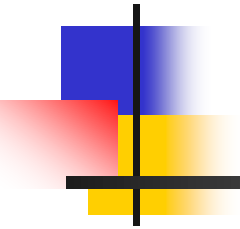
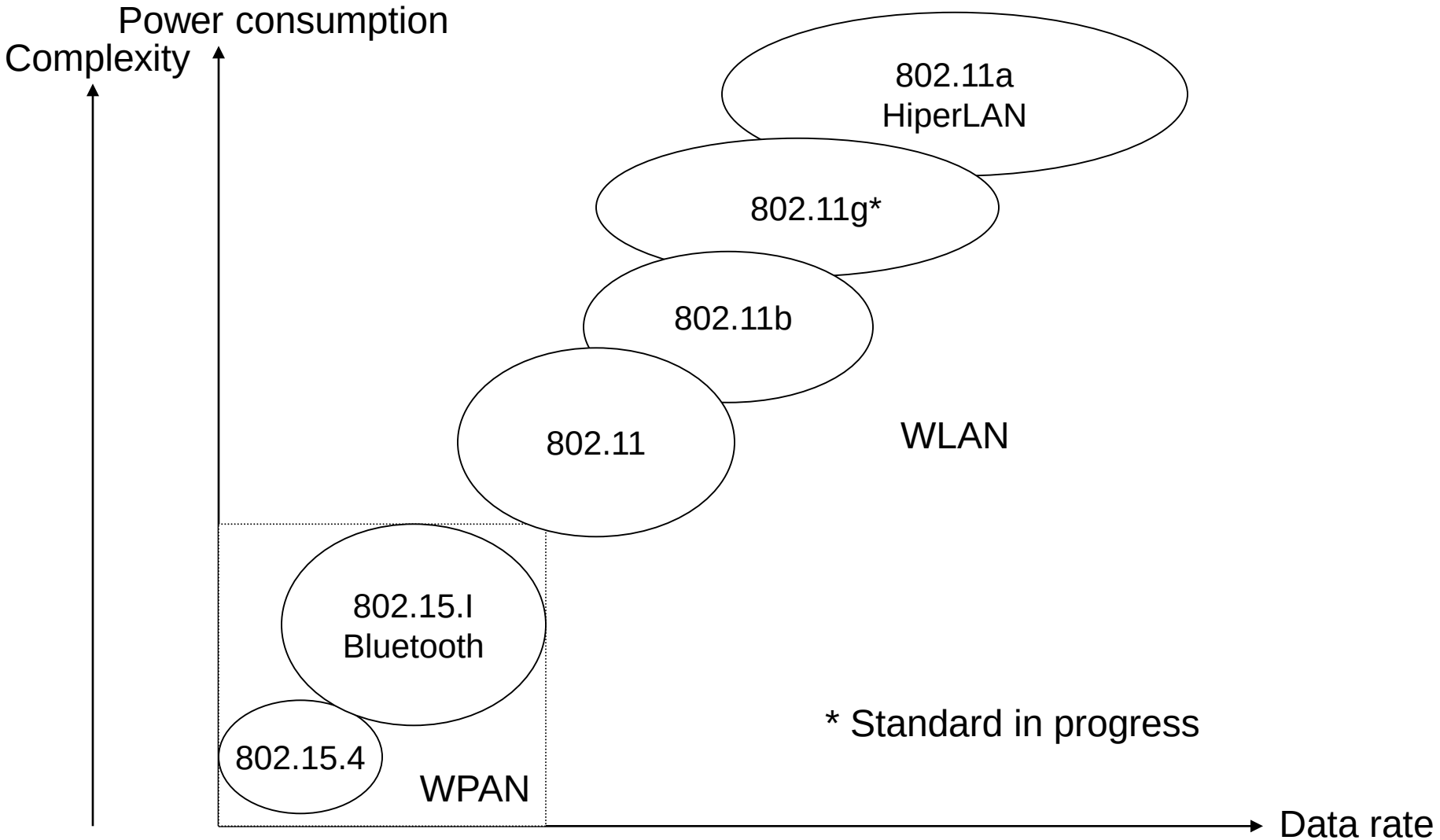


Wireless LANs
IEEE 802.11 (Wi-Fi)

Outline

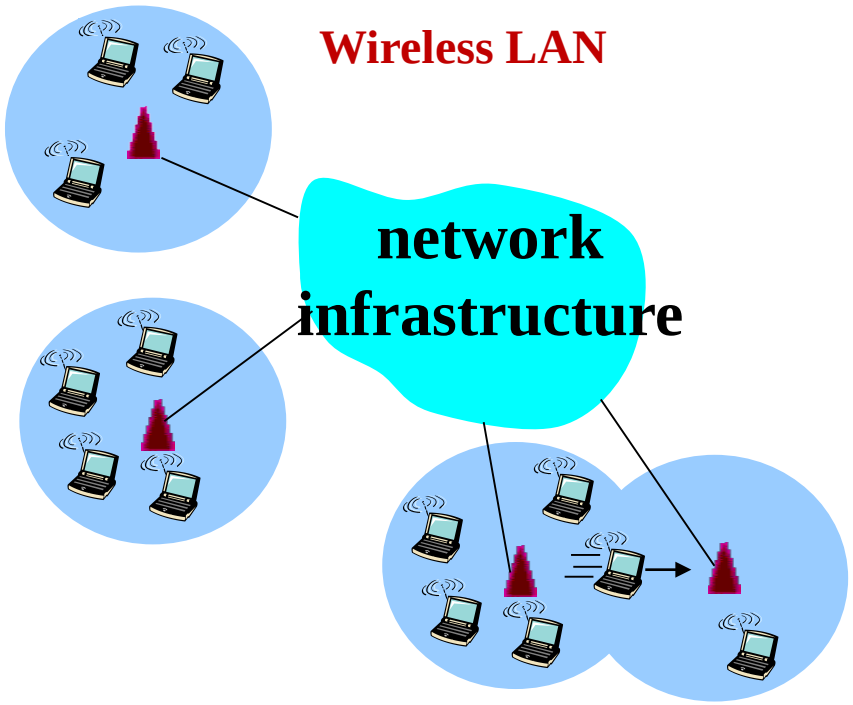
- Wireless Local Area Network (LAN) basis
- Infrastructure and ad hoc modes
- Association of a host to AP
- Media Access Control (MAC)
  - DCF's Basic Access mode
  - DCF's RTS/CTS mode
- AP Placement

Scope of Various WLAN and WPAN Standards



Wireless Local Area Network (WLAN)

- Provide access to wired LANs and the Internet
- Operate in a local area
  - less than 100 m
- Provide high data rates
  - currently, up to 54 Mbps
- Main Standard is IEEE 802.11

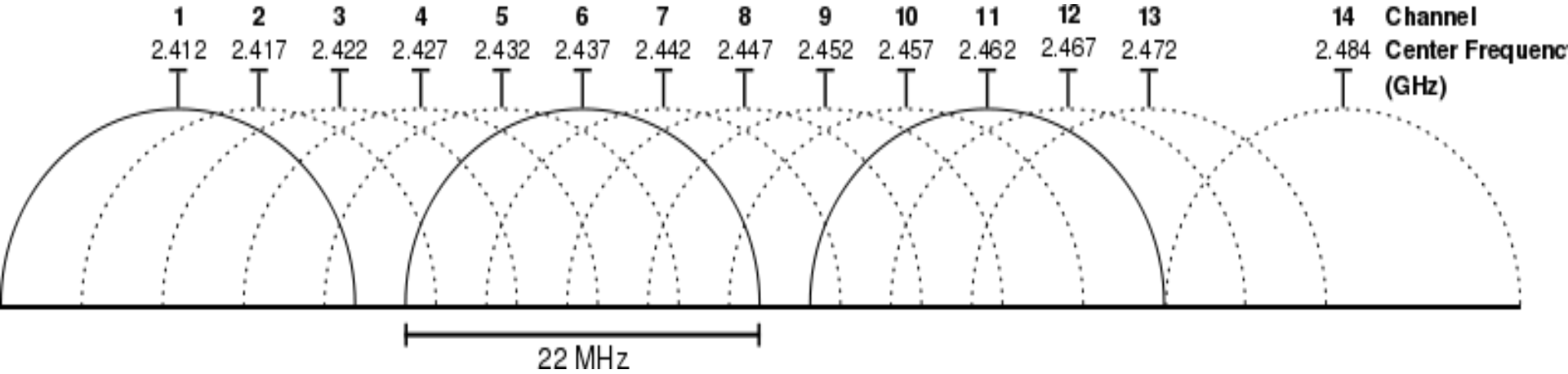


Wireless LAN: IEEE 802.11 Family

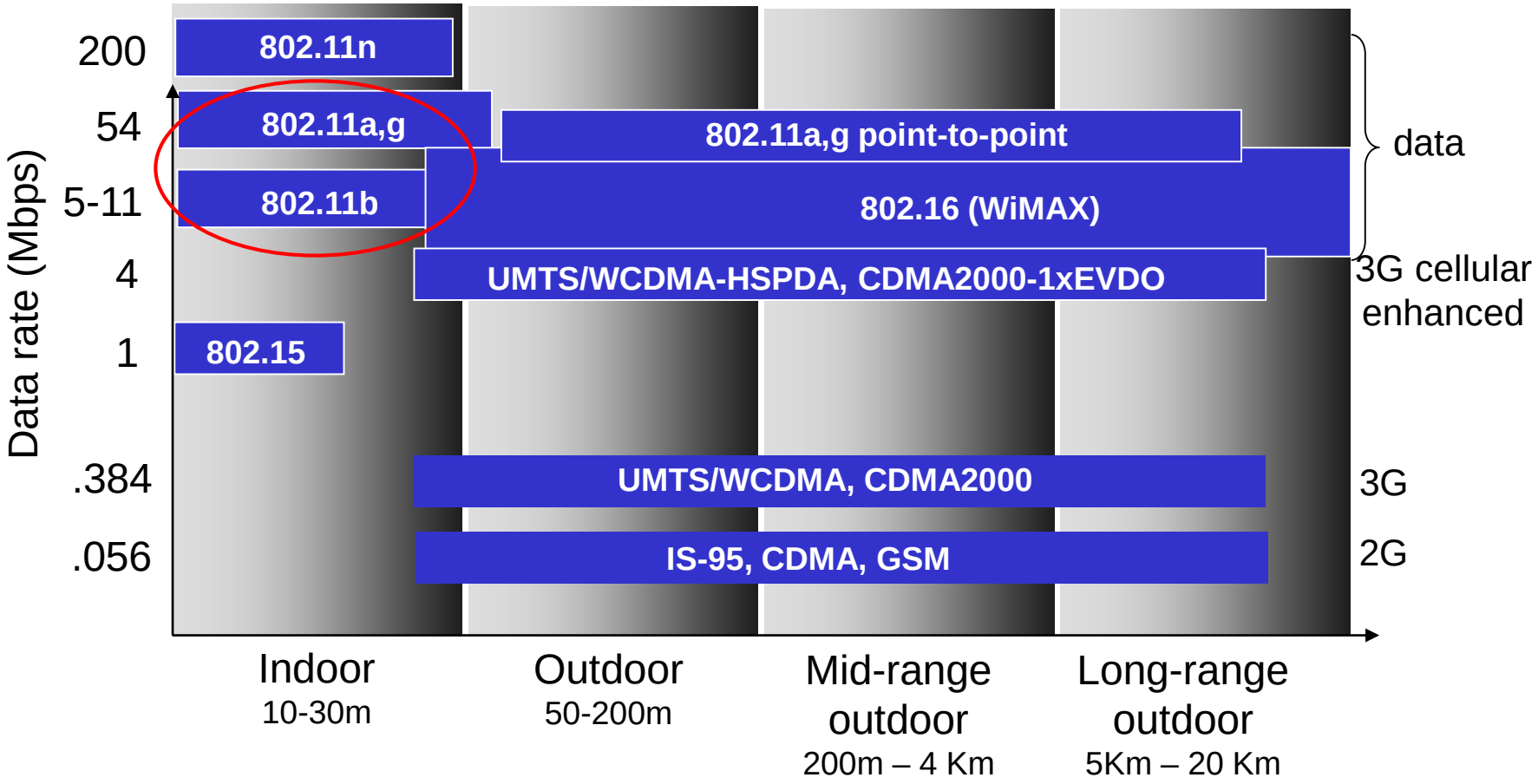
- 802.11b (Wi-Fi Alliance)
  - 2.4 GHz range
  - up to 11 Mbps
- 802.11a
  - 5-6 GHz range
  - up to 54 Mbps
- 802.11g
  - 2.4 GHz range
  - up to 54 Mbps
- 802.11n
  - 2.4 GHz range
  - up to 200 Mbps

