Case Study: 802.11 (Technology Overview)

Kameswari Chebrolu

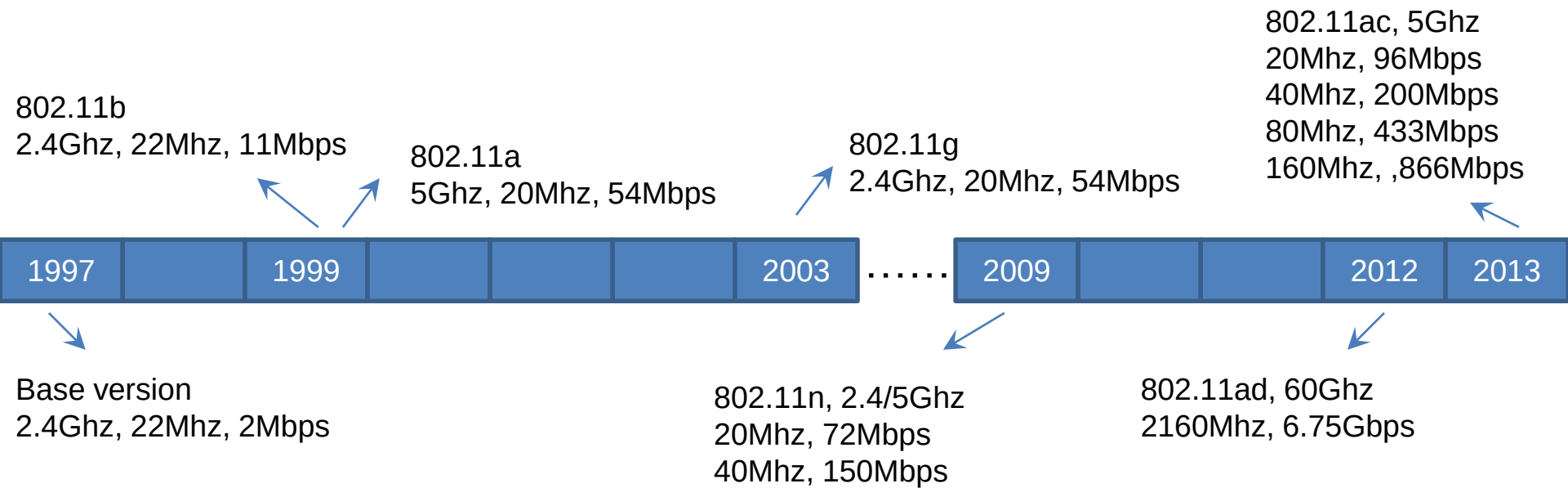
802 Protocol Family

- Family of IEEE (Institute of Electrical and Electronics Engineers) standards that deals with local and metropolitan area networks
  - 802.3 : Ethernet
  - 802.4: Token Ring
  - **802.11: Wireless LAN and Mesh**
  - 802.15: Wireless PAN (802.15.1: Bluetooth, 802.15.4: Zigbee)
  - 802.16: Broadband wireless (WiMAX)

IEEE 802.11

- LAN Technology: Range is 30 to 50m; can extend to kms also
- Extremely successful technology
  - Multi-billion dollar market
- Defines MAC and PHY layer specifications for implementing WLAN functionality

Evolution


802.11b
2.4Ghz, 22Mhz, 11Mbps
802.11a
5Ghz, 20Mhz, 54Mbps
802.11g
2.4Ghz, 20Mhz, 54Mbps
802.11ac, 5Ghz
20Mhz, 96Mbps
40Mhz, 200Mbps
80Mhz, 433Mbps
160Mhz, ,866Mbps
1997
1999
2003
2009
2012
2013
Base version
2.4Ghz, 22Mhz, 2Mbps
802.11n, 2.4/5Ghz
20Mhz, 72Mbps
40Mhz, 150Mbps
802.11ad, 60Ghz
2160Mhz, 6.75Gbps

