An Introduction to Wireless Networks and Wi-Fi (IEEE 802.11)

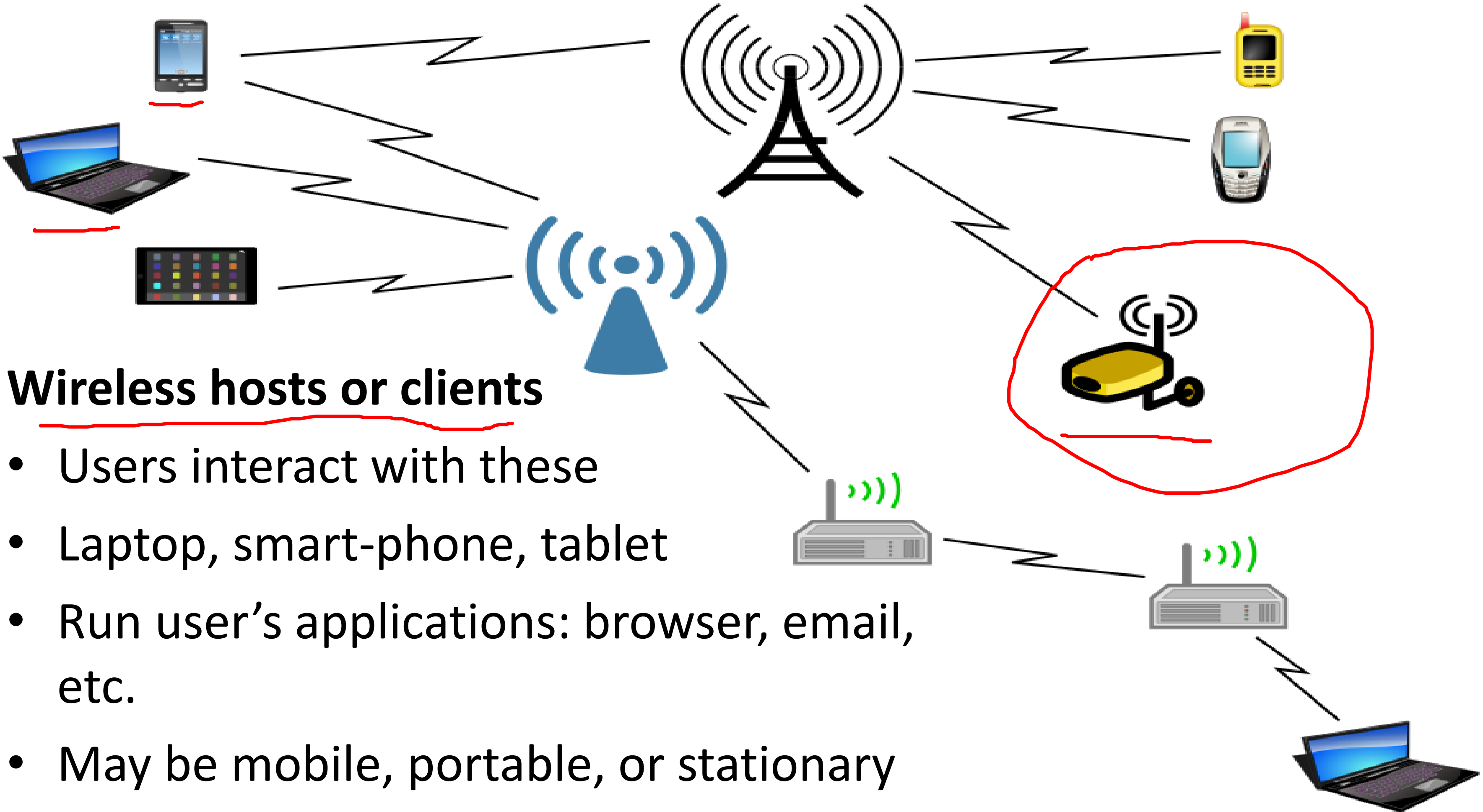
Bhaskaran Raman

Department of CSE, IIT Bombay

Wireless and Mobile Networks

- # wireless subscribers > # wireline subscribers
- India (TRAI report, Oct 2013):
  - 875 million wireless, only 29 million wireline!
- Wireless Internet on mobile and portable devices: laptops, tablets, smart-phones
  - Anytime, anywhere
- Several unique challenges

