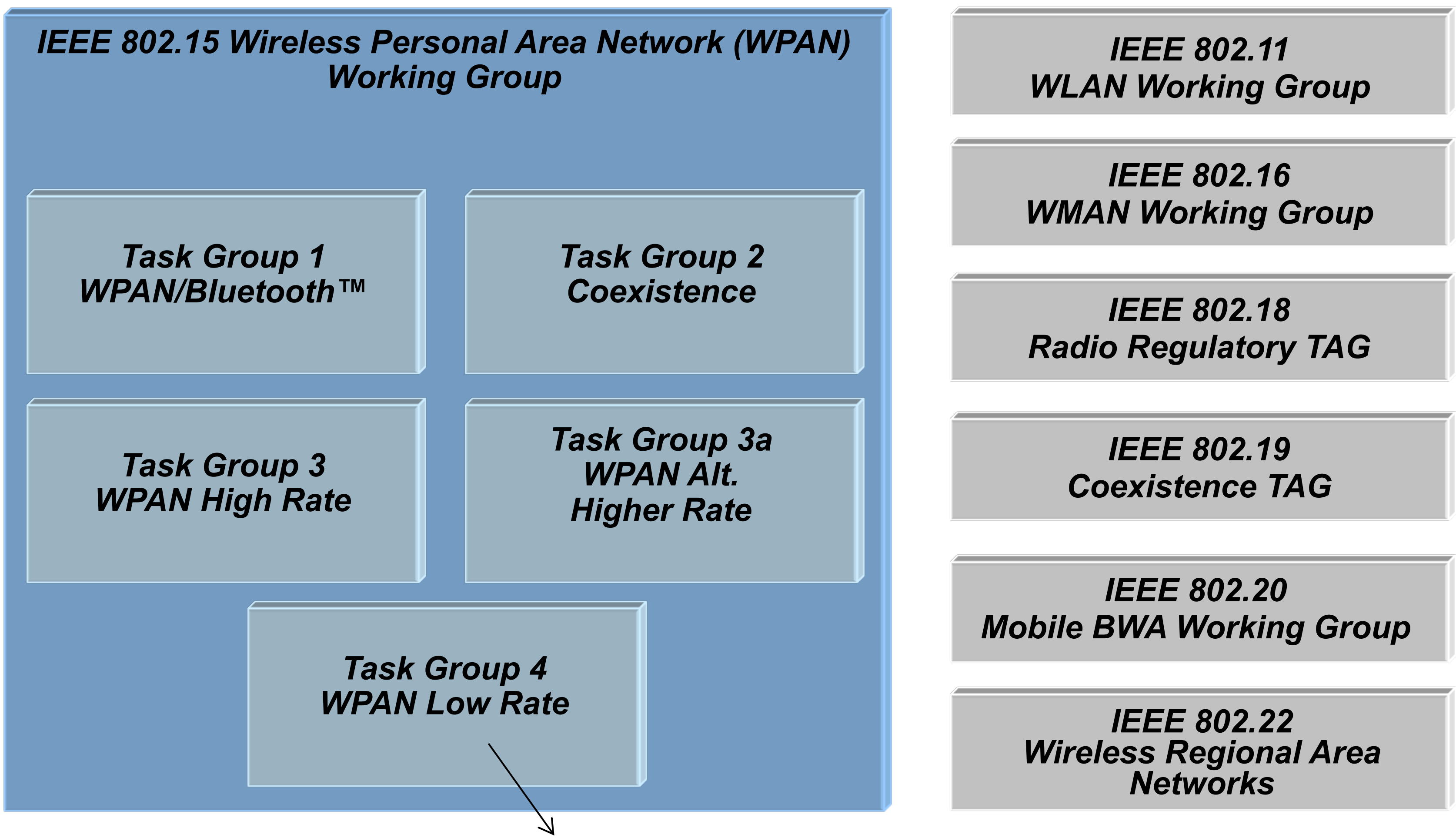
IEEE 802.15

Wireless Personal Area Networks (WPANs™)

- Short range
- Low power
- Low cost
- Small networks (including point-to-point links)
- "Personal Operating Space"

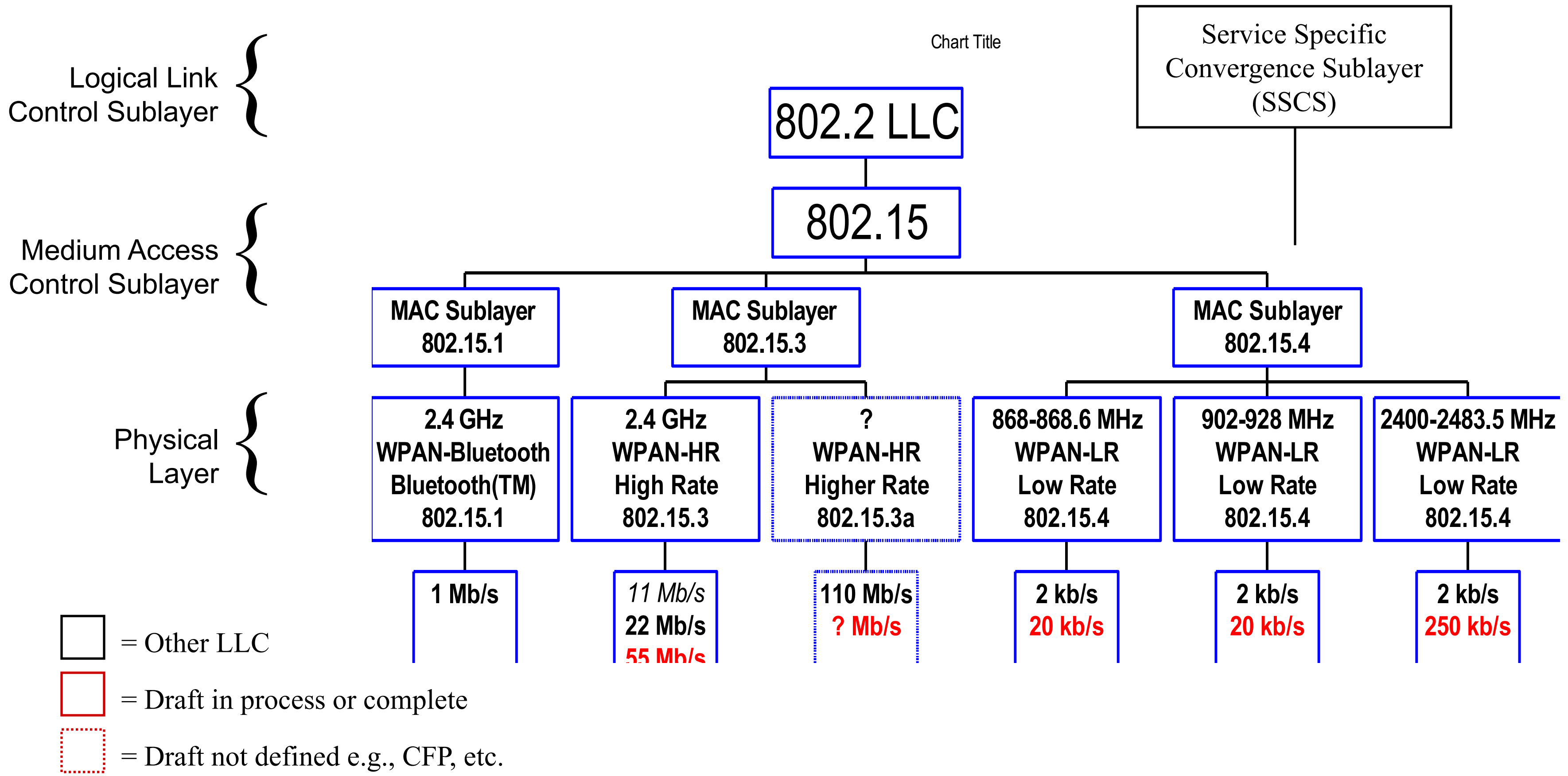
- Working Group (WG) created by IEEE, pushed by Bluetooth success

IEEE Wireless Standards



But very long life battery!

802.15 family

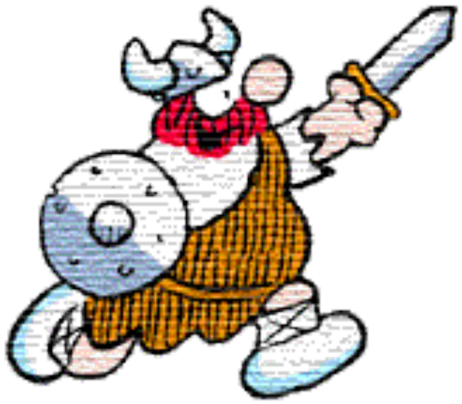


Bluetooth

Bluetooth vs. 802.15.1

- Bluetooth is an *industrial* standard for WPAN
- WG 802.15.1 adopted Bluetooth specifications for levels 1 and 2
- ’96-’97: Ericsson internal project
- ’98: Bluetooth Special Interest Group (SIG) (Ericsson, IBM, Intel, Toshiba, Nokia)
- ’99: Other companies join the SIG (3Com, Lucent Technologies, Microsoft, Motorola)

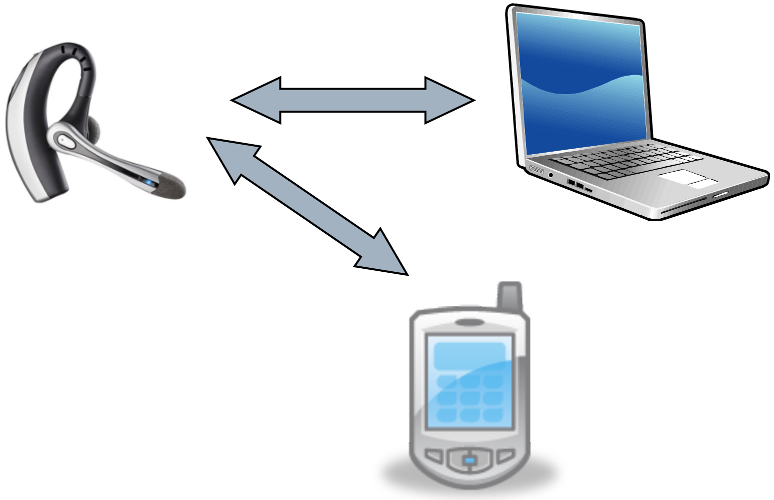
Bluetooth



- Danish king of the middle ages, Harald Blaatand II, alias *Bluetooth* (940-981)
- Unified Denmark and Sweden

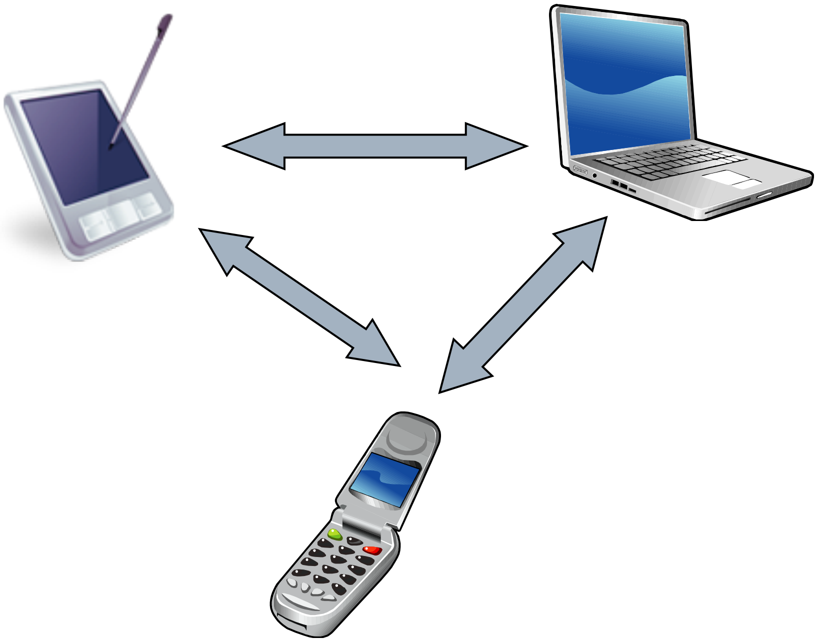
- Radio technology
- Low cost
- Short range (10-20 m)
- Low complexity
- Small size
- Transmission band ISM 2.4 GHz
- Only the first two levels are standardized by IEEE 802.15.1

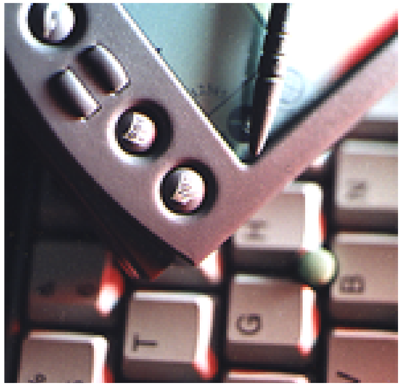
Application scenarios



- Headset

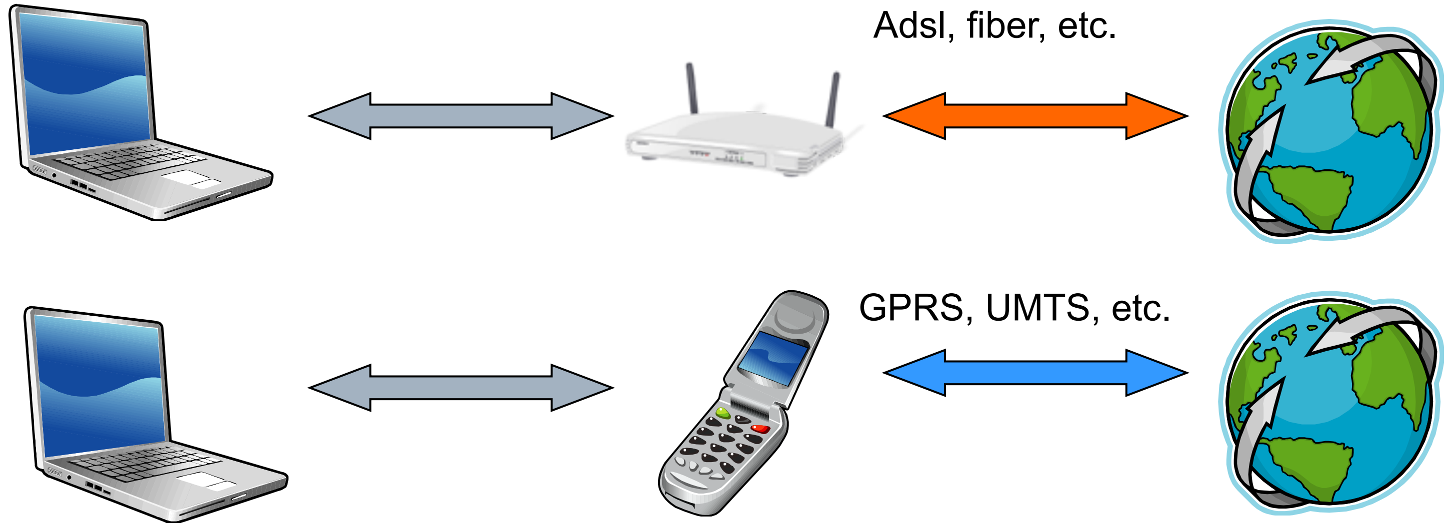
Application scenarios





- Data sinchronization

Application scenarios



- Access point

Physical layer

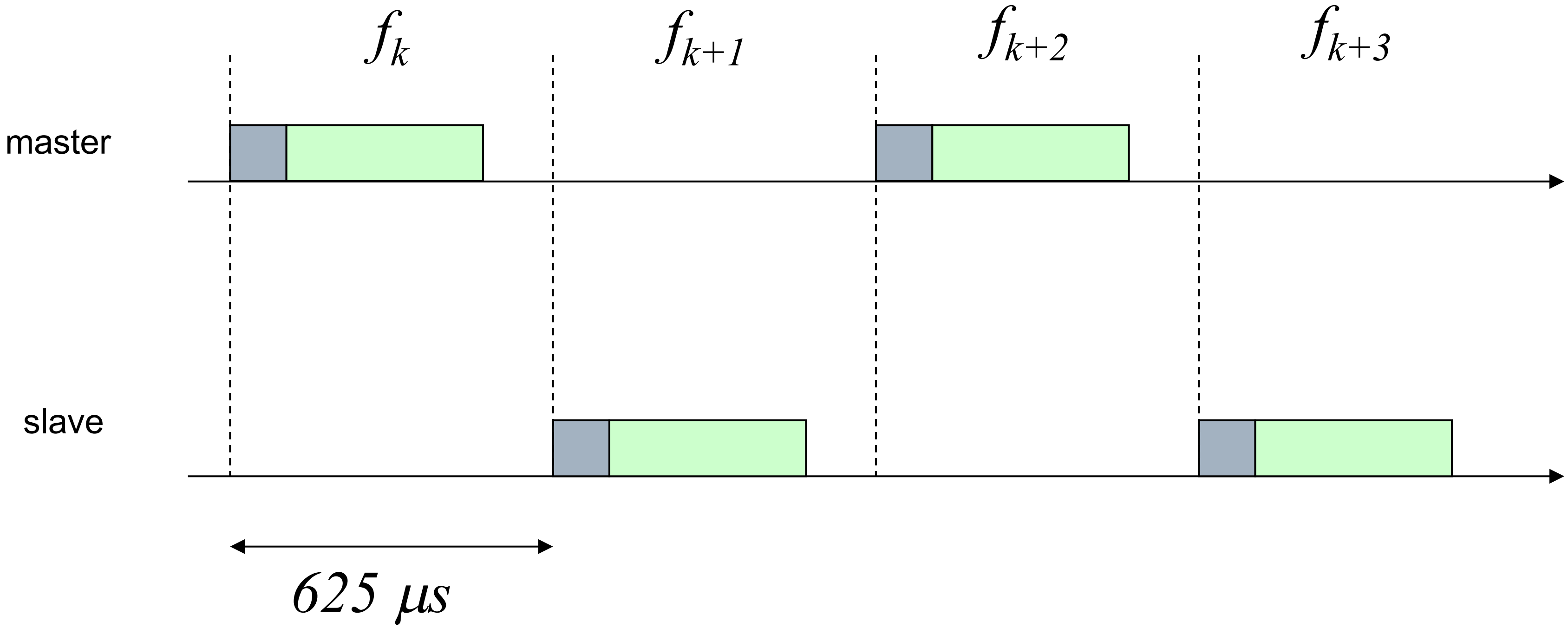
- ISM Band at 2.4 GHz
- 79 (only 23 in France and Japan) channels spaced by 1 MHz (2402-2480 MHz)
- G-FSK (Gaussian FSK) Modulation (1 Mb/s)
  - a binary one is represented by a positive frequency deviation and a binary zero by a negative frequency deviation
- Device classes

Class	**Power (mW)**	**Power (dBm)**	**Range (Approximated)**
Class 1	100 mW	20 dBm	~ 100 meters
Class 2	2,5 mW	4 dBm	~ 10 meters
Class 3	1 mW	0 dBm	~ 1 meter

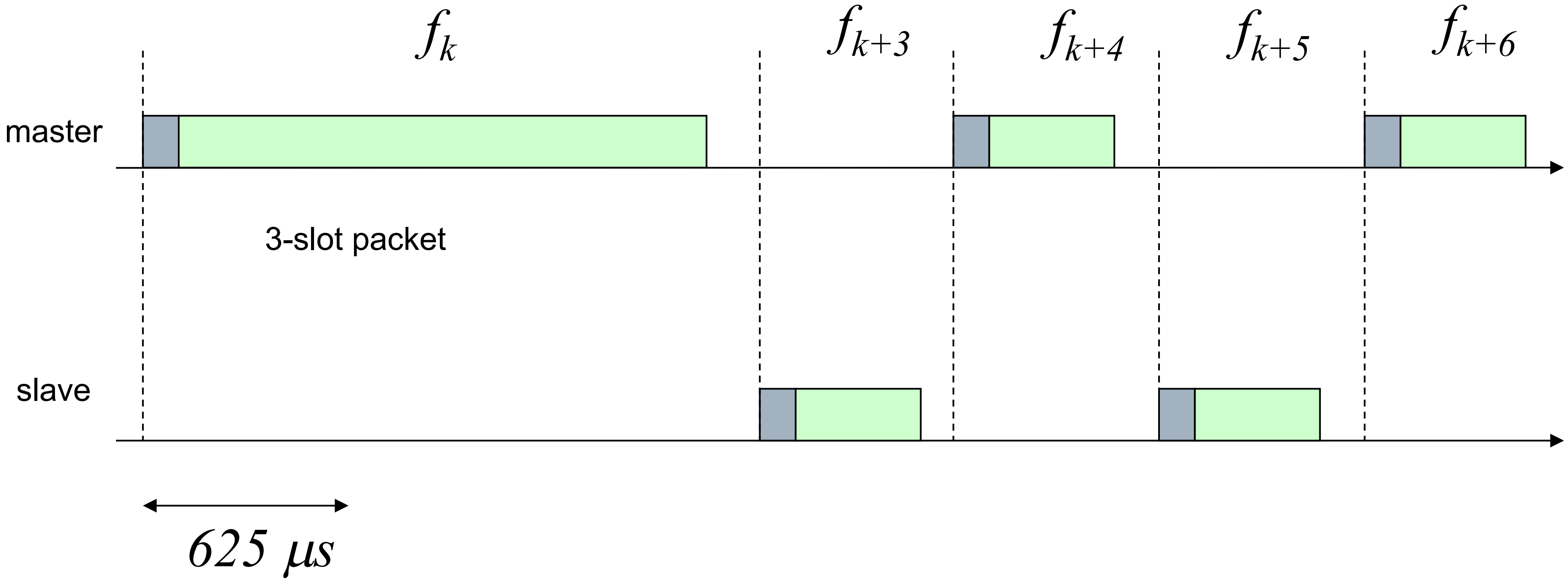
Physical layer

- Frequency Hopping (FH)
- 1600 hops/s (625 μs per hop)
- FH sequence is pseudo random and defined by the clock and the address of the *master* station that regulates channel access
- The other devices are *slave* and follow the sequence f_k defined by the master

Physical layer

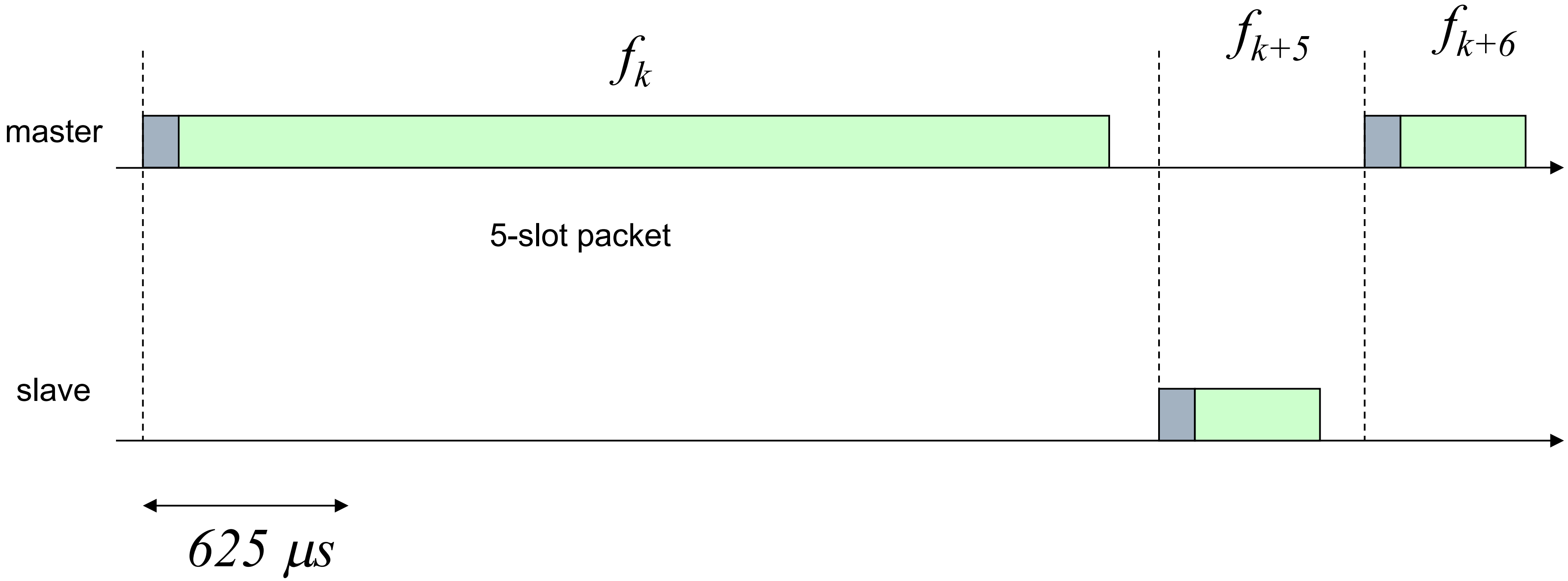


Physical layer



- Packets can span over 1, 3 or 5 slots (625 μs)

Physical layer

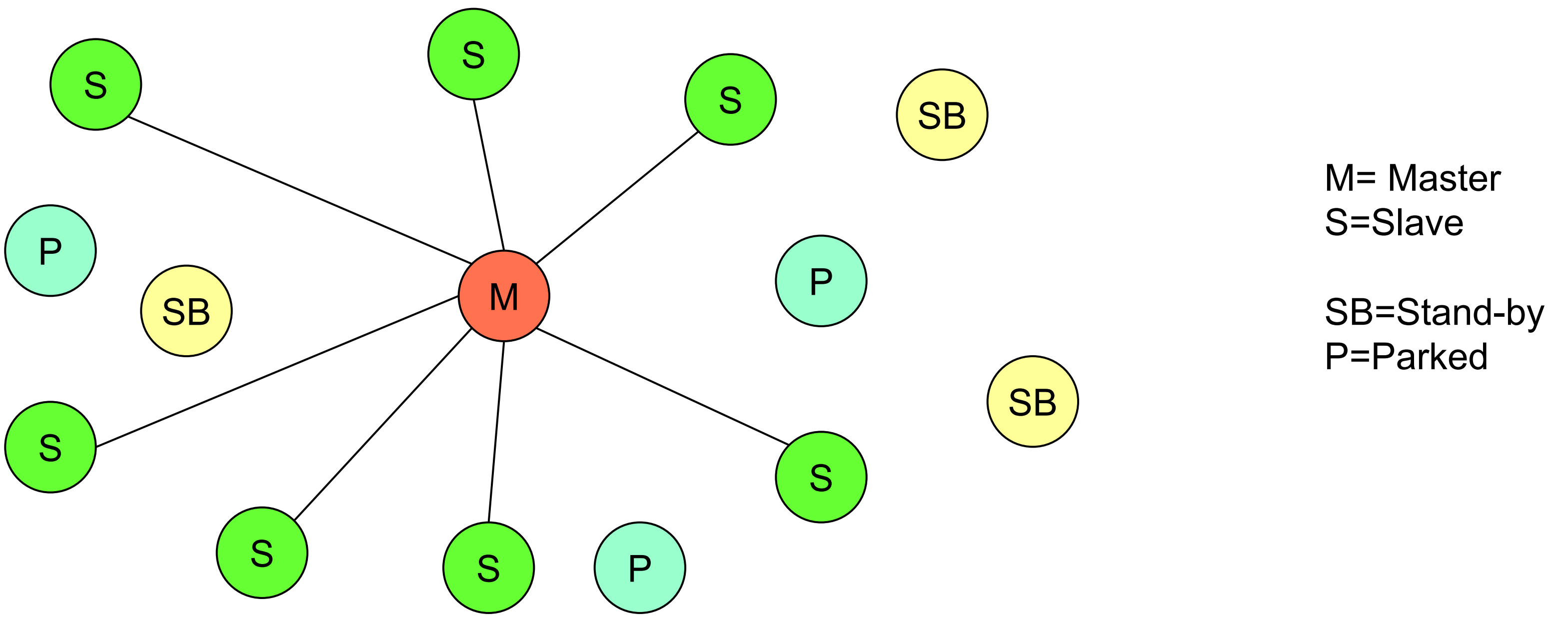


- Packets can span over 1, 3 o 5 slots

Piconet

- Piconet is the simplest architecture of a Bluetooth network
- A Piconet is an **ad hoc network** composed of **2 or more devices**
- One device acts as master, and all the other(s) as slave(s)
- The communication is *only* between master and slaves: slaves *cannot* communicate directly among themselves
- Up to 7 slaves can be activated
- The other nodes can be in:
  - Stand-by (not members of the piconet)
  - *Parked* (still members of the piconet, but not active; up to 256 parked slaves)