Alphabet Soup

IEEE 802.11a: 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
IEEE 802.11b: Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)
IEEE 802.11c: Bridge operation procedures; included in the IEEE 802.1D standard (2001)
IEEE 802.11d: International (country-to-country) roaming extensions (2001)
IEEE 802.11e: Enhancements: QoS, including packet bursting (2005)
IEEE 802.11F: Inter-Access Point Protocol (2003) Withdrawn February 2006
IEEE 802.11g: 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
IEEE 802.11h: Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)
IEEE 802.11i: Enhanced security (2004)
IEEE 802.11j: Extensions for Japan (2004) IEEE 802.11-2007: A new release of the standard that includes amendments a, b, d, e, g, h, i and j. (July 2007)
IEEE 802.11k: Radio resource measurement enhancements (2008)
IEEE 802.11n: Higher throughput improvements using MIMO (multiple input, multiple output antennas) (September 2009)
IEEE 802.11p: WAVE—Wireless Access for the Vehicular Environment (such as ambulances and passenger cars) (July 2010)
IEEE 802.11r: Fast BSS transition (FT) (2008)
IEEE 802.11s: Mesh Networking, Extended Service Set (ESS) (July 2011)

Alphabet Soup

IEEE 802.11u: Improvements related to HotSpots and 3rd party authorization of clients, e.g. cellular network offload (February 2011)

IEEE 802.11v: Wireless network management (February 2011)

IEEE 802.11w: Protected Management Frames (September 2009)

IEEE 802.11y: 3650–3700 MHz Operation in the U.S. (2008)

IEEE 802.11z: Extensions to Direct Link Setup (DLS) (September 2010) IEEE 802.11-2012: A new release of the standard that includes amendments k, n, p, r, s, u, v, w, y and z (March 2012)

IEEE 802.11aa: Robust streaming of Audio Video Transport Streams (June 2012)

IEEE 802.11ac: Very High Throughput <6 GHz; potential improvements over 802.11n: better modulation scheme (expected ~10% throughput increase), wider channels (estimate in future time 80 to 160 MHz), multi user MIMO; (December 2013)

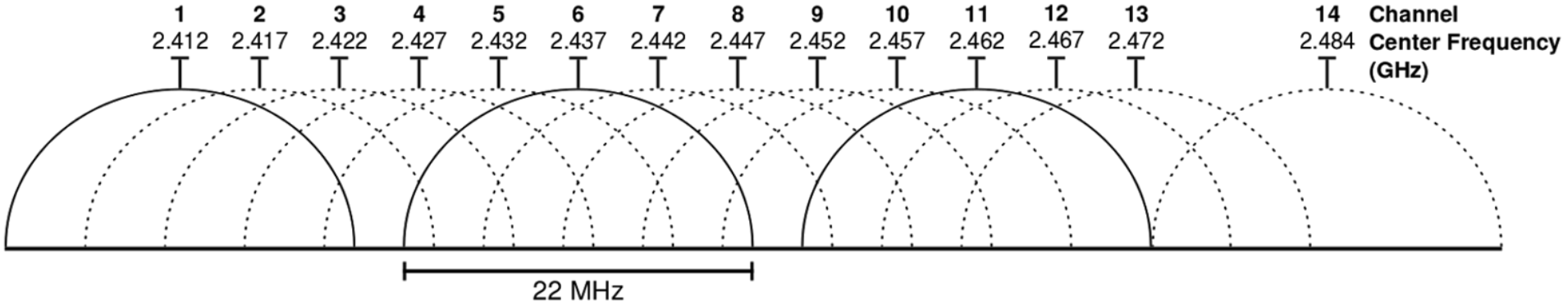
IEEE 802.11ad: Very High Throughput 60 GHz (December 2012)

IEEE 802.11ae: Prioritization of Management Frames (March 2012)

