WIRELESS NETWORKS

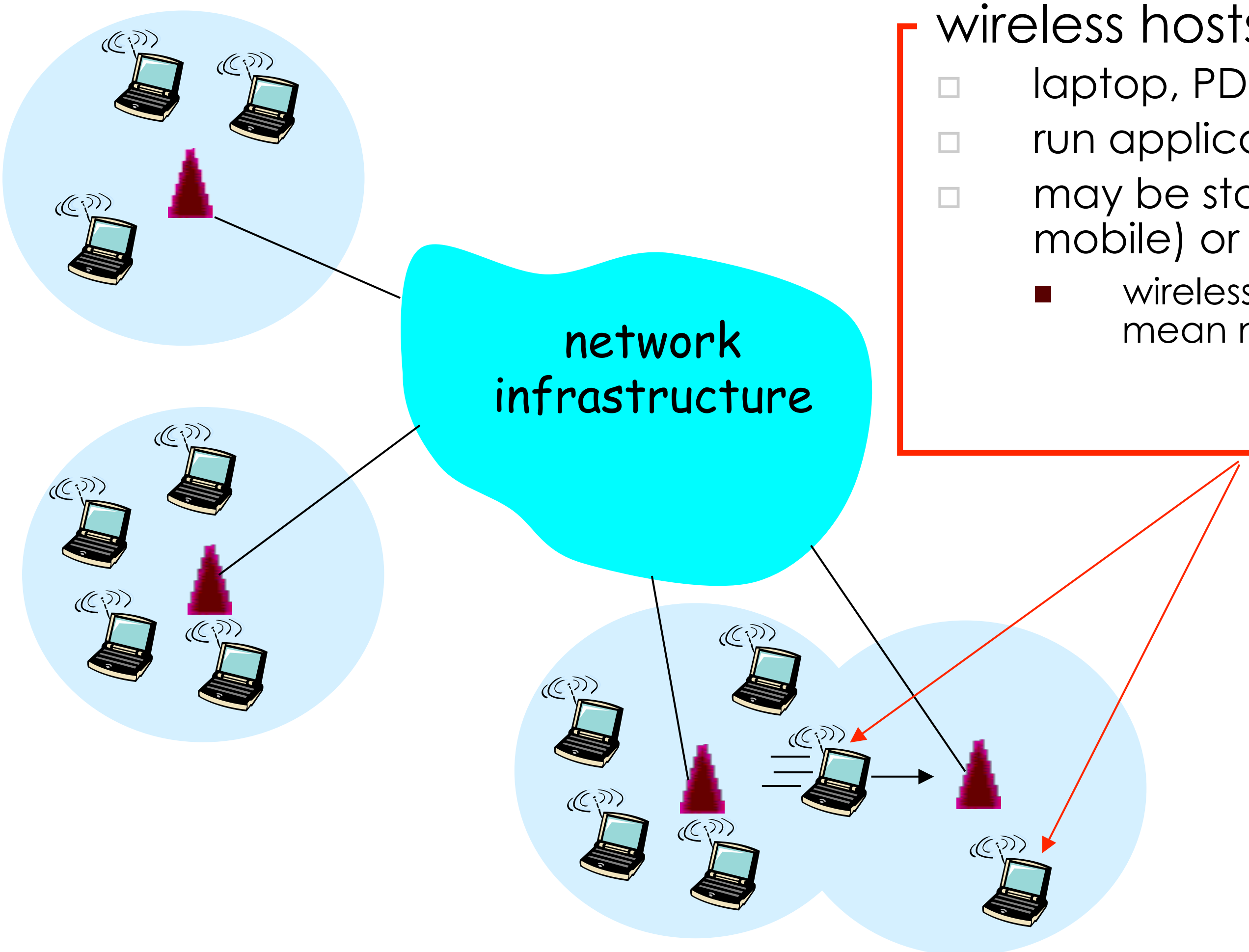
Outline

- Introduction
- CSMA/CA
- RTS/CTS
- Wi-Fi Direct

What is Wireless Networking?

- The use of infra-red (IR) or radio frequency (RF) signals to share information and resources between devices
- Promises *anytime*, *anywhere* connectivity
  - Laptops, PDAs, Internet-enabled phone
  - To make the connection of itinerant users easy, specially in collective spaces
  - Used to have a temporary connection (conference, meetings)
- Wireless is not intended to fully replace the hardwired cable (reliability, flow) : *Not used to connect servers!*
- Two important (but different) challenges
  - communication over wireless link
  - handling mobile user who changes point of attachment to network
- Examples
  - 802.11 (WiFi)
  - DECT (Digital Enhanced Cordless Telecommunications)
  - HiperLAN (High Performance Radio Local Area Network)
  - 802.15 (Bluetooth)
  - 802.16 (WiMax)