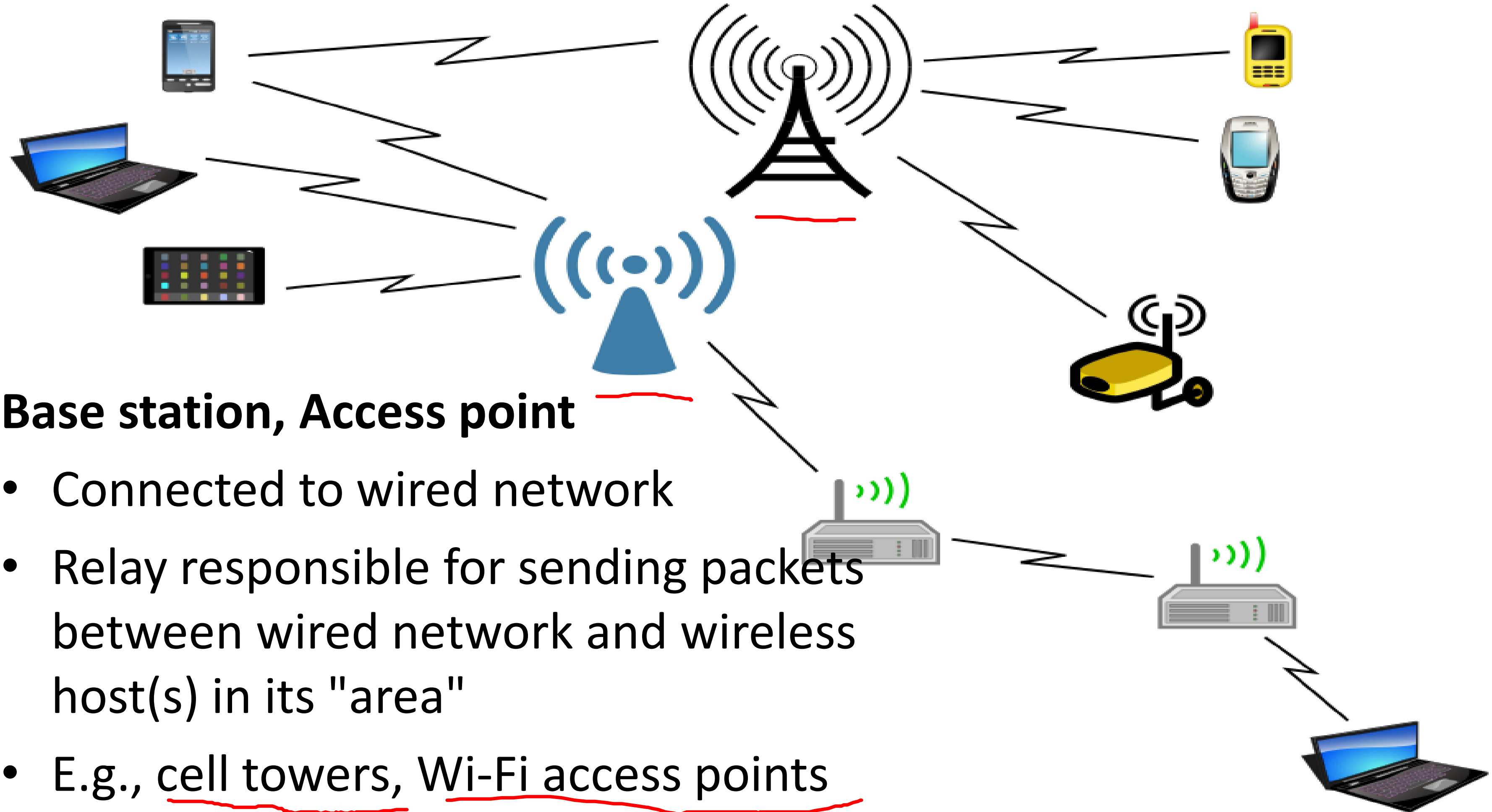
Elements of a Wireless Network



Wireless hosts or clients

- Users interact with these
- Laptop, smart-phone, tablet
- Run user's applications: browser, email, etc.
- May be mobile, portable, or stationary

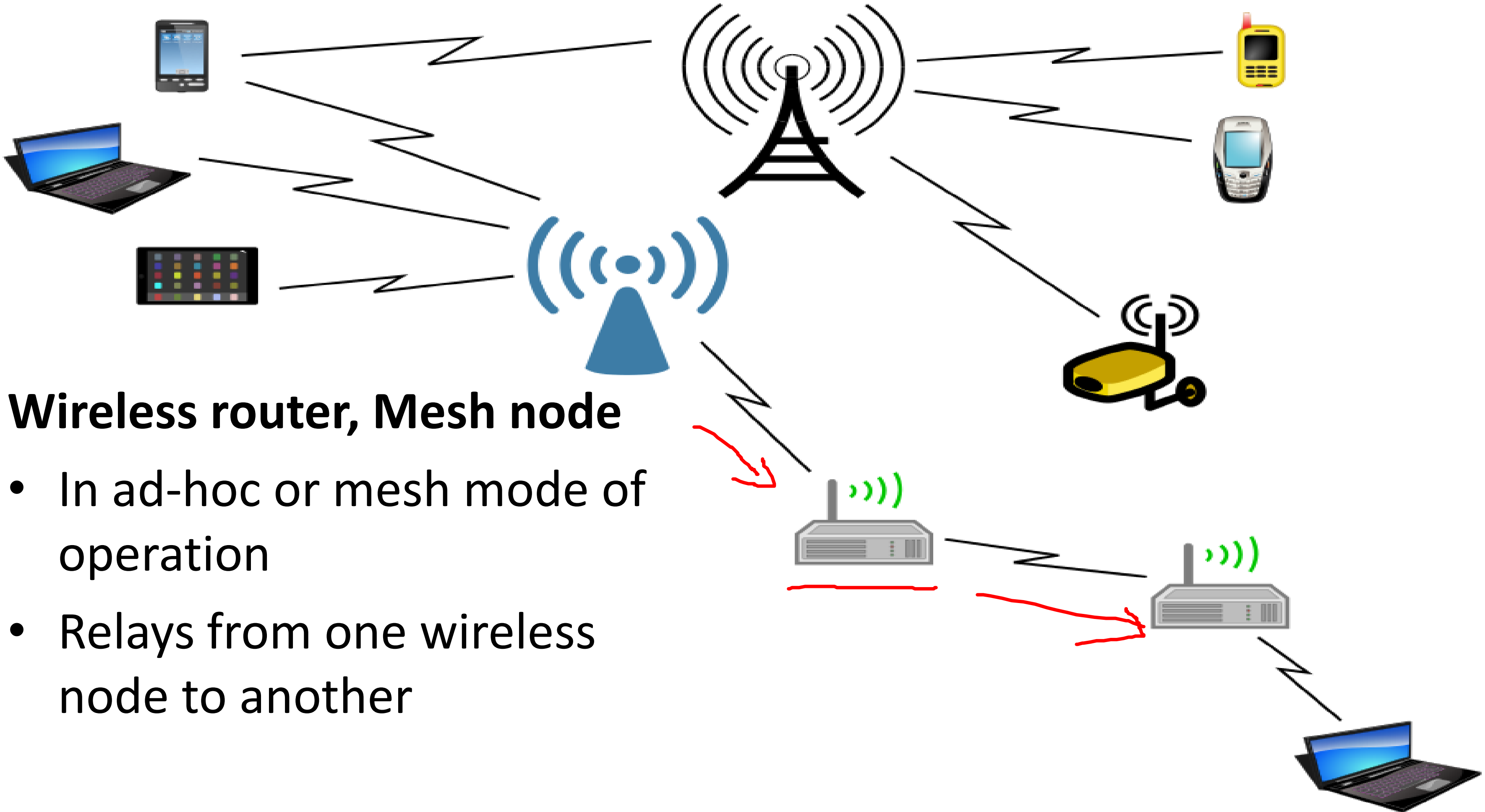
Elements of a Wireless Network



Base station, Access point

- Connected to wired network
- Relay responsible for sending packets between wired network and wireless host(s) in its "area"
- E.g., cell towers, Wi-Fi access points