Piconet

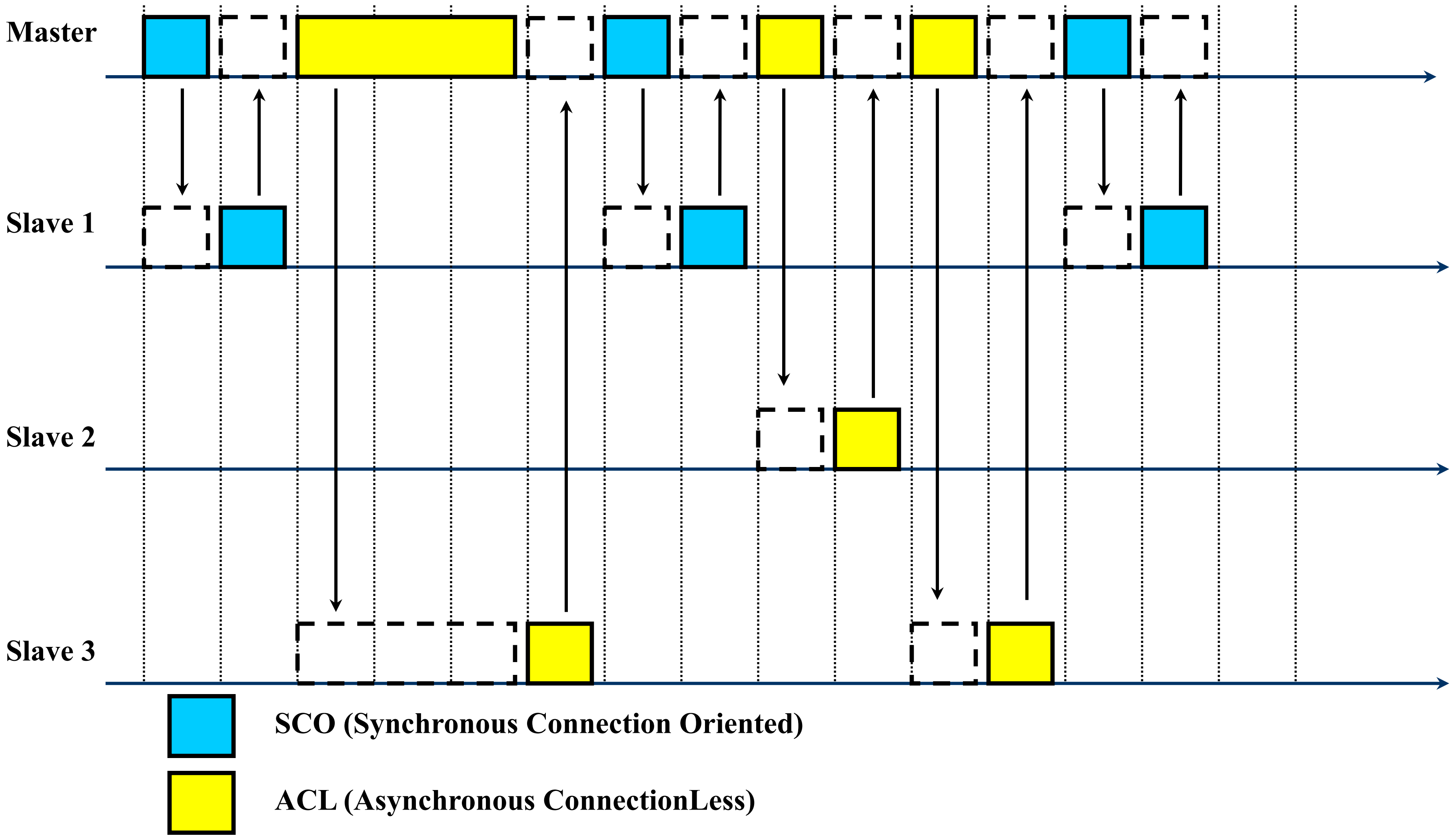


- Addresses
  - MAC address 48 bits
  - AMA (Active Member Address) 3 bits → Up to 8
  - PMA (Parked Member Address) 8 bits → Up to 256

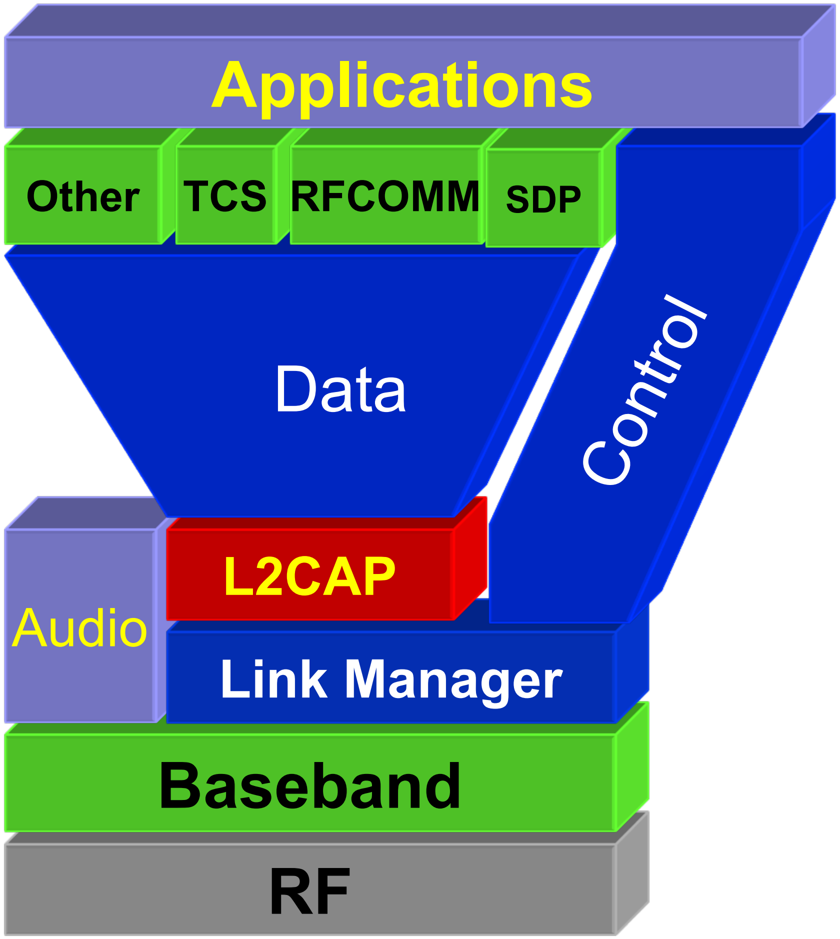
Connection types

- Bluetooth considers two types of connections
- SCO (Synchronous Connection Oriented)
  - Symmetric
  - Bidirectional fixed-capacity connection (“circuit”)
  - Optionally FEC
  - Basic speed 64 kbit/s
- ACL (Asynchronous ConnectionLess)
  - Packet service between master and slaves based on a polling mechanism
  - Several packet formats available
  - Rate up to 433.9 kbit/s symmetric (using 5 slot packets in both directions) and 723.2/57.6 kbit/s asymmetric (using 5 slots in one direction and 1 slot packet in the other)

Multiple access

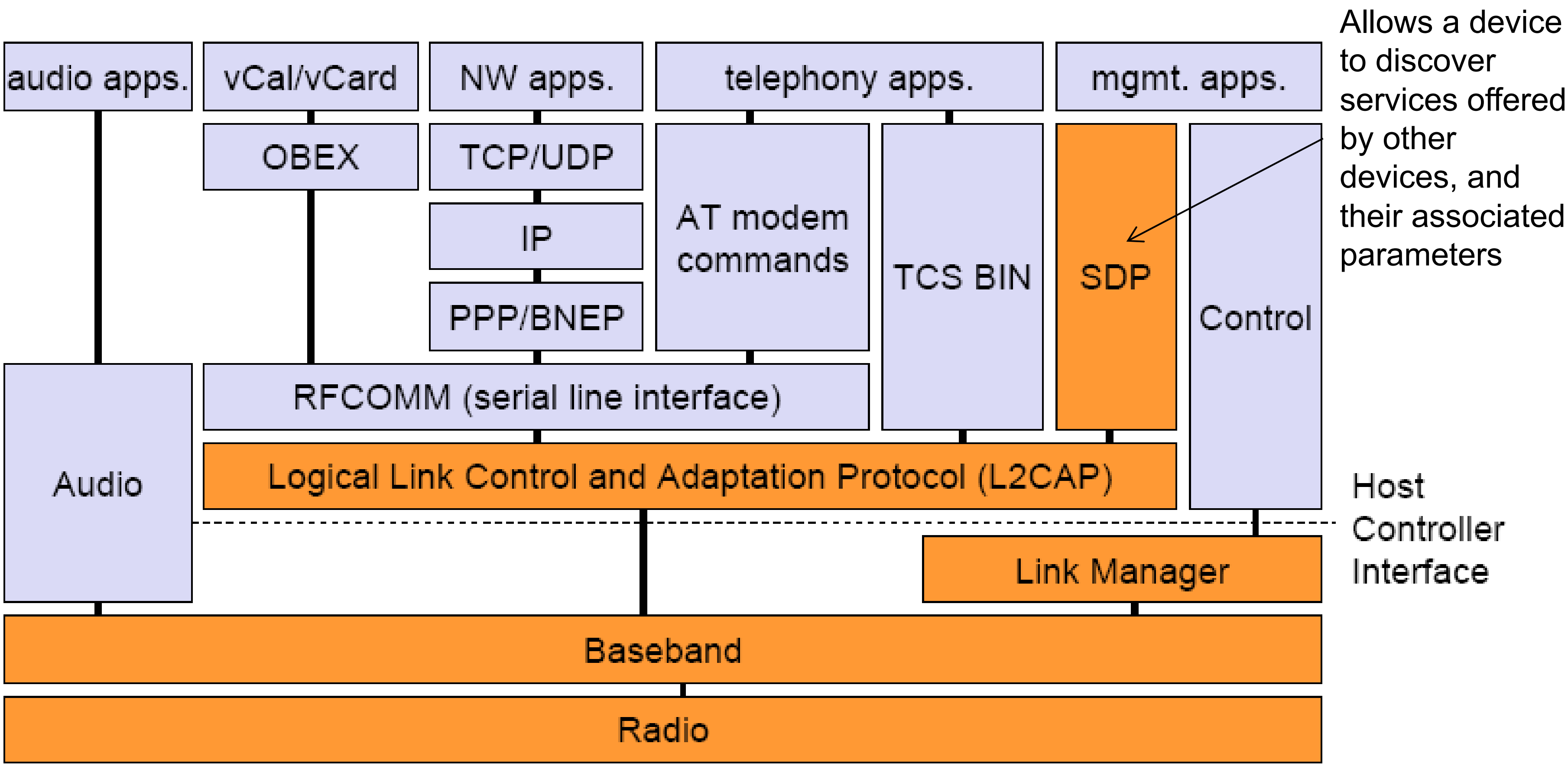


Protocol architecture



- Protocol stack *non compliant* with OSI model (adapted by 802.15.1 specifications with some compromise)
- RF + Baseband equivalent to PHY + MAC
- Control plane for network creation and connection management

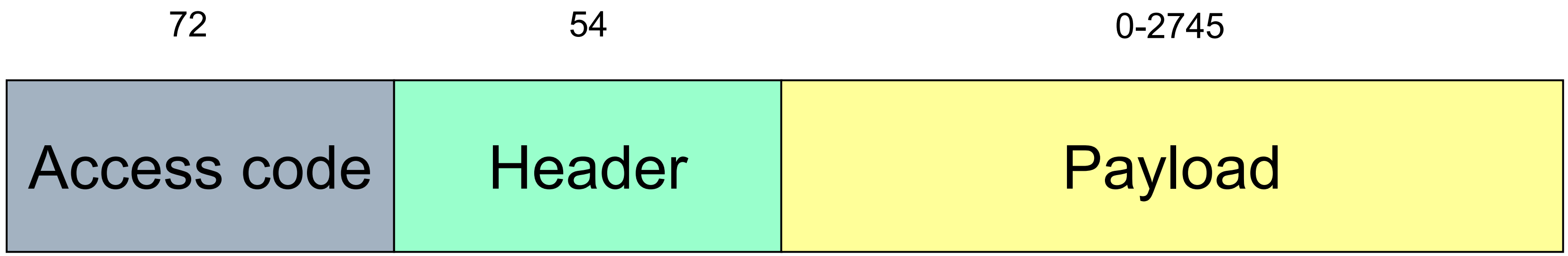
Protocol architecture



AT: attention sequence
OBEX: object exchange
TCS BIN: telephony control protocol specification – binary
BNEP: Bluetooth network encapsulation protocol

SDP: service discovery protocol
RFCOMM: radio frequency comm.

Packet Format



- BT includes three parts:
  - An **Access Code** used for synchronization and piconet identification
  - An **Header** used for Link Control (LC) and ARQ
  - A **Payload** whose format depends on the connection type and packet type (number of slots, FEC, etc.)

Packet Format: Access Code

4	64	4
Preamble	Synchronization word	Trailer

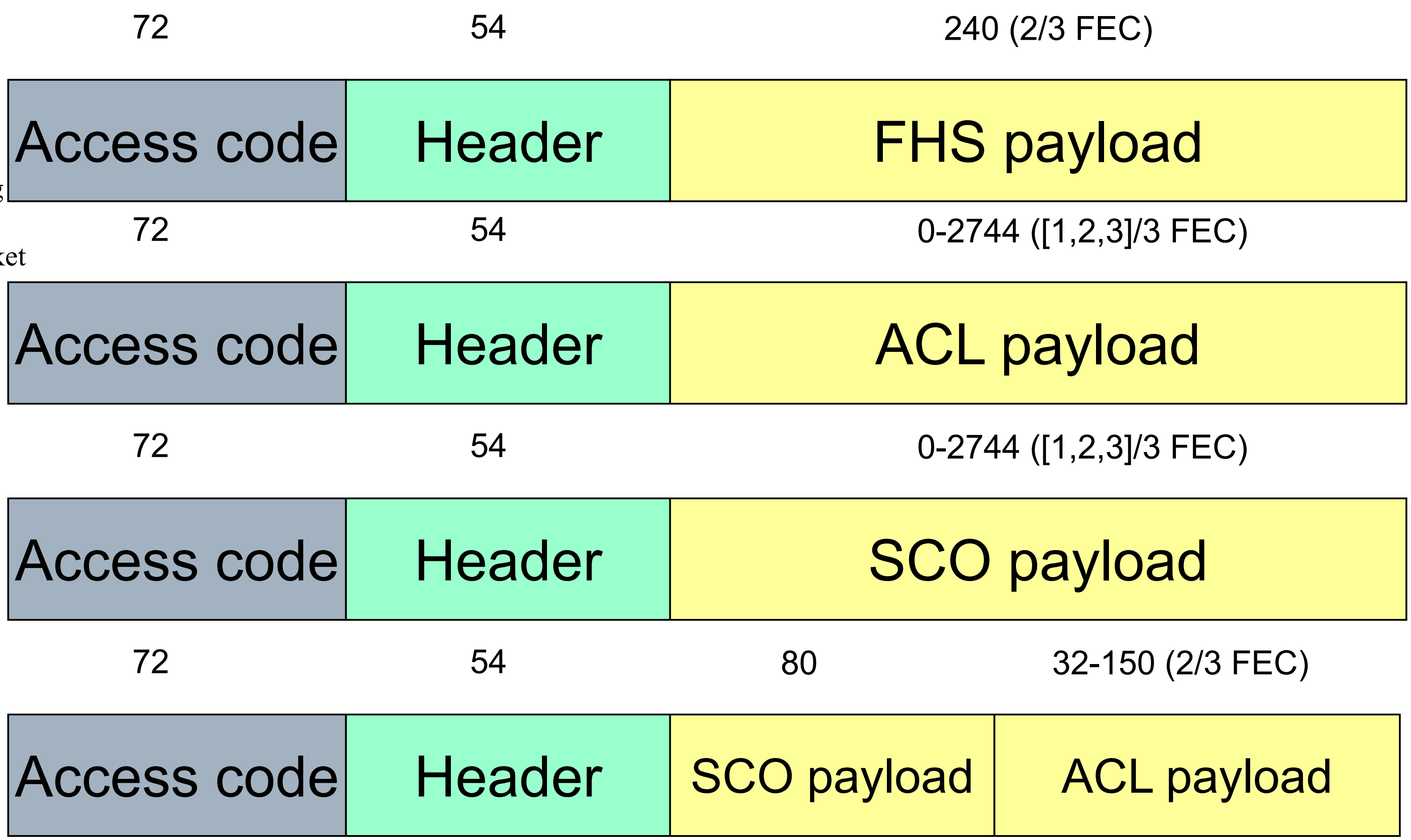
- Access code:
  - There are *three types* of access codes:
  - Channel Access Code (CAC): used to identify the piconet. It defines a piconet and is used in all transmissions; it is based on the *master* MAC address
  - Device Access Code (DAC): used for paging a device before network formation; it is derived directly from the device MAC address
  - Inquiry Access Code (IAC): used to search for all BT devices in range (inquiry)

Packet Format: Header

3	4	1	1	1	8	
AMA	Type	Flow	ARQ	SQN	HEC	X 3 FEC code rate 1/3

- Header:
  - Active Member Address (AMA)
  - Type: Packet type (there are 16 different types of packets)
  - Flow: Flow control
  - ARQ: Retransmission
  - SQN: Sequence number
  - HEC: checksum

Packet Format



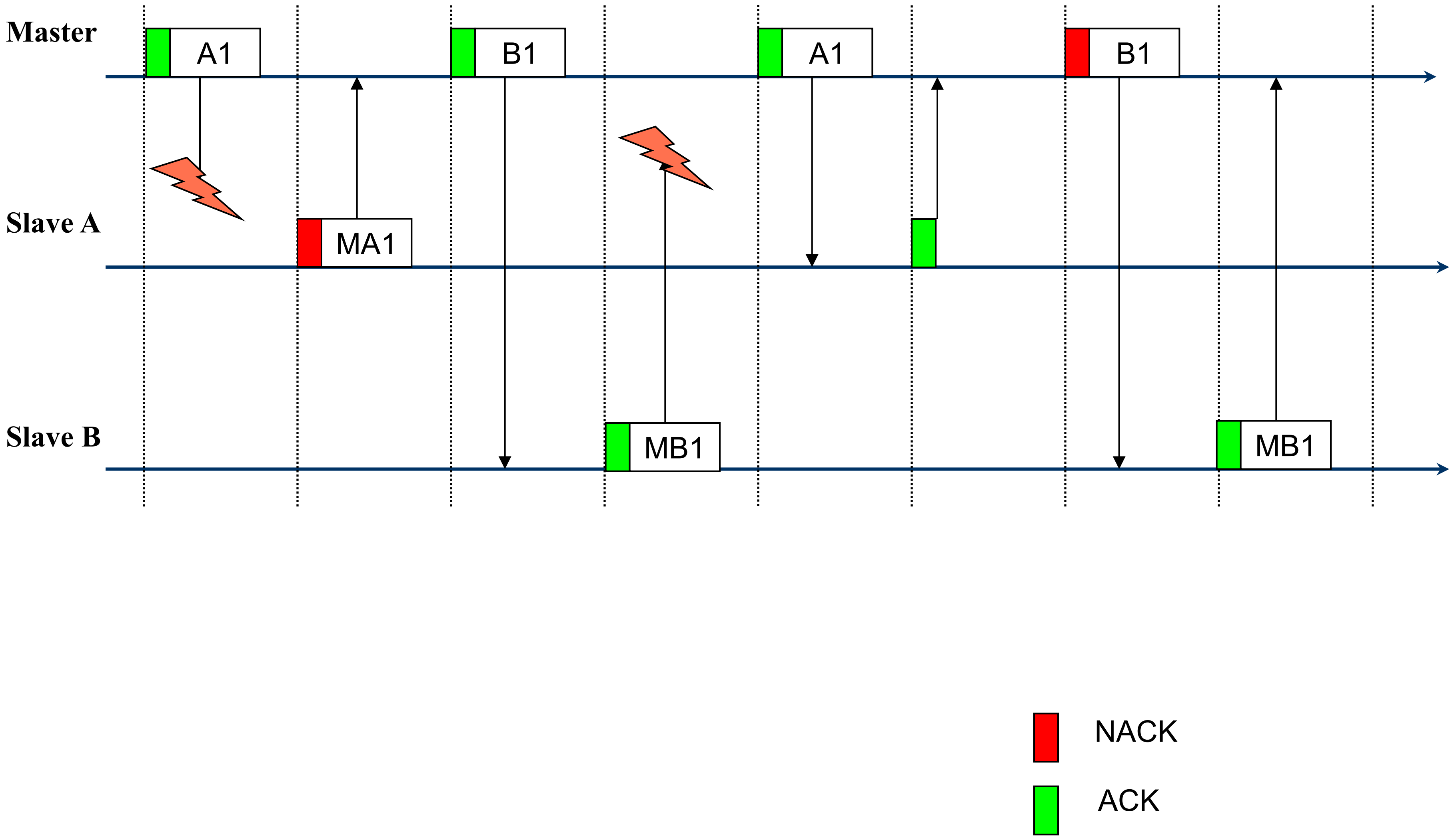
FHS
Frequency Hopping Synchronization, a special control packet

ACL
Asynchronous ConnectionLess

SCO
Synchronous Connection Oriented

DV
Data Voice.
A SCO data packet type for data and voice

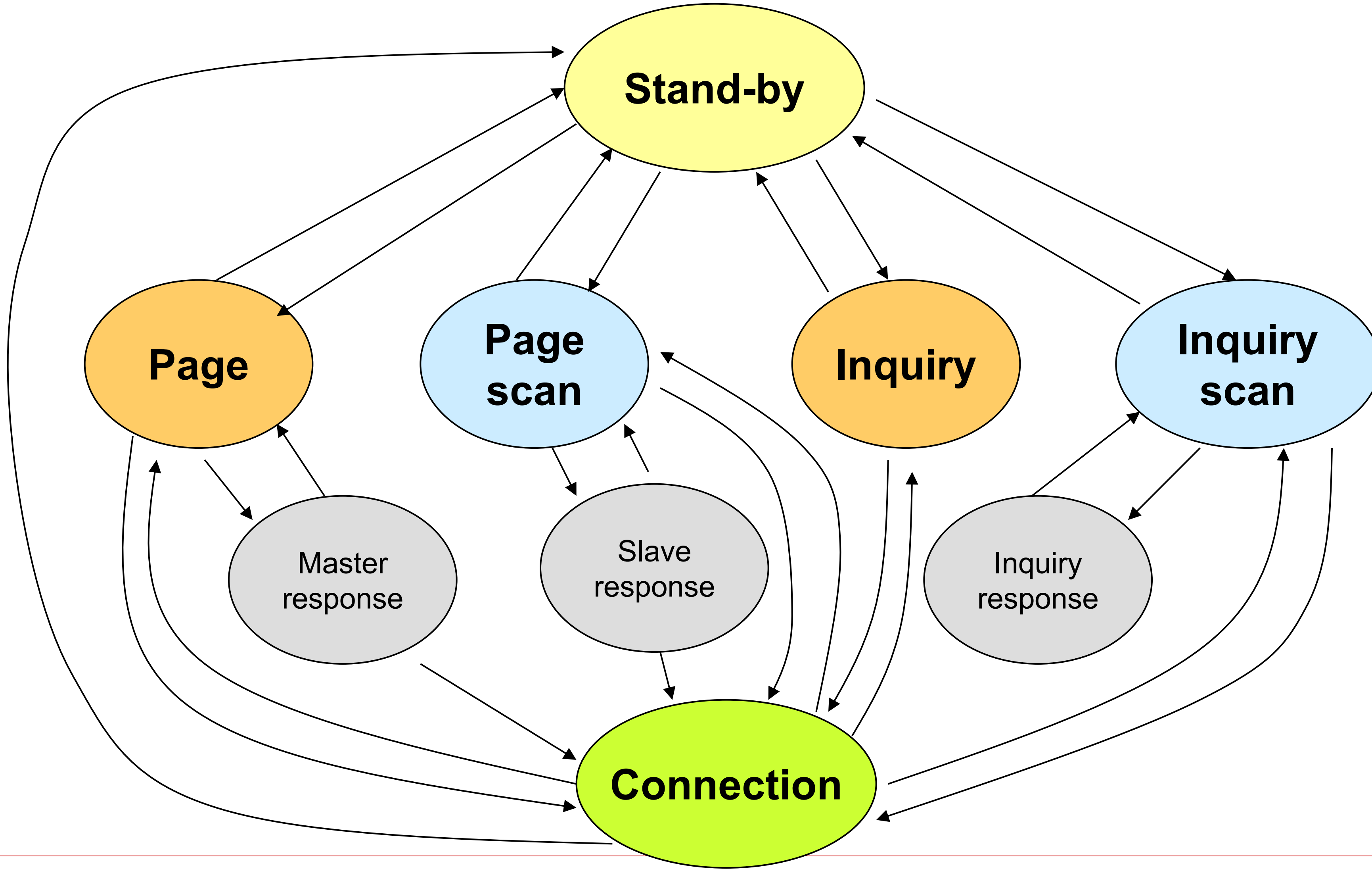
Link controller: ARQ



Link controller: states

- **Stand-by**: device is disconnetted and the radio is off
- **Connection**: device is connected with other devices
- **Inquiry**: device is searching for other devices in range
- **Inquiry Scan**: device is idle, but it listens to possible inquiry messages for short intervals of time (low duty cycle)
- **Page**: device is trying to connect to a specific device
- **Page Scan**: Similar to inquiry scan but for page messages

Link controller: states



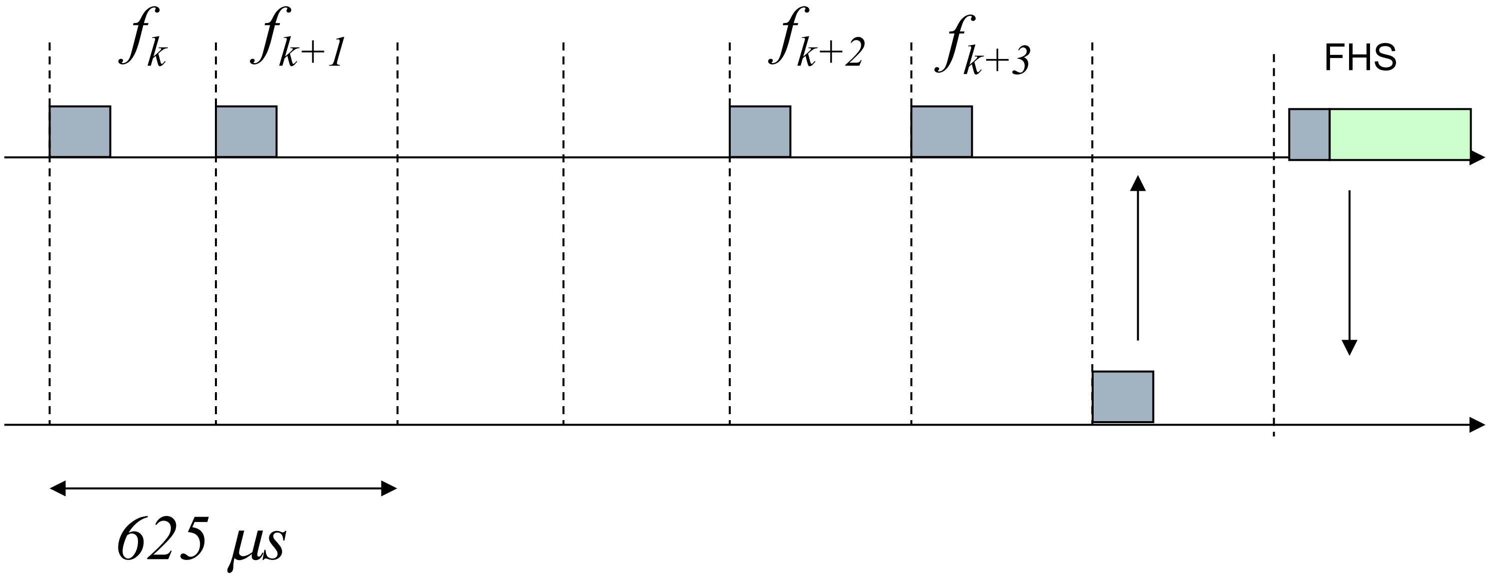
Page procedure

- If a device wants to connect to another device, it needs to know its address and then start the *page* procedure
- From the address, the Device Access Code (DAC) can be derived
- A stand-by device enters periodically in the page scan state and listens to receive its DAC
- Due to ISM band rules, page procedure cannot be performed on a fixed channel
- The device in page scan follows a pseudo random sequence tuning on 32 channels

Page procedure

- In order to limit the *energy consumption*, the device performs the page scan for **10 ms** on a channel and then goes to sleep for a **few seconds** (from 1.28 to 3.85 s)
- At every scan, a different channel is used according to the scanning pseudo-random sequence
- The paging device can calculate the sequence, but usually it doesn’t know the clock (phase)
- So it transmits the DAC on all possible frequencies sequentially

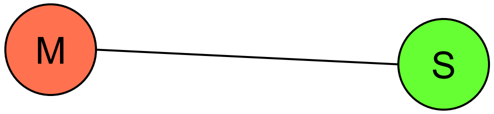
Page procedure



- In 10 ms, the paging device can transmit the DAC on 16 out of 32 channels
- The transmission sequence is repeated until a reply is received
- If after a sleep time no reply is received, the other 16 channels are considered

Page procedure

- The reply message is actually the same DAC
- The connection is established in 2 sleep times in the worst case
- The paging device replies with a FHS packet including all information on the device, including address and clock
- Connection is established
- The paging device becomes the Master, and the scanning device becomes the Slave



Page procedure

- What about energy consumption?
- Why the paging device continues to transmit the DAC, spending a lot of energy, while the scanning device just listen to channels every once and a while?
- Would a more fair approach be preferable?