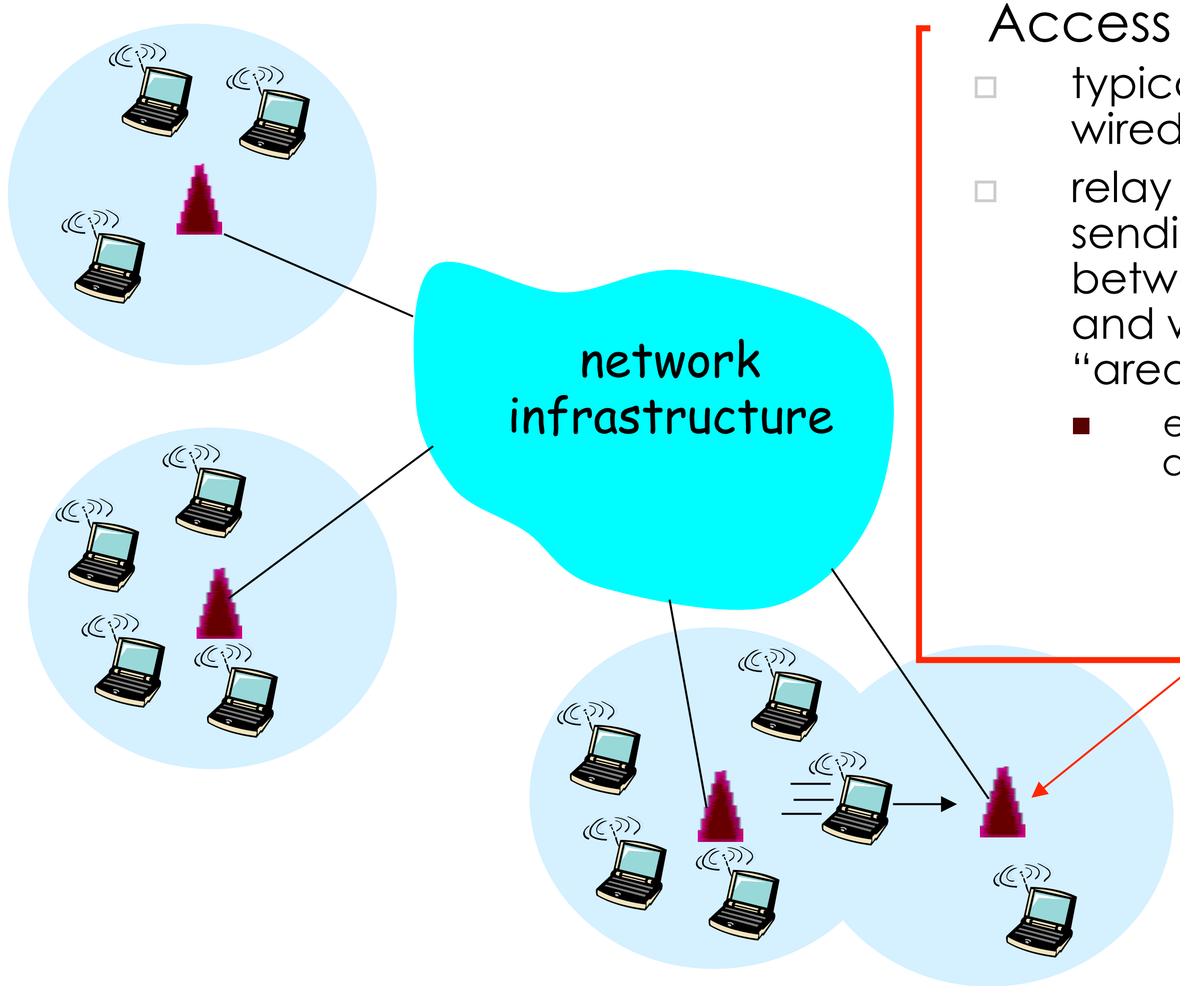
Elements of a wireless network



wireless hosts

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

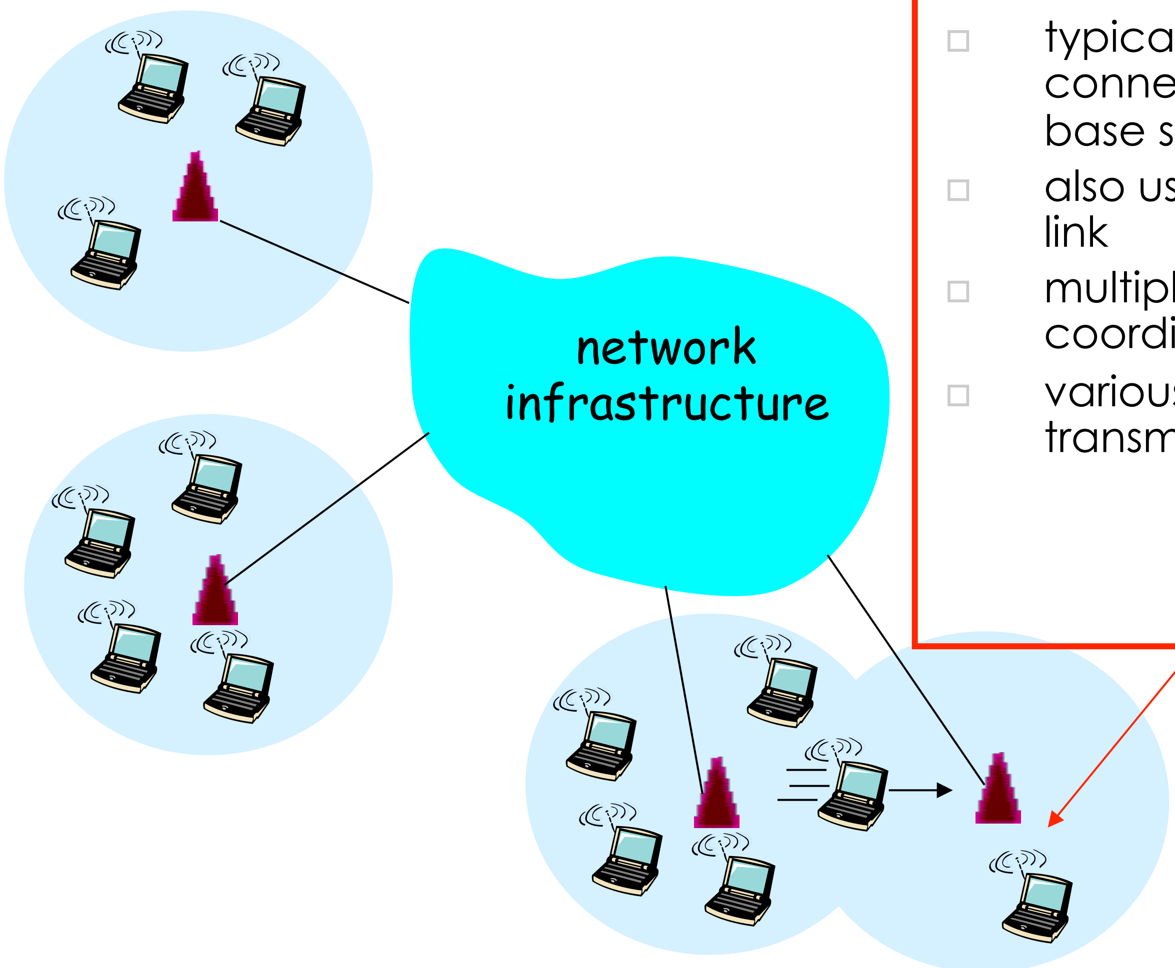
Elements of a wireless network



Access point

- 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

Wireless Link Characteristics

Differences from wired link ….

- Decreasing 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., microwave ovens use 2.43 GHz); cellular phones interfere as well
- Multi-path propagation: radio signal reflects off objects ground, arriving at destination at slightly different times

…. make communication across wireless link much more "difficult"

Two Popular 2.4 GHz, ISM band (Industrial, Scientific, Medicine) Standards

- IEEE 802.11
  - Fast (.11b)
  - High Power
  - Long range
  - Ethernet replacement
  - No exploitation license
  - Easily Available
    - Apple Airport, iBook
    - Cisco Aironet 350
- Bluetooth (802.15)
  - Slow
  - Low Power
  - Short range
  - Flexible
  - Cable replacement
  - No exploitation license