Elements of a Wireless Network

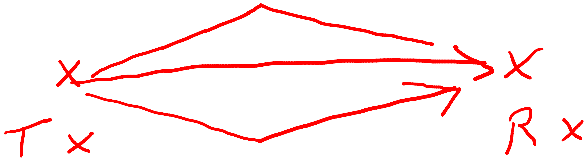


Wireless router, Mesh node

- In ad-hoc or mesh mode of operation
- Relays from one wireless node to another

Wireless Network Challenges

1. Bandwidth: scarce, variable, disconnection
   – No “wire” to contain signal
   – Weaker signal, prone to interference, multipath
2. Portability, mobility
   – Point of attachment to network varies

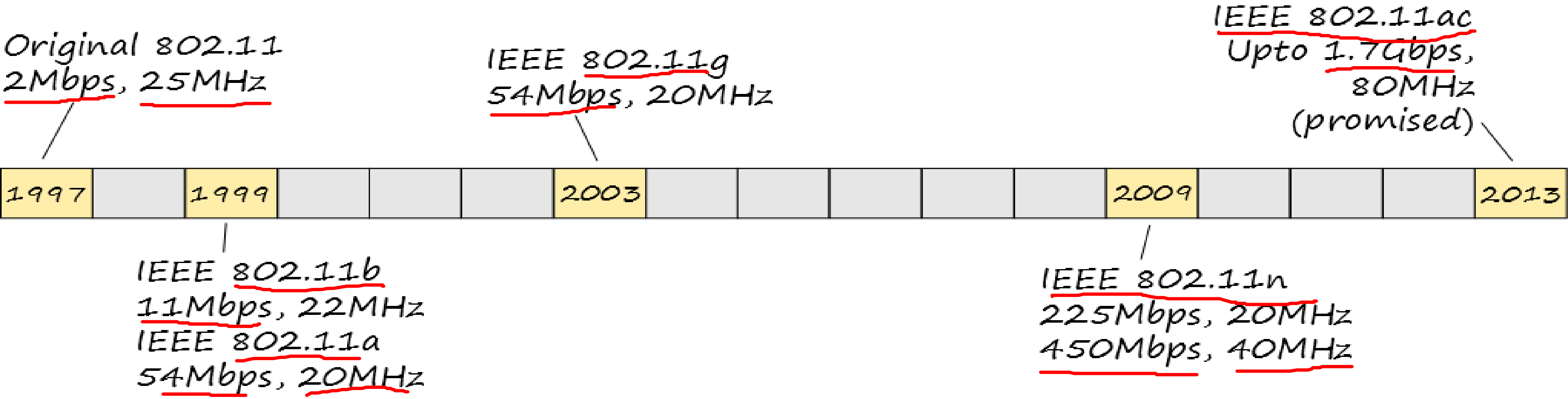


3. Limited capabilities
   – Power, screen size, CPU, storage
4. Security risks are higher
   – Broadcast medium, two-way authentication, device can get lost

Reference: “Adaptation and Mobility in Wireless Information Systems”, Randy H. Katz, IEEE Personal Communications, 1^{st} Quarter 1994, Vol. 1, Issue 1, pp 6-17.

Wi-Fi (IEEE 802.11)

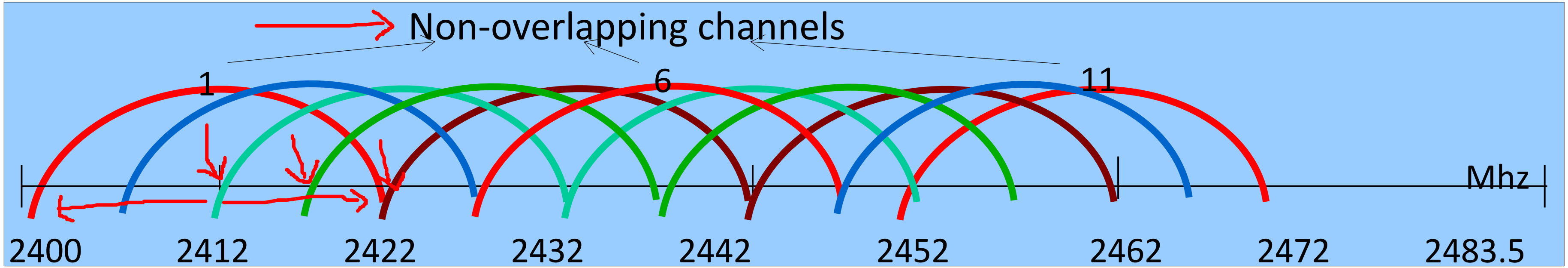
- Extremely successful technology
  - Part of layman's vocabulary
  - 3+ billion USD market, growing
- Part of IEEE 802.x series



802.11: What does it Specify?

- PHY sub-layer
  - 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac
  - Modulation and coding schemes
- MAC sub-layer
  - Independent of the PHY
  - DCF (Distributed Coordination Function) based on CSMA/CA
  - PCF (Point Coordination Function)
- Link sub-layer
  - Framing, addressing, fragmentation, aggregation
- Network management
  - Network formation and maintenance

802.11 PHY Layer: Channels



Chnl	36	40	44	48	149	153	157	161	165
Freq (MHz)	5180	5200	5220	5240	5745	5765	5785	5805	5825

- Designed to operate in ISM bands
- License free in most of the world, with transmit power restrictions
- Has been one of the keys to WiFi's success
- Also cause of performance problems!