Inquiry procedure

- The inquiry procedure allows to discover all the other active devices in range
- It is similar to the page procedure, but the Inquiry Access Code (IAC) is adopted instead of the DAC
- Also the inquiry scan sequence is pseudo random
- The reply is a FHS packet
- Collisions may occur due to multiple devices in range
- After an inquiry, the devices switch to scan in order to setup the connection
- However, since it knows the clock of the device, the scan time can be minimized

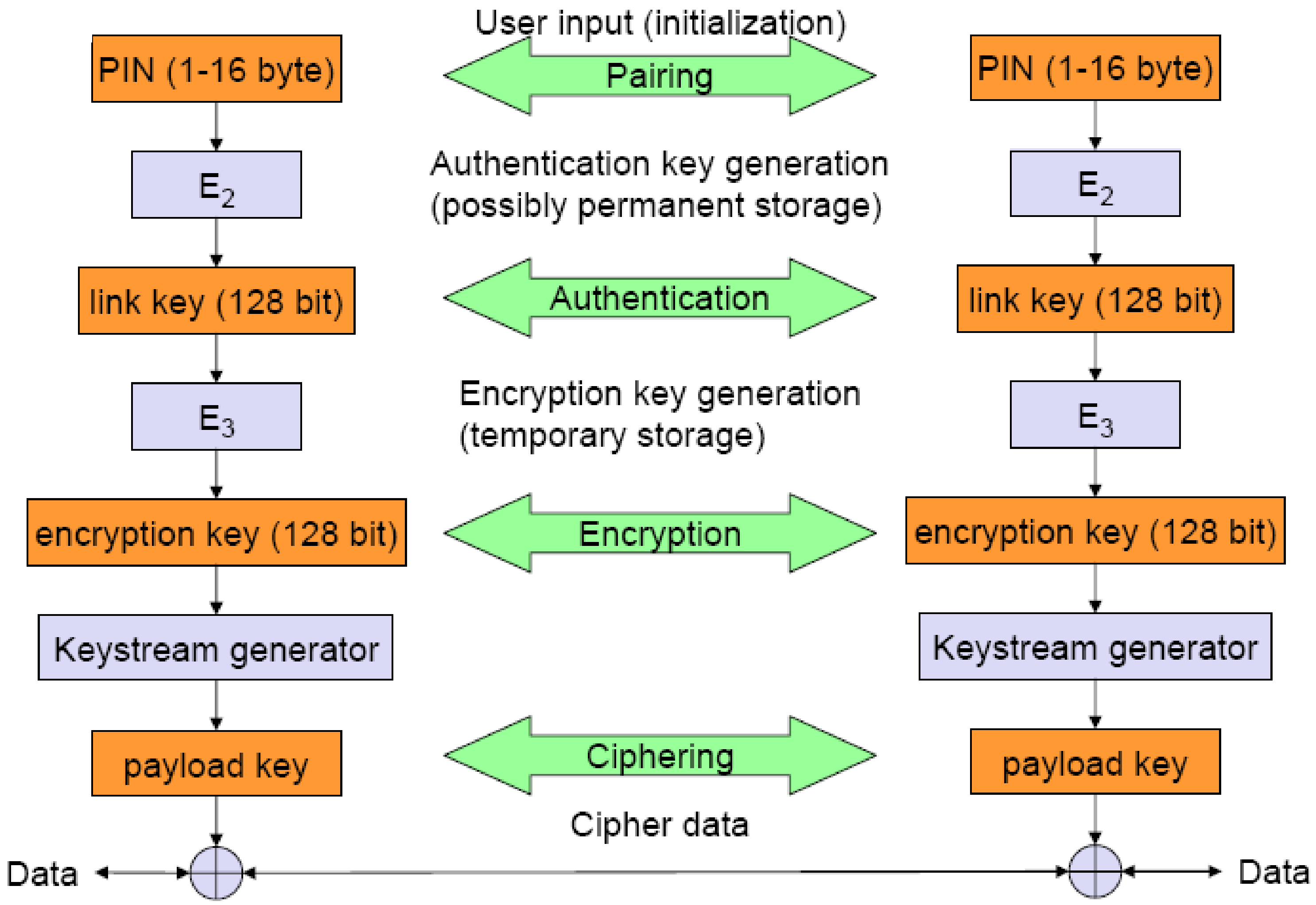
Low power modes

- When connected, the device can optionally enter *low power* modes
- **Hold**: slave stops listening to the channel for a time period agreed with the master (it keeps its AMA, Active Member Address)
- **Sniff**: slave alternates listening and sleep periods according to a cycle agreed with the master (also here it keeps its AMA)
- **Park**: in this state, the slave releases its AMA and gets a PMA (Parked Member Address) from the master. It listens to the channel with a low duty cycle for receiving *unpark* message from the master

Protocols: Link Management

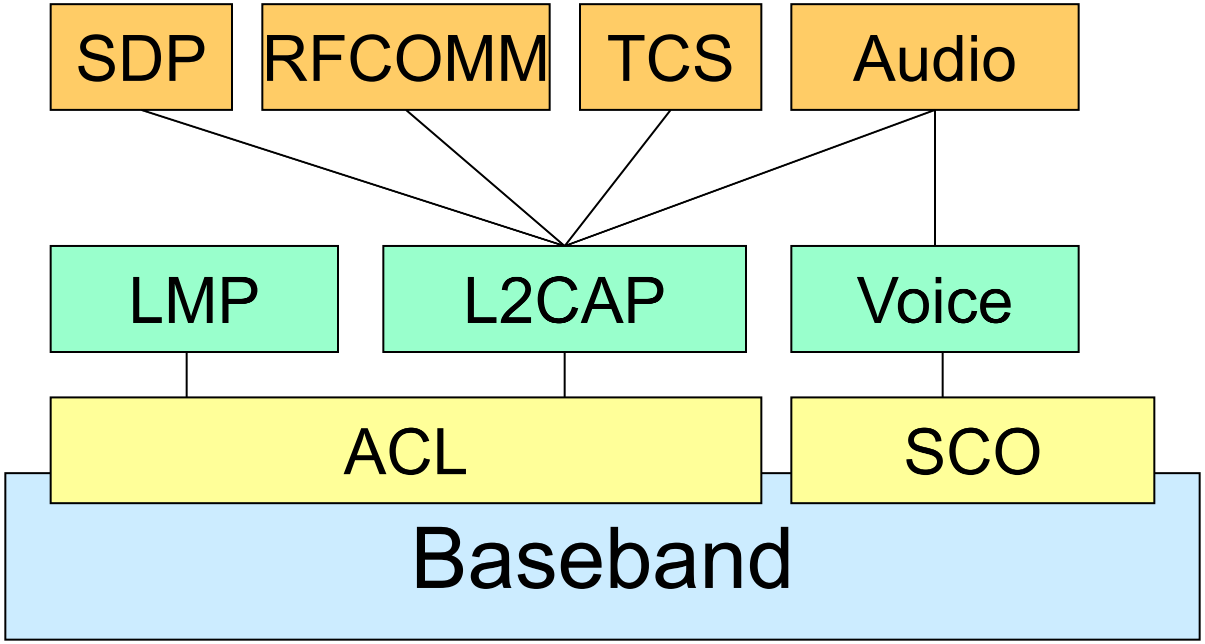
- The link management protocol is in charge of the connection setup, security and control procedures
- Setup of ACL and SCO links
- Management of security procedure
- Add and remove slaves from a piconet
- LMP messages have priority over all the others

Protocols: Security



Protocols: L2CAP

- Logical Link Control and Adaptation Protocol (L2CAP)
- Adaptation functions (segmentation and reassembly) and multiplexing

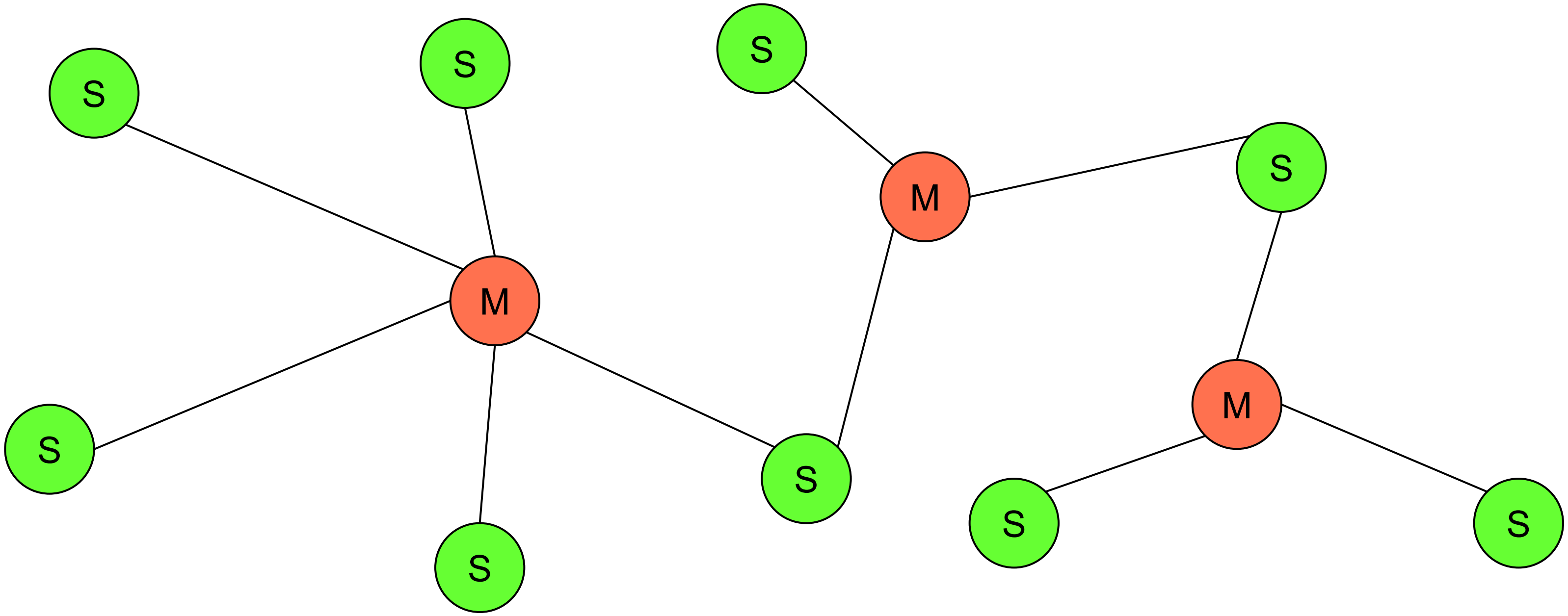


Profiles

- Profiles are sets of standard functions that allow interoperability of devices of different vendors through a standard implementation of specific applications

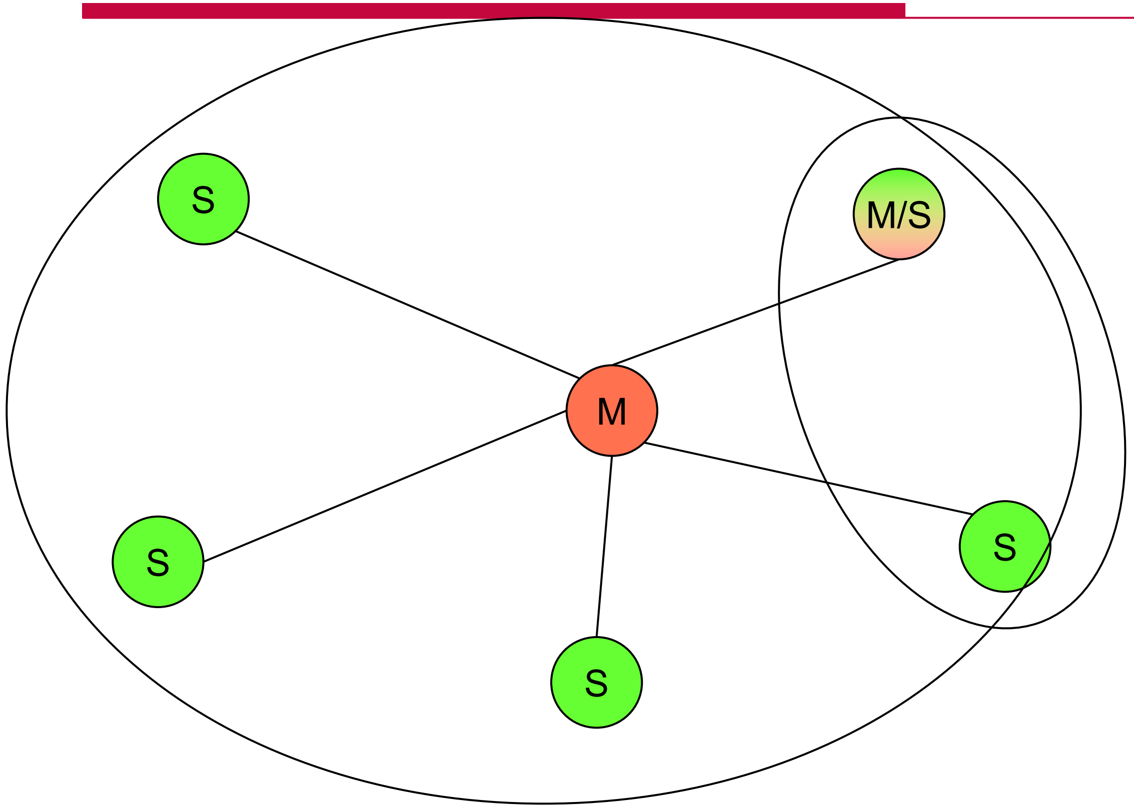
- Generic Access Profile
- Service Discovery Application Profile
- Cordless Telephony Profile
- Intercom Profile
- Serial Port Profile
- Headset Profile
- Dial-up Networking Profile
- Fax Profile
- LAN Access Profile
- Generic Object Exchange Profile
- Object Push Profile
- File Transfer Profile
- Synchronization Profile
- Advanced Audio Distribution
- PAN
- Audio Video Remote Control
- Basic Printing
- Basic Imaging
- Extended Service Discovery
- Generic Audio Video Distribution
- Hands Free
- Hardcopy Cable Replacement

Scatternet



- Devices can participate to different picones simultaneously
- A device can be Master only in one piconet (Why?)
- Devices can switch from one piconet to another using the *hold* and *sniff* modes
- Scatternet formation and routing are out of standard specifications

Scatternet (2)



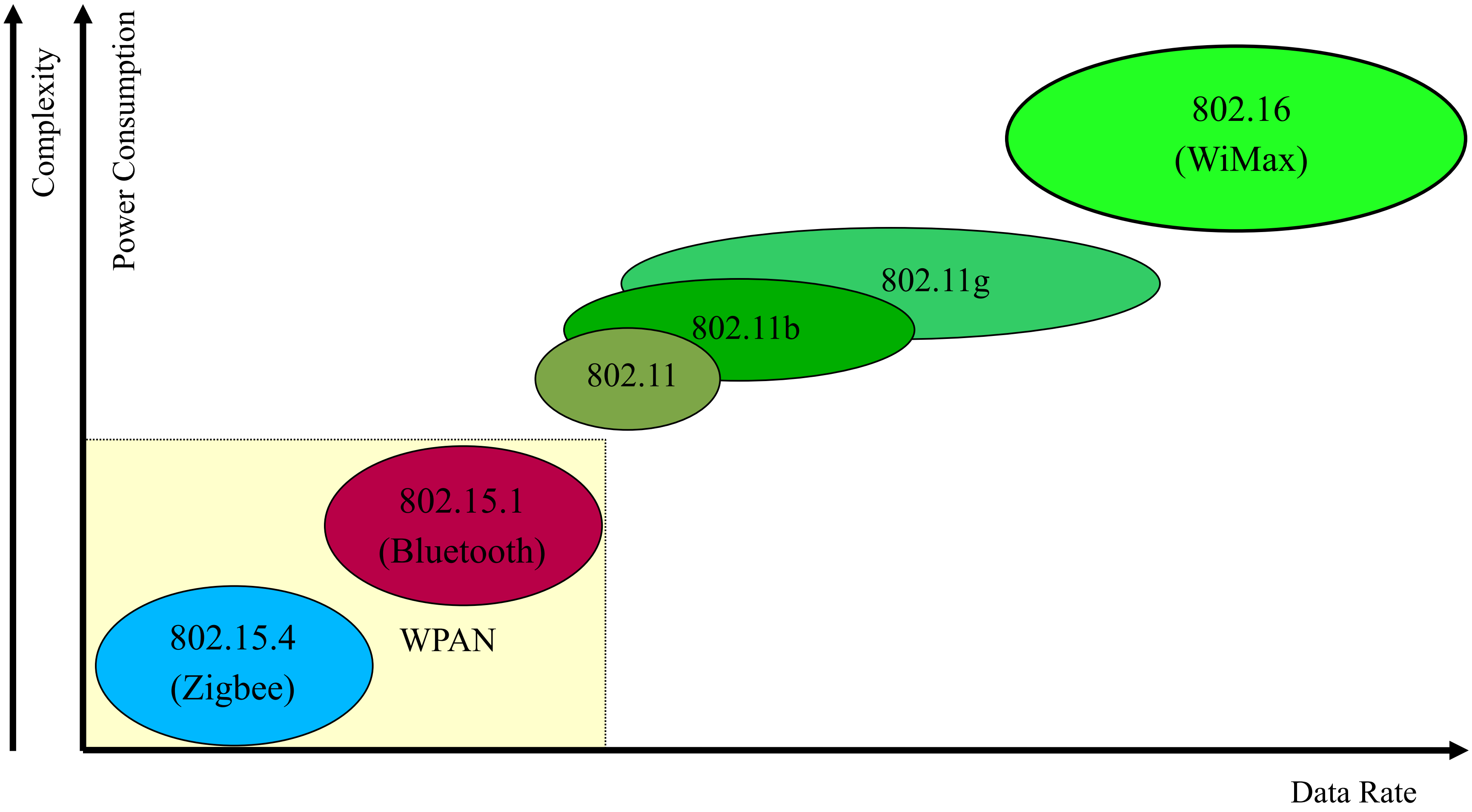
- Scatternet allows, when necessary, to create direct links

Zigbee

Low Rate - WPAN

- Most applications in Wireless Networking require high transmission rates
- Starting in the 90's, a lot of efforts have been devoted to these application and to high rate wireless technologies: WLAN (IEEE 802.11), BlueTooth (IEEE 802.15), WiMax (IEEE 802.16)
- However, there are also several applications that require short range, low energy consumption and low rate
- Low Rate WPAN (LR-WPAN) have been considered for this specific application segment

Low Rate - WPAN



Characteristics

- Low cost of the hardware (< 1$) and the software
- Low transmission range (~10-30m)
- Low latency, if necessary
- And, above all, low energy consumption!

Applications

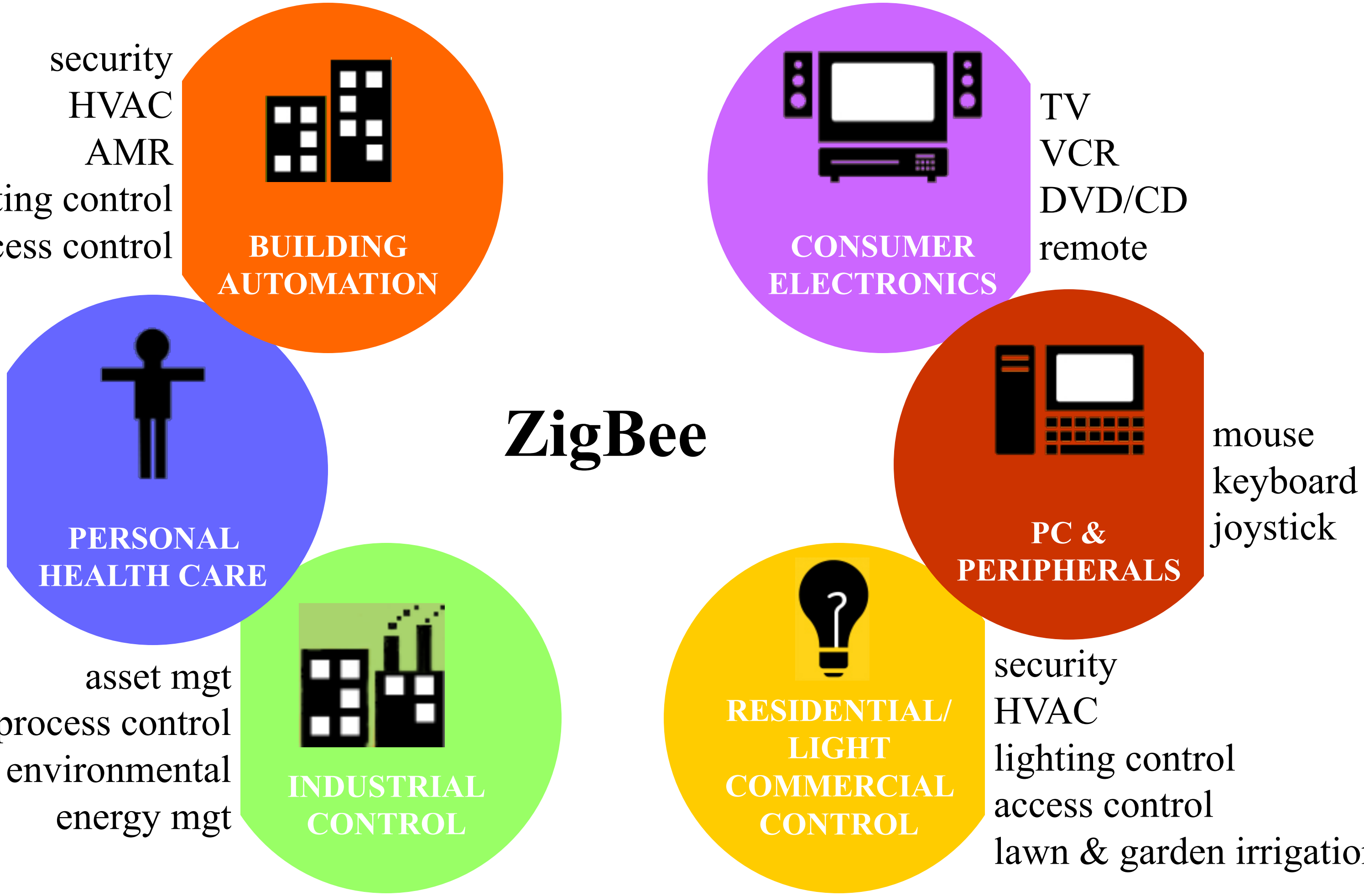
security
HVAC
AMR
lighting control
access control

TV
VCR
DVD/CD
remote

patient monitoring

fitness monitoring

mouse
keyboard
joystick



asset mgt
process control
environmental
energy mgt

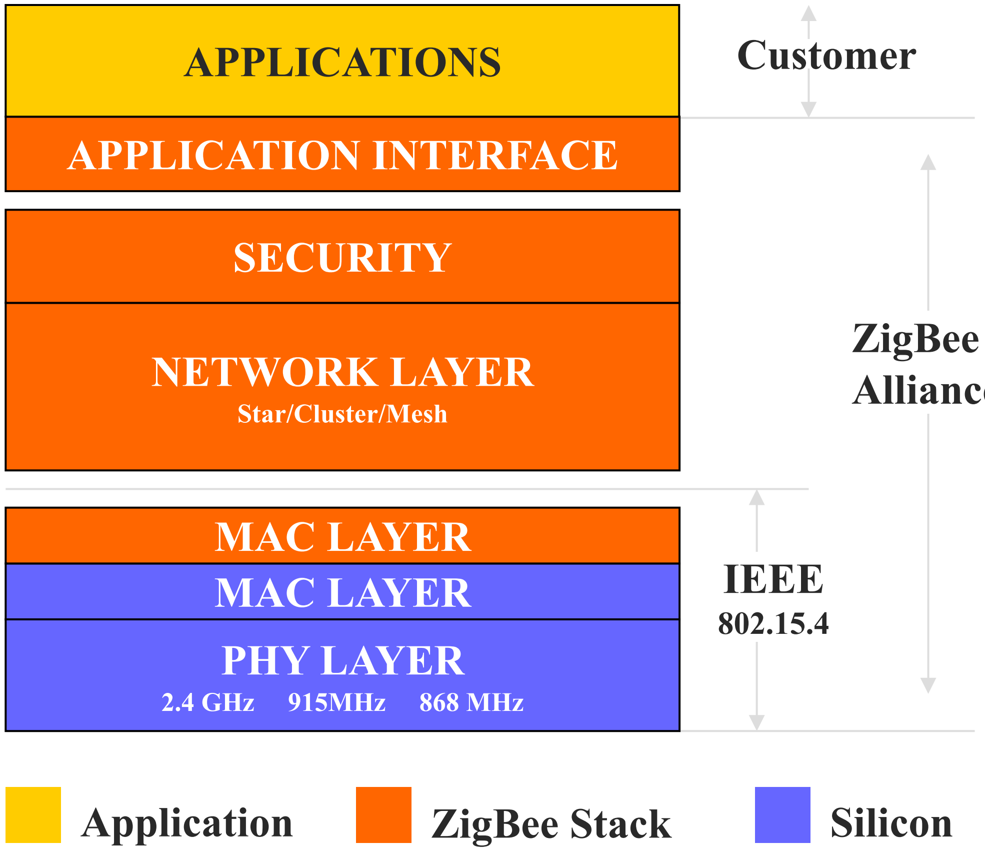
security
HVAC
lighting control
access control
lawn & garden irrigation

Toward Zigbee …

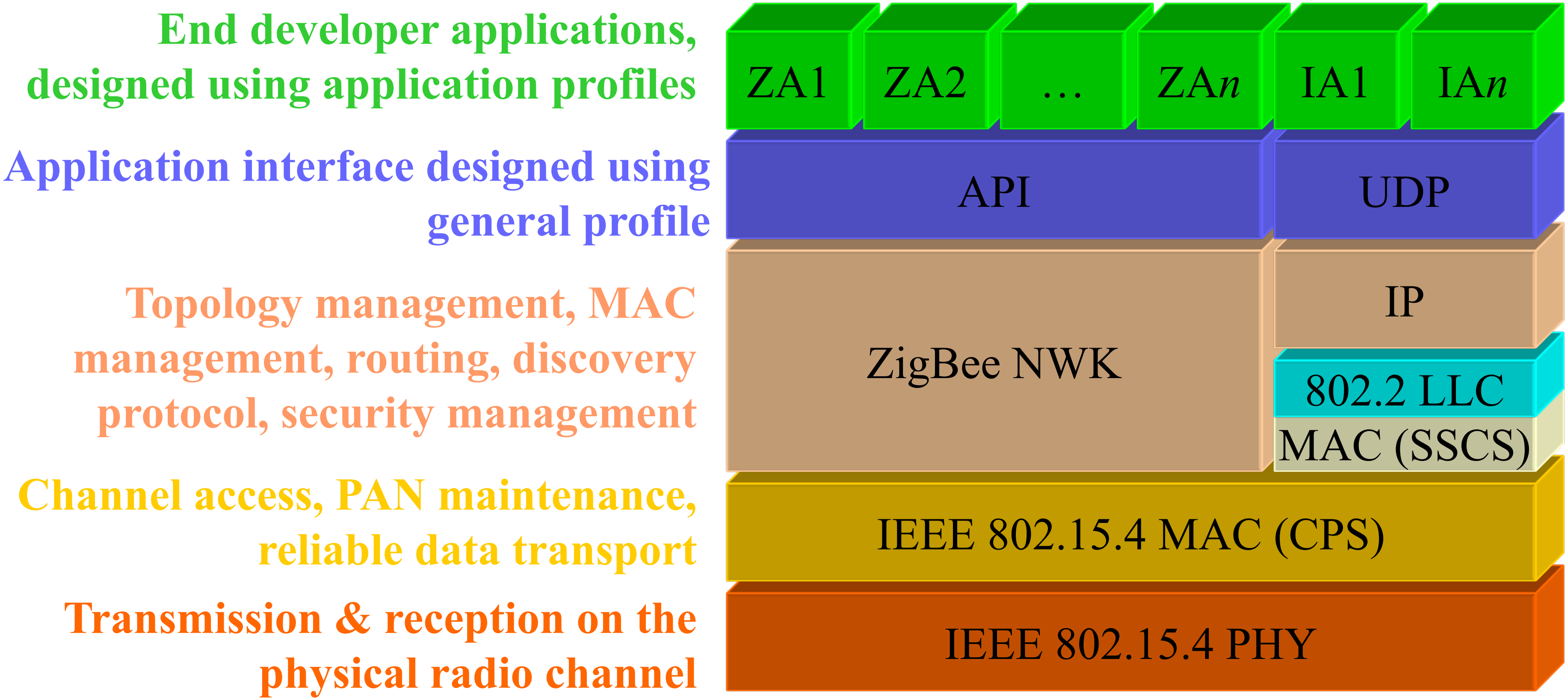
- Starting in mid 90s, several manufacturers designed proprietary solutions for *sensor networks* …
- … with obvious compatibility and high cost problems
- A standardization activity was necessary: the Working Group 4 is created within the IEEE 802.15 project (2001)
- IEEE 802.15.4 standard, considering physical and MAC layers, is published in May 2003
- The technology takes the commercial name of