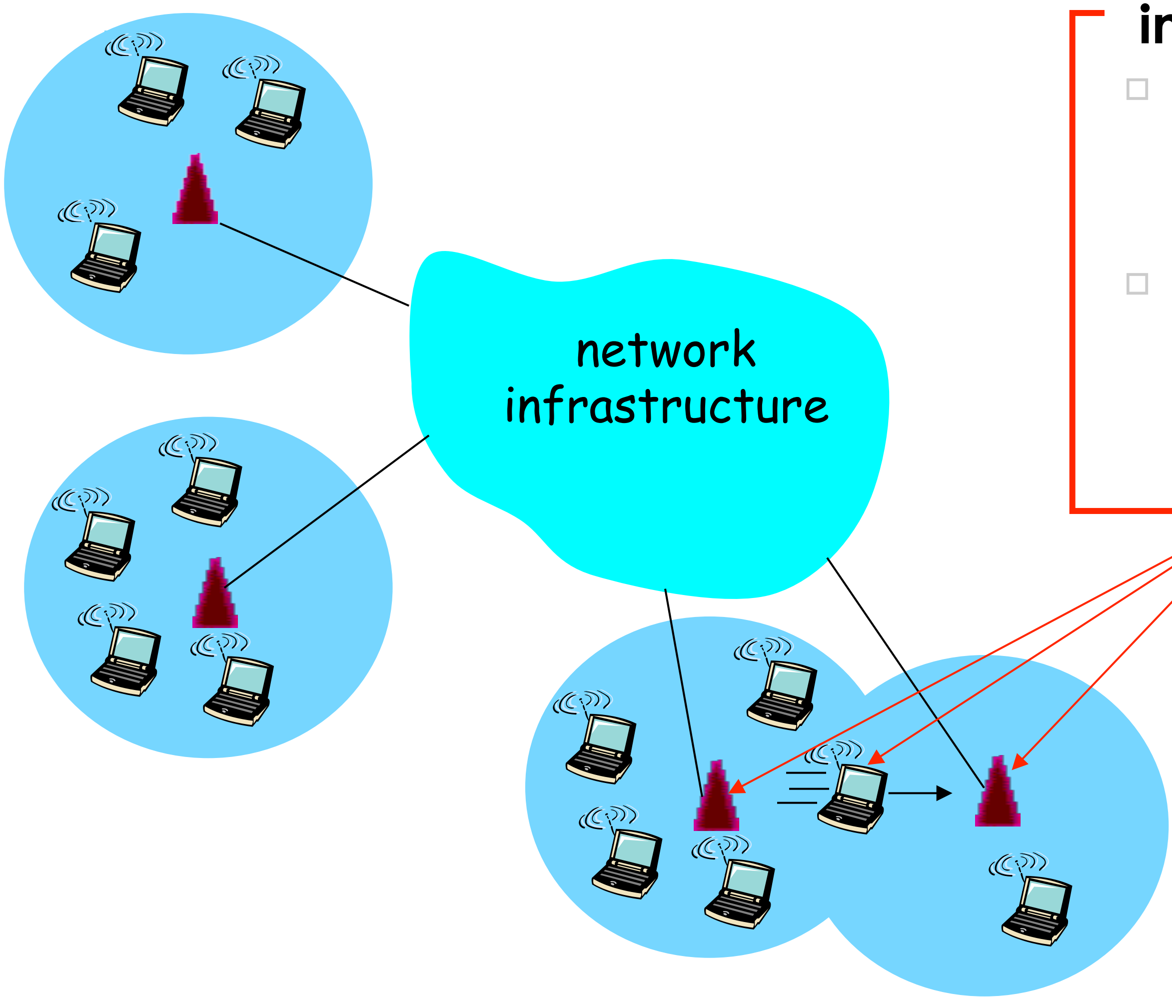
802.11 Normalization

- « Wi-Fi » an interoperability label delivered by the Wi-Fi alliance : group of constructors that publish lists of certified products (http://www.wi-fi.org/)
- 802.11 (1997) : up to 2 Mb/s
- 802.11 (1999) : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
- 802.11b (1999) : up to 11 Mb/s in the 2,4 GHz band
- 802.11a (1999) : up to 54 Mb/s in the 5 GHz band
- 802.11g (2003) : up to 54 Mb/s in the 2,4 GHz band
  - compatible with 802.11b
- 802.11f (2003) : Inter Access Point Protocol (IAPP) Mobility management

802.11 Normalization

- 802.11h (2003) : for the use of 802.11a in Europe: dynamic channel selection and transmission power management
- 802.11i (2004) : security
- 802.11e (2005) : quality of service
- 802.11r (2008) : fast transition between access points by redefining the security key negotiation protocol
- 802.11n (2009) : rate up to 600 Mb/s in 2,4 and 5 GHz bands
- 802.11ac (2012) : rate 2 Gb/s
- 802.11af (2014) : rate 10 Gb/s
- 802.11ah (2015) : long distance
- All use CSMA/CA for multiple access
- All have base-station and ad-hoc network versions

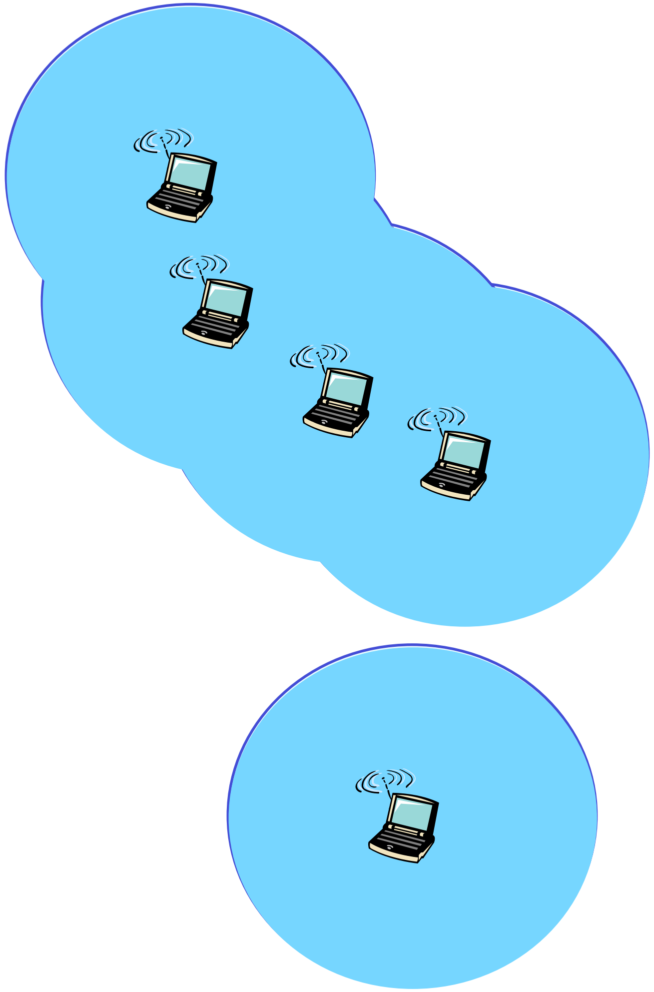
Infrastructure Mode (Access Point)



infrastructure mode

- Access point connects mobiles into wired network via a Distributed System (e.g. Ethernet).
- handoff: mobile changes access point providing connection into wired network