Modulation and Coding

- What is channel coding?
  - Data bits → Bits with redundancy
  - Essential in wireless channels since BER is high
  - Human analogy
    - “u cn rd ths tho ltrs r mssng”
- What is modulation?
  - Bits to be sent → Physical energy (e.g. RF signal)
  - Human analogy
    - Natural language → sound from the mouth
- Reverse at receiver: demodulation, decoding

802.11b PHY: Modulation Schemes

Modulation	Data rate
BPSK	1Mbps
QPSK	2Mbps
CCK	5.5Mbps
CCK	11Mbps

- 802.11b: spread spectrum
  - DSSS most common
  - Uses 11-bit coding sequence called Barker code

802.11a/g PHY: Modulation & Coding

Modulation	Coding rate	Data rate (Mbps)
BPSK	1/2	6
BPSK	3/4	9
QPSK	1/2	12
QPSK	3/4	18
16-QAM	1/2	24
16-QAM	3/4	36
64-QAM	2/3	48
64-QAM	3/4	54

- 802.11a/g: uses OFDM style modulation
- Varying bits/symbol & coding redundancy ➔ different data rates

802.11n Modulation & Coding

Modulation	Coding rate	Data rate (Mbps)
BPSK	1/2	6.5
QPSK	1/2	13
QPSK	3/4	19.5
16-QAM	1/2	26
16-QAM	3/4	39
64-QAM	2/3	52
64-QAM	3/4	58.5
64-QAM	5/6	65

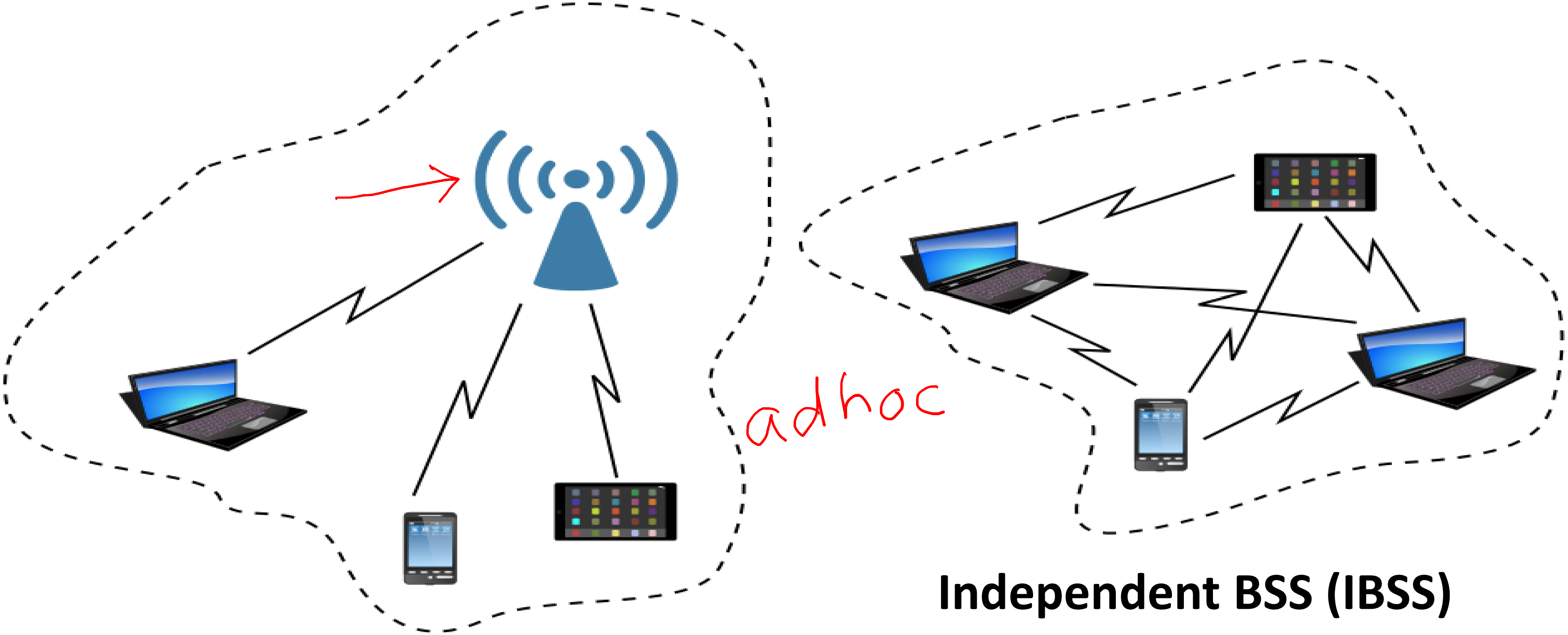
- Also OFDM based
- 802.11n has two main new PHY features:
  - Channel bonding, MIMO

Channel Bonding and MIMO

- Channel bonding
  - Use two adjacent 20 MHz channels
  - Doubles the data rate (approximately)
- MIMO: Multi-input, Multi-output
  - Take advantage of multiple independent paths between tx and rx antennas
  - Upto 3 tx antennas, 3 rx antennas: 3x3
  - Can triple the capacity: 3 spatial streams
- Overall: up to 450 Mbps
- Beware: a lot of hidden overheads