- All use CSMA/CA for multiple access
- All have both infrastructure and ad-hoc network modes

WiFi Channels in 2.4 GHz Frequency Band



Transmission Distance and Data Rate of Wireless Standards

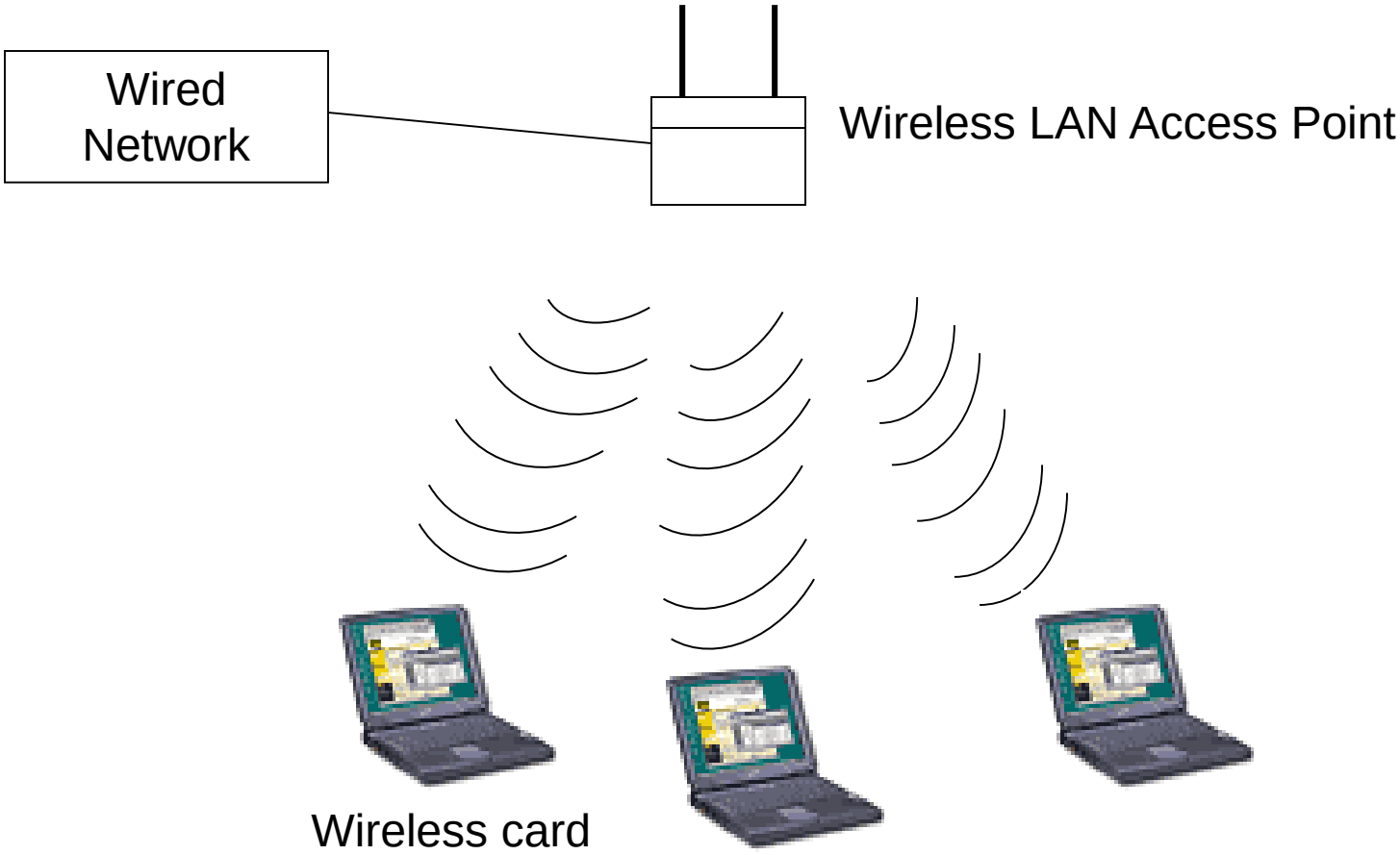


Two Modes of IEEE 802.11 Wireless LANs

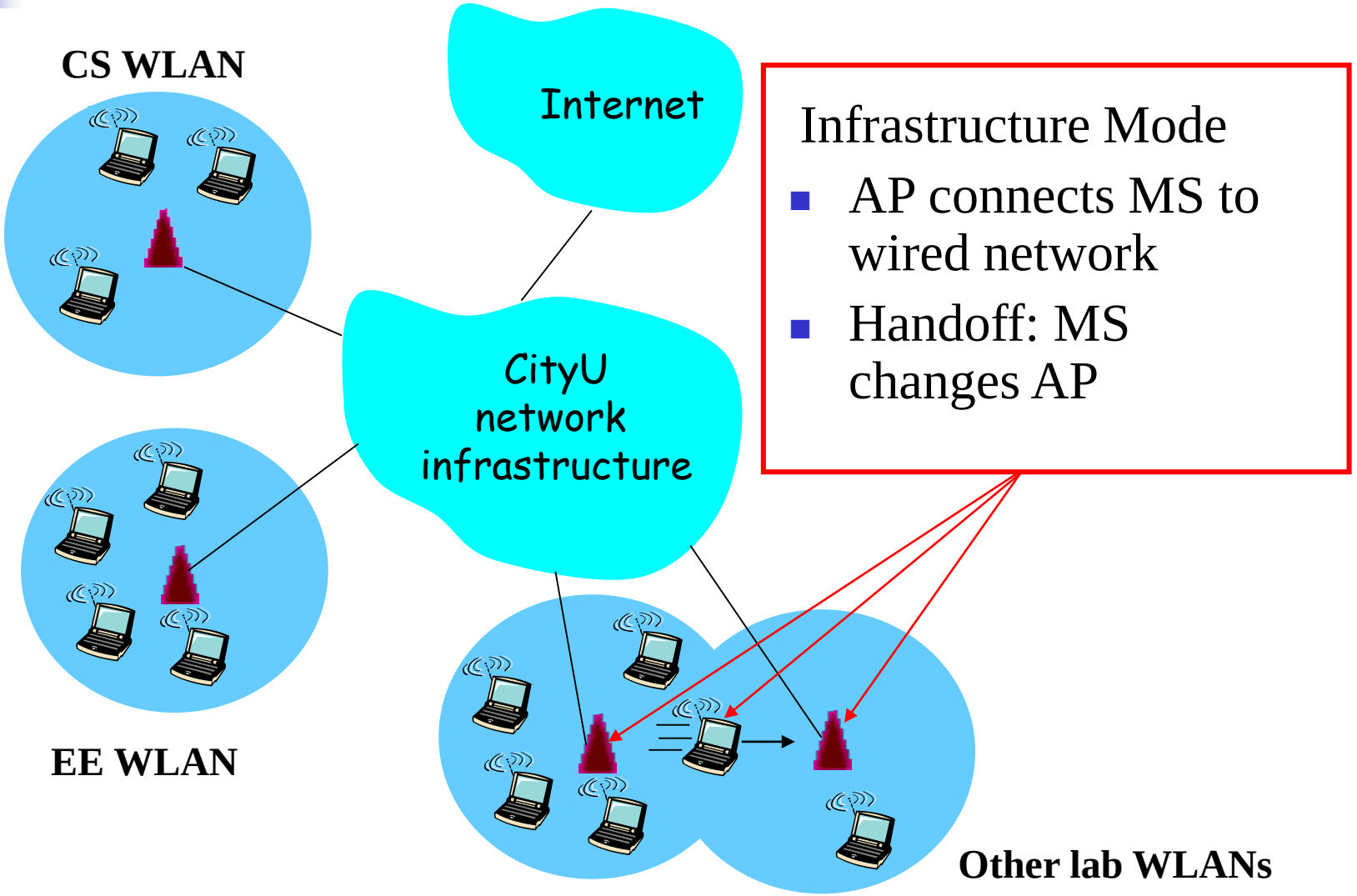
- Infrastructure Mode
  - Wireless hosts communicate to an access point (AP), which typically connects to wired networks.
  - AP is responsible for sending packets between wired networks and wireless hosts in its area.

- Ad Hoc Mode
  - Wireless hosts communicate in a peer-to-peer basis without any access point (AP).