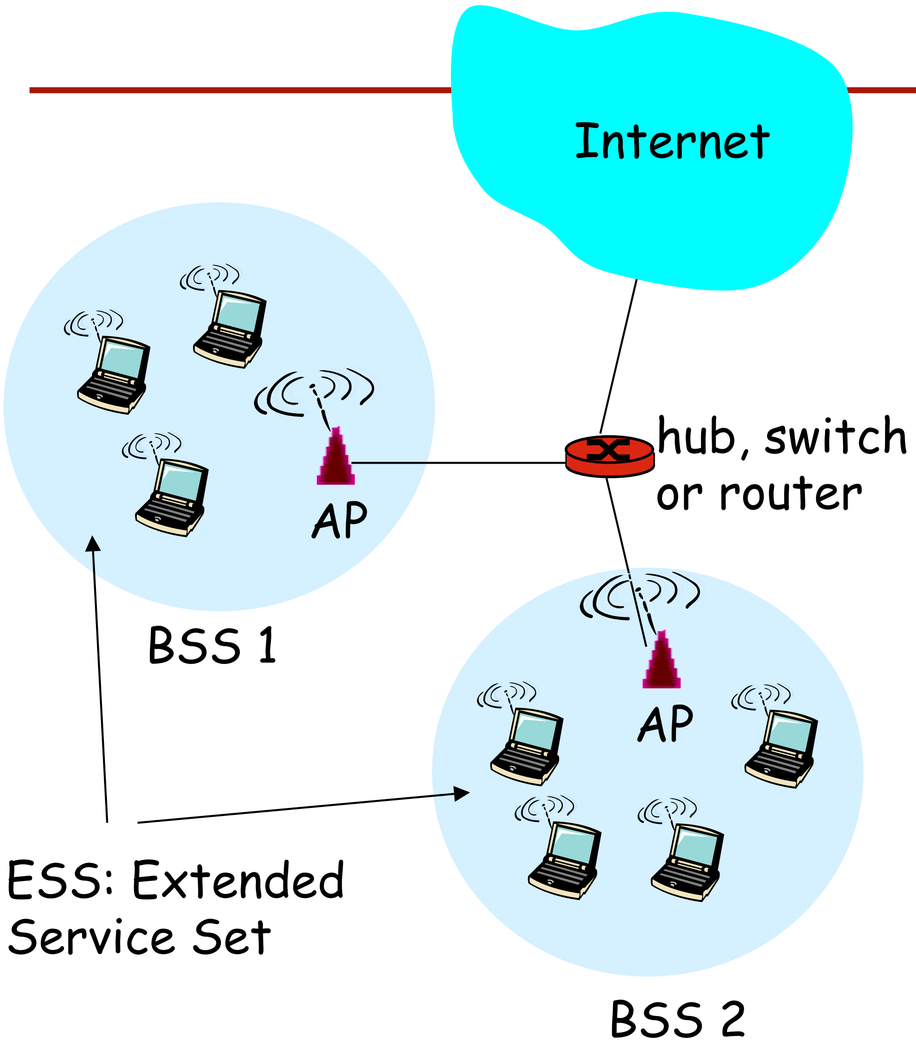
Ad hoc Mode



Ad hoc mode

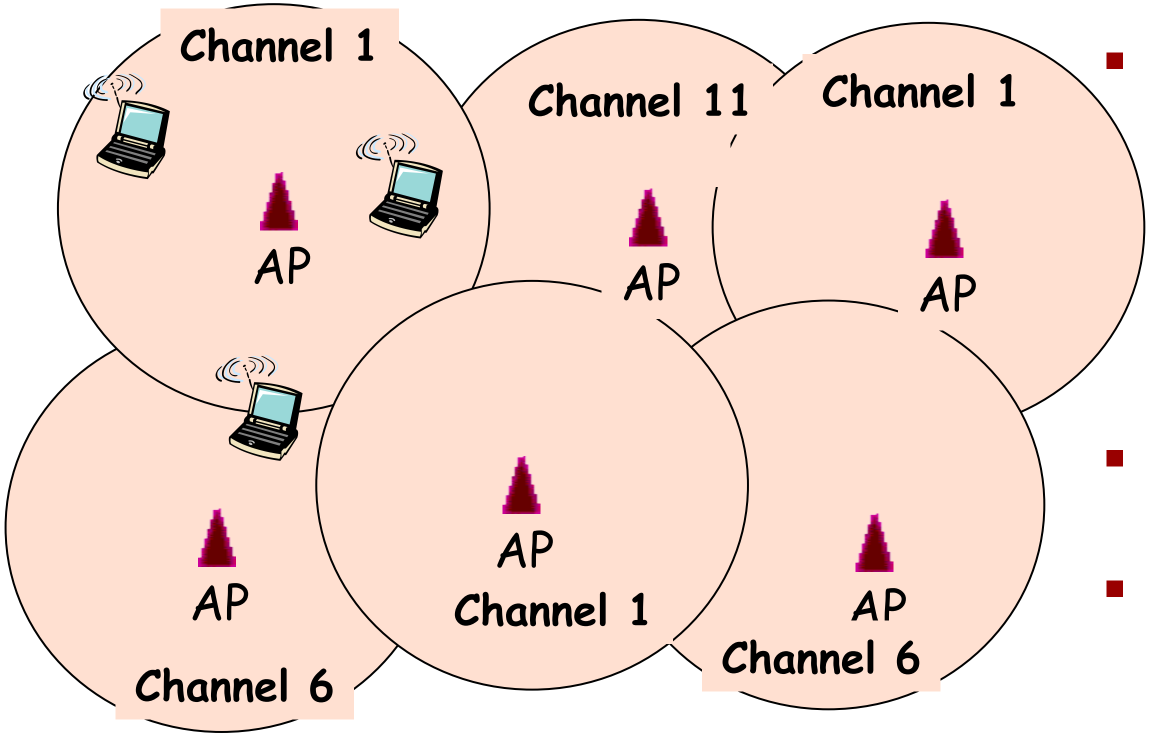
- No access point
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network
  - Need for a routing protocol within the nodes to route among themselves

802.11 LAN architecture



- wireless host communicates with access point
  - access point (AP) sends beacon frame periodically including the AP's Service Set Identifier (BSSID)
- Basic Service Set (BSS) in infrastructure mode contains
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

IEEE 802.11: Channels, association



- 802.11b has 11 channels. The 2.4 GHz spectrum is divided into 11 channels at different frequencies.
  - Channels 1, 6, and 11 are orthogonal
  - AP admin chooses frequency for AP
  - Interference possible: channel can be the same as that chosen by neighboring AP!
- Each AP coverage area is called a "cell"
- Wireless nodes can roam between cells

- Host: must *associate* with an AP
  - scans channels, listening for *beacon frames* containing AP's MAC@ (BSSID)
  - selects AP to associate with (may perform authentication)
  - will typically run DHCP to get IP address in AP's subnet

IEEE 802.11: data rate

802.11a	Data Rate	Range	Receiver Sensitivity
Max Tx Power is 40mW	6 Mbps	610 ft (186 m)	-89 dBm
	9 Mbps	610 ft (186 m)	-88 dBm
	12 Mbps	558 ft (170 m)	-86 dBm
	18 Mbps	541 ft (165 m)	-85 dBm
	24 Mbps	508 ft (155 m)	-82 dBm
	36 Mbps	426 ft (130 m)	-80 dBm
	48 Mbps	328 ft (100 m)	-76 dBm
	54 Mbps	295 ft (90 m)	-74 dBm
802.11g	**Data Rate**	**Range**	**Receiver Sensitivity**
Max Tx Power is 40mW	6 Mbps	722 ft (220 m)	-90 dBm
	9 Mbps	656 ft (200 m)	-89 dBm
	12 Mbps	623 ft (190 m)	-87 dBm
	18 Mbps	623 ft (190 m)	-85 dBm
	24 Mbps	623 ft (190 m)	-82 dBm
	36 Mbps	492 ft (150 m)	-78 dBm
	48 Mbps	410 ft (125 m)	-74 dBm
	54 Mbps	394 ft (120 m)	-73 dBm
802.11b	**Data Rate**	**Range**	**Receiver Sensitivity**
Max Tx Power is 50mW	1 Mbps	1,027 ft (313 m)	-95 dBm
	2 Mbps	951 ft (290 m)	-89 dBm
	5.5 Mbps	853 ft (260 m)	-89 dBm
	11 Mbps	787 ft (240 m)	-85 dBm

Source : cisco

IEEE 802.11: multiple access

- Medium Access Control divided into two parts
  - Distributed Coordination Function (DCF)
    - Symmetric, all stations (including APs) behave the same way
    - Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
    - Stations contend for access to medium
  - Optional Point Coordination Function (PCF)
    - Built on top of DCF
    - Allows periods of contention-free operation interleaved with periods of contention
    - One station (typically AP) polls others to control who transmits
    - Permits more efficient operation under heavy loads