2 x 2

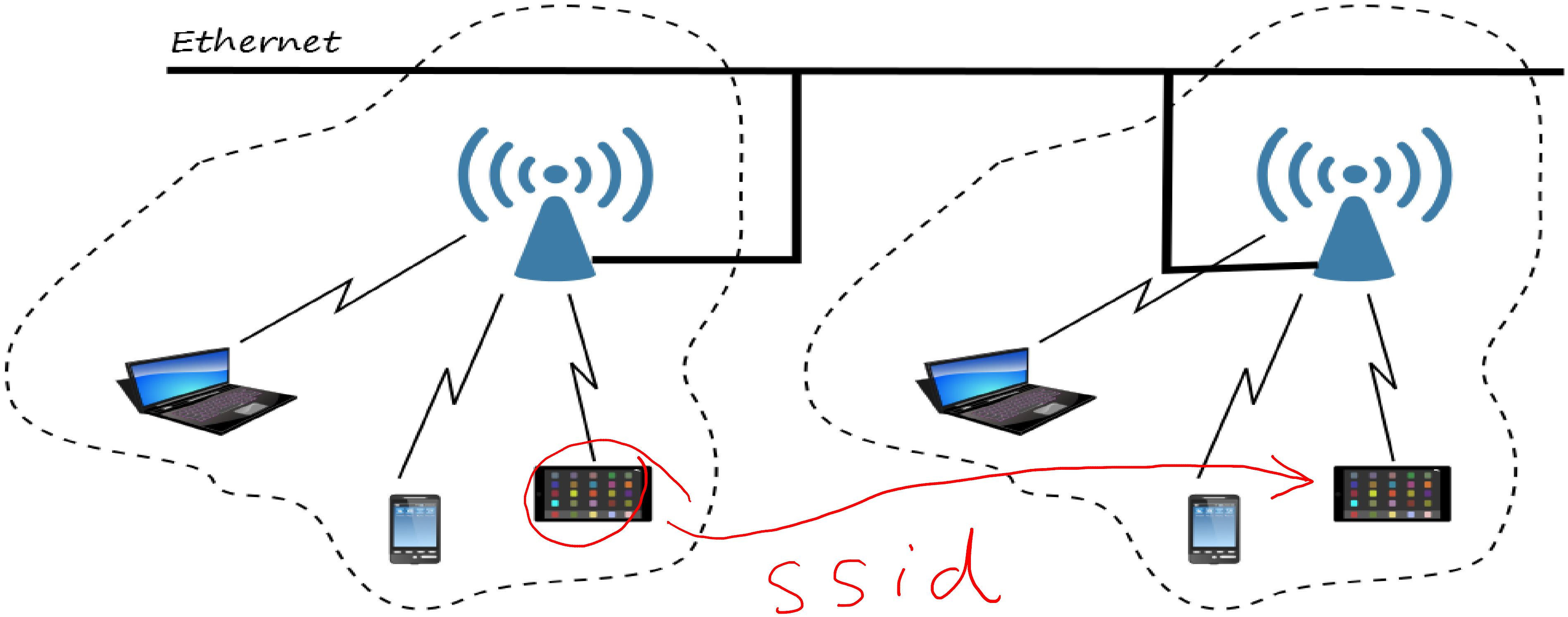
802.11 Basic Service Set (BSS)



Infrastructure BSS

Independent BSS (IBSS)

802.11 Extended Service Set (ESS)



Types of MAC

- What dimension is used for multiplexing?
  - Time (TDMA), frequency (FDMA), code (CDMA)
- How is control achieved?
  - Centralized versus distributed
- 802.11 specifies
  - DCF: Distributed Coordination Function (distributed)
  - PCF: Point Coordination Function (centralized)

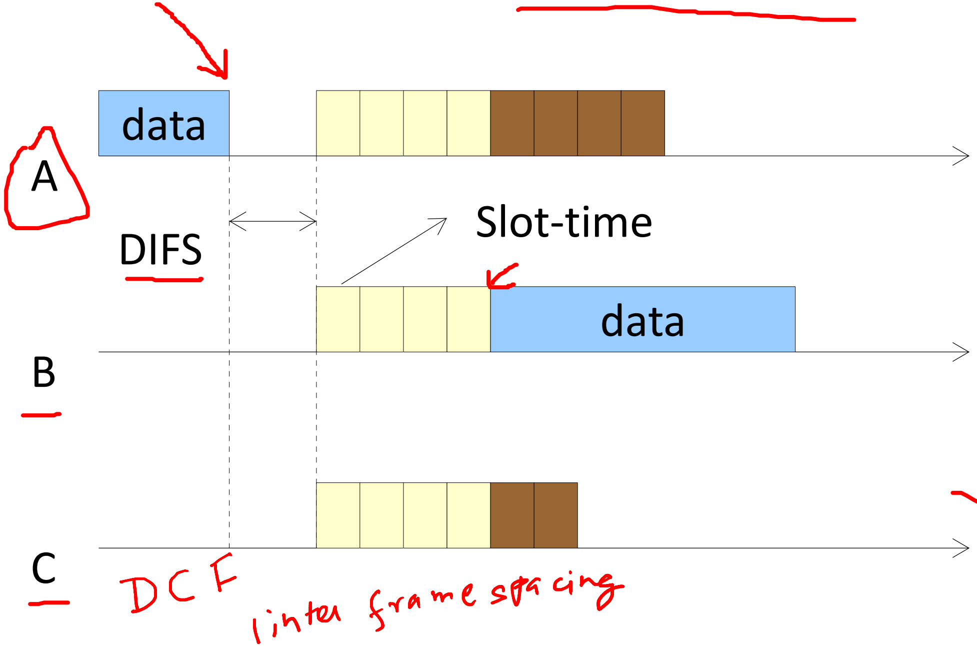
Ethernet CSMA/CD: Prelude to 802.11 → CSMA/CA (DCF)

- CSMA/CD: Carrier-Sense Multiple Access with Collision Detection
  - Listen before transmit (CS)
  - Tx when (as soon as) medium is free (1-persistent)
  - Collision Detection (CD)
  - Backoff (exponential) on collision