ZigBee™

Zigbee: protocol stack



Zigbee: protocol stack



Zigbee: channels and rates

	BAND	COVERAGE	DATA RATE	# OF CHANNEL(S)
2.4 GHz	ISM	Worldwide	250 kbps	16
868 MHz		Europe	20 kbps	1
915 MHz	ISM	Americas	40 kbps	10

ZigBee vs. Bluetooth

ZigBee

- DSSS- 11 chips/ symbol
- 62.5 K symbols/s
- 4 Bits/ symbol
- Peak Information Rate ~128 Kbit/second

Bluetooth

- FHSS
- 1 M Symbol / second
- Peak Information Rate ~720 Kbit / second

ZigBee vs. Bluetooth

ZigBee:

- Network join time = 30ms typically
- Sleeping slave changing to active = 15ms typically
- Active slave channel access time = 15ms typically

Bluetooth:

- Network join time = >3s
- Sleeping slave changing to active = 3s typically
- Active slave channel access time = 2ms typically

ZigBee vs. Bluetooth

	Bluetooth	ZigBee
AIR INTERFACE	FHSS	DSSS
PROTOCOL STACK	250 kb	28 kb
BATTERY	rechargeable	non-rechargeable
DEVICES/NETWORK	8	255
LINK RATE	1 Mbps	250 kbps
RANGE	~10 meters (w/o pa)	~30 meters

Zigbee: devices

Standard defines tow device types:

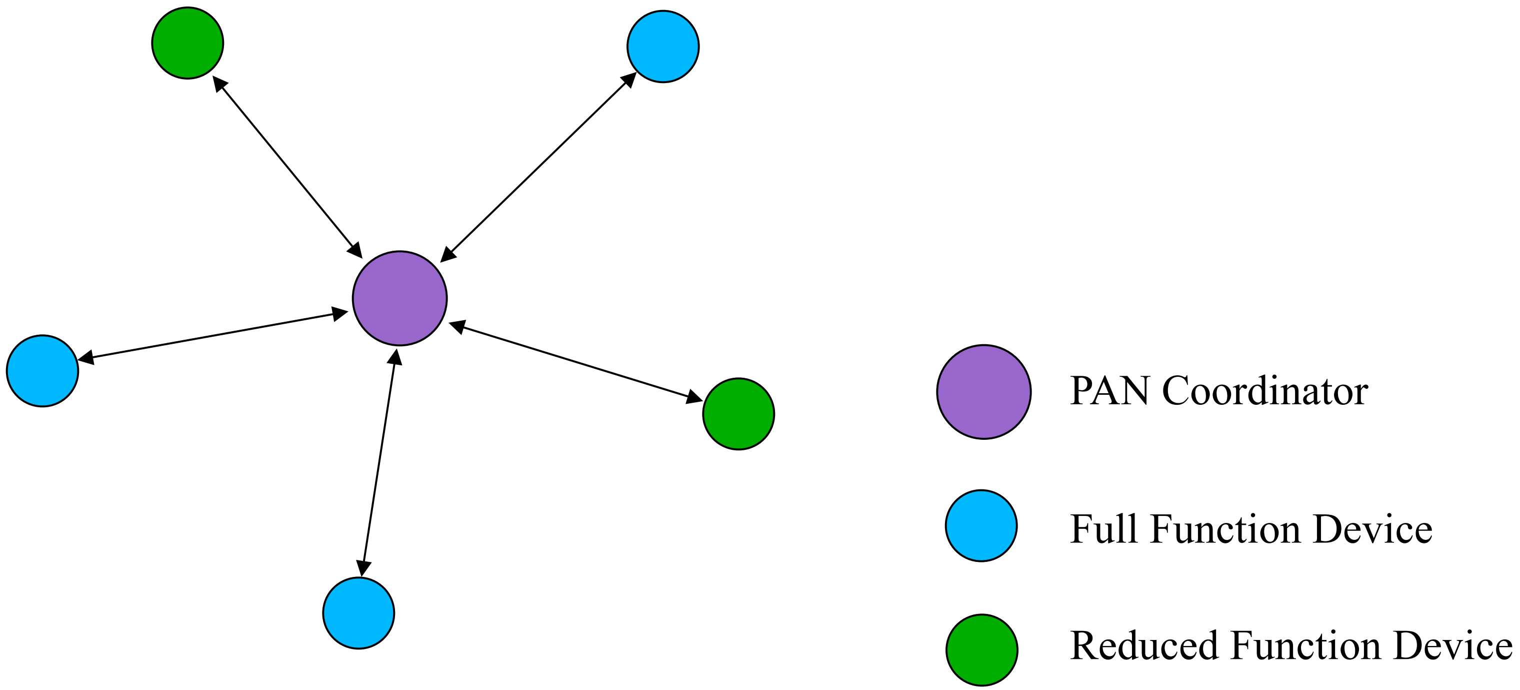
- **Full Function Device (FFD):**
  - Can transmit beacon frames
  - Can directly communicate with other FFD
  - Can make routing
  - Can act as PAN coordinator

- **Reduced Function Device (RFD):**
  - Cannot route traffic
  - Cannot communicate directly with other RFD
  - Can only communicate directly with one FFD

Zigbee: topologies

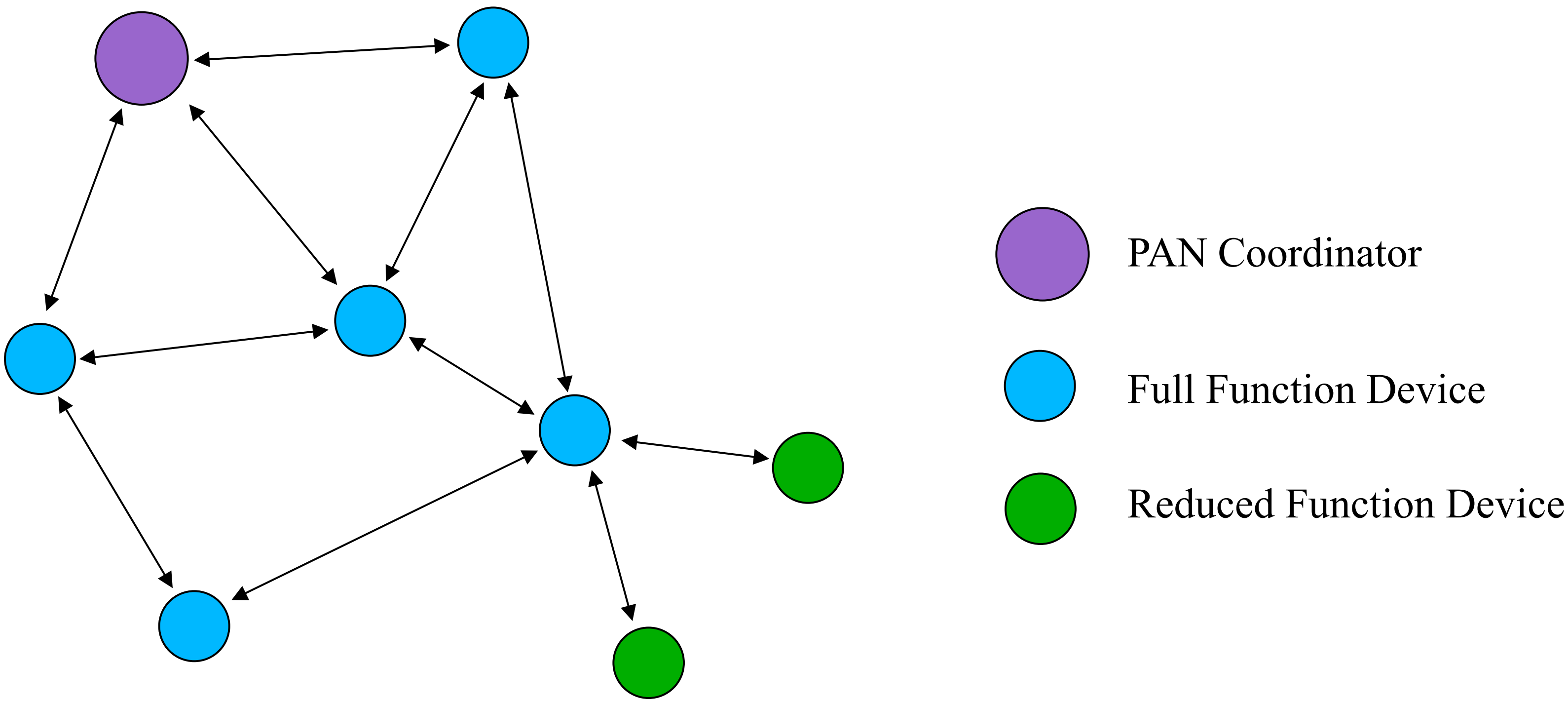
Three topologies are defined:

1 - STAR TOPOLOGY



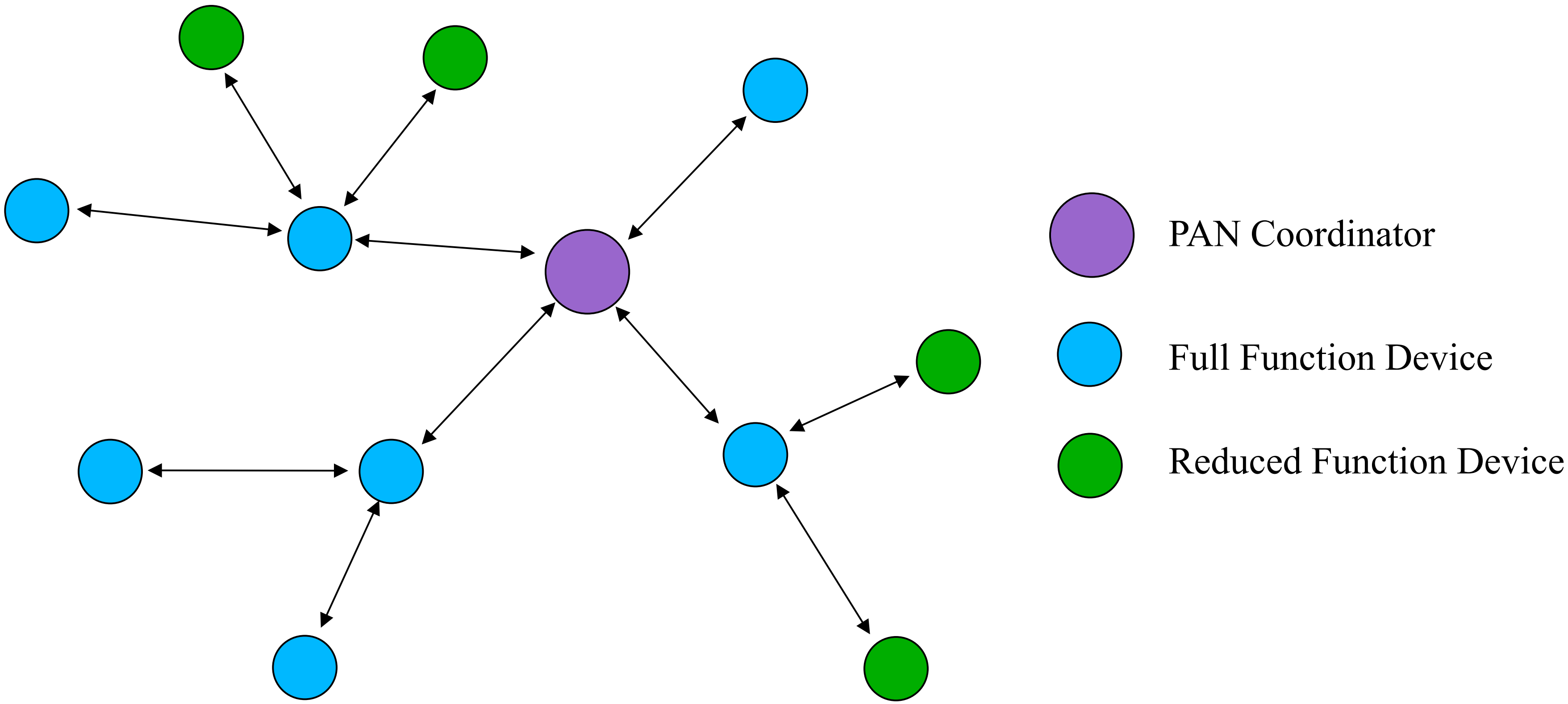
Zigbee: topologies

2 - MESH TOPOLOGY



Zigbee: topologies

3 - CLUSTER TREE



Physical layer

Direct Sequence Spread Spectrum (DSSS)

Frequency	Zone	Modulation	Bit-Rate	Channels
868 Mhz	Europa	BPSK	20 kbit/s	1
915 Mhz	USA	BPSK	40 kbit/s	10
2.45 Ghz	Everywhere	O-QPSK	250 kbit/s	16

Physical layer

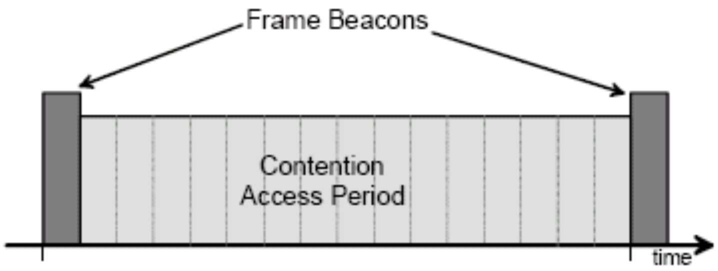
- Receiver Energy Detection (Free channels search)
- Scanning (Search for Beacon frames)
- Channel selection
- Clear Channel Assessment (channel busy/available)
- Link Quality Detection (LQI: estimation of channel quality)
- Quality feedbacks to upper layers

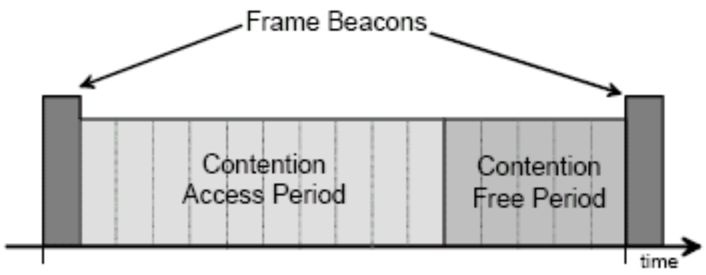
Physical layer

4 Byte	1 Byte	1 Byte		Variabile
PREAMBLE	START of FRAME DELIMITER (SFD)	FRAME LENGHT (7bit)	Reserved (1 bit)	PSDU
Synchronization Header (SHR)		Protocol Header (PHR)		Payload

MAC layer: overview

- Two operation modes are defined:
  - **Beacon Enabled** (slotted CSMA/CA)

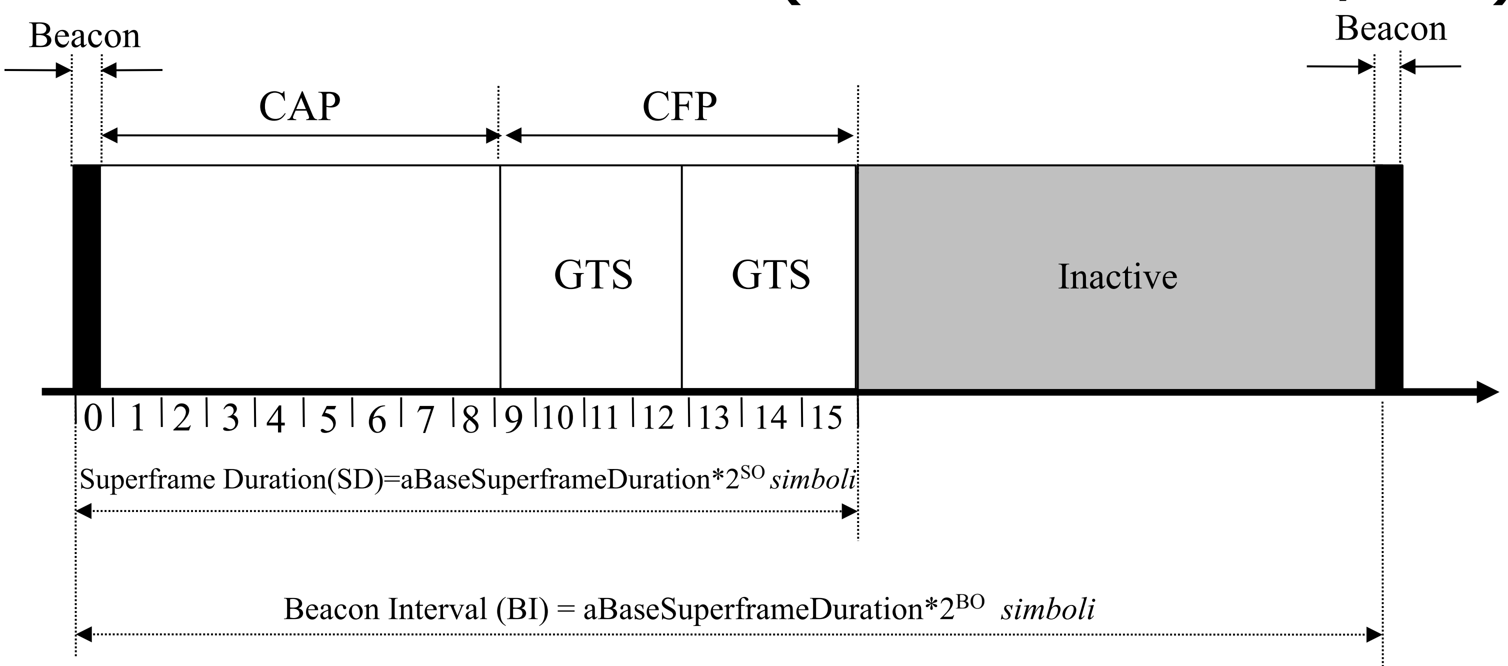




  - **Non Beacon Enabled** (unslotted CSMA/CA)

MAC layer: overview

- **Beacon Enabled** (slotted CSMA/CA)



- Guaranteed Time Slots assigned in the beacon frame
- The PAN coordinator may allocate up to seven of these GTSs and a GTS may occupy more than one slot period
- Frame duration: from 15ms to 252sec (15.38ms*2n where $0 \leq n \leq 14$)

Slotted CSMA/CA

- The time unit adopted is the backoff period (BP), usually equal to 20 symbols
- Three variables are adopted:
  - NB, number of access attempts for a packet
  - CW, number of free BPs to wait at the end of the backoff period before starting a transmission
  - BE, exponent that defines the maximum number of BPs required before starting the CCA (Clear Channel Assessment) procedure
- Data transmission (and optionally the ack) must end within the CAP
- In case this is not possible, MAC has to suspend the random backoff and wait for the beginning of next CAP
- If the macBattLifeExt bit is set to 1, countdown of the backoff can be executed onliy during the first 6 BPs following the beacon

Unslotted CSMA/CA

- Classical access scheme CSMA/CA (data - ACK) without synchronization

MAC layer: functionalities

- Beacon Management (Synchronization)
- Channel access management
- Guaranteed Time Slot (GTS) Management
- Association and disassociation
- Frame Acknowledgement

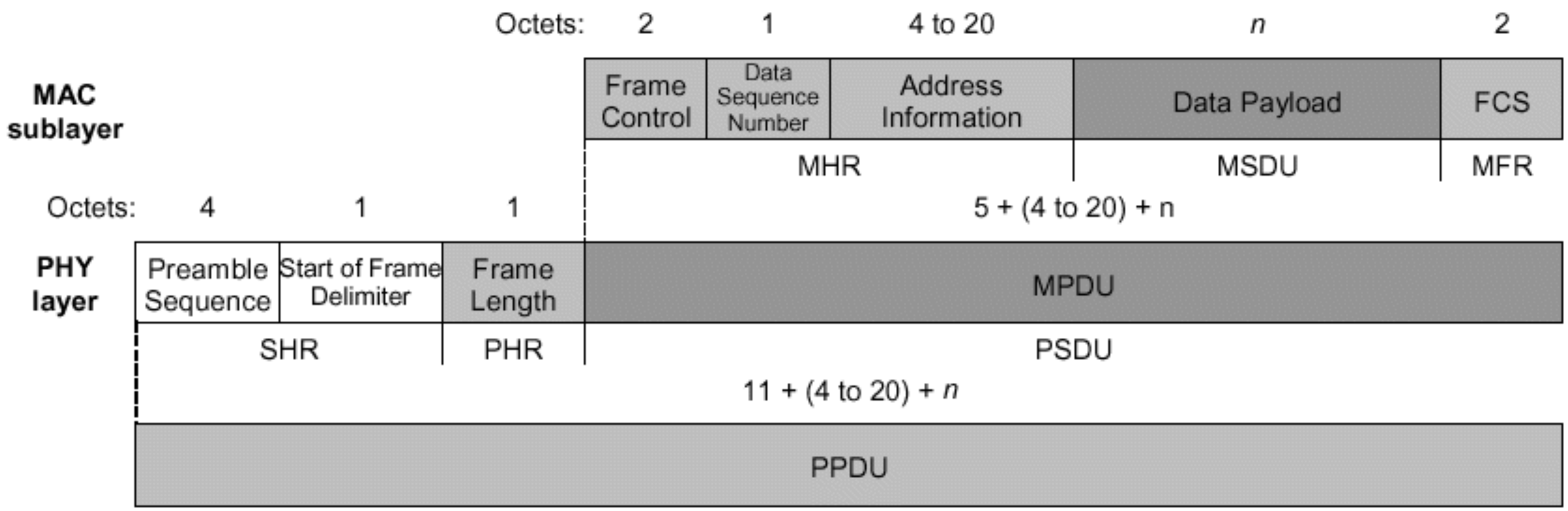
MAC layer: frame format

2 Byte	1 Byte	0/2	0/2/8	0/2	0/2/8	variable	2 Byte
FRAME CONTROL	SEQUENCE NUMBER	Destination PAN Identifier	Destination Address	Source PAN Identifier	Source Address	FRAME PAYLOAD	FCS
		Address fields					
MAC Header						MAC Payload	Codice CRC

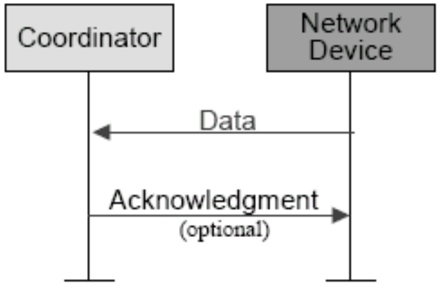
FRAME CONTROL → Identify frame type address type, security, etc.

Address fields → Address can be *long* (48 bit, IEEE) or *short* (16 bit, assigned by PAN coordinator)

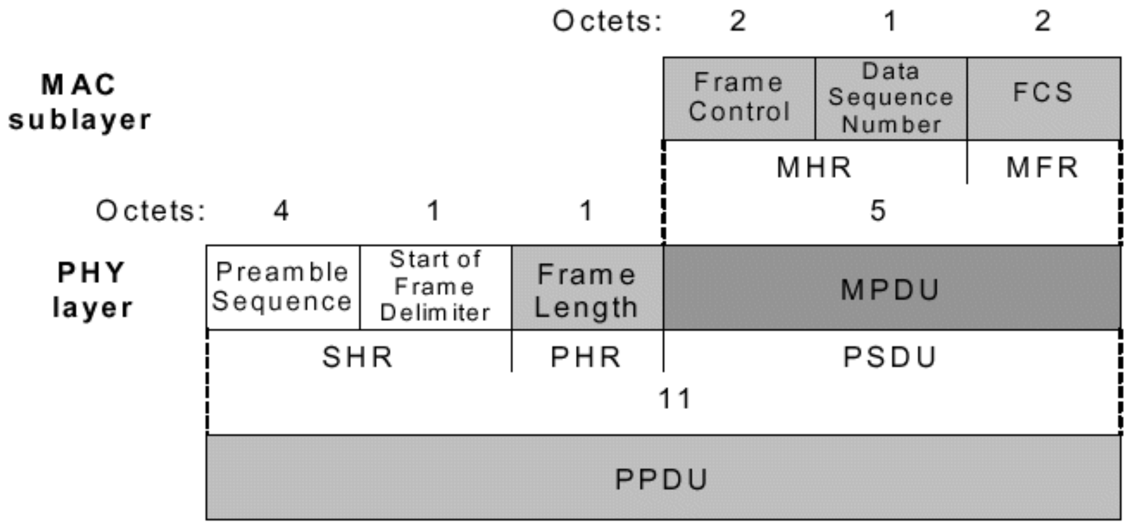
Data Frame



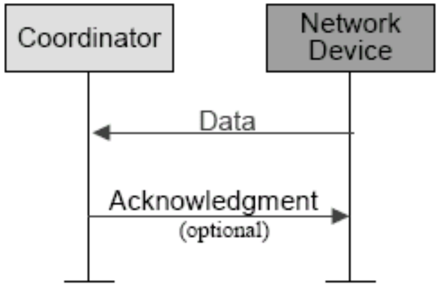
- Up to 104 bytes payload



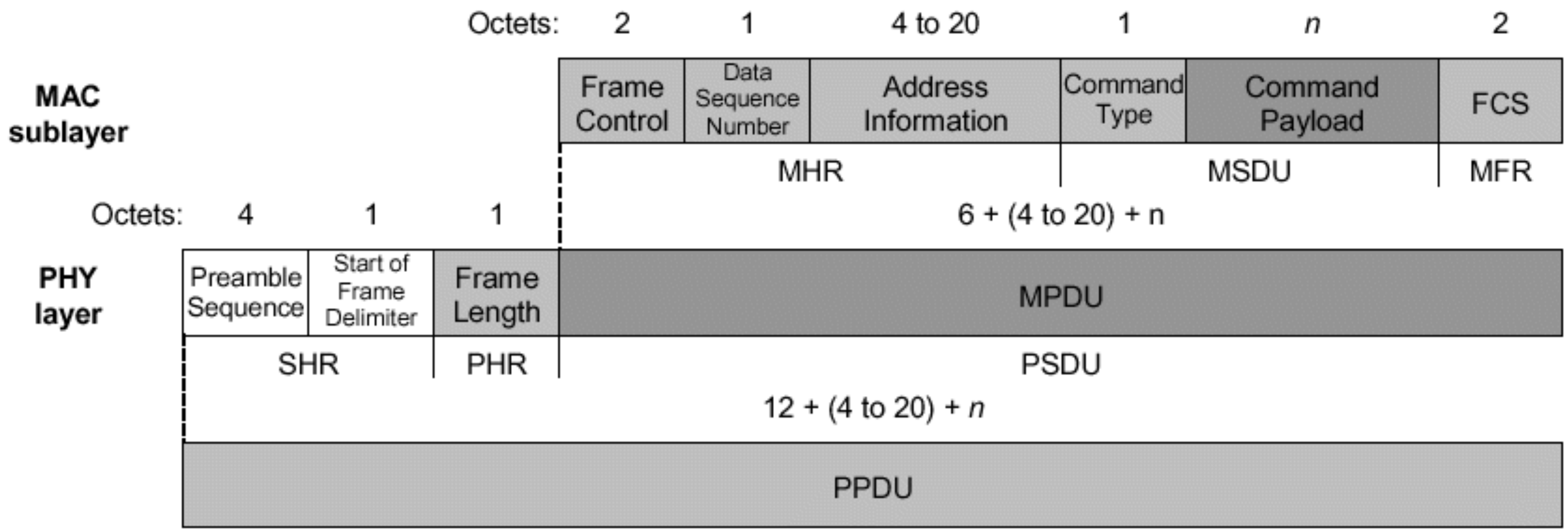
Ack Frame



- Transmitted right after data frame

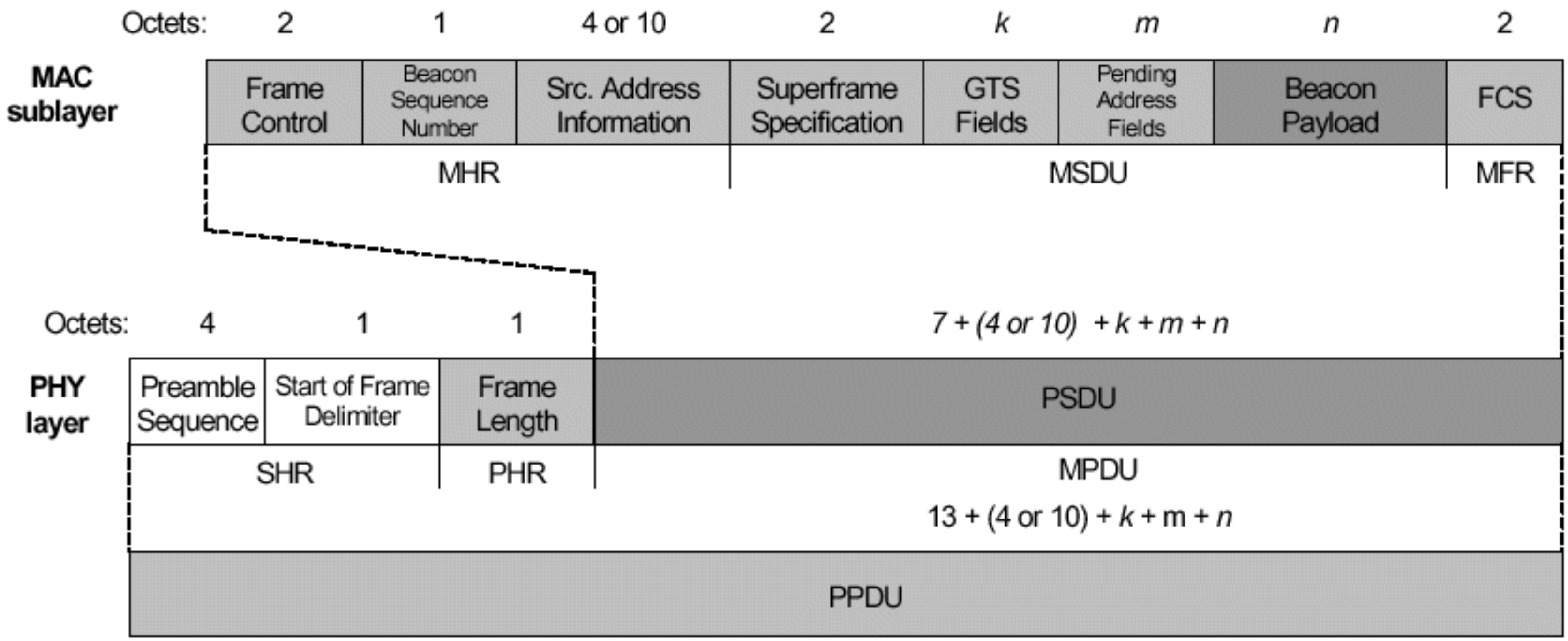


Command Frame



- It allows the remote configuration and control of client devices
- It basically allows the implementation of a centralized network management and control for large size networks

Beacon Frame format



- Frame synchronization and GTS assignment

Network formation

- An FFD device searches for a free channel and select a PANid *(Channel Scanning)*. Then it starts transmitting Beacon frames
- A device that wants to associate to a network, scans the channel and listens to Beacon frames
- Once scan is completed, a network is selected setting the access parameters according to the information in the beacon frame
- Association is performed issuing an Associate Request Command to PAN Coordinator
- PAN Coordinator replies with a Association Response Command

Network layer: frame format

Short MAC address

2 Byte	2 Byte	2 Byte	1 Byte	1 Byte	Variabile
FRAME CONTROL	Destination Address	Source Address	Broadcast Radius	Broadcast Sequence Number	FRAME PAYLOAD
	Campi di Routing				
NWK Header					NWK Payload

Frame type, version, route discovery, etc.