IEEE 802.11: MAC protocol design

- 802.11: CSMA - sense before transmitting
  - don't collide with ongoing transmission by another node
- 802.11: *no* collision detection!
  - difficult to receive (sense collisions) when transmitting
  - If a collision happens, the station continues to transmit the whole frame: network performance loss
  - can't sense all collisions in any case: hidden terminal
  - goal: *avoid collisions:* CSMA/C(ollision)A(voidance)
  - Stations choose a random backoff interval before colliding! (Compare to CSMA/CD: backoff only after colliding)

IEEE 802.11: Basic DCF MAC Protocol

- Reliable data delivery using a frame exchange protocols at the MAC level: use of ACK frames
  - ACK sent by the destination station to confirm the reception of the data
- Avoids collisions using IFS (Inter-Frame Spacing)
  - Time interval between the transmission of 2 frames
  - IFS Intervals = periods of inactivity on the transmission medium
  - There are several types of IFS
  - 3 Timer types
    - SIFS (Short Interframe Space): used to separate transmissions in the same dialog (e.g., fragment – ACK). Value: e.g. 28 μs
    - PIFS (PCF Interframe Space): used by the AP to gain access to the medium before any other station. This value is SIFS + TimeSlot (e.g. 50 µs) = 78 μs
    - DIFS (DCF Interframe Space): Inter-frame space used when the station wants to start a new transmission. Value: PIFS + TimeSlot = 128 μs

Medium Listening

- Terminals of a same BSS can listen to the activity of all the stations in that same BSS thanks to the other stations' signal relative power
- When a station sends a frame
  - The remaining stations update their NAV (Network Allocation Vector) timer
  - NAV allows to delay all scheduled transmissions
  - NAV is calculated based on the information of the *duration* field in the sent frames

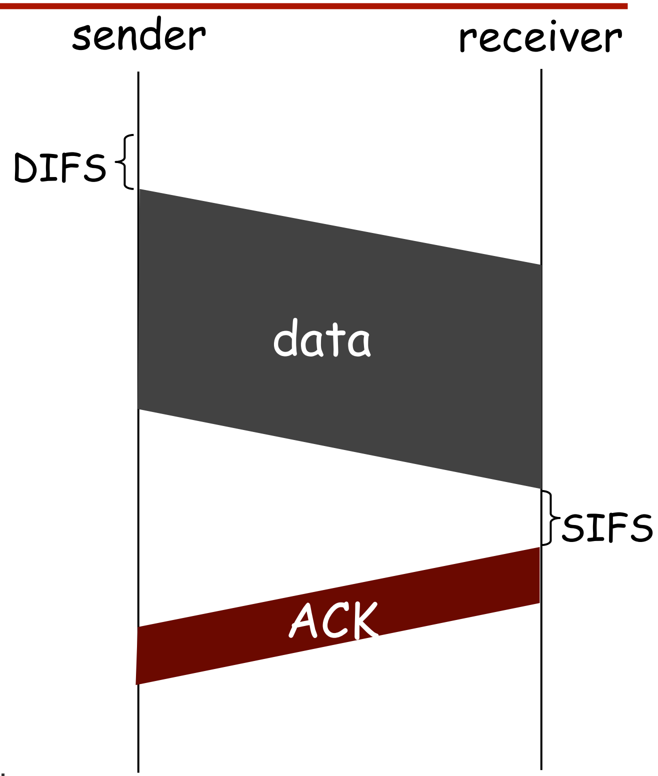
IEEE 802.11 DCF MAC Protocol: CSMA/CA

802.11 sender

1 if sense channel idle for **DIFS** then
transmit entire frame

2 if sense channel busy then
Listen until it is free (thanks to NAV)
When medium free for DIFS, start random backoff time
Timer counts down while channel idle
Transmit when timer expires

3 if no ACK, increase random backoff interval, repeat 2



802.11 receiver

- if frame received OK (verification of the frame CRC)

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

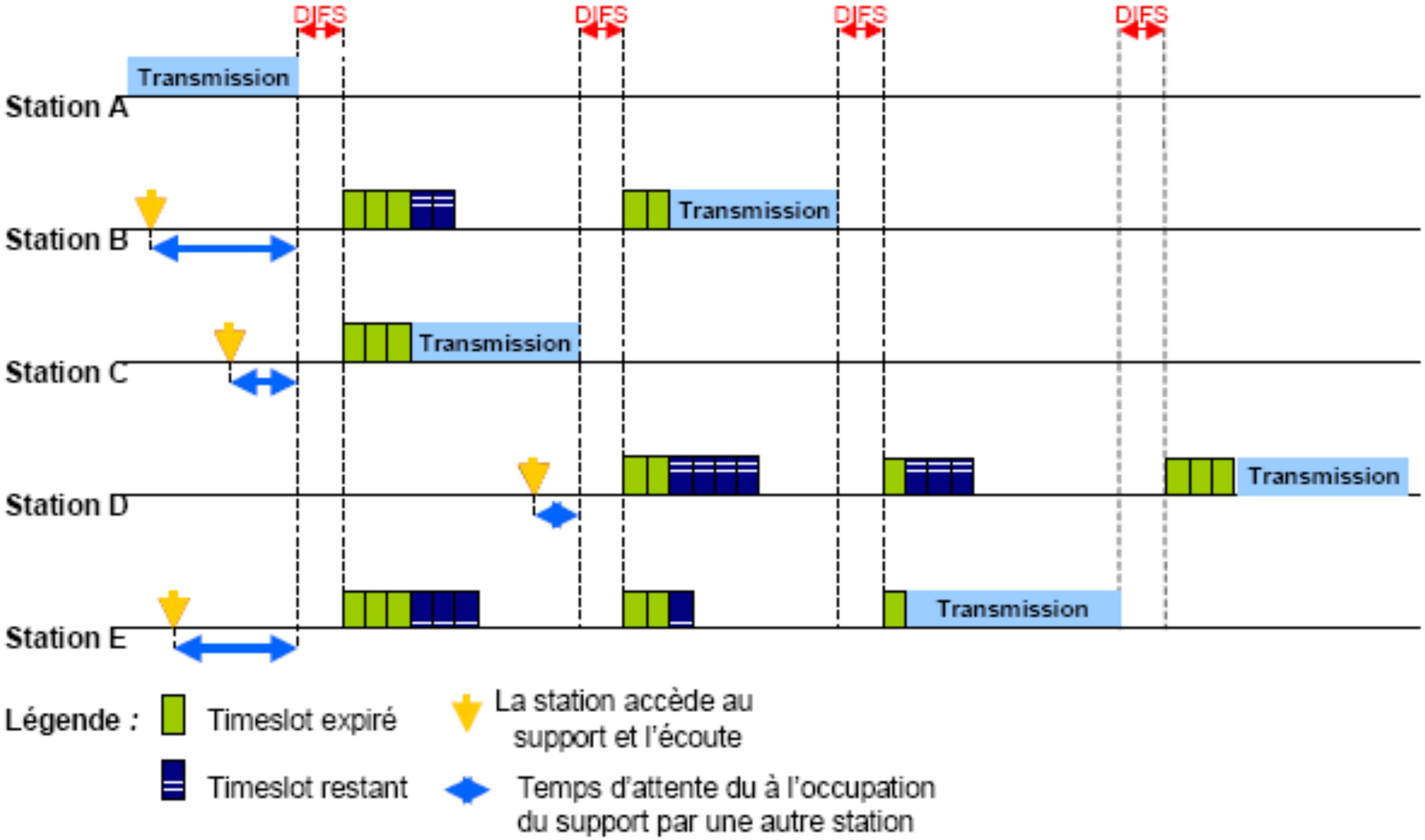
- if the ACK is not detected, or DATA is corrupted

collision is happened, retransmission of the frame

Backoff algorithm

- Allow to solve the medium accessing problem when several stations intend to transmit data at the same time
- Time is divided into TimeSlots (TS = 50 μs). It is used to define the IFS intervals.
- Principle
  - Initially, a station calculates the timer value = timer backoff, included between 0 and 7 (i.e., a certain number of timeslots)
  - When the medium is free, stations decrement their timers until the medium is busy or that the timer reaches 0
  - If the timer did not reach 0 and that the medium is busy again, the station blocks (freezes) the timer
  - When the timer reaches 0, the station transmits its frame
  - If 2 or several stations reach 0 at the same time, a collision happens and each station has to regenerate a new timer, included between 0 and 15
  - For each retransmission attempt, the timer increases as follows : $[2^{2+i} * randf()] * TS$
    - i corresponds to the number of successive attempts, randf() is a uniform random variable that returns values between 0 and 1.
    - The size of the Contention Window (CW) starts with CWmin = 8 and is doubled with each collision up to CWmax = 256.