802.11 CSMA/CA

- Collision detection (near) impossible in wireless
  - Tx power is relatively very high near the transmitter
- Conceptual name is CSMA/CA: Carrier-Sense Multiple Access with Collision Avoidance
  - 802.11 calls it DCF (Distributed Coordination Function)
- Collision Avoidance:
  - Backoff before tx (even when no collision)
  - Contention Window (CW) in terms of number of slots

The Backoff Procedure



Contention *window:*

Num slots = Random[0, CW)

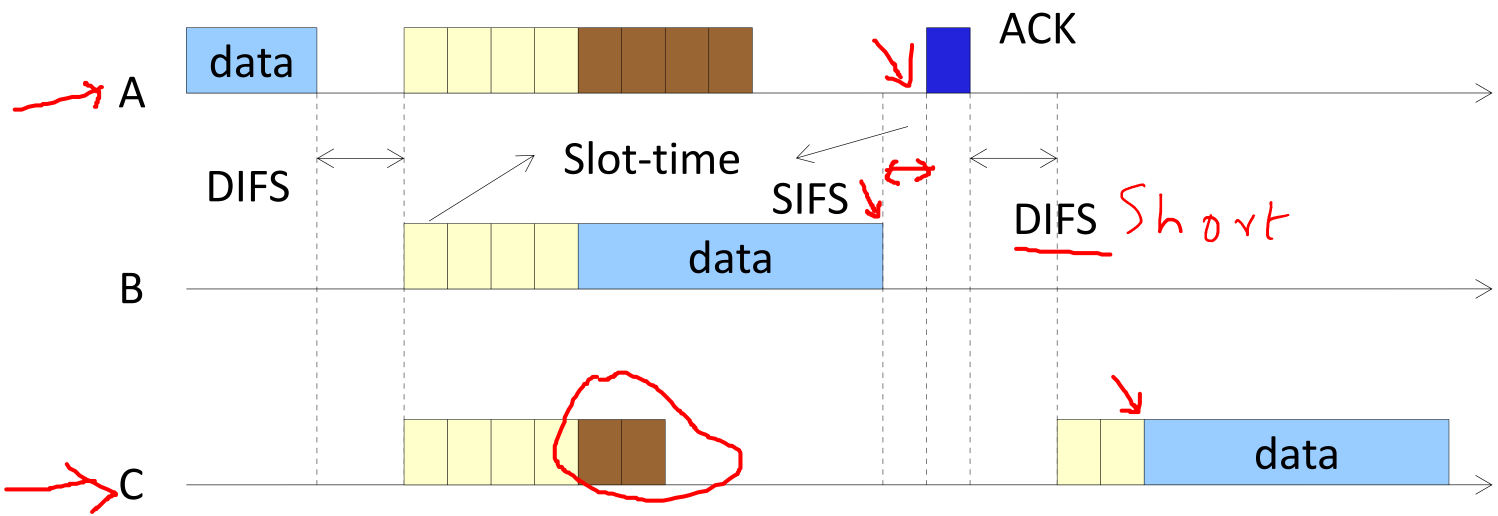
CW = 16, 32, 64, ..., 1024

Double CW on collision

Question: Why DIFS?

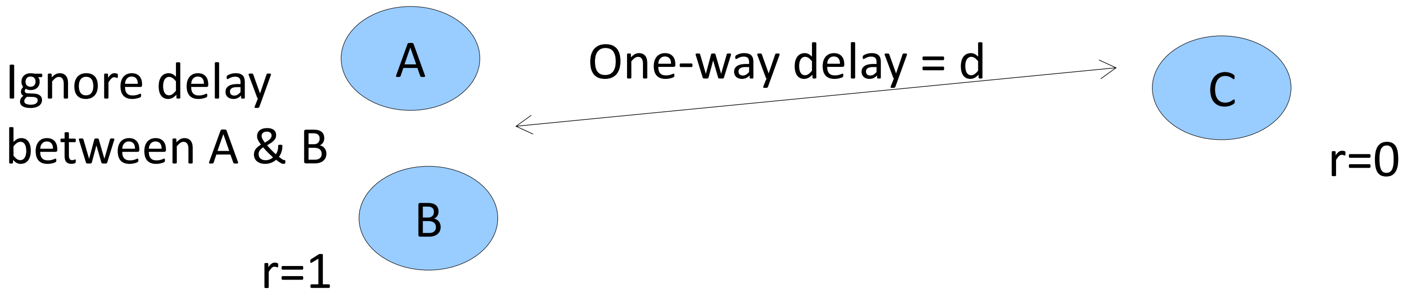
Use immediate ACK; no ACK ➔ *assume collision*

CSMA/CA + ACK



- ACK missing ➔ deduce collision, retransmit
  - Have to contend anew
- SIFS should be < DIFS
  - Else, ACK timeout may occur unnecessarily

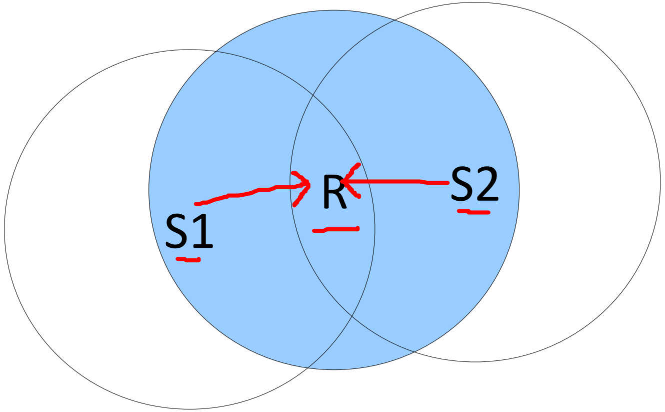
What Determines Slot Time?