Infrastructure Mode



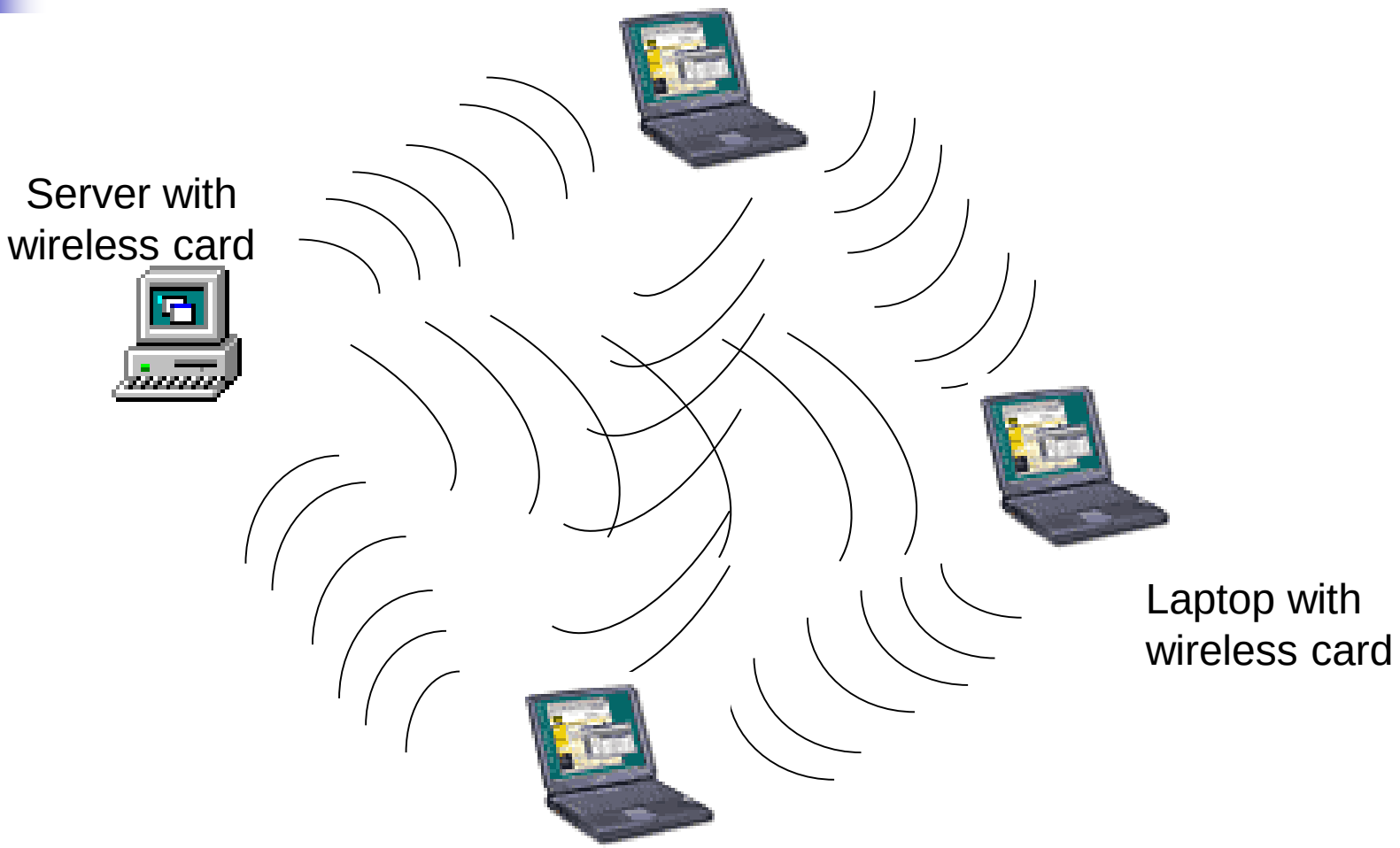
802.11 - Infrastructure Mode



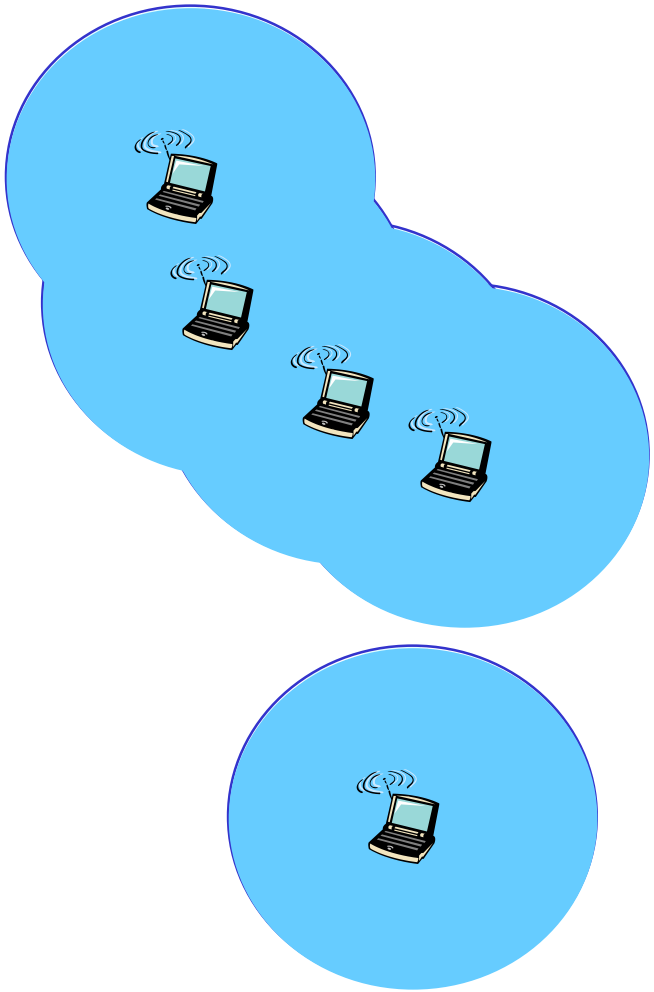
Infrastructure Mode

- AP connects MS to wired network
- Handoff: MS changes AP

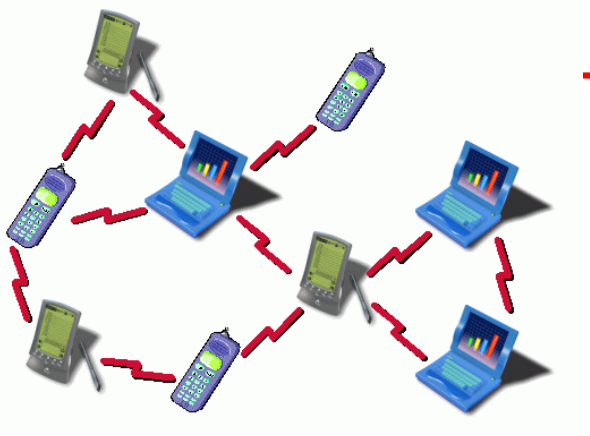
Ad Hoc (Peer-to-Peer) Mode



802.11 - Ad Hoc Mode



- No infrastructure (no AP)
- A node can directly communicate with other nodes within its signal range
- Nodes organize themselves into a network: route among themselves



Summary of infrastructure and ad hoc modes

infrastructure	MSs connect to APs (e.g., WiFi, WiMAX, cellular) that are further connected to the Internet
no infrastructure	No AP, no connection to the Internet (e.g., Bluetooth, ad hoc networks)

Q: How does your MS join a network?

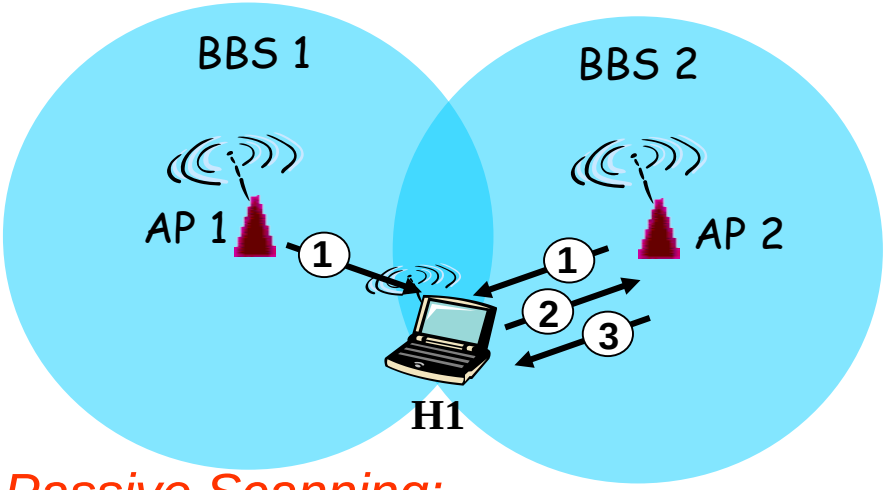
Infrastructure Mode

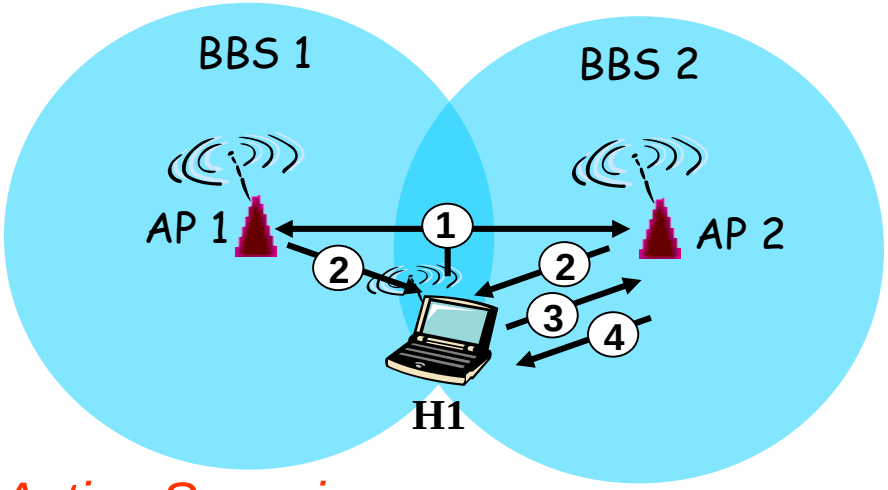
Steps to Join a Network

Steps for a mobile host to join a network:

1. Discover available networks
2. Select a network
3. Authentication
4. Association (registration)

1. Discovering Available Networks
802.11: passive/active scanning





Passive Scanning:

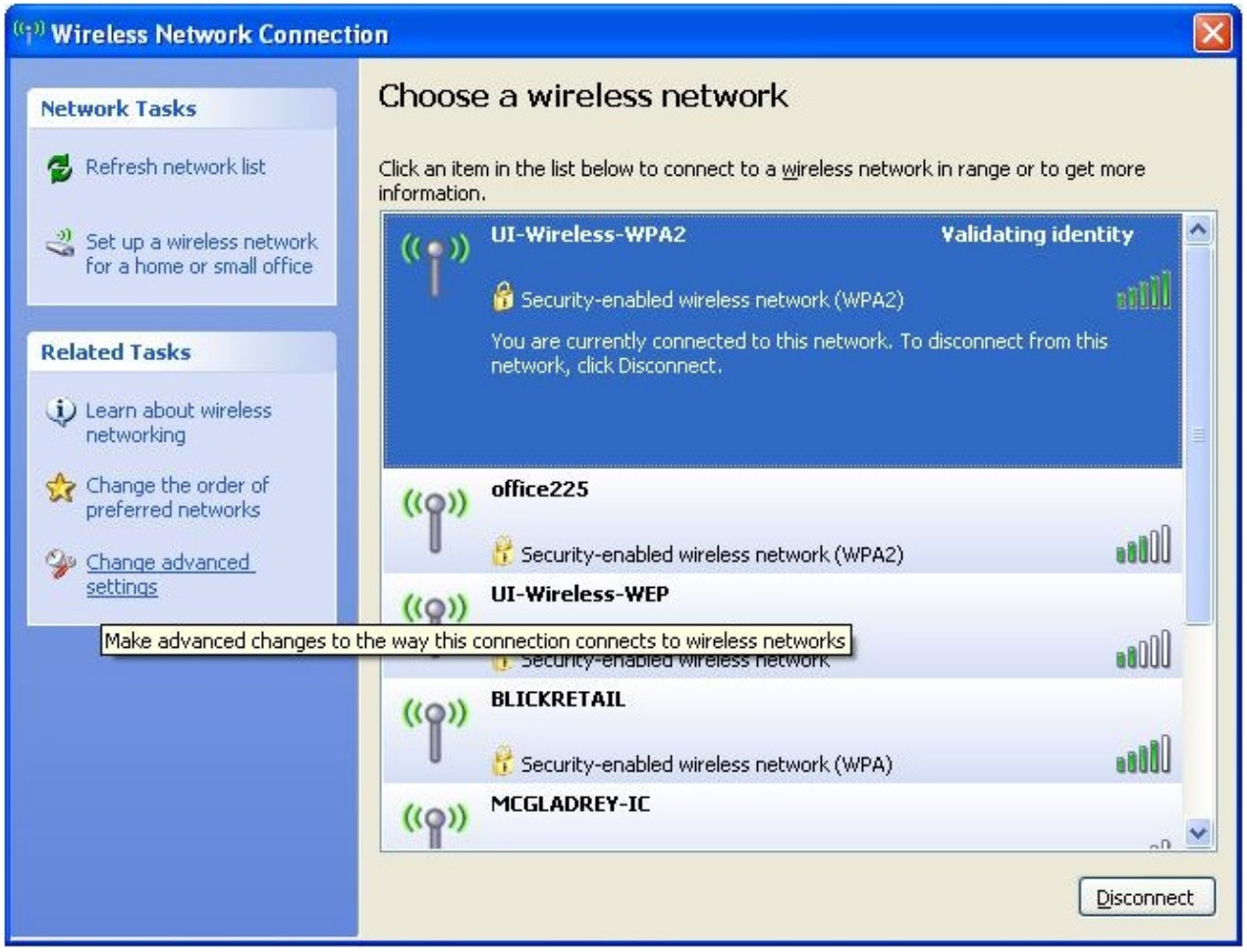
(1) Beacon frames periodically sent from APs, which include AP's MAC address, Network name, etc.
(2) Association Request frame sent: H1 to selected AP2
(3) Association Response frame sent: AP2 to selected H1

Active Scanning:

(1) Probe Request frame broadcast from H1
(2) Probes response frame sent from APs, which include AP's MAC address, SSID, etc.
(3) Association Request frame sent: H1 to selected AP2
(4) Association Response frame sent: AP2 to selected H1

2. Select a Network

- The user selects from a list of available networks



- Common criteria:
  - User choice
  - Strongest signal
  - Most recently used

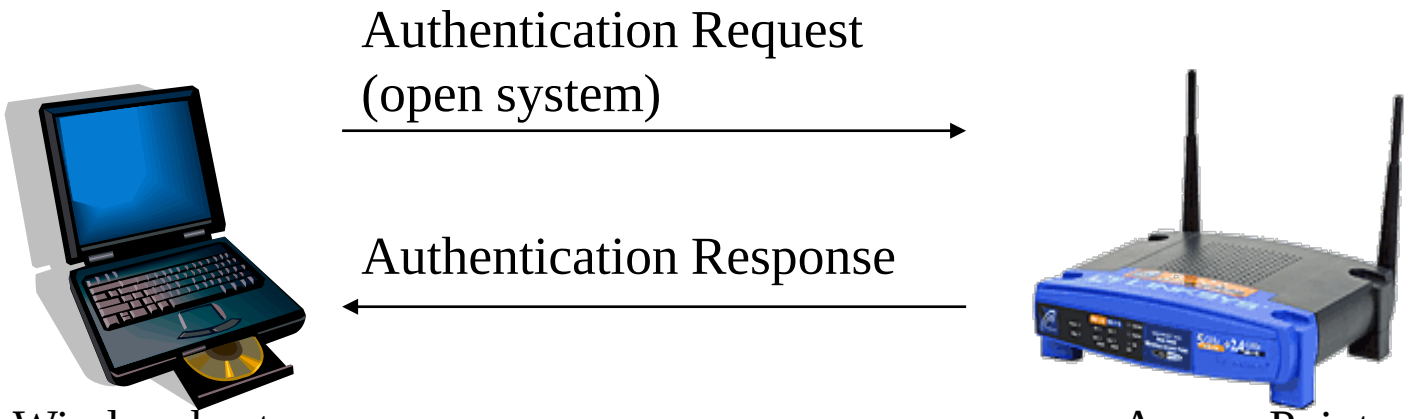
3. Authentication

- Authentication
  - A wireless host proves its identity to the AP

- Two Mechanisms
  - Open System Authentication
  - Shared Key Authentication

3a. Open System Authentication

- The default authentication protocol for 802.11
- Authenticate anyone who requests authentication
  - NULL authentication (no authentication at all)



3b. Shared Key Authentication

It is assumed that the wireless host and the AP somehow agrees on a shared secret key (usually, you set a pwd for your AP and you input the pwd on your MS when you make connection)

Wireless host

Authentication Request →

← 128-byte randomly generated "challenge" plain text string

"challenge" string encrypted with the shared key →

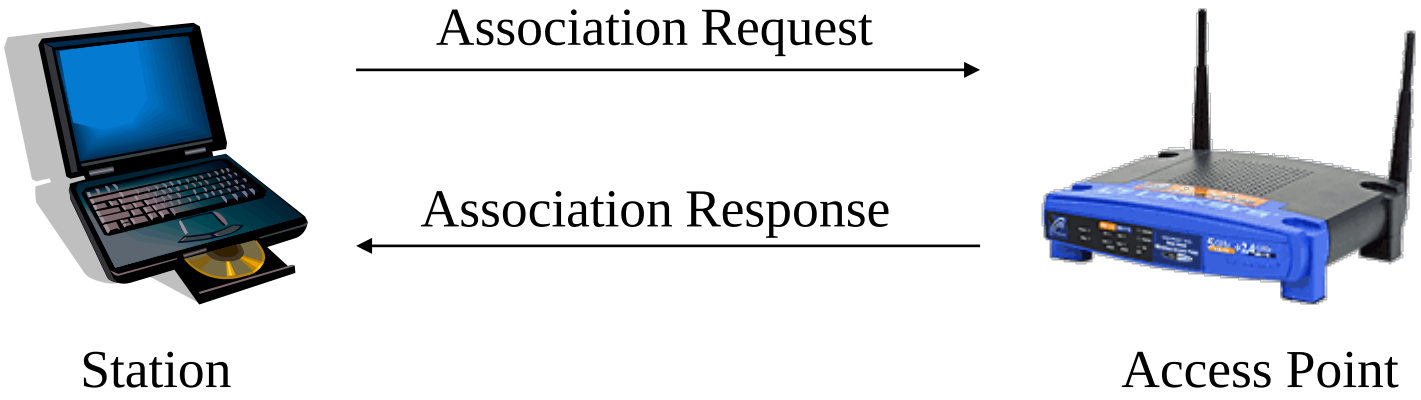
← Positive or negative response based on decryption result

Access Point (AP)

Note: "challenge" is encrypted by WPA algorithm

4. Association (Registration)

The wireless hosts need to associate (i.e. register) with the AP

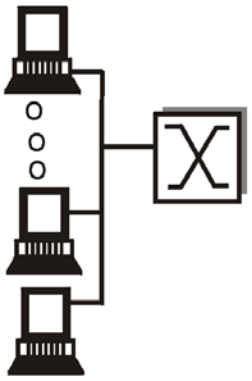


Q: After your MS is connected to a network, how to transmit data?

The MAC layer

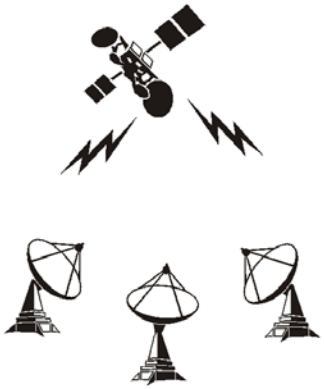
Medium Access Control (MAC)

- How to share a common medium among the users?



shared wire
(e.g. Ethernet)

shared wireless
(e.g. Wavelan)



satellite

cocktail party

What is Medium Access Control (MAC)

- Medium access control (MAC)
  - Regulate accesses to a common medium from multiple transmitters, aiming to prevent collisions
  - Limit interference to an acceptable level
- Multiplexing techniques (MAC) for cellular networks:
  - Frequency Division Multiple Access (FDMA)
  - Time Division Multiple Access (TDMA)
  - Code Division Multiple Access (CDMA)

MAC for Wired Networks

- Can we apply media access methods from wired networks?

- Example: CSMA/CD
  - Carrier Sense Multiple Access with Collision Detection
  - Method used in IEEE 802.3 Ethernet (wired network)

Principles of CSMA/CD

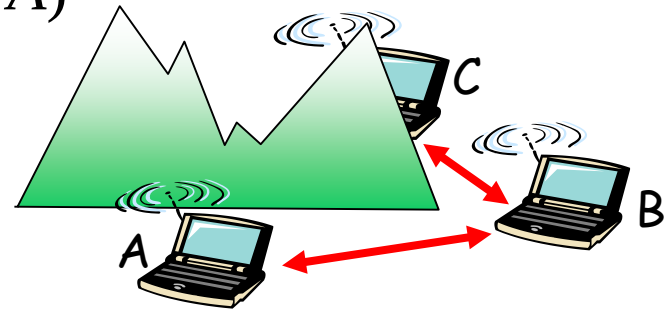
- Carrier Sense Multiple Access (CSMA): Listen before talk
  1. Sense the channel
  2. If the channel is idle, transmit immediately
  3. Otherwise (if the channel is busy)
     - wait for a random amount of time (random backoff time)
     - goto step1 to sense the channel again
- Collision Detection (CD): Stop if collision occurs
  4. If collision is detected during the transmission:
     - stop transmission immediately
     - wait for a random amount of time
     - goto step 1

IEEE 802.3 LAN: CSMA/CD

- MAC is a typical problem in local area network (LAN)
- How a sender sends data in wired LAN: CSMA/CD (Carrier Sense Multiple Access with Collision Detection)
  - Carrier sensing: a sender senses the medium to see if it is free. It sends as soon as the medium is free
  - Collision detection: sender listens the medium while transmitting. If it detects any collision, it stops at once and sends a jamming signal to cause other senders stop too
- Can we apply the CSMA/CD for wired LAN to Wireless LAN?
  - Yes. But need modifications