Backoff algorithm



Backoff algorithm

- Stations have the same probability to access the medium because each station, after each retransmission, has to reuse the same algorithm
- Disadvantage: no guarantee on the minimum delay
  - Make the integration of real time applications, such as voice and video, more complicated

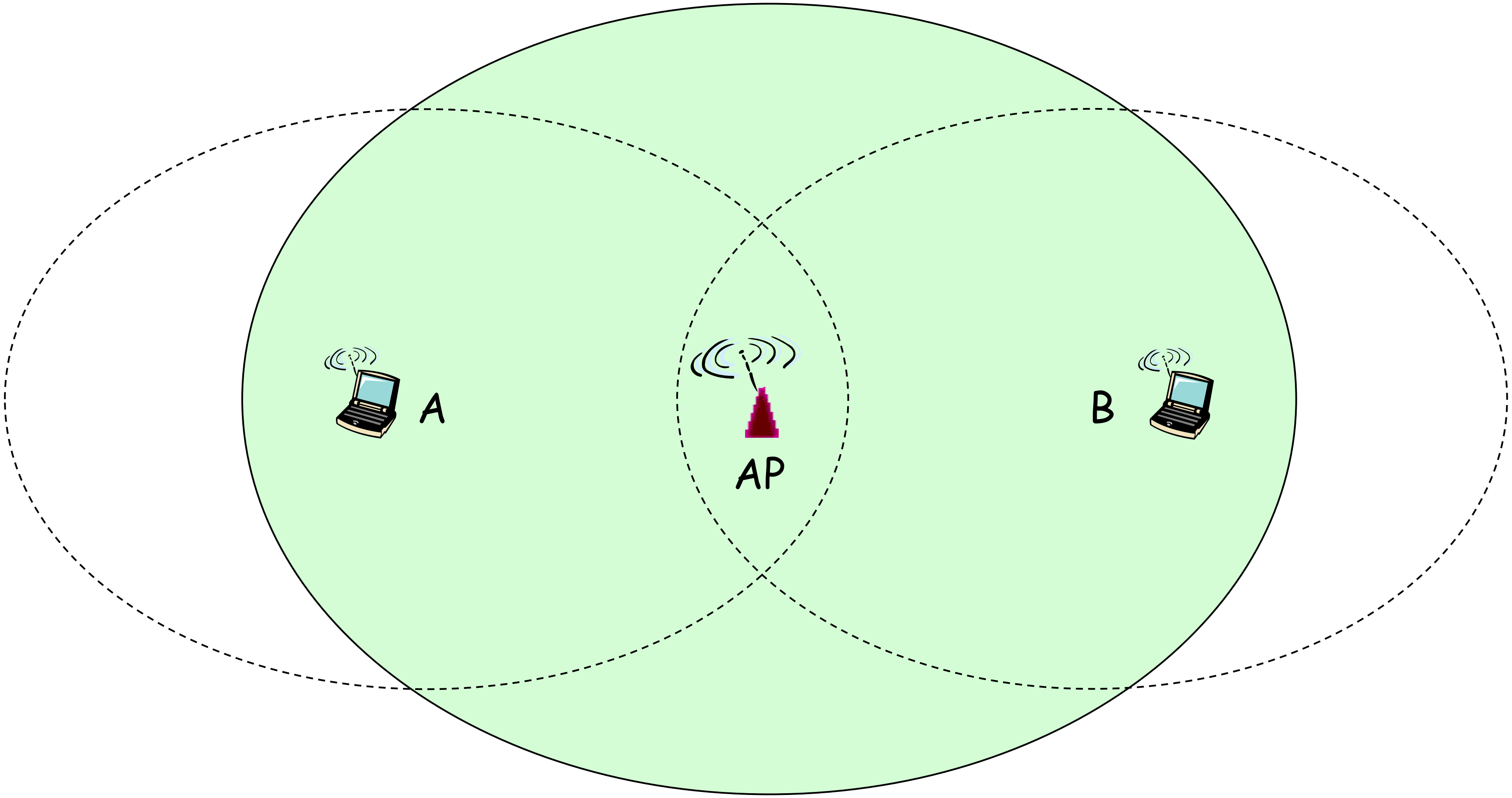
Avoiding collisions (more)

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

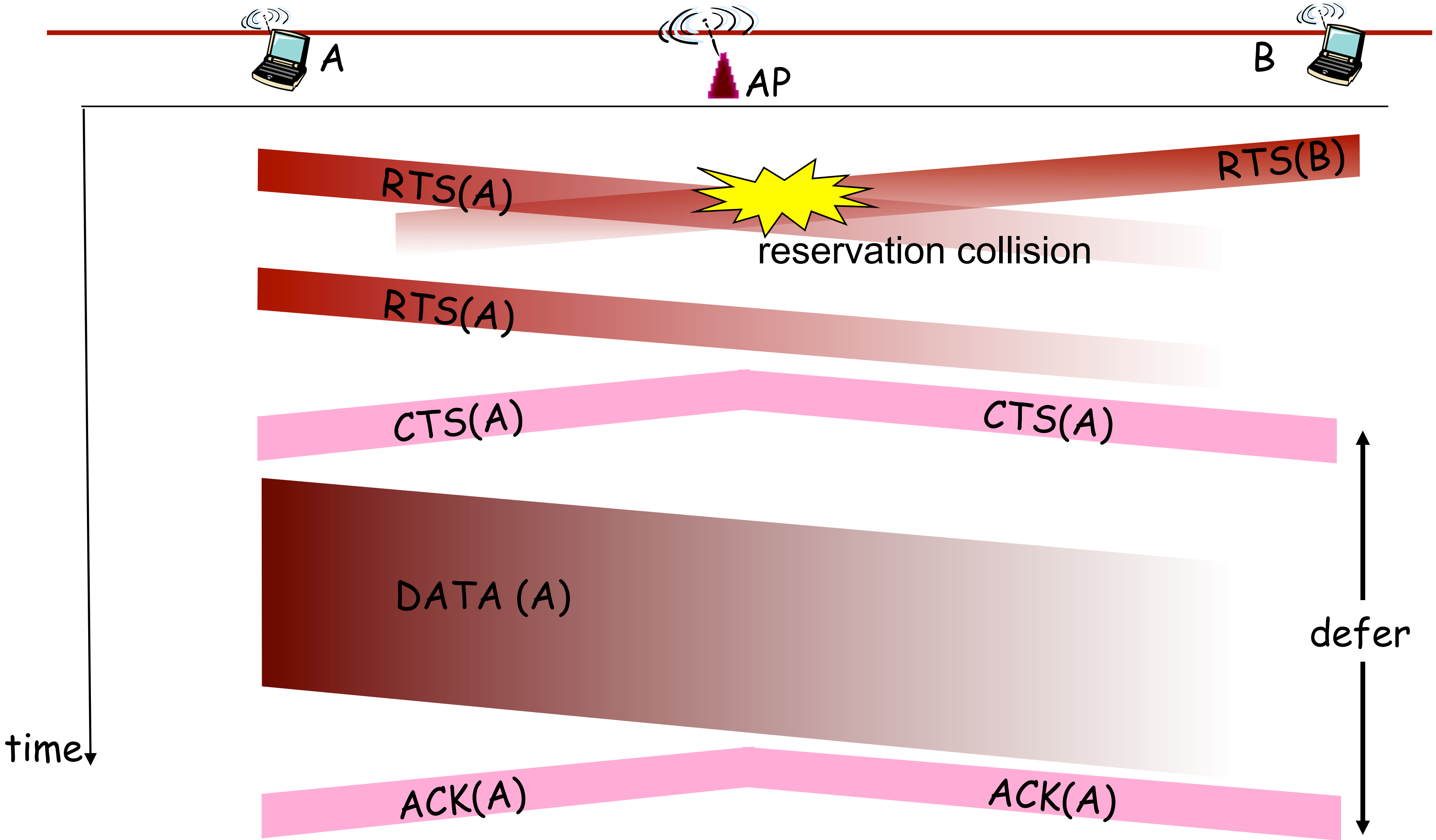
- sender first transmits *small* request-to-send (RTS) packets to AP using CSMA
  - RTSs may still collide with each other (but they're short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions by reading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