1. A finishes tx at time t
2. B senses channel as free at t, C senses channel as free at t+d
3. C starts sending at t+d+DIFS, this reaches B at t+d+DIFS+d
4. B should not have started tx by then → slot-time should be > 2d

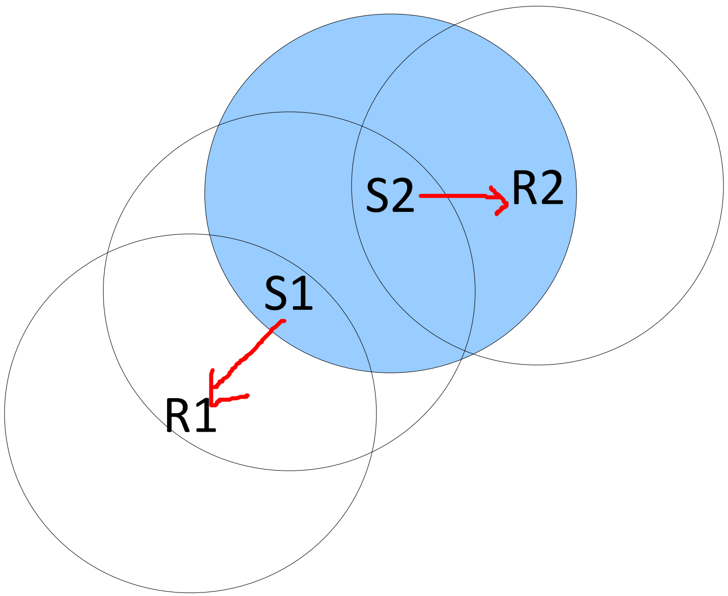
- Slot-time has other dependences as well
- Slot-time: 802.11b is 20 micro-sec, for 802.11g/a/n is 9 micro-sec

The Hidden Node Problem



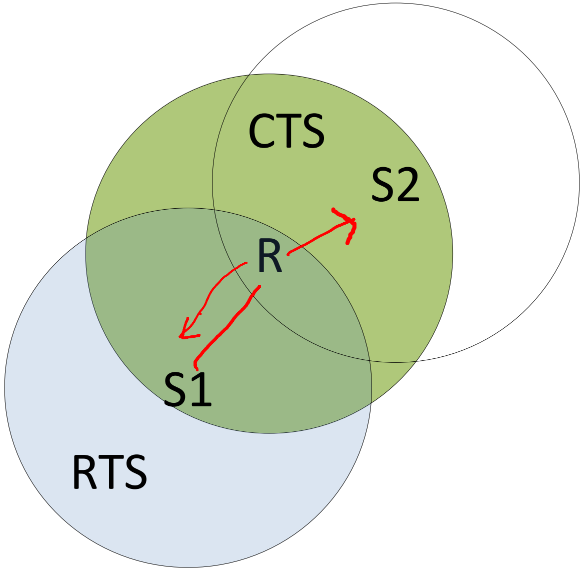
Medium is free DOES NOT IMPLY ok to transmit

The Exposed Node Problem



Medium is busy DOES NOT IMPLY not-ok to transmit

Hidden Node Solution: RTS/CTS

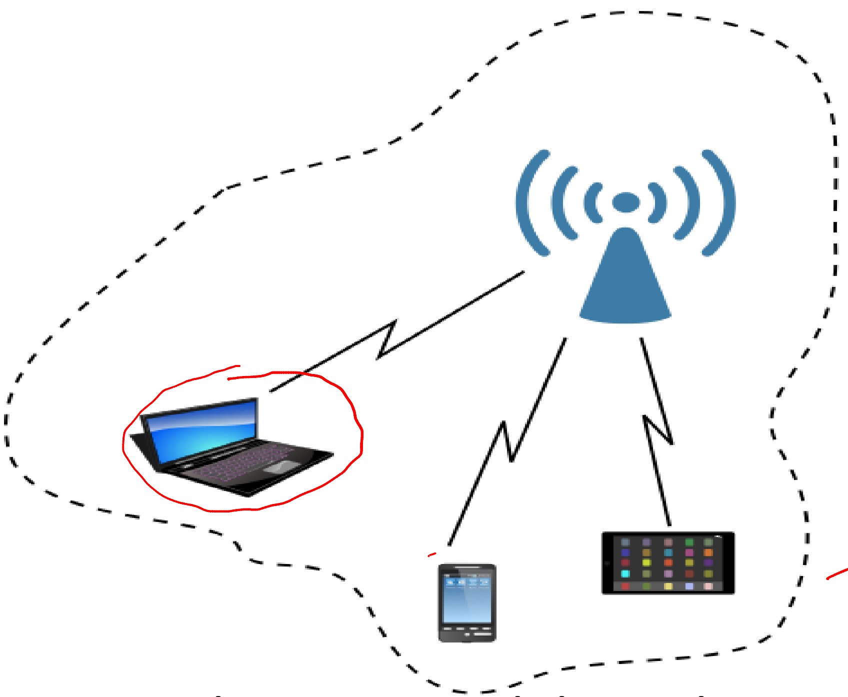


1. S1 says "can I send for X duration?" (RTS)
2. R says "yes, send for Y duration" (CTS)
3. S2 knows to be silent for Y duration

RTS/CTS Questions

1. Access mechanism before sending RTS?
2. Gap between RTS & CTS?
3. Gap between CTS & ~~ACK~~ Data?
4. Can there be collision of two RTS frames?
5. What if range is non-circular? Will it work?
6. Does RTS/CTS address the exposed node problem?