IEEE 802.11af: TV Whitespace (February 2014)

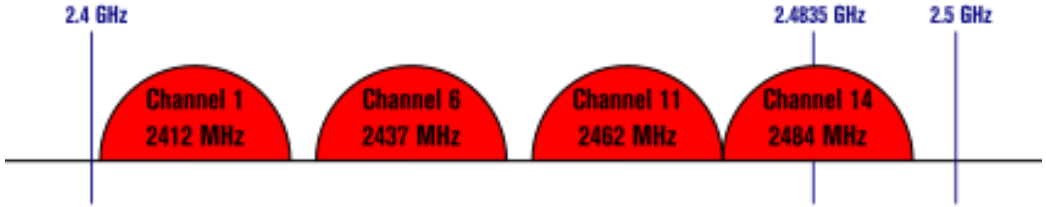
Frequency Band

- WiFi operates over many bands: 900Mhz, **2.4Ghz,** 3.6Ghz, 4.8Ghz, **5Ghz**, 5.9 Ghz, 60Ghz
  - Countries apply their own regulations



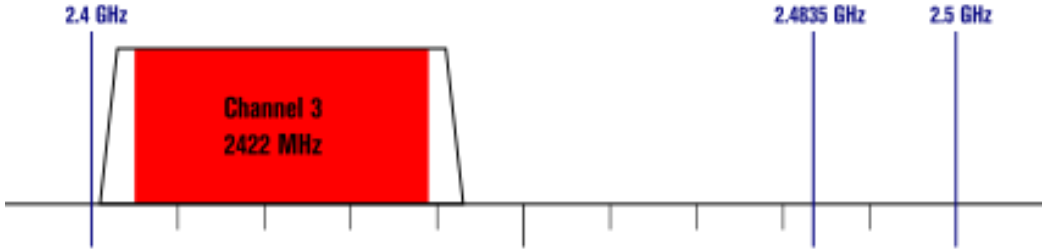
Non-Overlapping Channels for 2.4 GHz WLAN

802.11b (DSSS) channel width 22 MHz



802.11g/n (OFDM) 20 MHz ch. width – 16.25 MHz used by sub-carriers

802.11n (OFDM) 40 MHz ch. width – 33.75 MHz used by sub-carriers



Terminology

- Station: A unit that access the media (equipped with a wireless network interface)
  - Access Point: Act as wireless router
  - Client: Laptops, smart phones etc

- Basic Service Set (BSS): Set of stations that communicate with each other
  - Associated with an ID called BSSID (MAC address of the AP servicing the BSS)
  - Two types of BSS: Infrastructure and Independent