Avoid data frame collisions completely using small reservation packets!

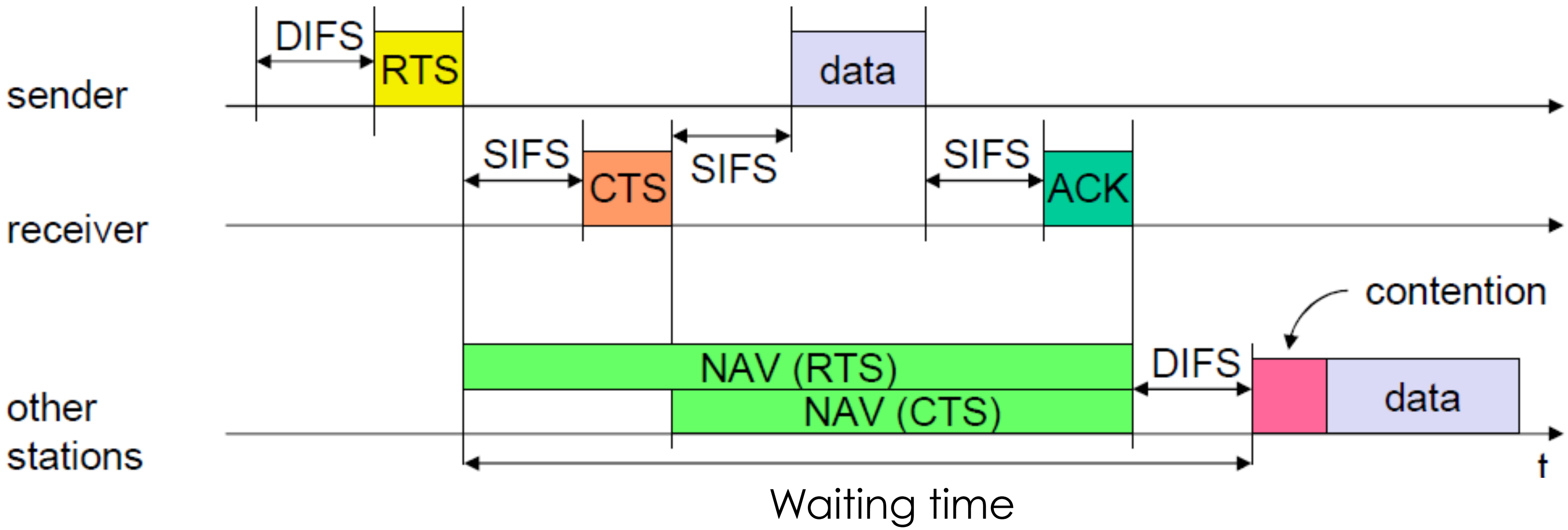
Hidden station problem



Hidden station problem solving: RTS-CTS exchange

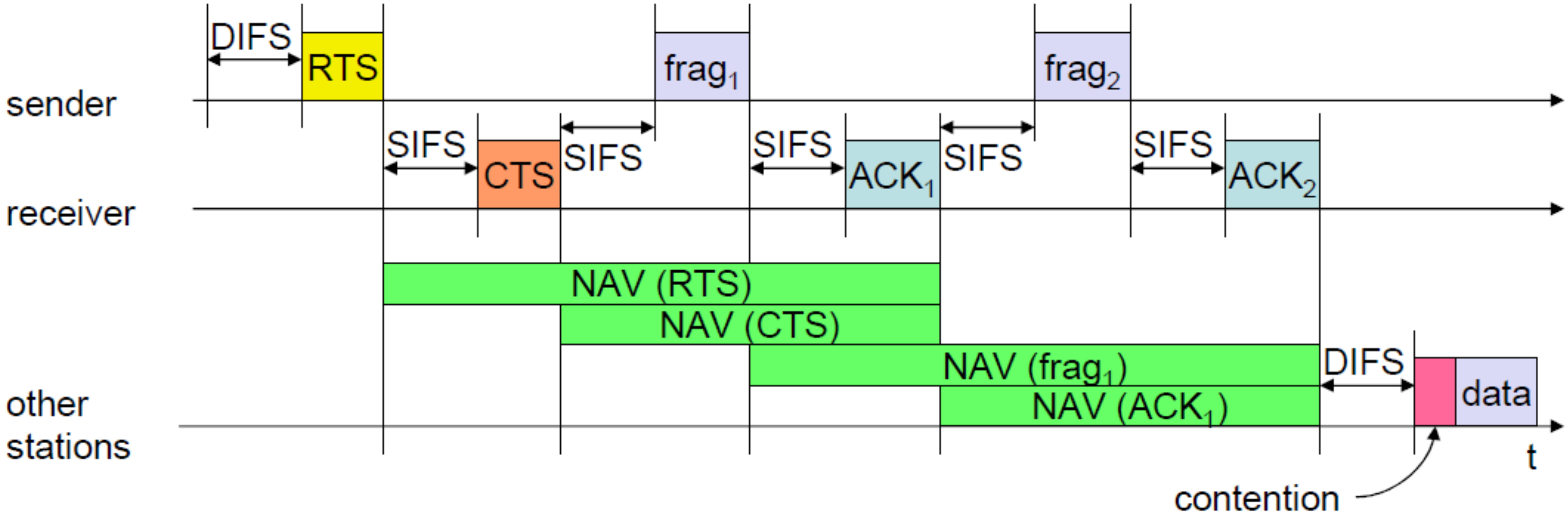


Collision Avoidance: reservation mechanism



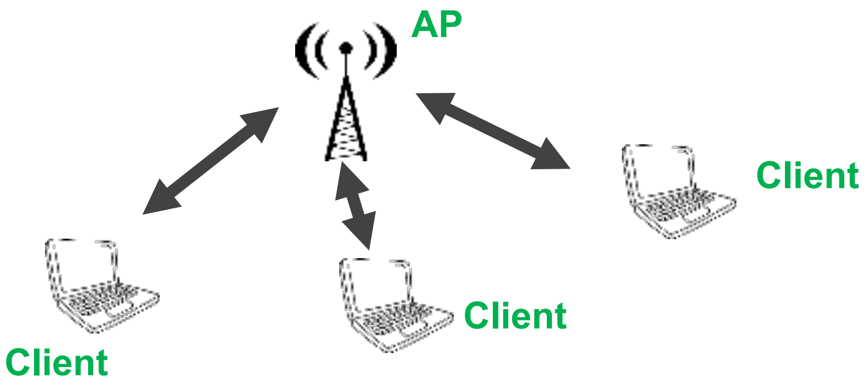
Collision Avoidance: fragmentation

- Fragmenting data can decrease the damage caused by transfer errors
- First fragment: normal reservation with RTS/CTS