MAC Problems in Wireless Network

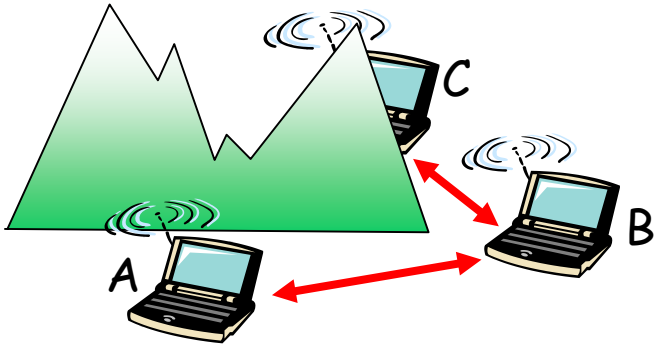
- In wireless networks, the sender and receiver are not on the same cable as in wired LAN. The sender may not “hear” the collision that occurs at the receiver (e.g., *A* doesn’t know collision at *B*)
  - Thus, CD (collision detection) does not work.
- CS may not work either if a hidden terminal (e.g., *C*) is out of detection range of the sender (e.g., *A*)

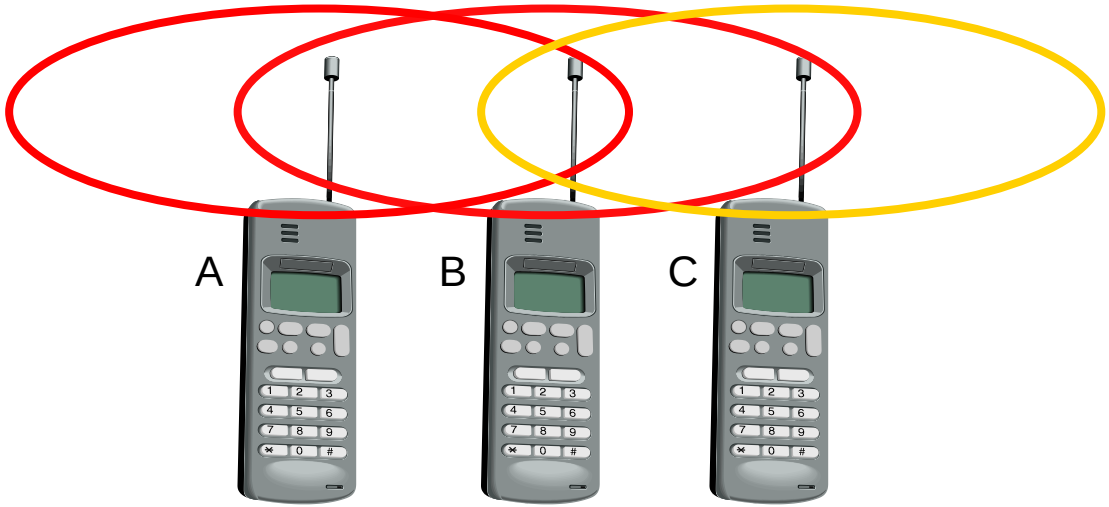


- Hidden terminal problem
  - Collision undetected
- Far and near terminals problem
  - The signal strength received depends on the distance between the sender and receiver (unlike signals on a cable)

Hidden Terminal Problem

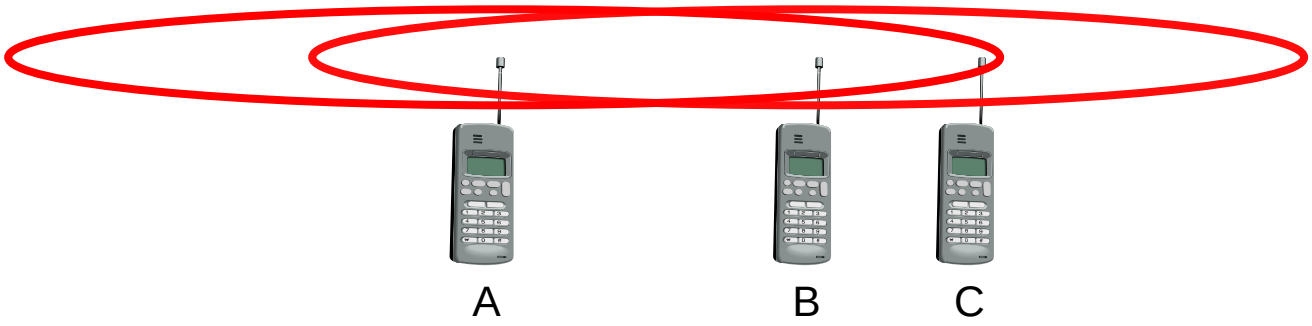
- A wants to send to B, but it cannot sense C (CS fails); the same for C vs A
- Thus, A and C both transmit to B at the same time
- B cannot receive data properly, because A's signal collides with C's at B (even worse, A couldn't sense this collision)
- C is a "hidden terminal" for A, vice versa for C





Near and Far Terminal Problem

- A near terminal's signal overpowers a farther one
- Suppose both A and B send to C (all with the same Tx power)
  - It's possible because both of them may sense the medium free at the same time
  - B's signal is much stronger than A's at C (Signal strength decreases proportional to the square of distance)
  - Thus, C receives B's signals, but not A's (not exact a collision)
- Challenging issue for CSMA-networks: precise power control is needed



CSMA/CA in 802.11 Networks

- 802.11 Wireless Network: NO collision detection!
  - Collision detection requires the ability to send and receive at the same time, but most of the handsets have only one pair of transceivers that perform one operation at a time
  - Impossible to detect collision at the sender, because the strength of the signal at receiving side is typically much smaller than the transmitted signal
  - Instead of simply detecting collisions, the goal becomes to avoid collisions: CSMA/CA (Collision Avoidance)

Collision Avoidance in 802.11 Networks

- Collision Avoidance: prevent two or more nodes from transmitting at same time
  - Sense before transmitting (i.e., CSMA)
  - 802.11 two modes of operation:
    - DCF (Distributed Coordination Function)
      - Must be included in all implementations
    - PCF (Point Coordination Function)
      - AP acts as the coordinator (infrastructure mode only)
      - AP sends *CF-Poll* msg to all stations and decides who transmits (centralized control)
      - Optional (implemented on top of DCF)

802.11 DCF (Distributed Coordination Function)

- DCF uses CSMA/CA (NOT CSMA/CD)
- DCF supports two modes for CA (collision avoidance)
  - Basic Access Mode (also called DIFS/SIFS mode)
    - Unlike CSMA/CD, when the sender senses the channel idle, it does not transmit immediately, but waits for DIFS (Distributed Inter-frame Space) amount of time. Why?
    - If the channel is continuously idle for DIFS, it transmits; otherwise waits for a random backoff time
    - Receiver replies ACK if data is received successfuly
    - A 2-way handshaking protocol (data-ACK)
  - RTS/CTS mode
    - The sender broadcasts a Request To Send (RTS) message
    - The receiver replies a Clear To Send (CTS) message
    - A 4-way handshaking protocol (RTC-CTS-data-ACK)

Time Parameters of DCF MAC Protocol

Basic Time Parameters

- Slot Time: basic unit of backoff algorithm

  = Time required for station to sense end of frame, start transmitting, and beginning of frame to propagate to others

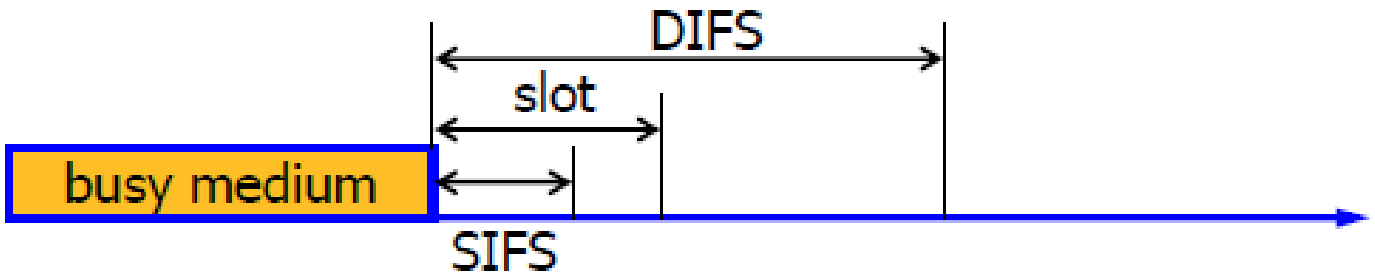
- SIFS: Short Inter-Frame Space

  = Time required for a station to sense the end of frame and start transmitting

- DIFS: DCF Inter-Frame Space

  = Time to wait before starting backoff interval ("contending")

  = SIFS + 2 slot times



DCF: Basic Access Mode (DIFS/SIFS)

802.11 sender

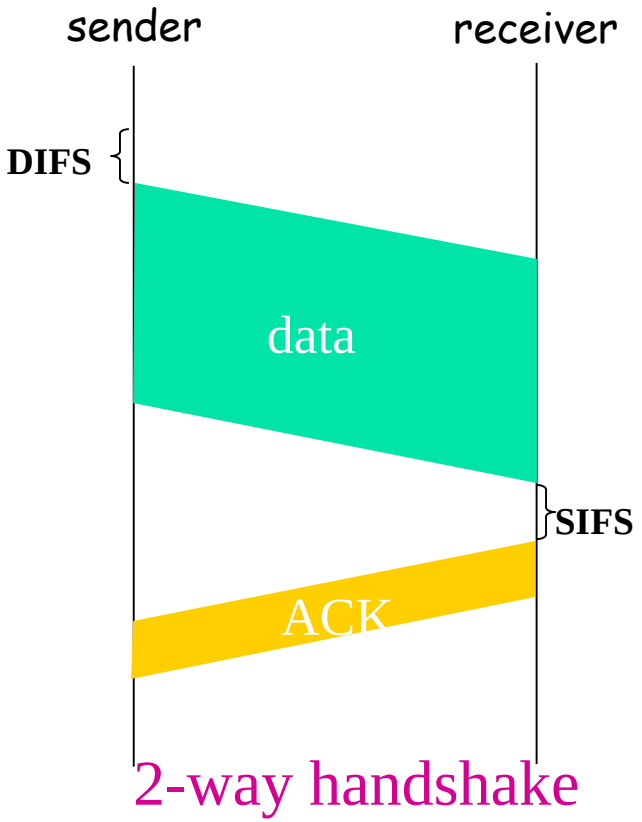
1. if sender senses channel idle for DIFS,
   Transmit the frame and CW = CW/2
2. if it senses channel busy,
   Wait for medium to be free for DIFS;
   Choose a random counter *r* in [0, CW];
   While *r* > 0 {
   sense medium for one slot time;
   If medium is free for this slot *r* = *r* −1; }
   Transmit the frame; // after backoff waiting
   if no ACK,
   CW = CW×2 and goto step2

802.11 receiver

1. if frame is received, reply ACK after **SIFS**

N.B.: ACK is used for collision detection!