Maximum number of hops that a message can cross (like TTL in IP)

Zigbee Routing: overview

- Defined by Zigbee Specification, published by the Zigbee Alliance (7/2005)
- Three types of devices:
  - *ZB Coordinator (FFD)*
  - *ZB Router (FFD)*
  - *ZB End-Device (RFD o FFD)*
- Routing is “zigbee oriented” and considers the two types of physical device (FFD RFD)
- Routing used two algorithms:
  - *Ad-hoc On-demand Distance Vector (AODV)*
  - *Cluster Tree Algorithm*

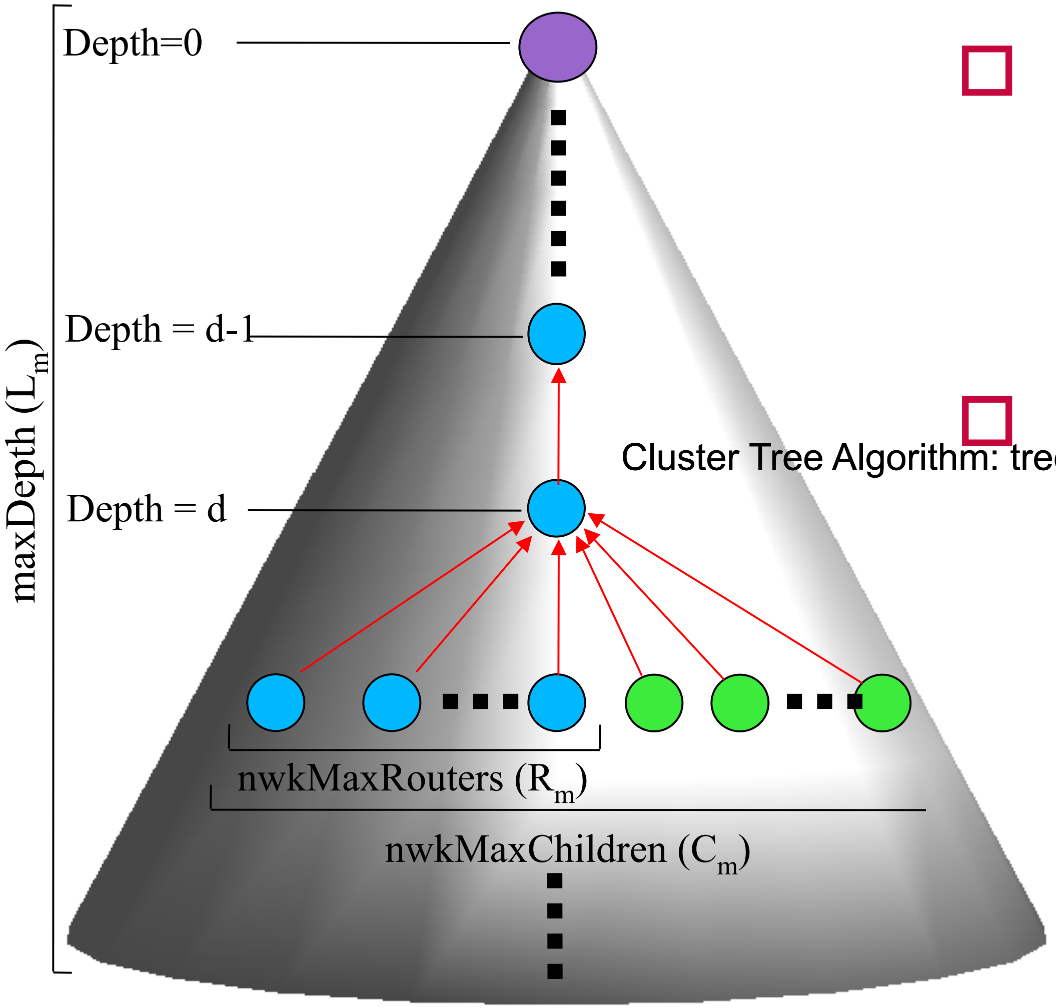
Ad-hoc On-demand Distance Vector

- Simple on-demand routing protocol
- See part on ad hoc networks (…)

Cluster Tree Algorithm: tree creation

- Procedure is started from a FFD that acts as network coordinator
- Network coordinator selects one of the available channels (MAC function)
- It selects a PAN*identifier* to the network and assign to itself the *Network Address* “0” (Coordinator)
- The other devices can now join the network associating with the *Network Coordinator*. They can act as *ZB Router* (FFD) or *ZB End-Device*
- Once connected, *ZB Routers* can then allow other devices to join the network
- Address assignment is completely distributed and hierarchical

Cluster Tree Algorithm: tree creation



Cluster Tree Algorithm: tree creation

- Hierarchical addressing simplifies routing in the tree
- Routes along the tree or along paths created with AODV can be used based on needs

Part C
Ad Hoc Networks

Acknowlegments

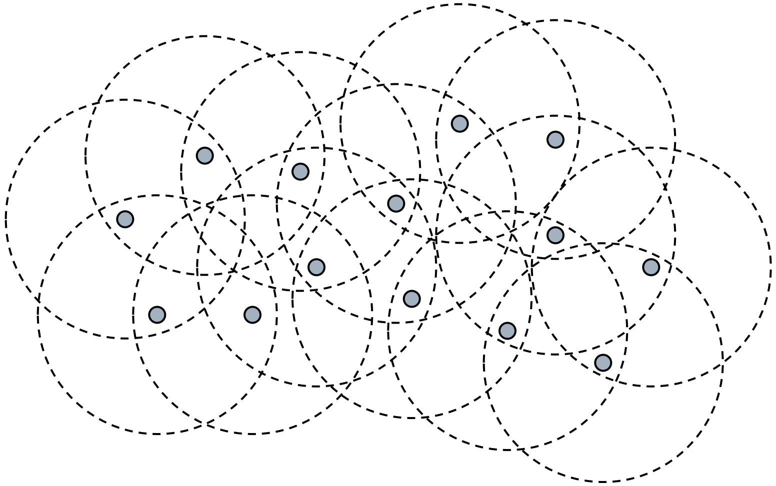
- This class notes are mostly based on the teaching material of:
  - Prof. Eylem Ekici (Ohio State University at Columbus)
  - Prof. Nitin H. Vaidya (University of Illinois at Urbana-Champaign)

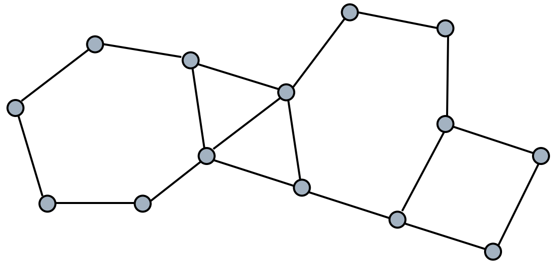
Introduction

- Mobile Ad Hoc Networks (MANET):
  - Networks of potentially mobile network nodes
  - Nodes equipped with wireless communication interfaces
  - No pre-established infrastructure
  - Communication between peers involve multiple hops
- Implications
  - Nodes act both as hosts as well as routers
  - Dynamic network topology

Ad Hoc Network Abstractions

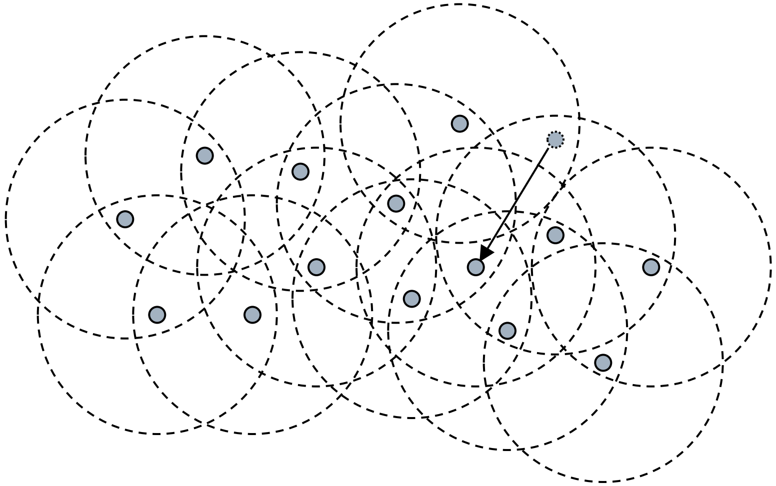
- Every node can communicate directly with a subset of mobile nodes (*neighbors*)
  - Communication "range" of a node varies depending on physical changes
  - Communication range abstracted as circles





Mobile Ad Hoc Networks

- Mobility causes topology changes
  - Topology changes lead to changes in data delivery decisions
  - Introduces real-time adaptation requirements



Example Applications

- Disaster recovery, emergency, security applications
  - Law enforcement
  - Natural and man-made disaster recovery
- Civilian applications
  - Conference room networks
  - Networking in large vessels
  - Personal area networks
  - Vehicular networks
- Military applications
  - Ground-based battlefield networks
  - Hybrid platform networks (land, air, and sea based)

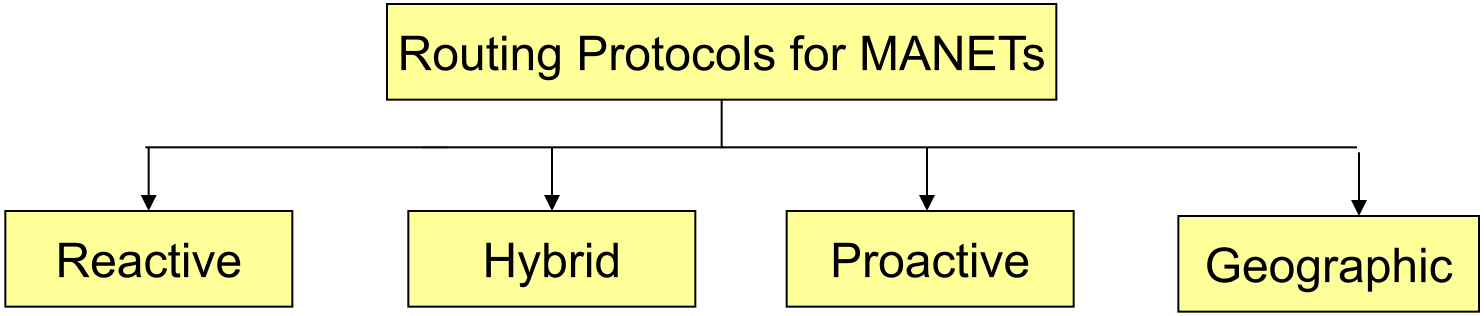
Problems to Address

- Physical layer
  - Range, symmetry, power control…
- MAC layer
  - Hidden terminal problem, asymmetrical links, error control, energy efficiency, fairness
- Network layer
  - Point-to-point, point-to-multi-point, flat, hierarchical, proactive, reactive, hybrid, mobility-tailored
- Transport layer
  - Packet loss discrimination, intermediate buffering

Introduction to routing

- Routing in ad hoc networks should account for host mobility, which leads to dynamic topologies
- Routing protocols designed for static (or slowly changing) networks
  - May not keep up with the rate of change
  - Waste limited resources
  - May not cater to specific performance criteria such as energy consumption
- As usual, no single protocol is optimal for all ad hoc network types and conditions

Protocol Classification



- Reactive Protocols
  - Determine the paths on-demand
- Proactive Protocols
  - Maintain paths regardless of traffic conditions
- Hybrid Protocols
  - Generally maintain local paths proactively, and create large scale paths reactively
- Geographic Protocols
  - Based on geographical location of nodes

Protocol Classification

- Reactive Protocols
  - Generally involve large delays between the request and first packet delivery
  - Incur low overhead in low traffic scenarios
- Proactive Protocols
  - Packets are immediately delivered as paths are already established
  - Results in high path maintenance overhead since the paths are kept regardless of traffic patterns
- Hybrid Protocols
  - Operate midway of delay and overhead performance
- Geographic Protocols
  - Can be used only when location information is available

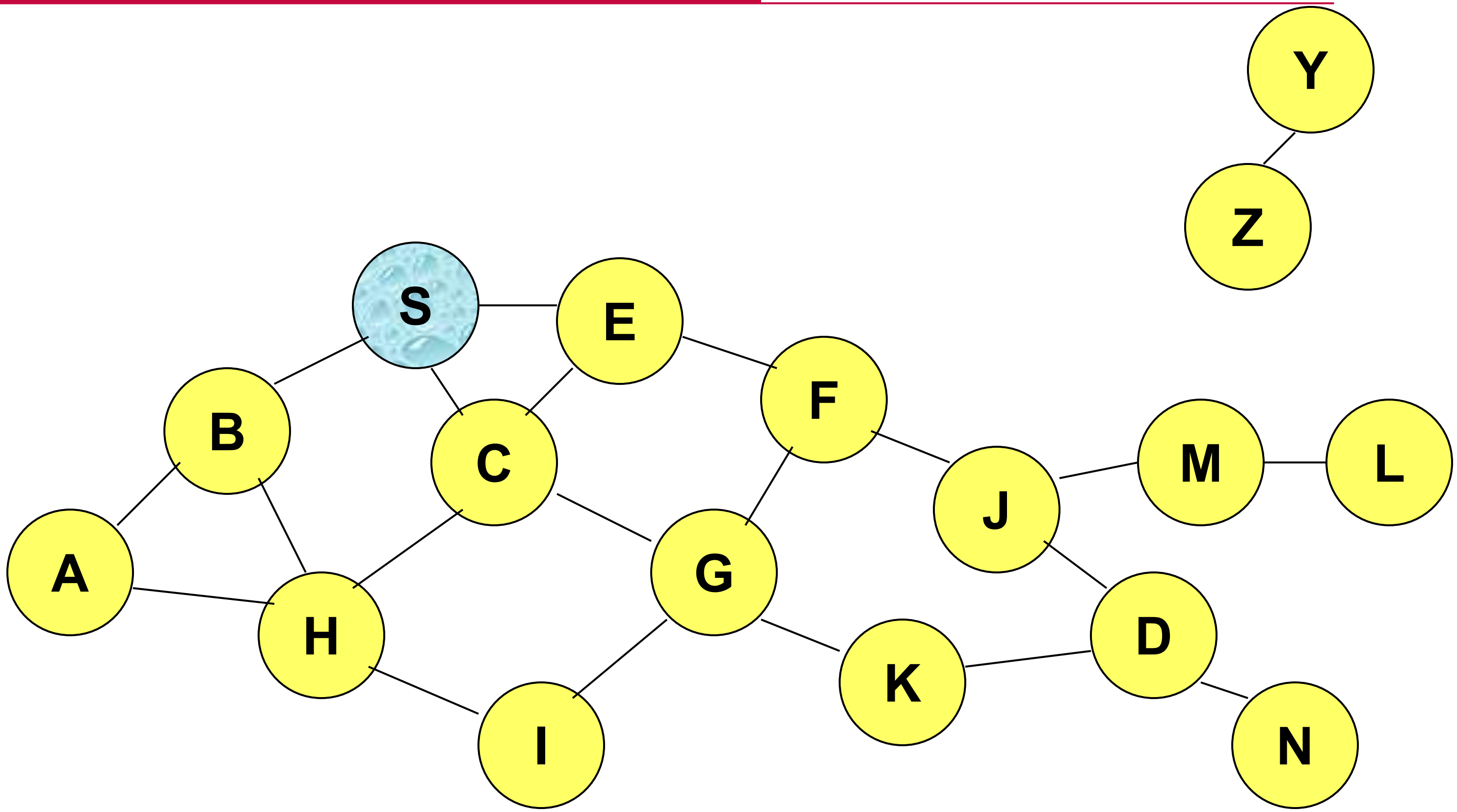
Trade-Off

- Latency of route discovery
  - Proactive protocols may have lower latency since routes are maintained at all times
  - Reactive protocols may have higher latency because a route from X to Y will be found only when X attempts to send to Y
- Overhead of route discovery/maintenance
  - Reactive protocols may have lower overhead since routes are determined only if needed
  - Proactive protocols can (but not necessarily) result in higher overhead due to continuous route updating
- Which approach achieves a better trade-off depends on the traffic and mobility patterns

Flooding for Data Delivery

- Sender S broadcasts data packet P to all its neighbors
- Each node receiving P forwards P to its neighbors
- Sequence numbers used to avoid the possibility of forwarding the same packet more than once
- Packet P reaches destination D provided that D is reachable from sender S
- Node D does not forward the packet