- Fragments and ACKs (except the last) contain reservation durations

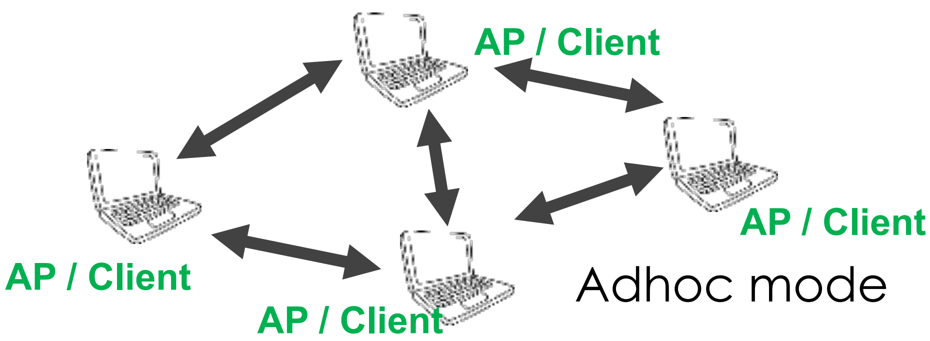


Wi-Fi Direct

- WiFi-Direct is a new operation mode in Wi-Fi networks

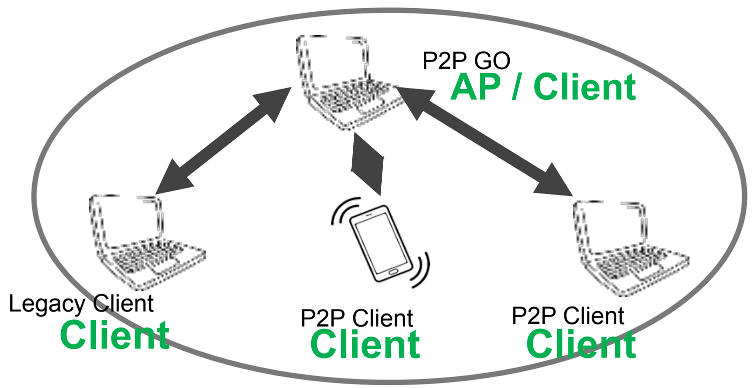


Infrastructure mode



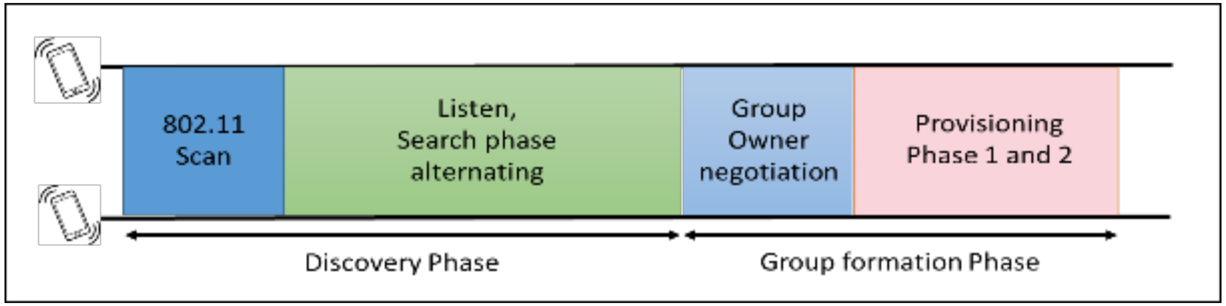
Adhoc mode

WiFi-Direct mode

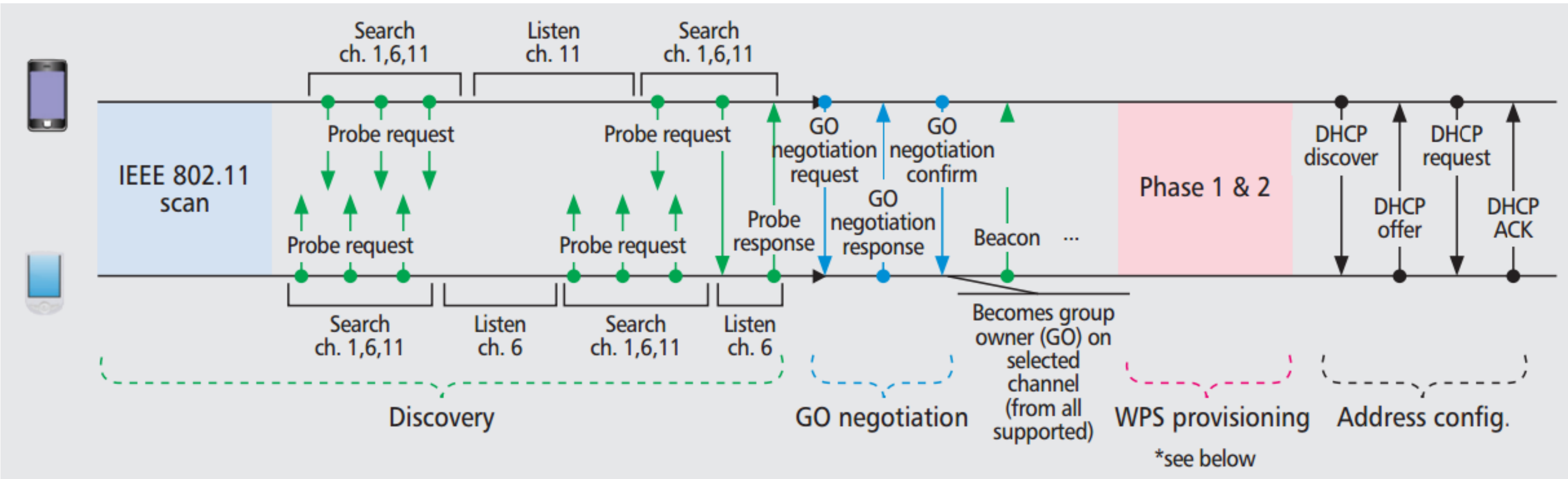


P2P Group

Group formation



- 3 cases
  - Standard
  - Autonomous
  - Persistent



GO Negotiation

- Device declaring the highest *GO Intent* value becomes P2P GO