802.11 Management: Beacons and Probes

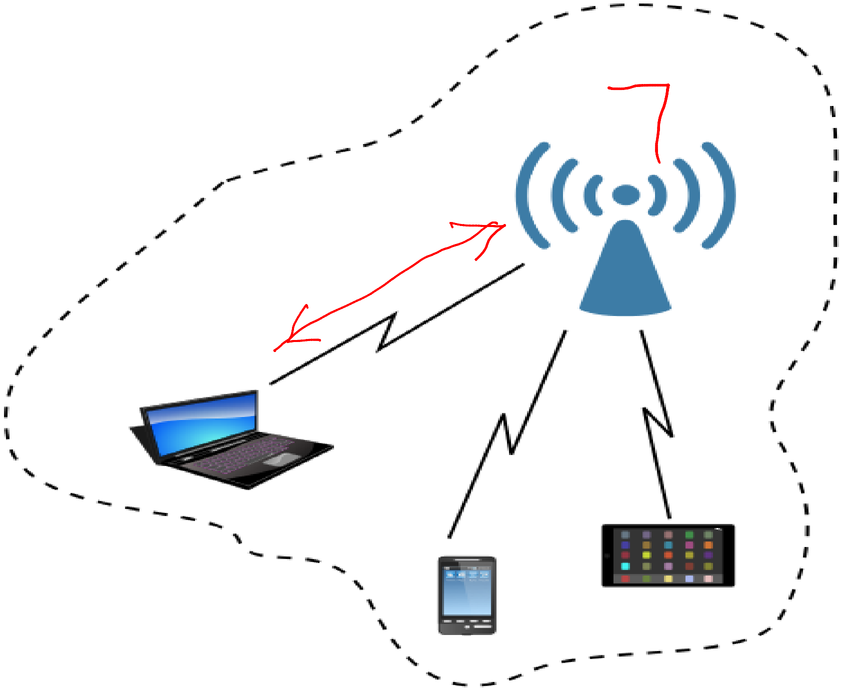


- A client may be in the coverage area of many APs
- APs send periodic beacons
- Client may passively scan these
- Or, probe-response for active scanning

Probe request

Beacon has: AP capabilities, beacon period, SSID, Traffic Indication Map (TIM)

802.11 Management: Authentication and Association



- A client has to
  - Authenticate itself to an AP
  - Then Associate itself
- A client may authenticate itself to many APs to speed-up roaming

802.11n Frame Format

Duration of reserved transmission time (RTS/CTS)

Frame seq # (for reliable ARQ)

For error detection

2	2	6	6	6	2	6	2	4	0 - 7951	4
Frame control	Durn/ ID	Addr1	Addr2	Addr3	Seq ctl	Addr4	QoS ctl	HT ctl	MAC payload	CRC

Address 1: always the receiver's address (RA)

Address 2: always the transmitter's address

Address 3: depends on ToDS/FromDS fields in Frame control; BSSID in most cases (MAC address of AP)

Address 4: needed, used only in mesh mode

802.11n Frame Control

2	2	4	1	1	1	1	1	1	1	1
Protocol version	Type	Subtype	To DS	From DS	More frag	Retry	Power mgt	More data	Prot. frame	Order

Management
Control
Data

Mgt: beacon, probe req/resp, assoc req/resp, auth req/resp
Ctl: ack, RTS, CTS
Data: data, poll

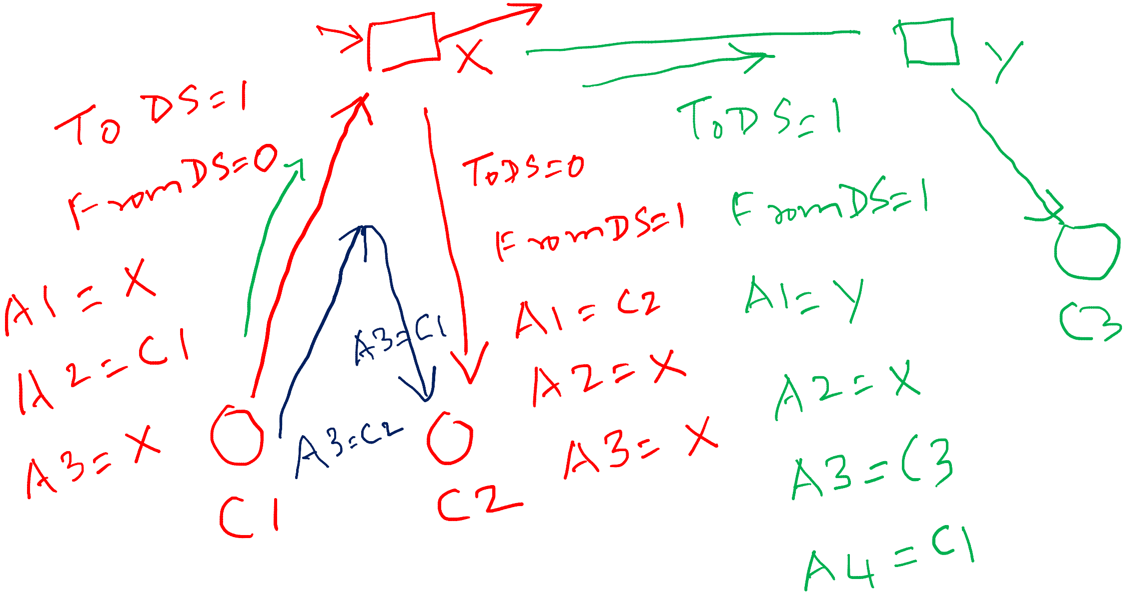
Is frame to DS?

Is frame from DS?

Used by client to indicate to AP that it is going into power save mode

Used by AP to tell client that AP has more data buffered for client at the AP

Address Field Usage Examples

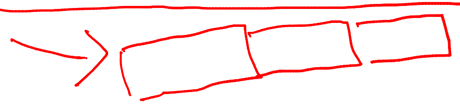


Throughput Estimation in 802.11

- PHY preamble + header: 24 bytes
- RTS: 20 bytes, CTS: 14 bytes
- MAC header: 28 or 34 bytes
- IP header: 20 bytes
- TCP header: 20 bytes
- UDP header: 8 bytes
- Bottomline: too much per-packet overhead!
- 802.11n introduces frame aggregation

DCF

DIFS
random backoff
RTS ↔ CTS ↔ DATA ↔ ACK



Summary

- Wireless flexible, but poses challenges
- Wi-Fi: PHY, MAC, Link, Management