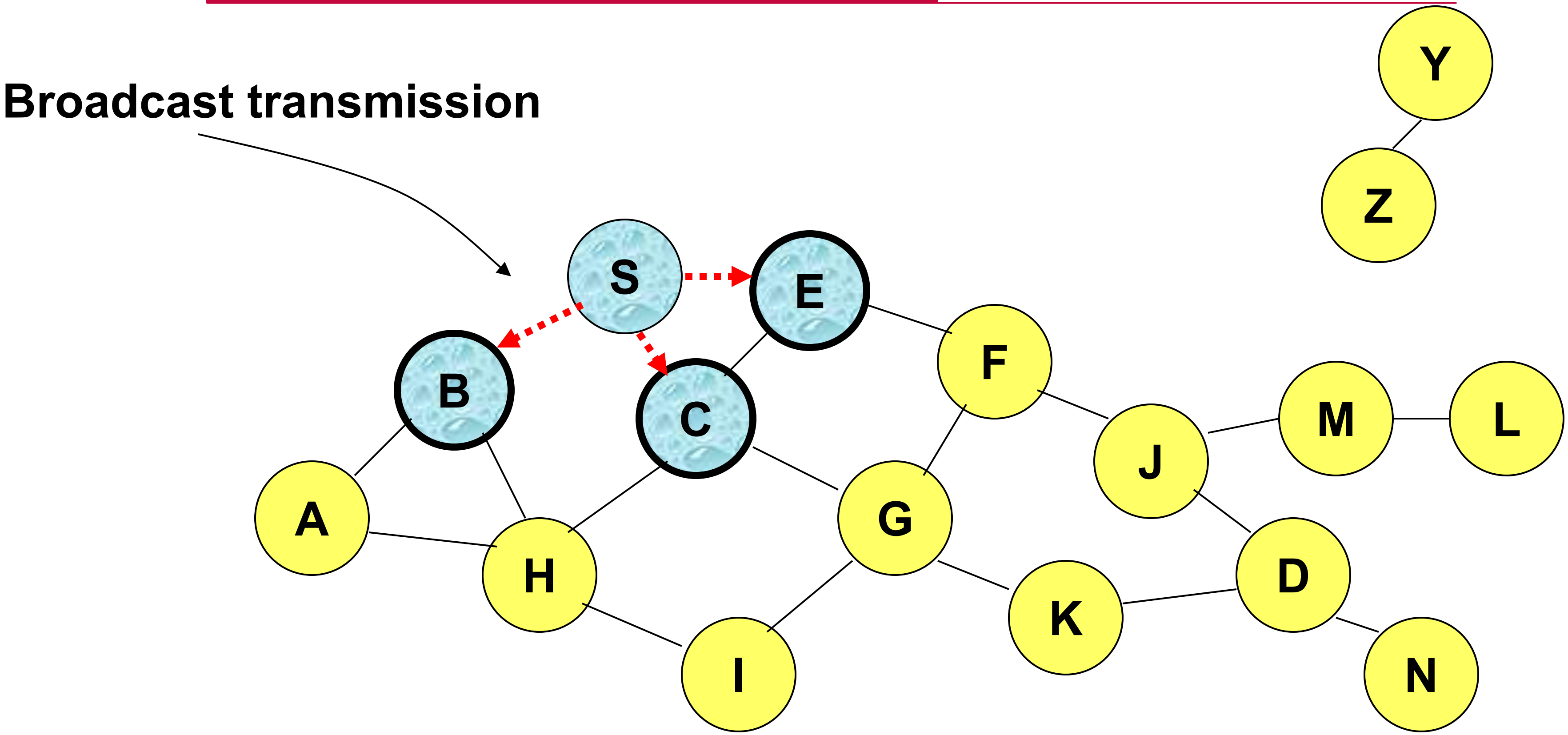
Flooding for Data Delivery



Represents a node that has received packet P

Represents that connected nodes are within each other's transmission range

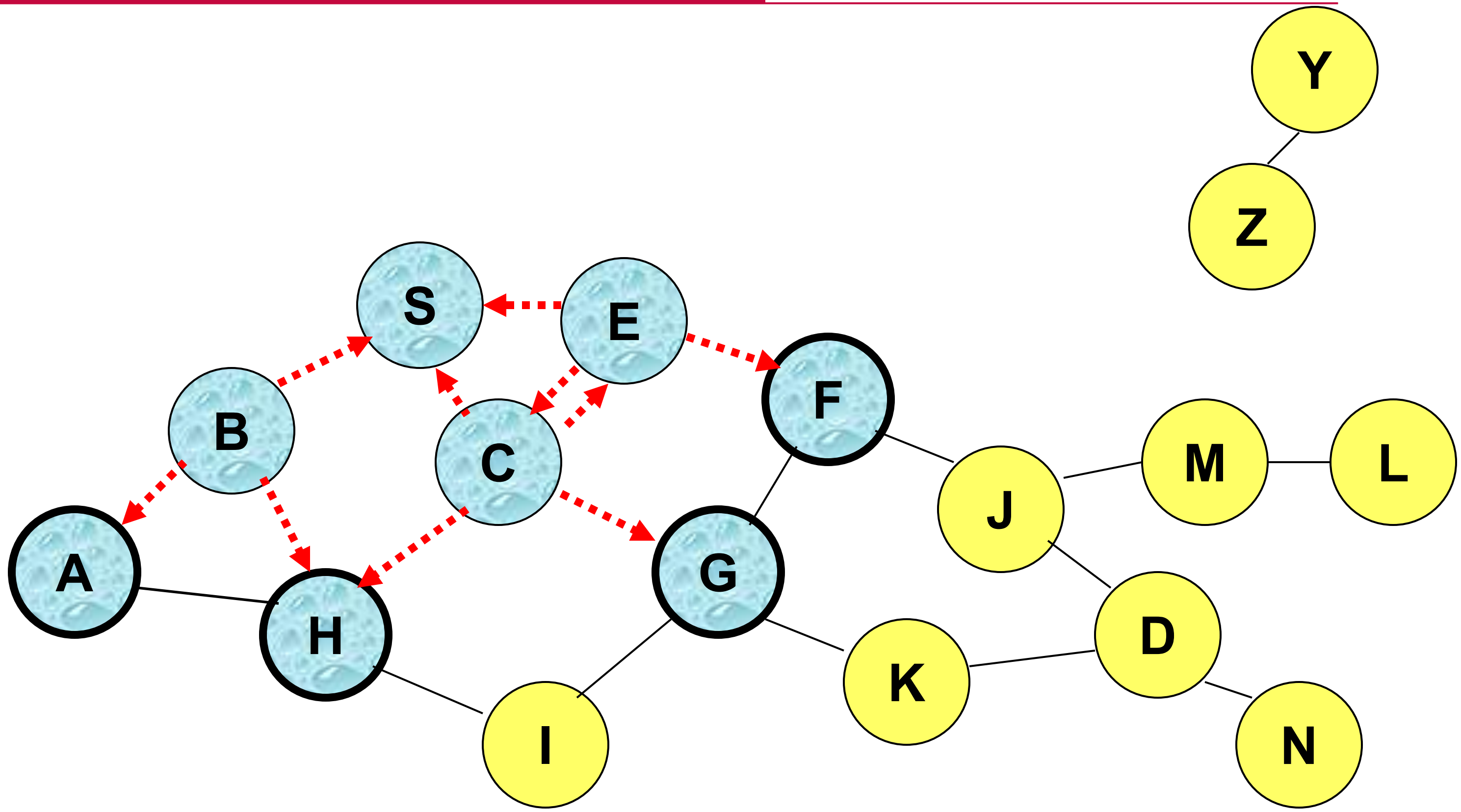
Flooding for Data Delivery



Represents a node that receives packet P for the first time

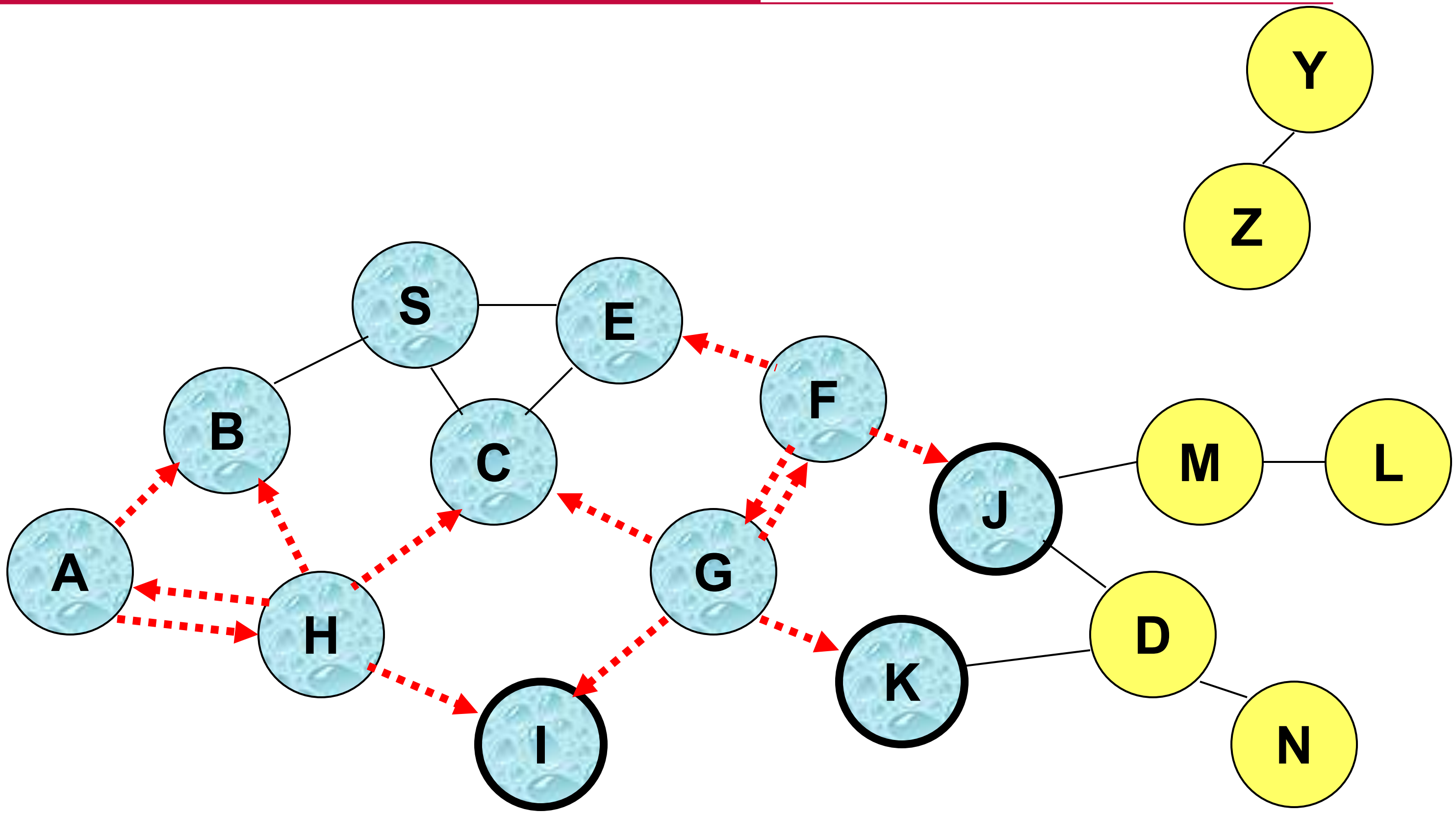
Represents transmission of packet P

Flooding for Data Delivery



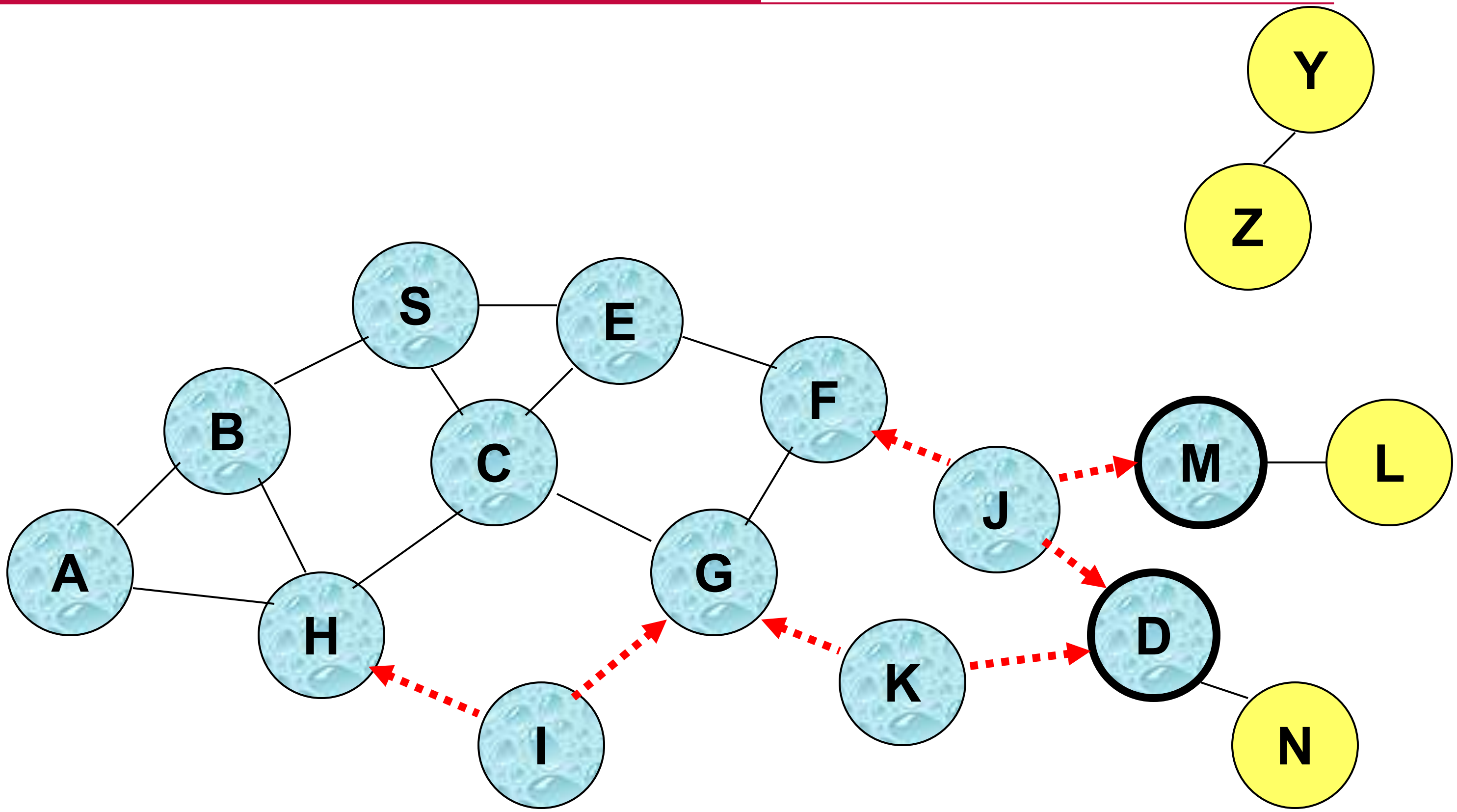
- Node H receives packet P from two neighbors: potential for collision

Flooding for Data Delivery



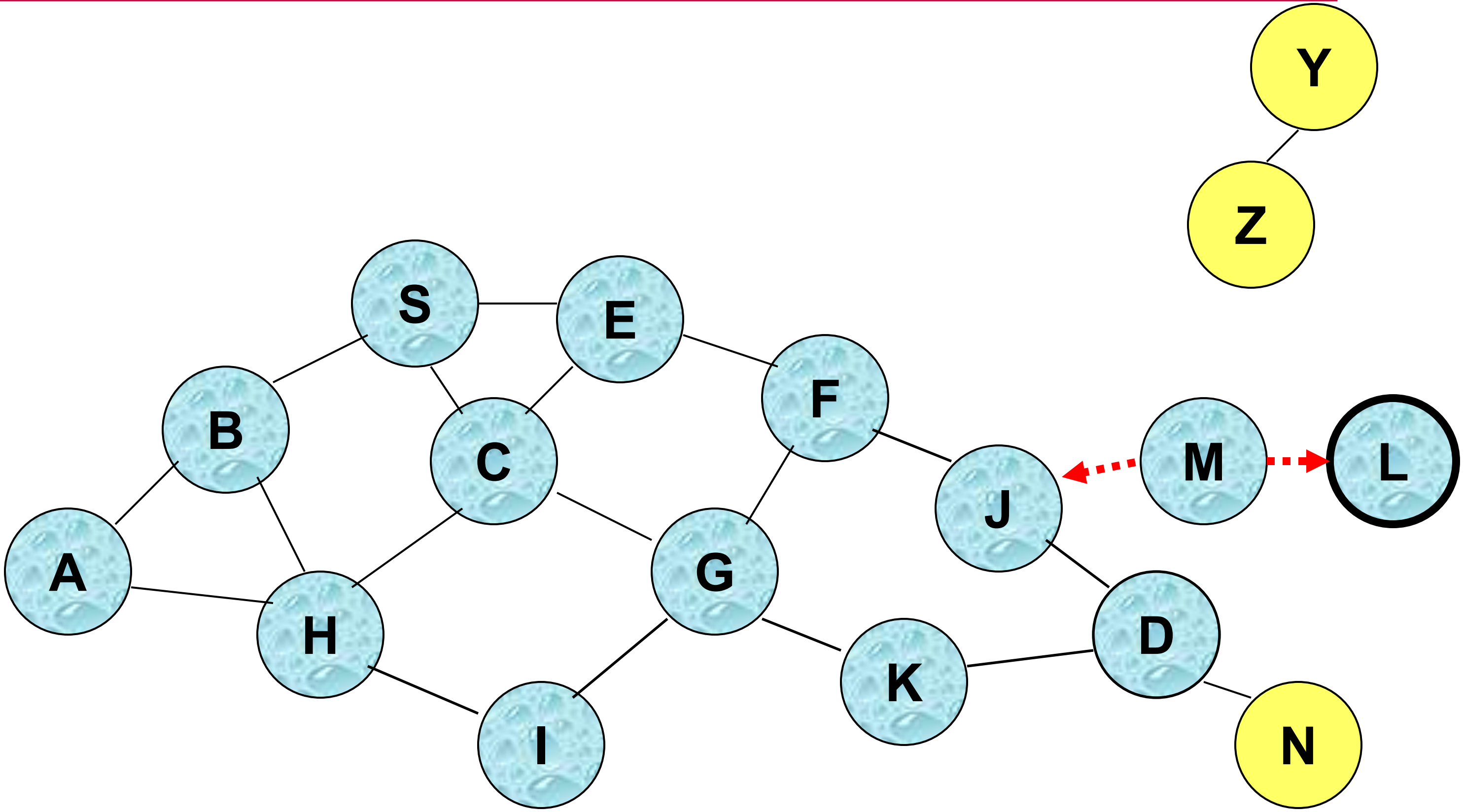
- Node C receives packet P from G and H, but does not forward it again, because node C has already forwarded packet P once

Flooding for Data Delivery



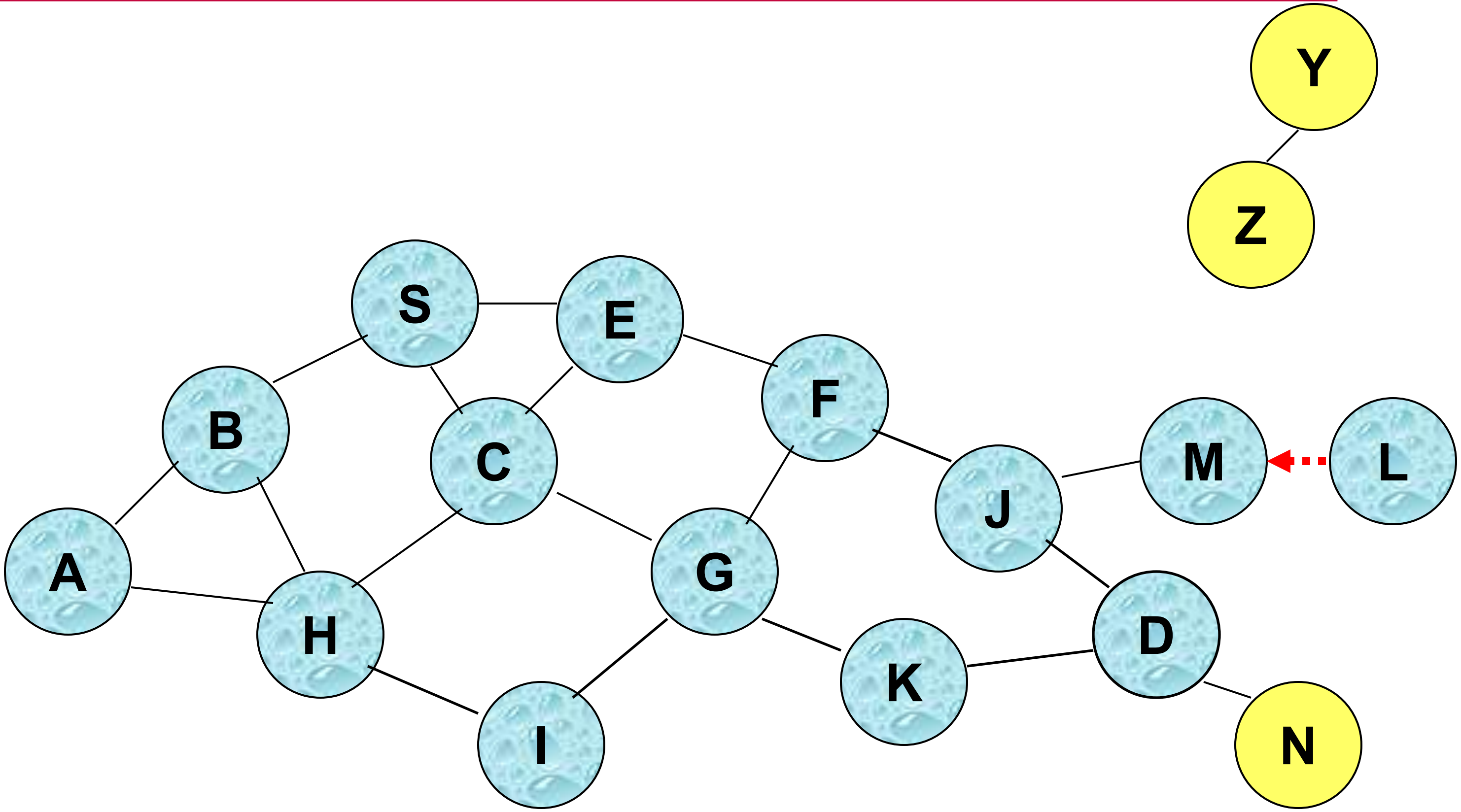
- Nodes J and K both broadcast packet P to node D
- Since nodes J and K are hidden from each other, their transmissions may collide => Packet P may not be delivered to node D at all, despite the use of flooding

Flooding for Data Delivery



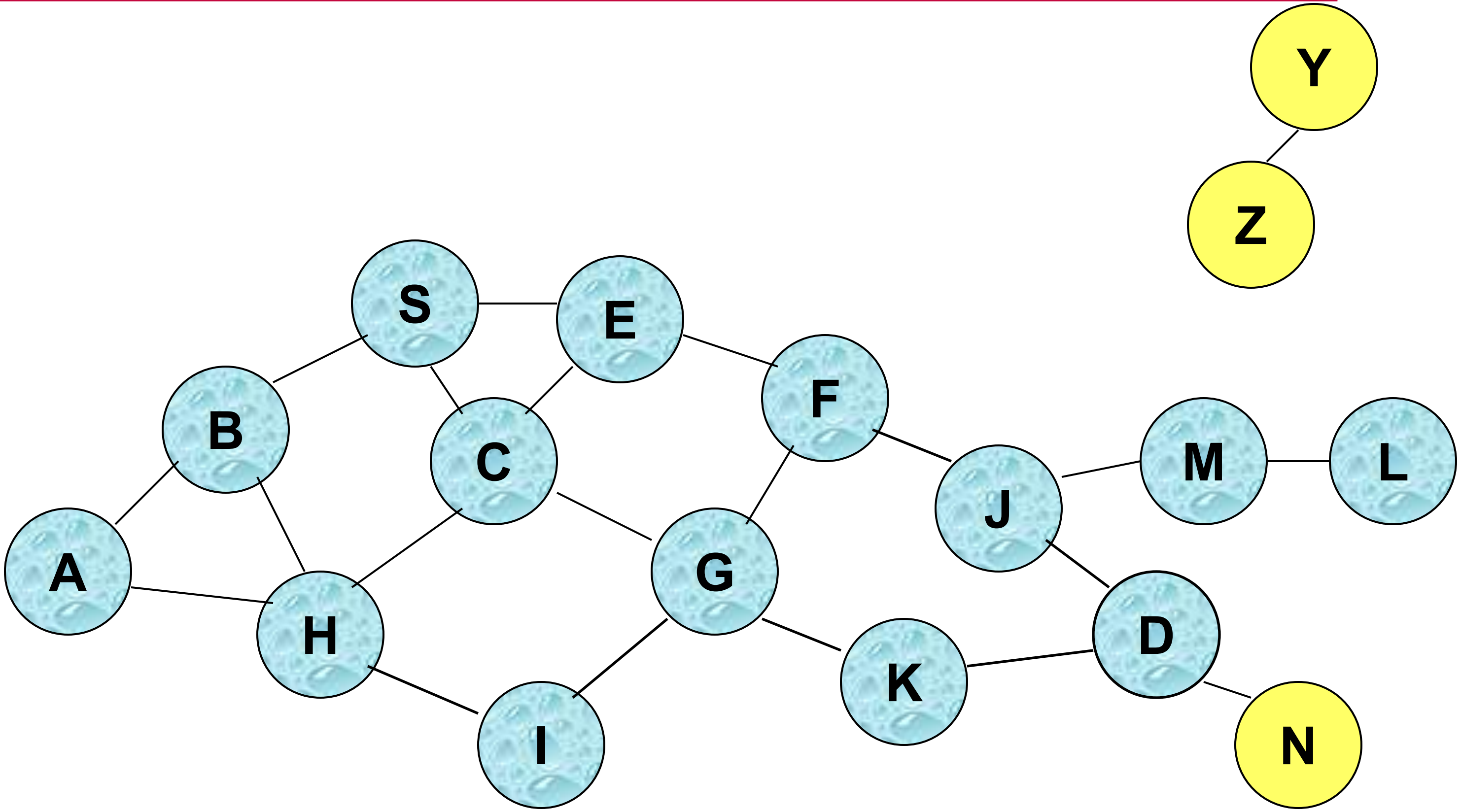
- Node D **does not forward** packet P, because node D is the intended destination of packet P

Flooding for Data Delivery



- Flooding completed
- Nodes unreachable from S do not receive packet P (e.g., node Z)
- Nodes for which all paths from S go through the destination D also do not receive packet P (example: node N)

Flooding for Data Delivery



- Flooding may deliver packets to too many nodes (in the **worst case**, all nodes reachable from sender may receive the packet)

Flooding for Data Delivery: Advantages

- Simplicity
- May be more efficient than other protocols when rate of information transmission is low enough that the overhead of explicit route discovery/maintenance incurred by other protocols is relatively higher
  - this scenario may occur, for instance, when nodes transmit small data packets relatively infrequently, and many topology changes occur between consecutive packet transmissions
- Potentially higher reliability of data delivery
  - Because packets may be delivered to the destination on multiple paths

Flooding for Data Delivery: Disadvantages

- Potentially, very high overhead
  - Data packets may be delivered to too many nodes who do not need to receive them
- Potentially lower reliability of data delivery
  - Flooding uses broadcasting -- hard to implement reliable broadcast delivery without significantly increasing overhead
    - Broadcasting in IEEE 802.11 MAC is unreliable
  - In our example, nodes J and K may transmit to node D simultaneously, resulting in loss of the packet
    - in this case, destination would not receive the packet at all

Flooding of Control Packets

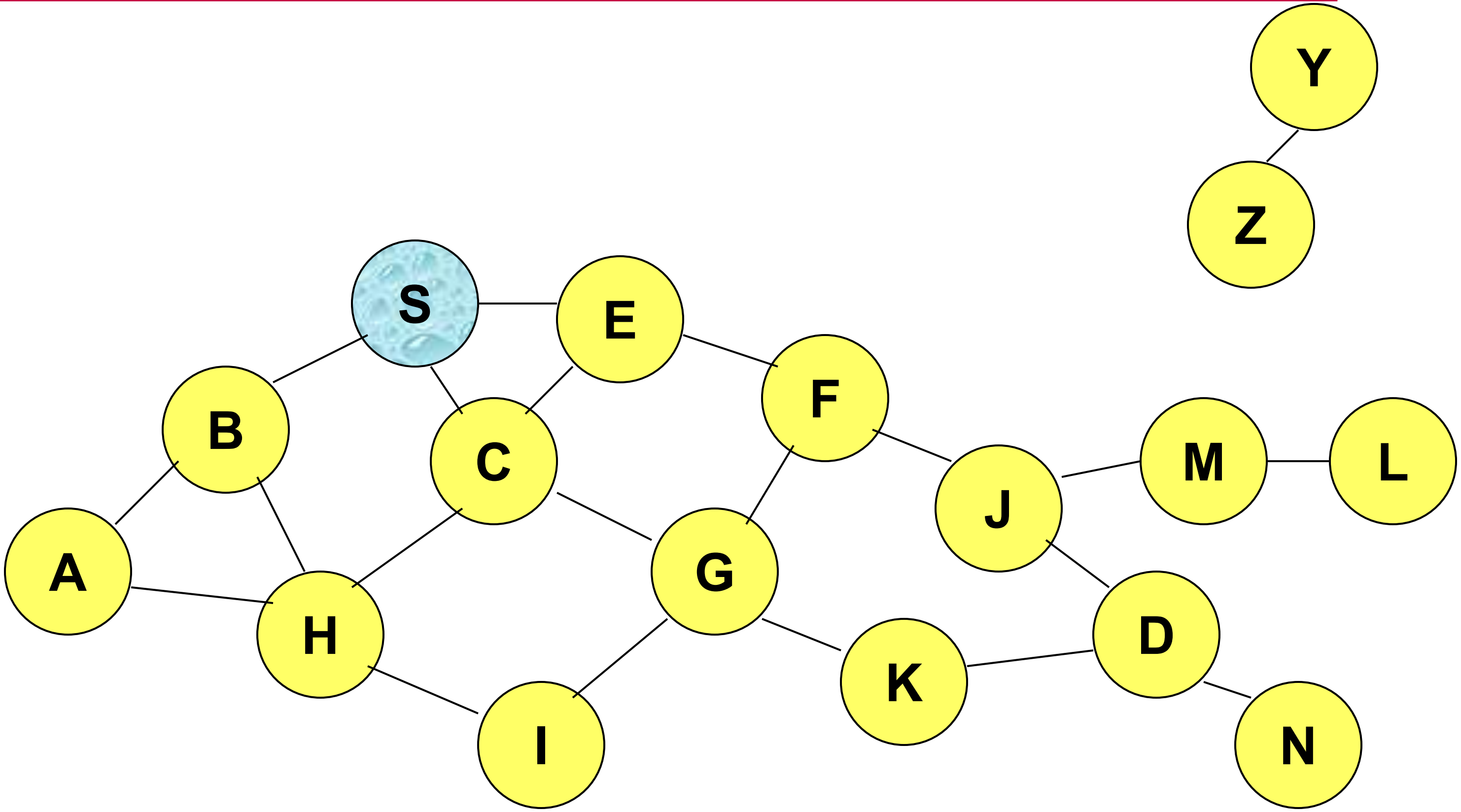
- Many protocols perform (potentially *limited*) flooding of control packets, instead of data packets
- The control packets are used to discover routes
- Discovered routes are subsequently used to send data packet(s)
- Overhead of control packet flooding is amortized over data packets transmitted between consecutive control packet floods

Reactive Protocols

Dynamic Source Routing (DSR)

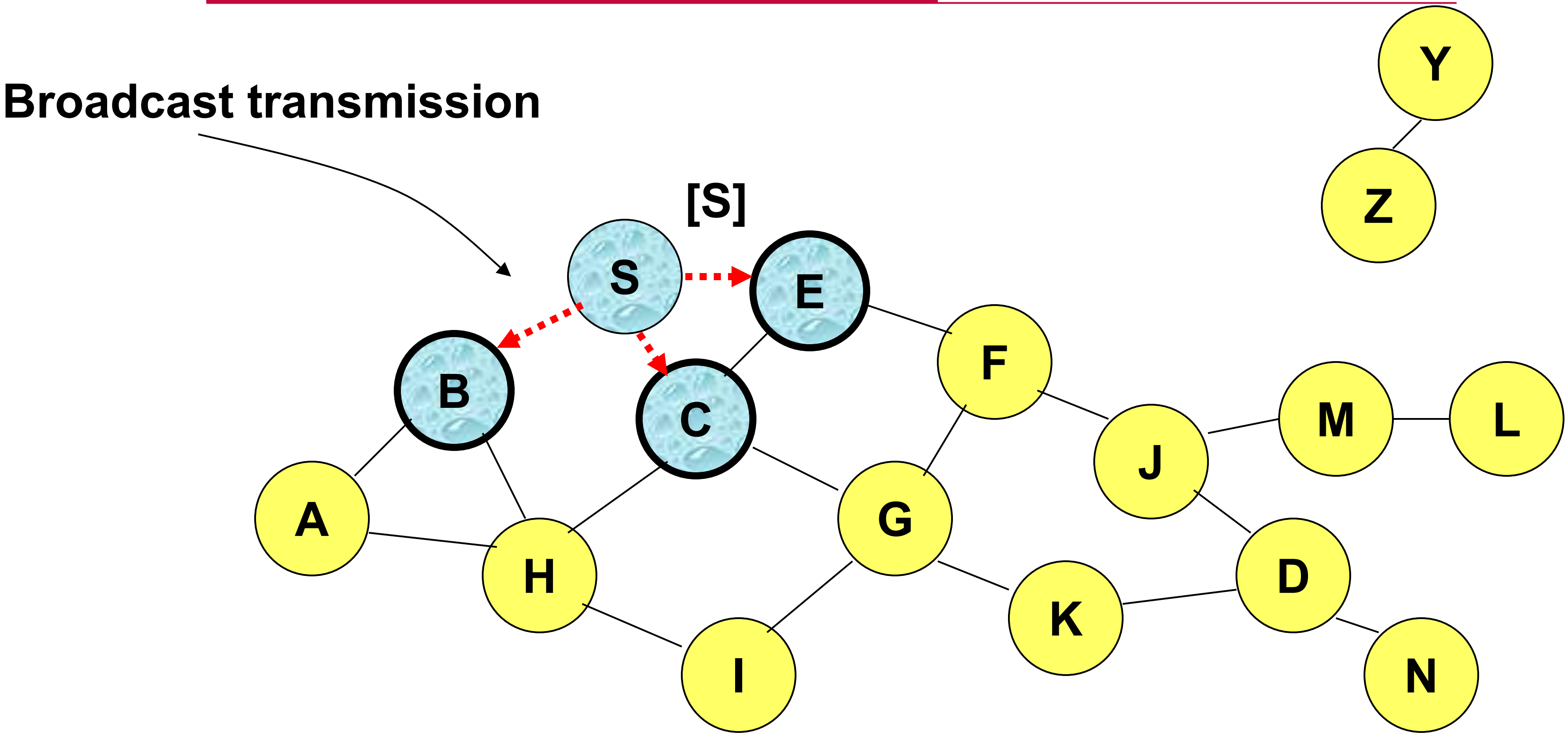
- When node S wants to send a packet to node D, but does not know a route to D, node S initiates a route discovery
- Source node S floods Route Request (RREQ)
- Each node appends own identifier when forwarding RREQ