DIFS – Distributed Inter-frame Space
SIFS – Short Inter-frame Space

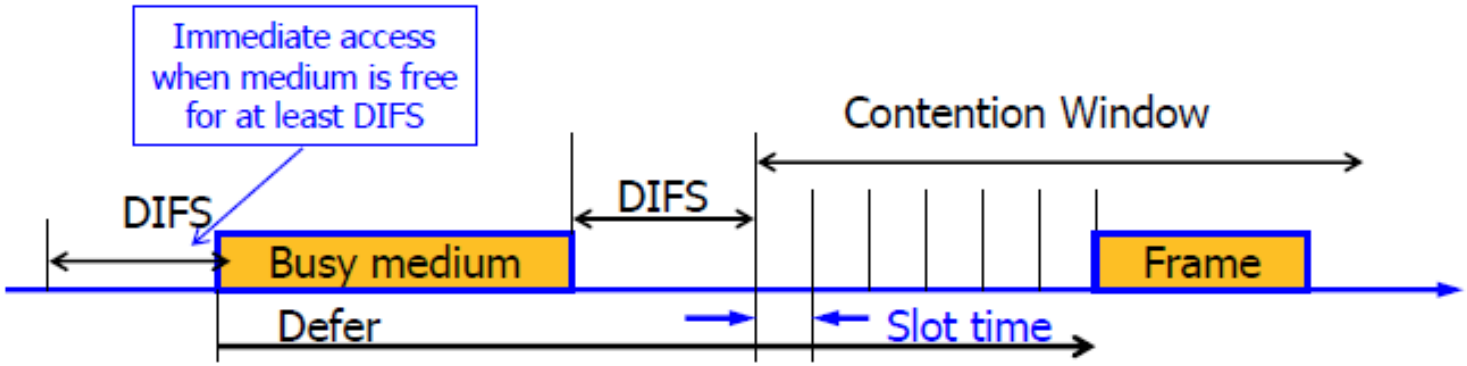


2-way handshake

DCF: Random Backoff and Contention Window

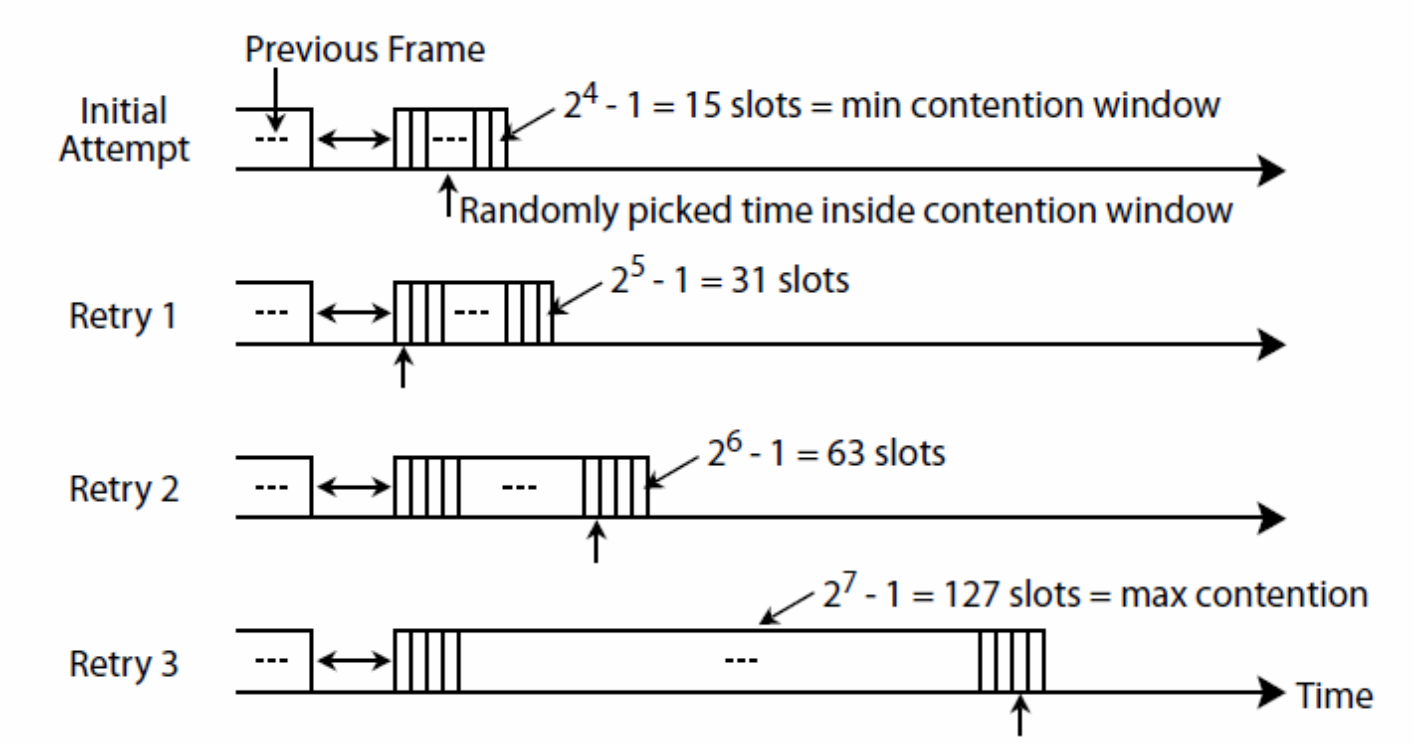
Binary exponential backoff:

- When two frames collide, both senders need to backoff.
- The backoff counter is an integer randomly chosen over the contention window (CW), i.e., an integer in [0, CW].
- The value of CW (contention window size) is doubled for every continuous collision; and halved for each successful transmission.
- CW is in unit of slot and has a minimum and a maximum size.



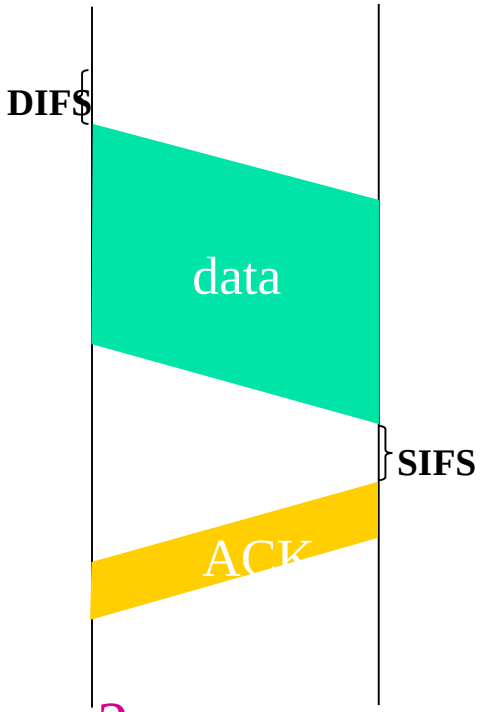
DCF: Random Exponential Backoff

- Why increasing CW exponentially?
- Why choosing a random number in [0, CW] (instead of using CW) as backoff time?



DIFS/SIFS mode is NOT Efficient

- DIFS/SIFS mode is contention-based. It cannot completely avoid collisions (though the chance is slim)
  - Two nodes may both sense medium free for DIFS at the same time and decide to transmit simultaneously (purely distributed protocol)
  - Collision of data transmission is costly!
  - Combined CA (backoff waiting) with CD (using ACK for collision detection)
- The exponential random backoff is not efficient when collision occurs

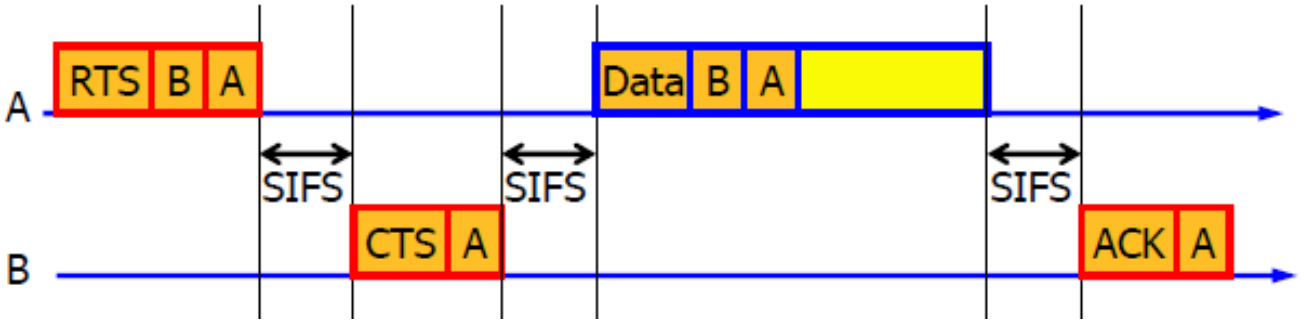


2-way handshake

DCF RTS/CTS Mode: Collision Avoidance

- Use short signaling packets to reserve channel to avoid collision
  - RTS (request to send): sender sends a short RTS packet to the receiver before it sends data
  - CTS (clear to send): the receiver grants the permission to send by replying a CTS packet
- RTS/CTS packets contain: sender address, receiver address, packet size

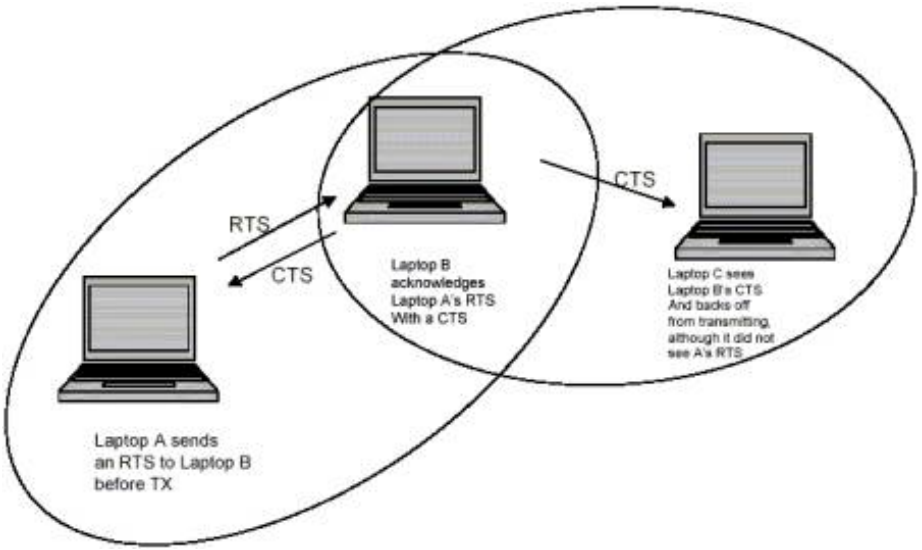
Note: SIFS is shorter than ~~DIFS~~ slot, so stations contending for access do not decrement their backoff counters during these exchanges



How does RTS/CTS avoid collisions?