Mode of Operation

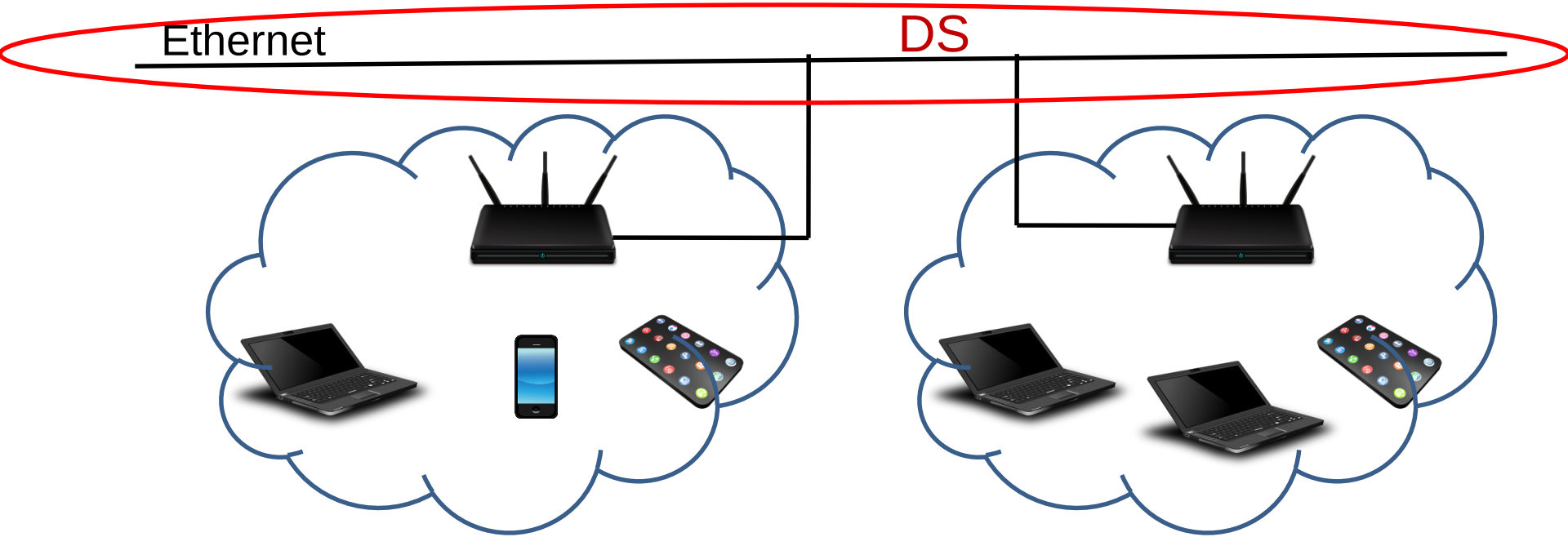
- Infrastructure Mode: Stations communicate with others via an Access Point (AP)
  - **Distributed Coordinated Function (DCF)**
  - Point Coordinated Function (PCF)
    - Centralized polling based implementation (not used)

Infrastructure BSS

- Adhoc Mode: Stations communicate with each other directly (no AP)

Independent BSS (IBSS)

- Extended Service Set (ESS): Set of connected BSSs.
  - Associated with an SSID (32 byte character string)
- Distributed System (DS): Connects the APs that are part of an extended service set.

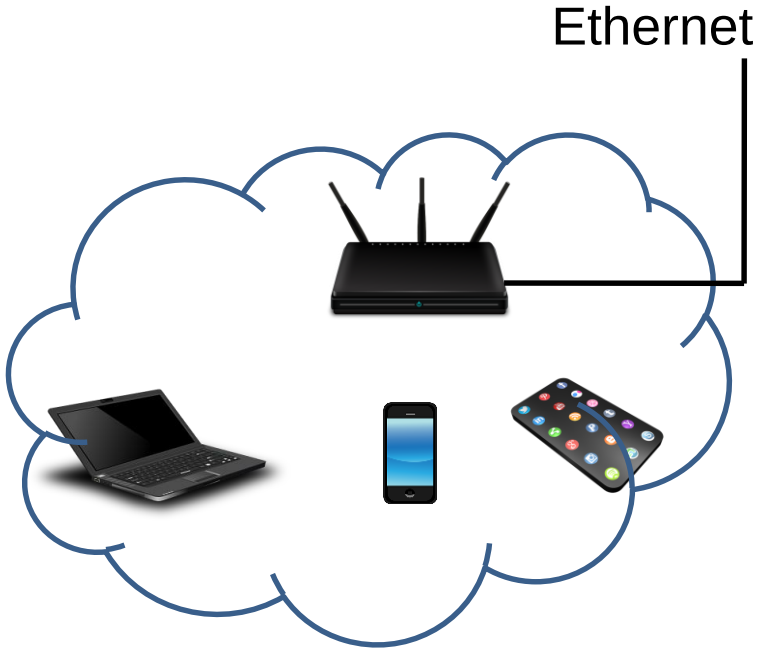


Break

Slurp!