Route Discovery in DSR



Represents a node that has received RREQ for D from S

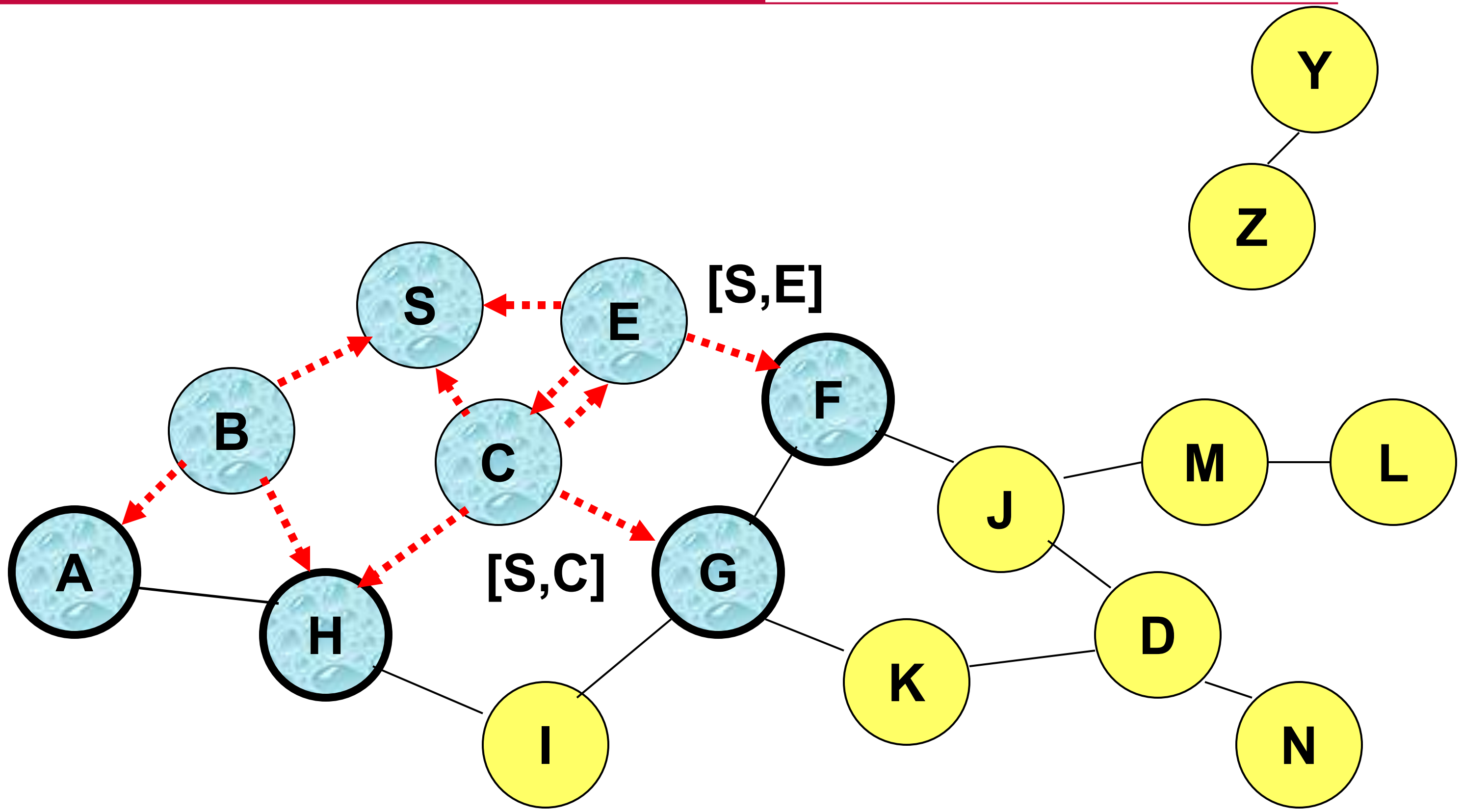
Route Discovery in DSR



Represents transmission of RREQ

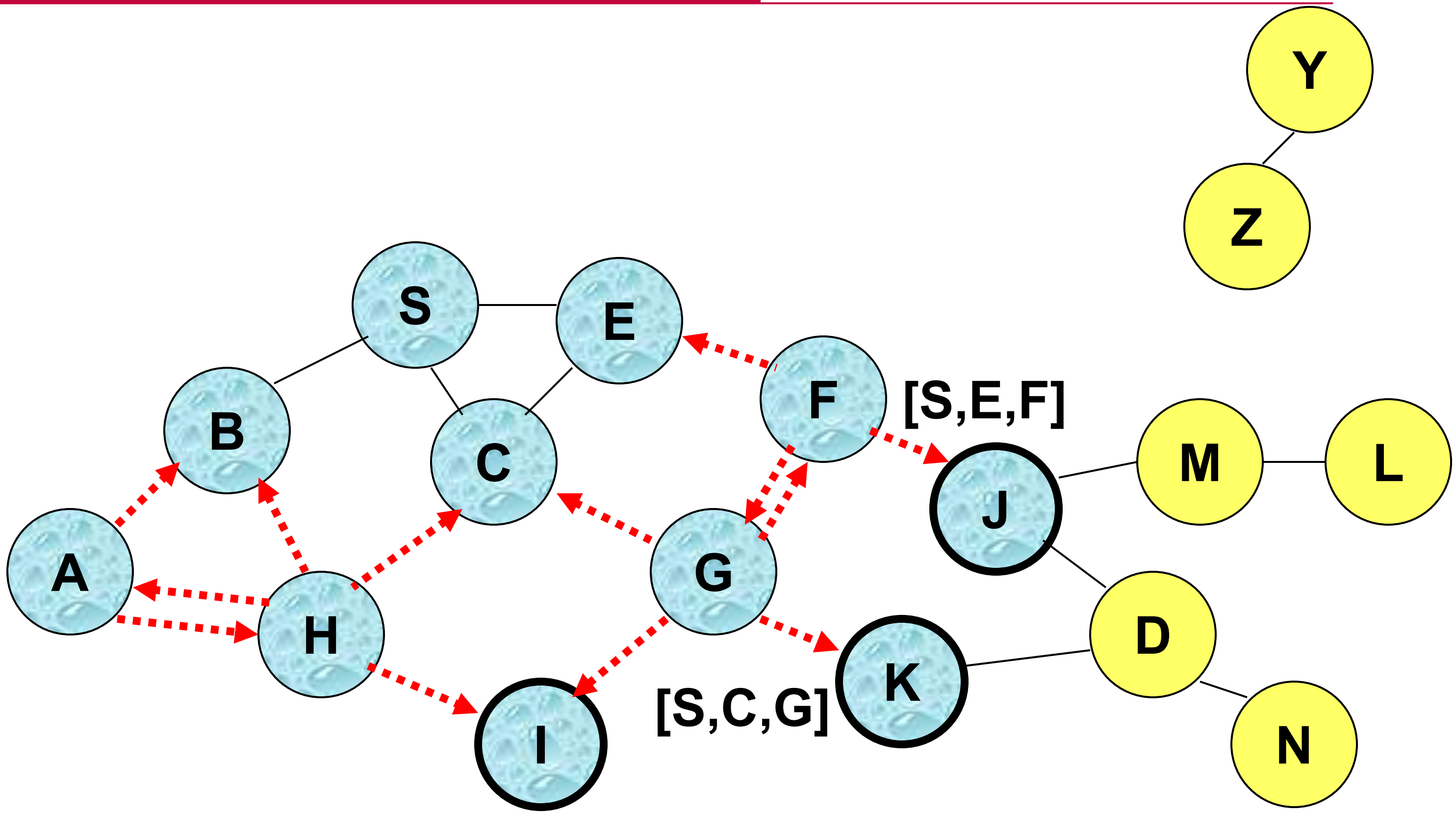
[X,Y] Represents list of identifiers appended to RREQ

Route Discovery in DSR



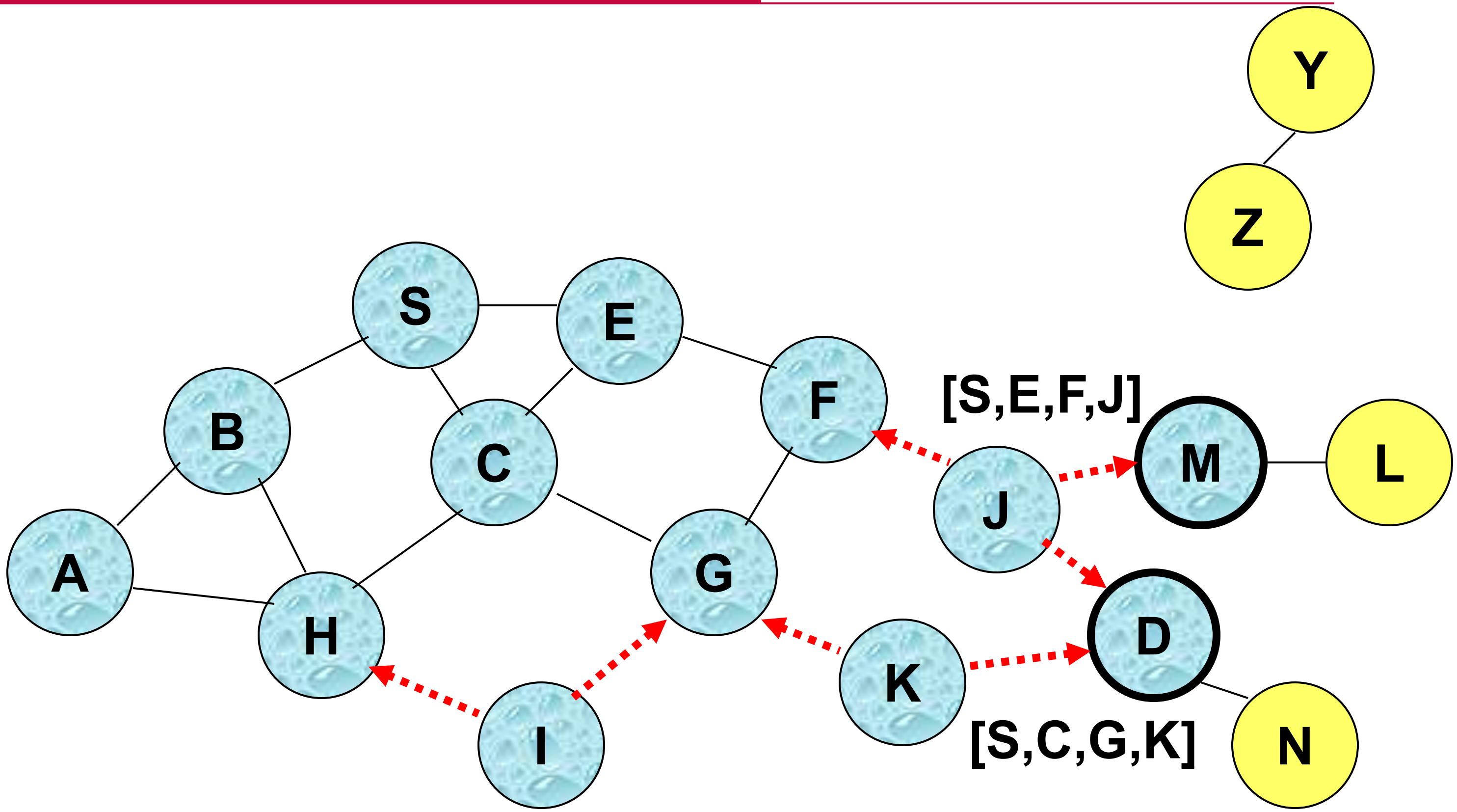
• Node H receives packet RREQ from two neighbors: **potential for collision**

Route Discovery in DSR



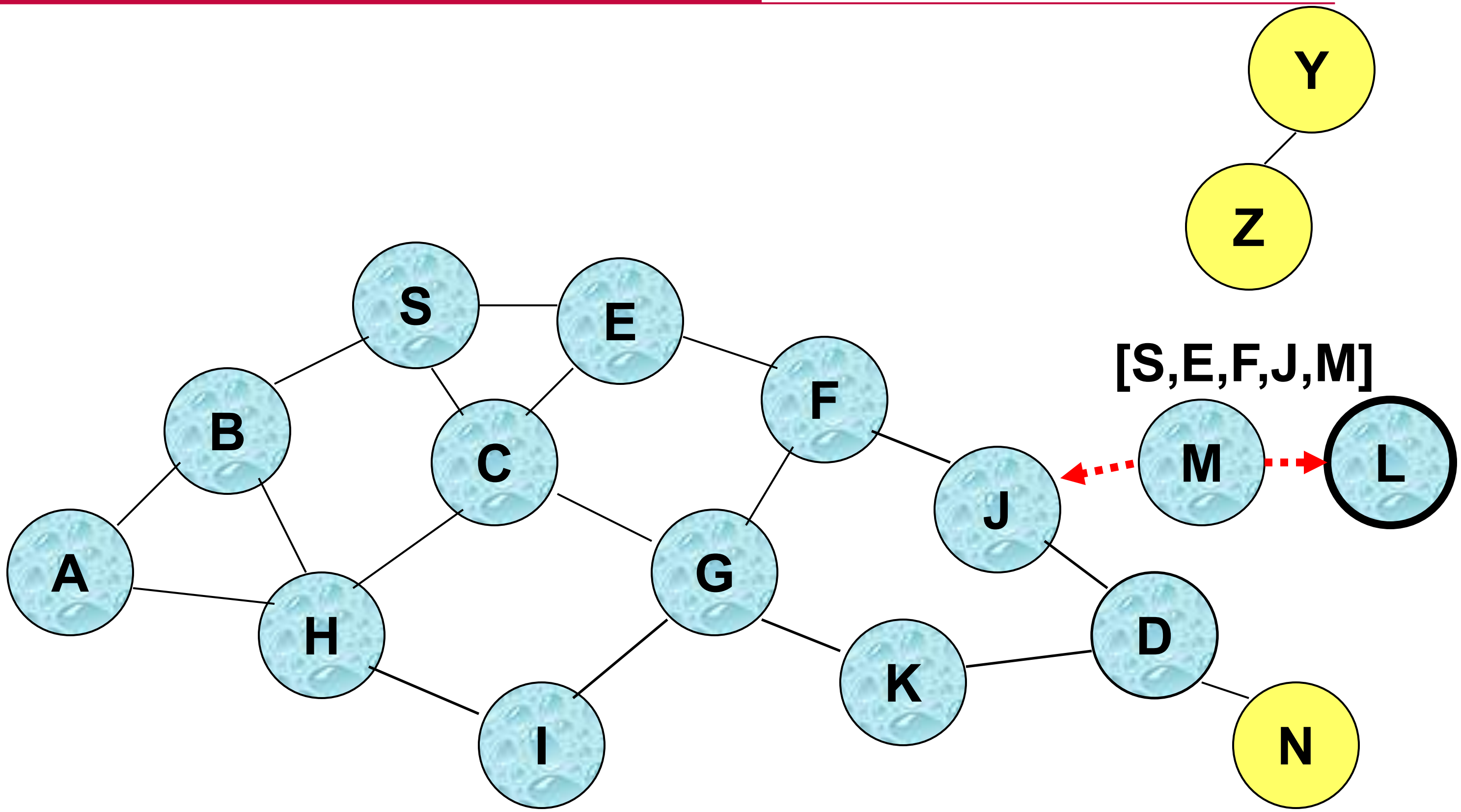
- Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

Route Discovery in DSR



- Nodes J and K both broadcast RREQ to node D
- Since nodes J and K are hidden from each other, their transmissions may collide

Route Discovery in DSR

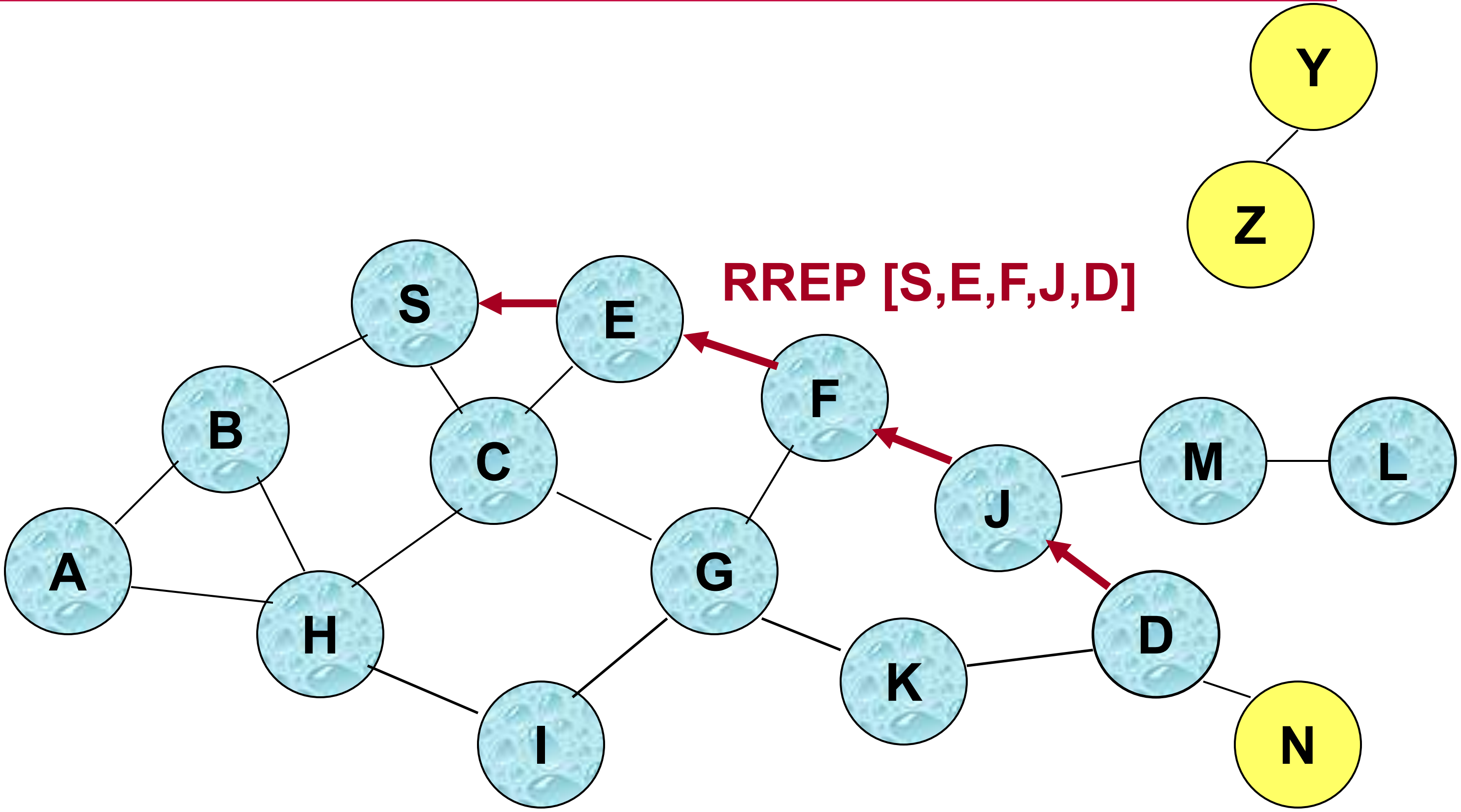


• Node D **does not forward** RREQ, because node D is the **intended target** of the route discovery

Route Discovery in DSR

- Destination D on receiving the first RREQ, sends a Route Reply (RREP)
- RREP is sent on a route obtained by reversing the route appended to received RREQ
- RREP includes the route from S to D on which RREQ was received by node D

Route Reply in DSR



Represents RREP control message

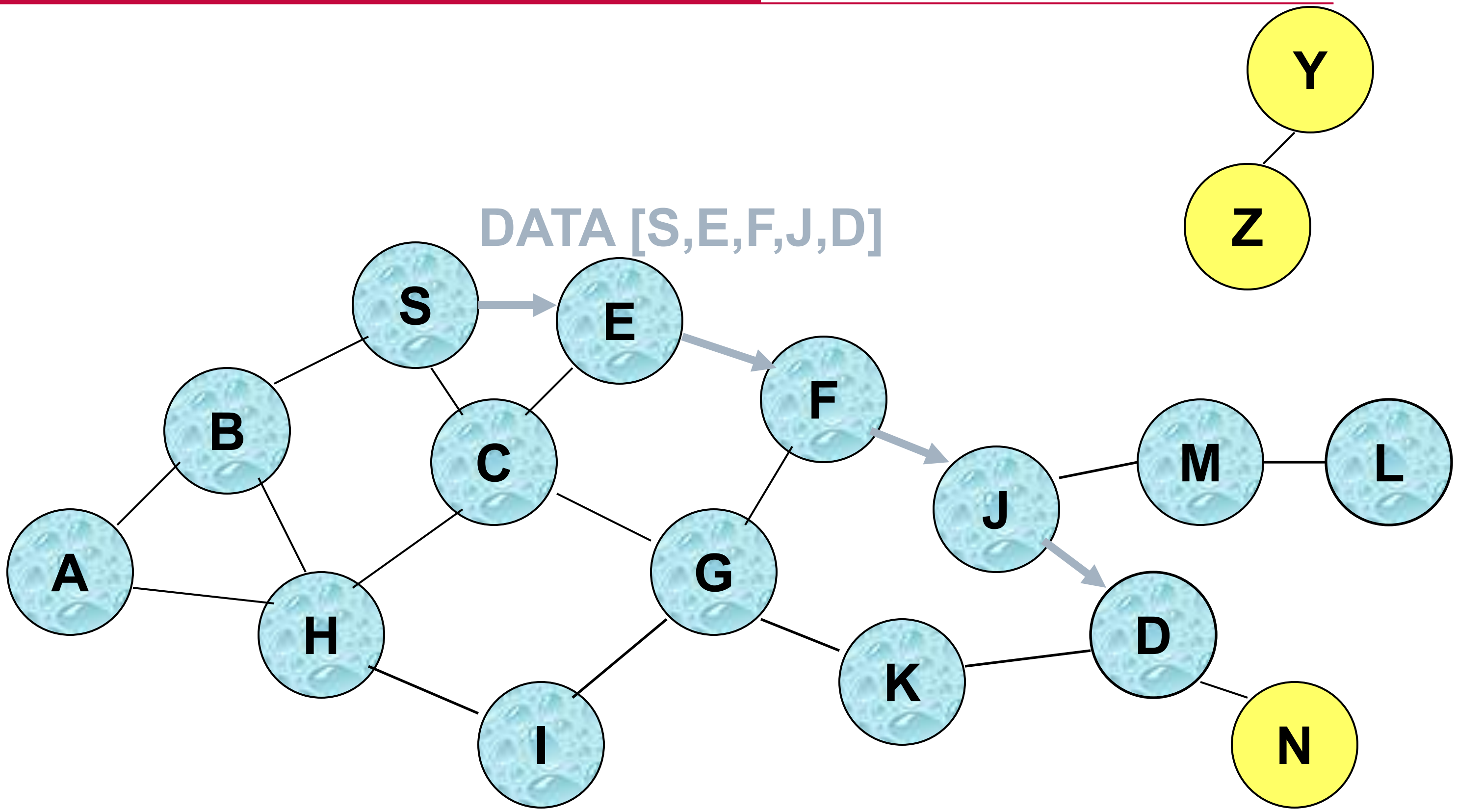
Route Reply in DSR

- Route Reply can be sent by reversing the route in Route Request (RREQ) only if links are guaranteed to be bi-directional
  - To ensure this, RREQ should be forwarded only if it received on a link that is known to be bi-directional
- If unidirectional (asymmetric) links are allowed, then RREP may need a route discovery for S from node D
  - Unless node D already knows a route to node S
  - If a route discovery is initiated by D for a route to S, then the Route Reply is piggybacked on the Route Request from D.
- If IEEE 802.11 MAC is used to send data, then links have to be bi-directional (since Ack is used)

Dynamic Source Routing (DSR)

- Node S on receiving RREP, caches the route included in the RREP
- When node S sends a data packet to D, the entire route is included in the packet header
  - hence the name source routing
- Intermediate nodes use the source route included in a packet to determine to whom a packet should be forwarded

Data Delivery in DSR



Packet header size grows with route length

When to Perform a Route Discovery

- When node S wants to send data to node D, but does not know a valid route node D

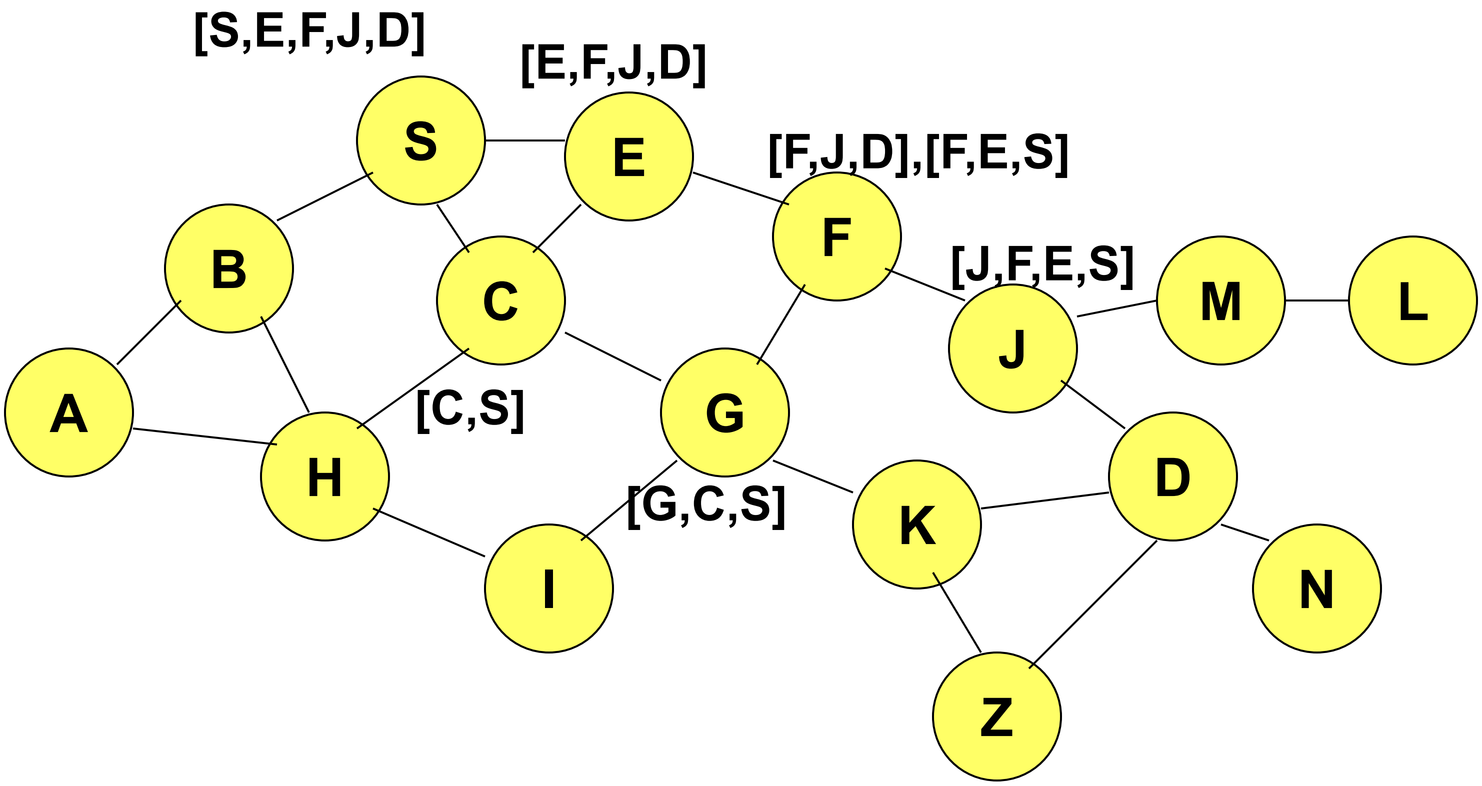
DSR Optimization: Route Caching

- Each node caches a new route it learns by *any means*
- When node S finds route [S,E,F,J,D] to node D, node S also learns route [S,E,F] to node F
- When node K receives Route Request [S,C,G] destined for node, node K learns route [K,G,C,S] to node S
- When node F forwards Route Reply RREP [S,E,F,J,D], node F learns route [F,J,D] to node D
- When node E forwards Data [S,E,F,J,D] it learns route [E,F,J,D] to node D
- A node may also learn a route when it overhears Data packets