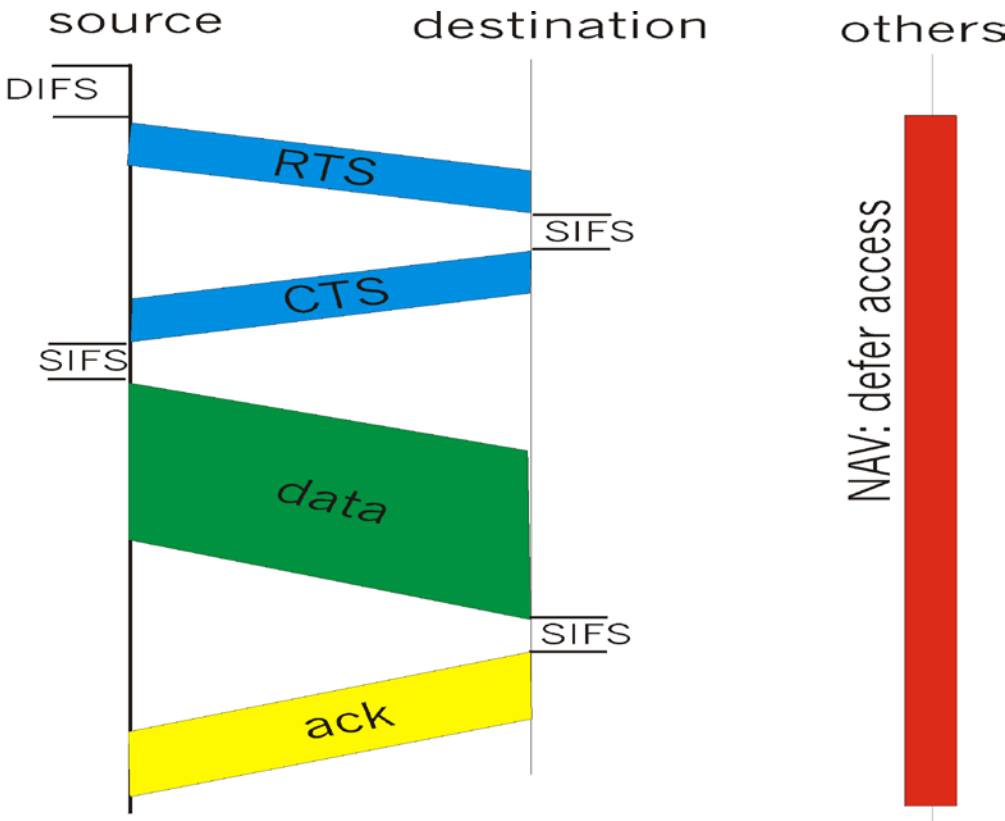
RTC/CTS allows sender to reserve channel rather than random access of data frames: avoid collisions of long data frames

- Sender first broadcasts a small RTS packet using CSMA
  - RTSs may still collide with others (but they're short)
- Receiver broadcasts CTS in response to RTS, which can be heard by all hidden terminals potentially interfering the receiver
- Collisions mostly avoided
  - RTS prohibits nodes within the range of the sender from transmitting
  - CTS prohibits nodes within receiver's range from transmitting



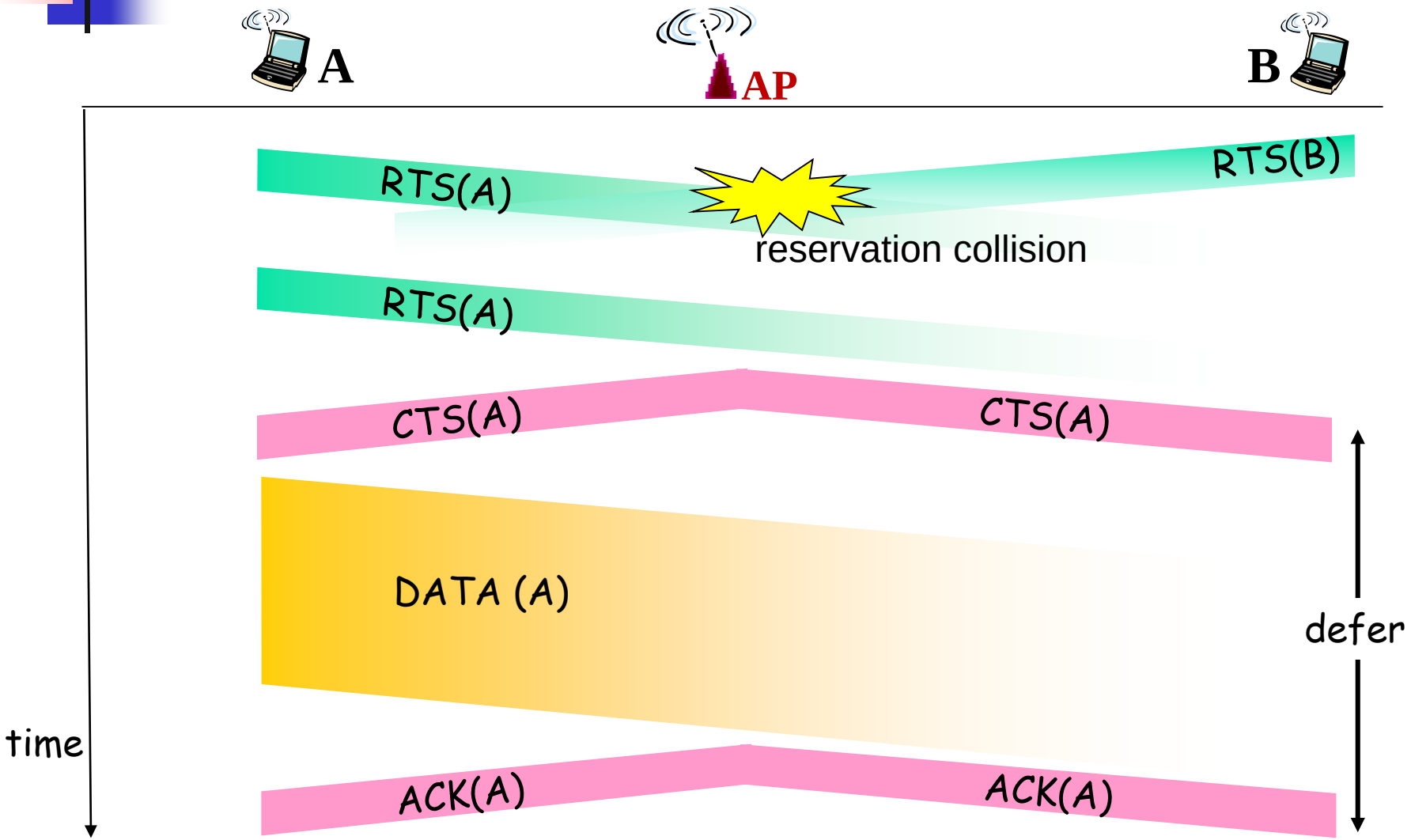
802.11: CSMA/CA with RTS/CTS

- CSMA/CA: explicit channel reservation
  - sender: send RTS (20 bytes)
  - receiver: reply CTS (16 bytes)
- RTS reserves channel for the receiver
- CTS reserves channel for the sender, notifying all surrounding terminals (no hidden terminals)

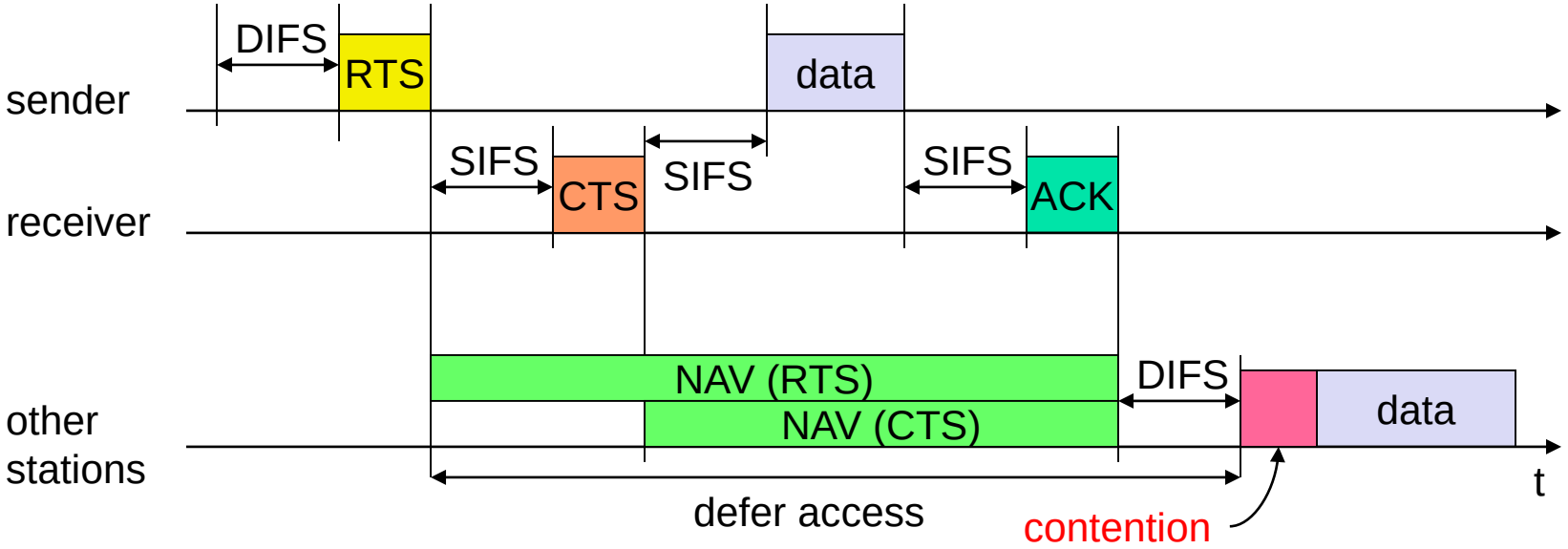


4-way handshake

Still Collision in RTS-CTS exchange but No Data collision



How long do I have to wait? - Network Allocation Vector (NAV)



- The RTS packet has a duration field, which contains information about the length of data packet.
- Other stations hear the RTS packet set their NAV accordingly.

- The CTS packet also has the duration field.
- Other stations only hear the CTS packet can also set their NAV accordingly.