Use of Route Caching

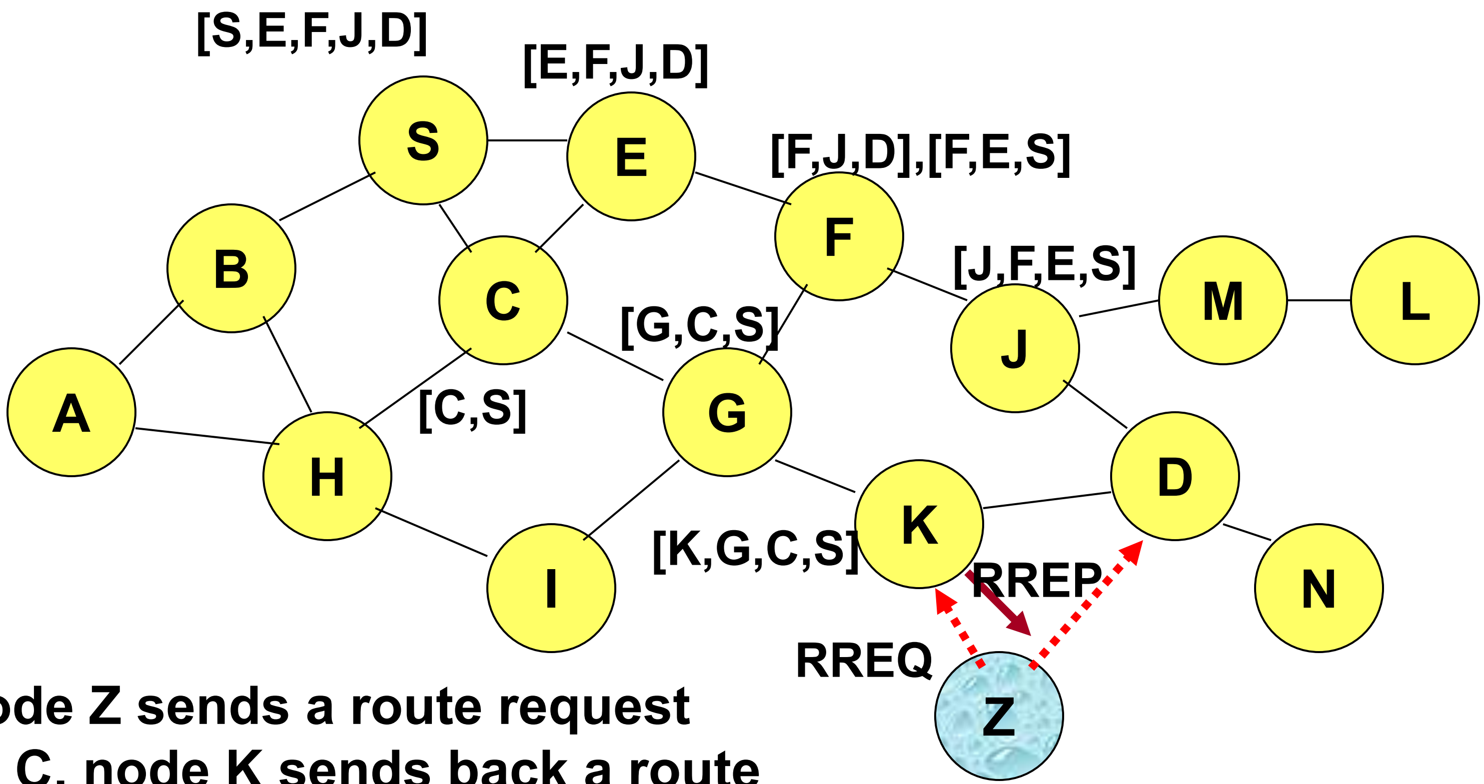
- When node S learns that a route to node D is broken, it uses another route from its local cache, if such a route to D exists in its cache. Otherwise, node S initiates route discovery by sending a route request
- Node X on receiving a Route Request for some node D can send a Route Reply if node X knows a route to node D
- Use of route cache
  - can speed up route discovery
  - can reduce propagation of route requests

Use of Route Caching



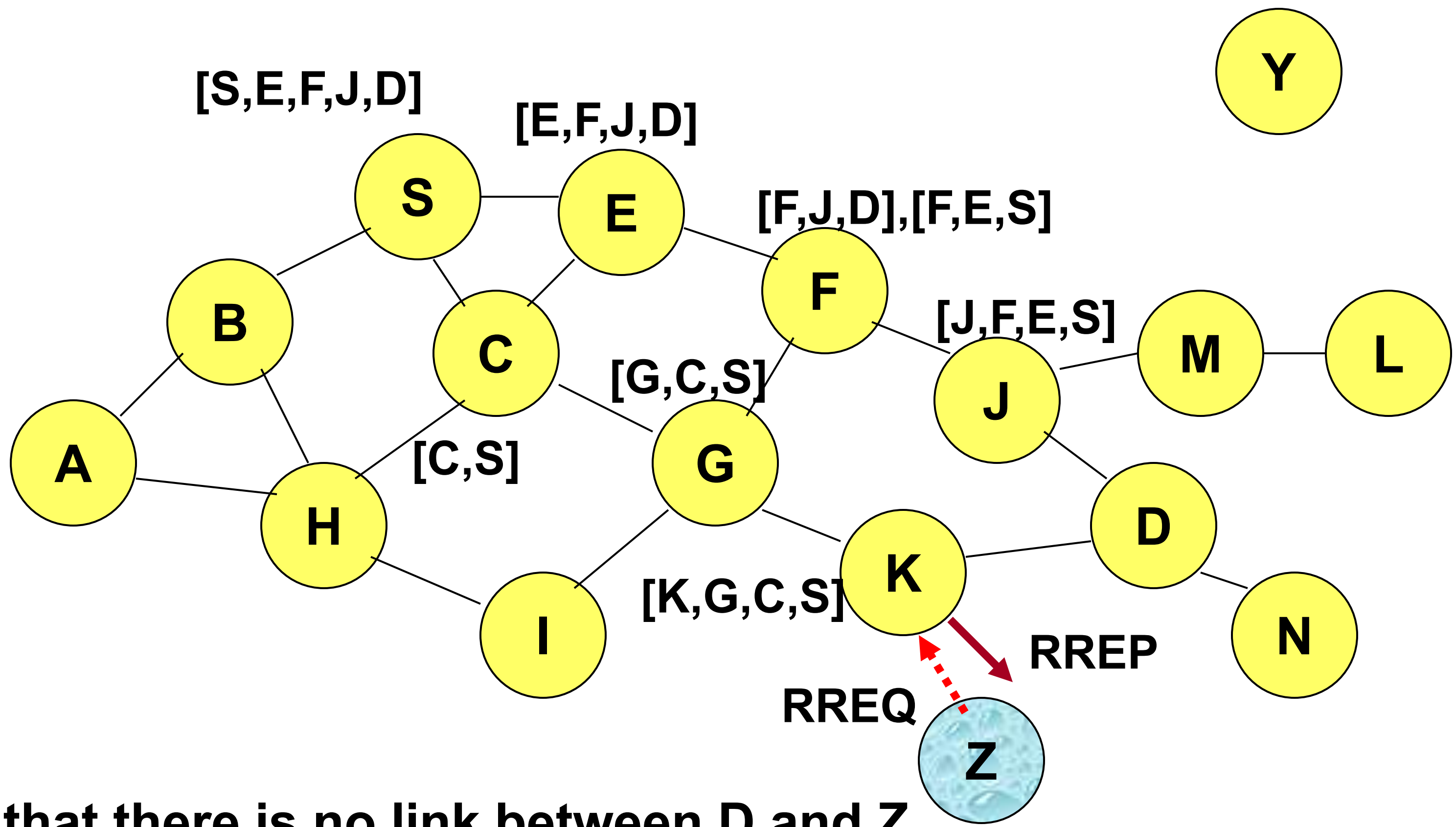
[P,Q,R] Represents cached route at a node
(DSR maintains the cached routes in a tree format)

Route Caching: Can Speed up Route Discovery



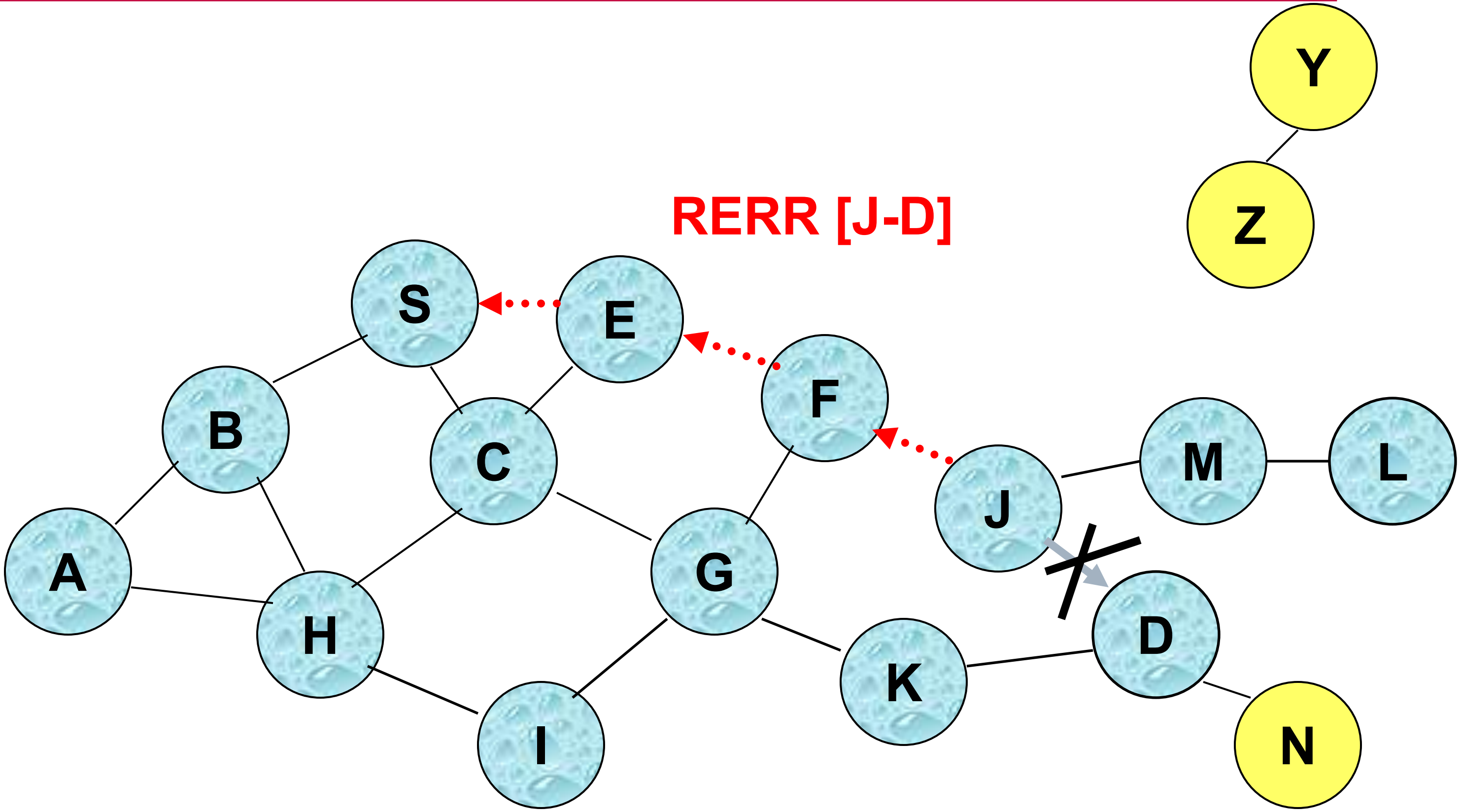
When node Z sends a route request for node C, node K sends back a route reply [Z,K,G,C] to node Z using a locally cached route

Route Caching: Can Reduce Propagation of Route Requests



Assume that there is no link between D and Z.
Route Reply (RREP) from node K limits flooding of RREQ.
In general, the reduction may be less dramatic.

Route Error (RERR)



J sends a route error to S along route J-F-E-S when its attempt to forward the data packet S (with route SEFJD) on J-D fails

Nodes hearing RERR update their route cache to remove link J-D

Route Caching: Beware!

- Stale caches can adversely affect performance
- With passage of time and host mobility, cached routes may become invalid
- A sender host may try several stale routes (obtained from local cache, or replied from cache by other nodes), before finding a good route

Dynamic Source Routing: Advantages

- Routes maintained only between nodes who need to communicate
  - reduces overhead of route maintenance
- Route caching can further reduce route discovery overhead
- A single route discovery may yield many routes to the destination, due to intermediate nodes replying from local caches

Dynamic Source Routing: Disadvantages

- Packet header size grows with route length due to source routing
- Flood of route requests may potentially reach all nodes in the network
- Care must be taken to avoid collisions between route requests propagated by neighboring nodes
  - insertion of random delays before forwarding RREQ
- Increased contention if too many route replies come back due to nodes replying using their local cache
  - Route Reply *Storm* problem
  - Reply storm may be eased by preventing a node from sending RREP if it hears another RREP with a shorter route

Dynamic Source Routing: Disadvantages

- An intermediate node may send Route Reply using a stale cached route, thus polluting other caches
- This problem can be eased if some mechanism to purge (potentially) invalid cached routes is incorporated.

Ad Hoc On-Demand Distance Vector Routing (AODV)

- DSR includes source routes in packet headers
- Resulting large headers can sometimes degrade performance
  - particularly when data contents of a packet are small
- AODV attempts to improve on DSR by maintaining routing tables at the nodes, so that data packets do not have to contain routes
- AODV retains the desirable feature of DSR that routes are maintained only between nodes which need to communicate

Proactive Protocols

Link State Routing

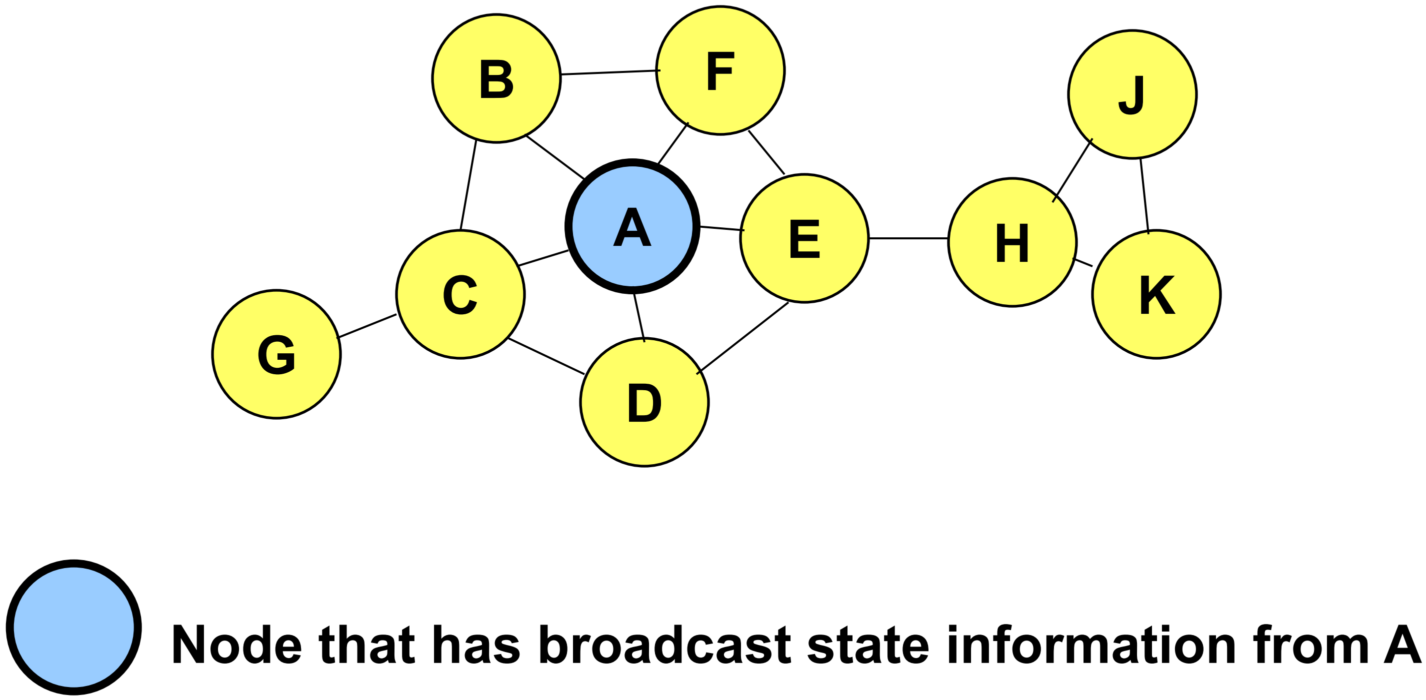
- Each node periodically floods status of its links
- Each node re-broadcasts link state information received from its neighbor
- Each node keeps track of link state information received from other nodes
- Each node uses above information to determine next hop to each destination

Optimized Link State Routing (OLSR)

- The overhead of flooding link state information is reduced by requiring fewer nodes to forward the information
- A broadcast from node X is only forwarded by its *multipoint relays*
- Multipoint relays of node X are its neighbors such that each two-hop neighbor of X is a one-hop neighbor of at least one multipoint relay of X
  - Each node transmits its neighbor list in periodic beacons, so that all nodes can know their 2-hop neighbors, in order to choose the multipoint relays

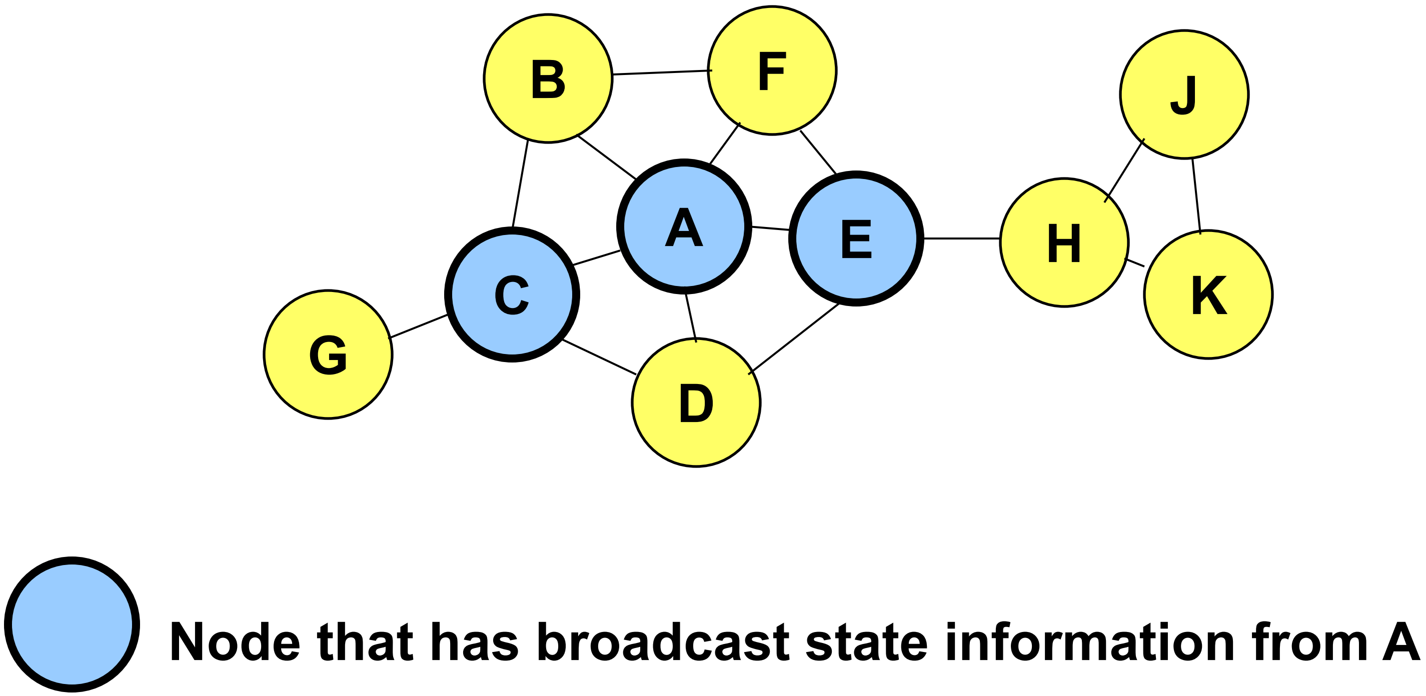
Optimized Link State Routing (OLSR)

- Nodes C and E are multipoint relays of node A



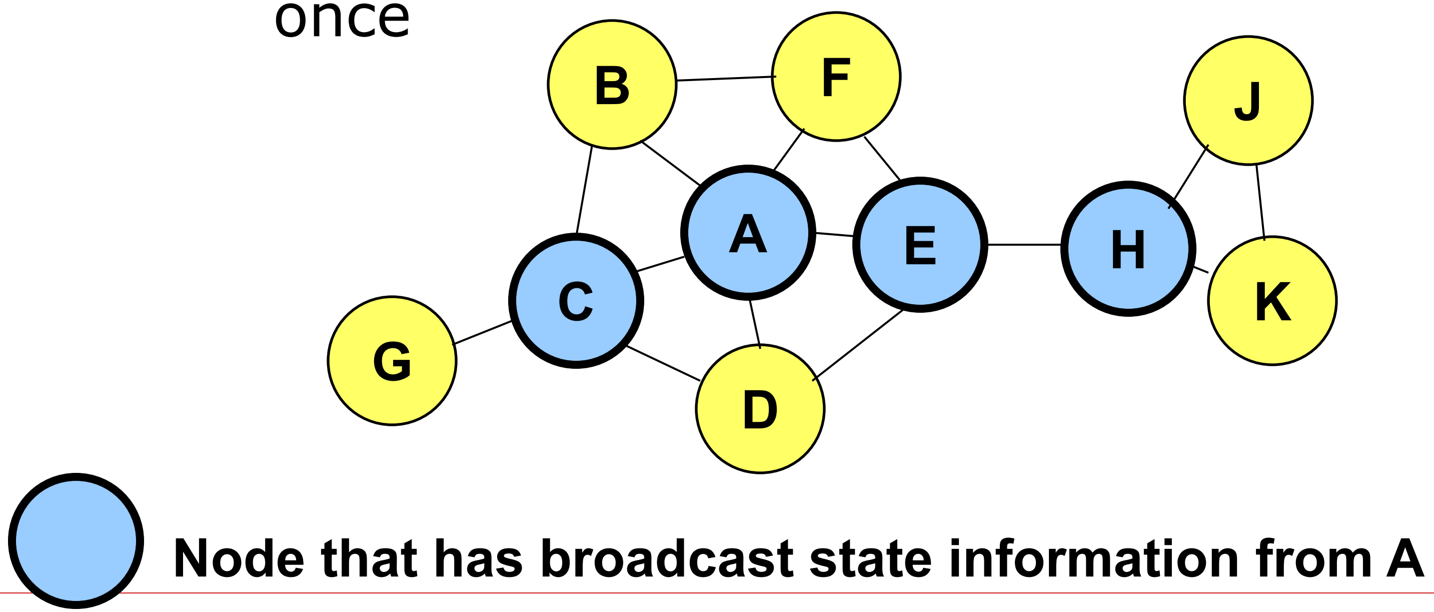
Optimized Link State Routing (OLSR)

- Nodes C and E forward information received from A



Optimized Link State Routing (OLSR)

- Nodes E and K are multipoint relays for node H
- Node K forwards information received from H
  - E has already forwarded the same information once



OLSR

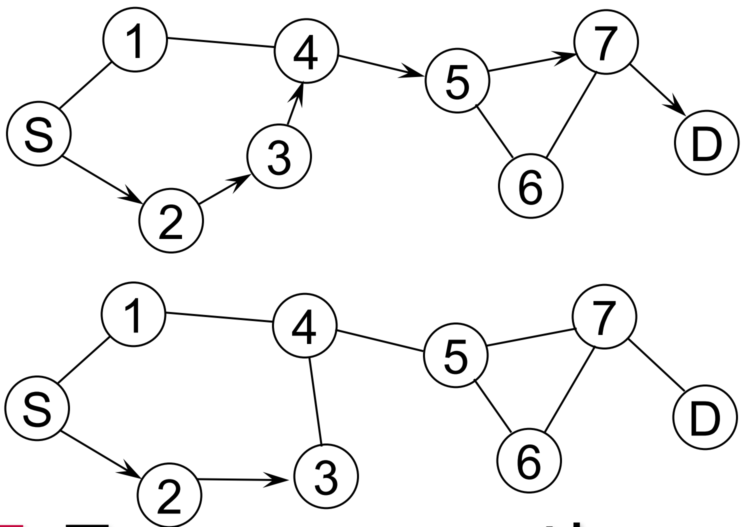
- OLSR floods information through the multipoint relays
- The flooded information itself is for links connecting nodes to respective multipoint relays
- Routes used by OLSR only include multipoint relays as intermediate nodes

Geographic routing

Geographic Distance Routing (GEDIR)

- Rather than maintaining routing tables and discovering paths, one can also use the geographic location of nodes
  - Requires that each node knows it own location (e.g., using GPS)
  - Requires knowledge of all neighbor locations
- It is based on sending the packet to the neighbor that is closest to the destination
  - Works only if nodes are located densely
  - Obstacles and low node density may lead to routing failures

GEDIR – Example



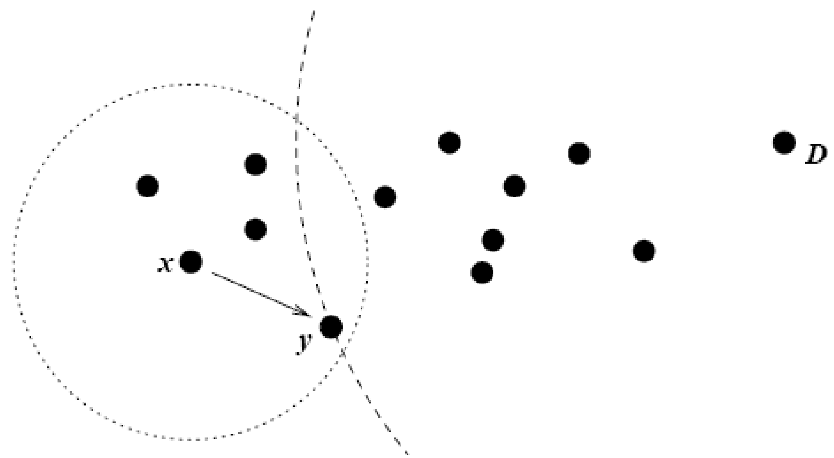
Regular Operation
(not necessarily minimum hop)

Routing fails because 3 has no neighbors closer to D than itself

- To overcome the problem of not finding closer neighbors, expanded local search algorithms are also proposed
  - When stuck, broadcast a path discovery request with small TTL, use discovered path for forwarding data

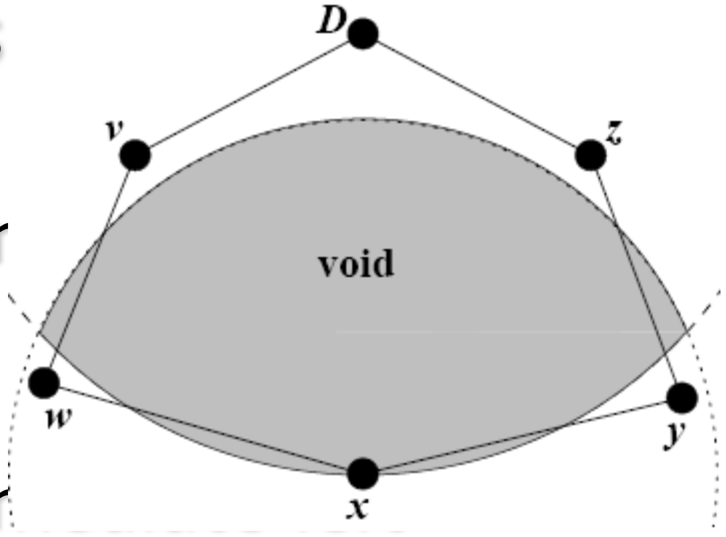
Greedy Perimeter Stateless Routing (GPSR)

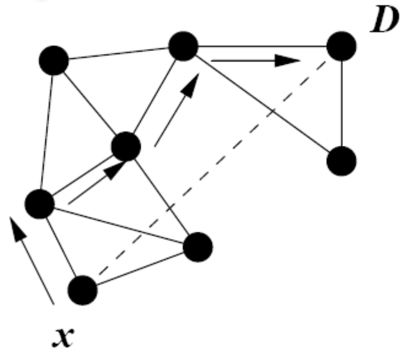
- Another geographic routing algorithm
- Like GEDIR, it is also based on greedy forwarding
  - Maintain a list of neighbors with their locations
  - Send the packet to the node nearest to the destination (Most Forward within Radiu – MFR)
  - Avoid routing loops

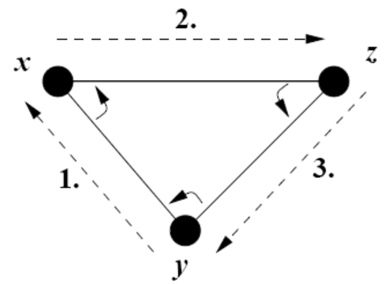


GPSR

- Avoiding routing gaps
  - Use perimeter routing
  - Mark the line connectir the intermediate node with destination
  - Take the hop to its imr (counter-clockwise)
  - Right hand rule!

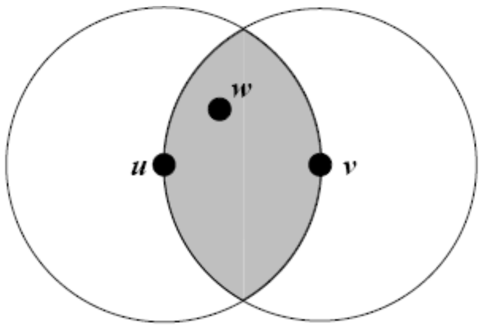




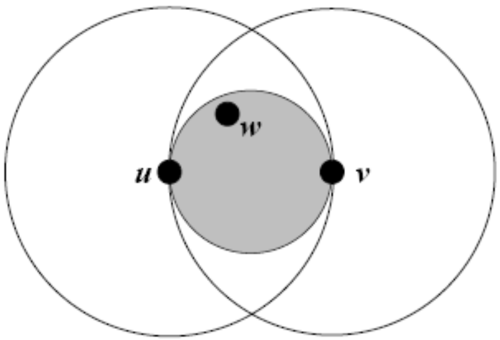


GPSR

- Perimeter routing requires that graphs are planar
  - No edge in the graph crosses another edge
- Planarization algorithms



Relative Neighbor Graph



Gabriel Graph

In both cases, eliminate link uv