Network Allocation Vector (NAV)

- Each station maintains a countdown timer that tells how far into the future the medium has been "reserved" by RTS/CTS exchanges
- Stations set NAV counter based on the value in the duration field of RTS/CTS frames
  - Even if a station only hears one of the RTS or CTS , it still knows how long the medium will be "busy"
- This RTS/CTS mode combines NAV and physical sensing
  - Medium considered busy if NAV value > 0

Which is better: DIFS/SIFS or RTS/CTS

- DIFS/SIFS mode
  - Contention based method: random backoff to avoid collision
  - No overhead for message exchange (no coordination)
  - Possible collision of data transmission and inefficiency of backoff waiting

- RTS/CTS Mode
  - Channel reservation method: RTS and CTS for channel reservation
  - No collision of data transmission
  - Overhead/delay of exchanges of RTS/CTS

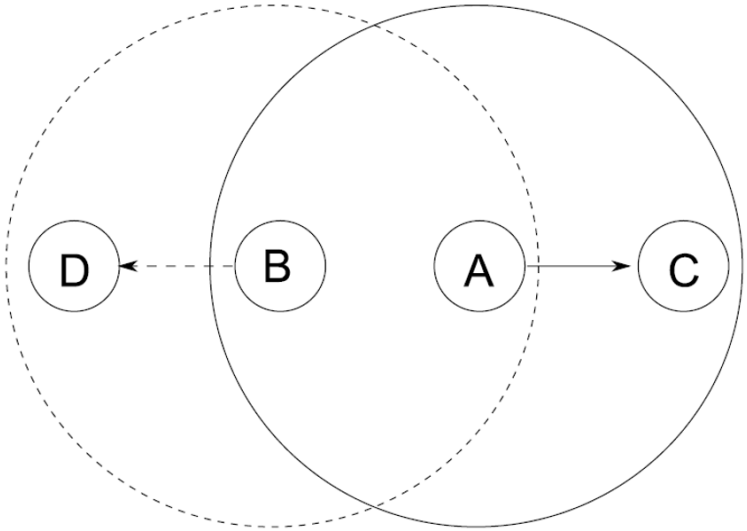
Summary

- Wireless LAN types and modes
  - 802.11 a/b/g, infrastructure and ad hoc modes
- Medium Access Control of WiFi
  - CSMA/CA is the solution
  - DCF (Distributed Coordination Function) protocol
    - Basic Access Mode (DIFS/SIFS mode)
      - Contention based method
    - RTS/CTS Mode
      - Channel reservation method

Exercise: RTC/CTS is over strong Exposed Terminal Problem

- As in the Figure, A requests to send to C, and B requests to send to D at the same time
- After hearing A's RTS, B won't proceed with the protocol
- But, in this case, it's fine that both A and B transmit their data at the same time (and both C and D can receive correctly)

- This is called Exposed Terminal Problem
  - B is the exposed terminal
- How to solve it?



Exercise (cont'd)

1. List three major differences between the Basic Access mode and the RTS/CTS mode in DCF protocol

2. Explain why there is NO hidden terminal problem in RTS/CTS protocol

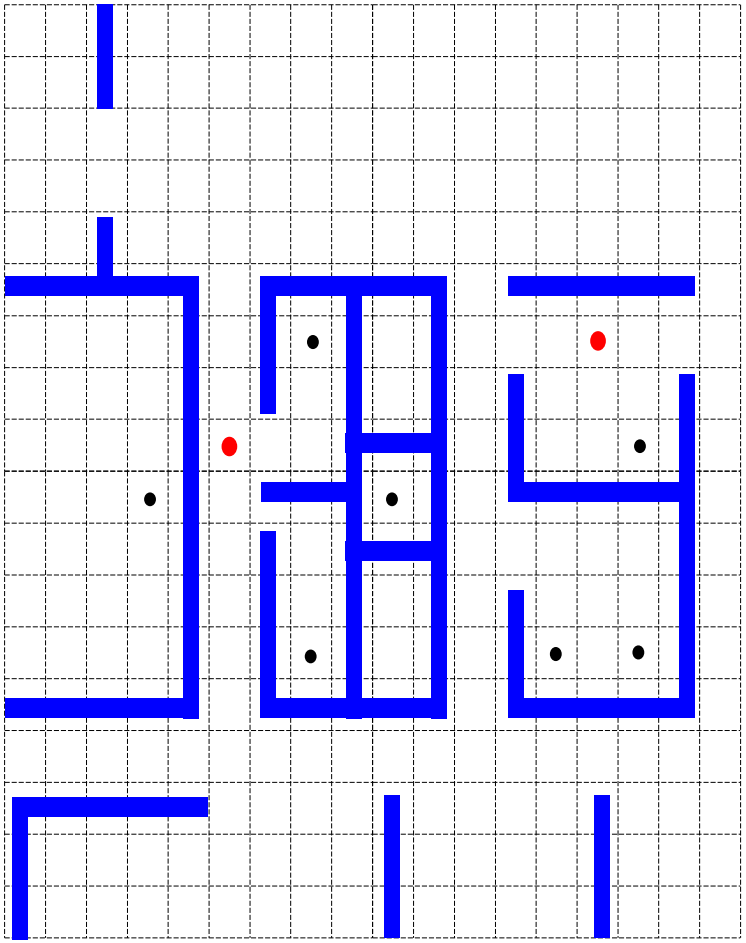
3. Why a user needs to wait for the channel to be continuously free for DIFS time before transmitting data?

4. How does NAV (network allocation vector) prevent users from continuously sensing if the channel is free?

AP Placement with power control

Problem: given a set of users in a floor plan, each user has bandwidth requirement γ. Place a minimum set of APs W, such that each user's bandwidth requirement γ can be met.

- Divide the region into grids
- Traffic demands (users) originate from grids
- APs are placed at the center of grids
- $A_{M \times M}$: signal attenuation array



Transmission power, data rate & interference

- $A_{M\times M}$: signal attenuation array, M: the number of grids
- User v can receive data from AP w if:

  $A(w,v)P_w \geq \alpha$ // α: threshold for decoding data
- User v is interfered by w if:

  $A(w,v)P_w \geq \beta$ // β: threshold for interference
- Data rate from v to w is (similarly for $R(w,v)$):

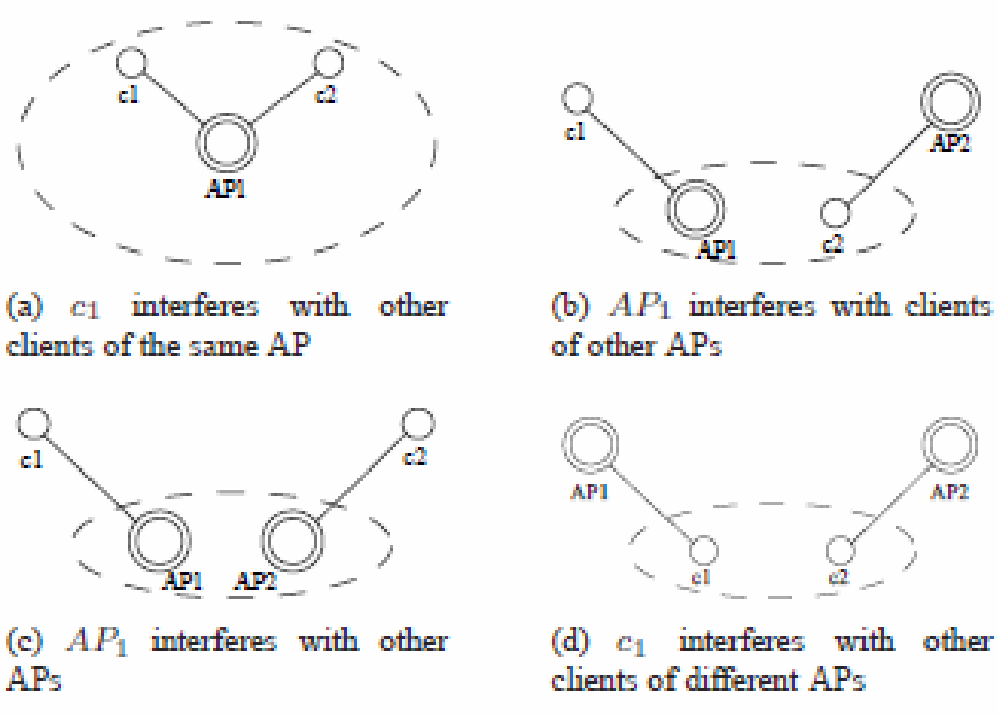
  $R(v,w) = f(A(v,w)P_v)$

A table of transmission range, data rate & interference range

Range (m)	Rate	TX power (dBm)					
	(Mbps)	8	11	14	17	20	23
Transmission Range (m)	6	29	36	43	53	64	78
	9	20	24	29	36	43	53
	12	17	21	26	31	38	46
	18	15	18	22	27	33	41
	24	12	15	18	22	27	33
	36	10	12	14	17	21	26
	48	7	9	11	13	16	20
	54	7	8	10	12	15	18
Interference Range (m)	-	33	41	49	60	73	89

Interference and Bandwidth Constraint

- Network G(V, E): V set of users and APs. A link l in E is between a user and an AP.
- $I(l)$: Interference set of link l is a set of links that either interfere with l or are interfered by l, including l itself.



(a) c_1 interferes with other clients of the same AP

(b) AP_1 interferes with clients of other APs

(c) AP_1 interferes with other APs

(d) c_1 interferes with other clients of different APs

Bandwidth constraint among multiple interfering links

- γ_v^{up}, γ_v^{dn} : up link and down link traffics of v

- Channel bandwidth is shared by all links in the collision set $I(l)$. That is:

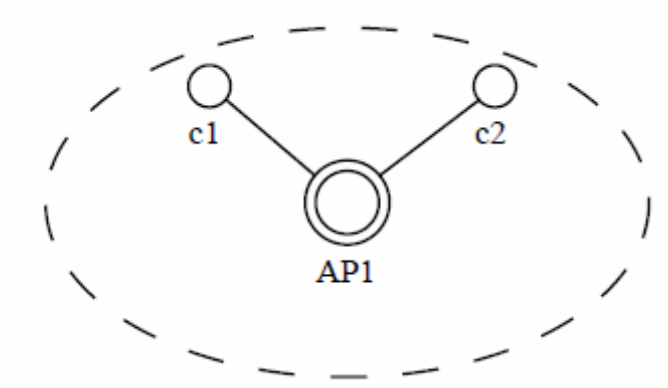
$$T_{I(l)} = \sum_{(v,w)\in I(l)} \left(\frac{\gamma_v^{up}}{R(v,w)} + \frac{\gamma_v^{dn}}{R(w,v)}\right) \le 1$$

Performance metric for a greedy method

- $S(w)$: users served by AP w
- Max collision load: $T_{I(lw)}$
- Client to Interference Ratio CIR(w):

$$T_{I(l_w)} = \max_{v \in S(w)} T_{I(l_{vw})}, l_{vw} \in E$$

$$CIR(w) = \frac{|S(w)|}{T_{I(l_w)}}$$



A Greedy Placement Method

1) Initially, each position of a user is placed with an AP.
2) Choose two *neighboring* APs to merge to a new AP *w*, such that:
   a) AP *w* can serve all users of two old APs (*w*'s power is set to cover all users), and meet the bandwidth constraint;
   b) CIR(*w*) is maximal (locate *w*'s new location);
3) Repeat step (2) until no more merge can be done (i.e., CIR(*w*) cannot be increased anymore by merging any two APs).