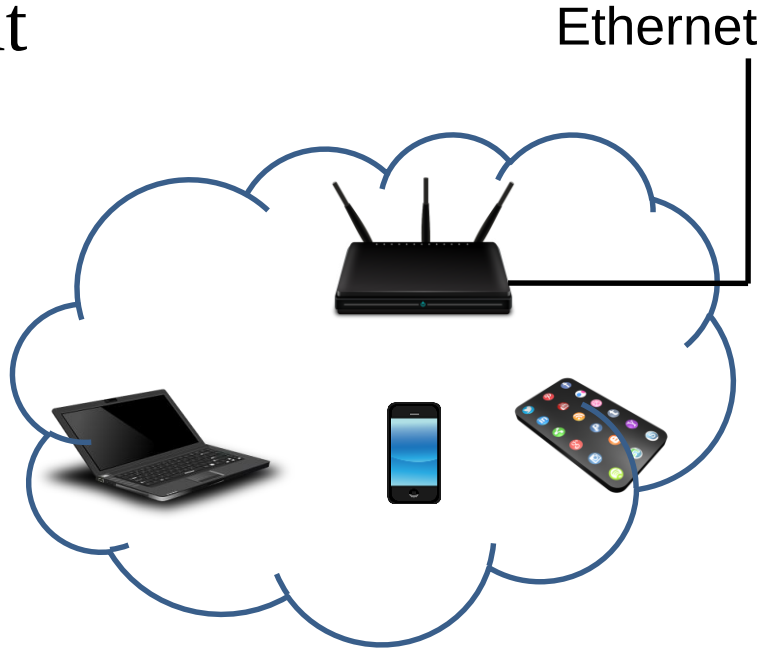
Working of WiFi: SSID -- 1

- Every AP configured with an SSID
- SSID broadcast via periodic beacons
  - Beacons carry other information: AP capabilities, time-stamp, beacon interval, Traffic Indication Map (TIM, used in power save mode)
  - Typically sent once every 100ms



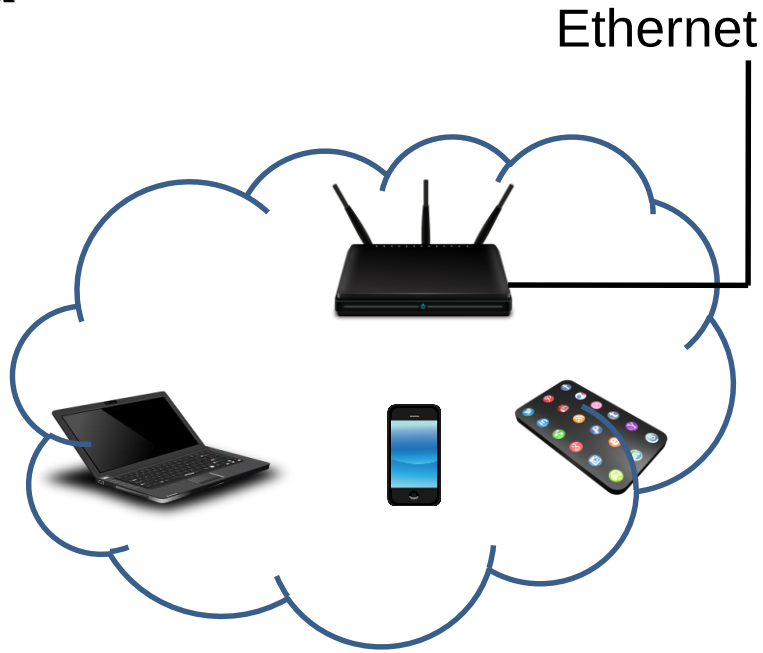
Working of WiFi: Scanning -- 2

- Client can be in coverage area of many APs operating over different channels
- Passive Scanning: Scan channels and simply listen to beacons
- Active Scanning: Probe request from client elicits probe response from AP
  - Scanning all channels time consuming; can save time



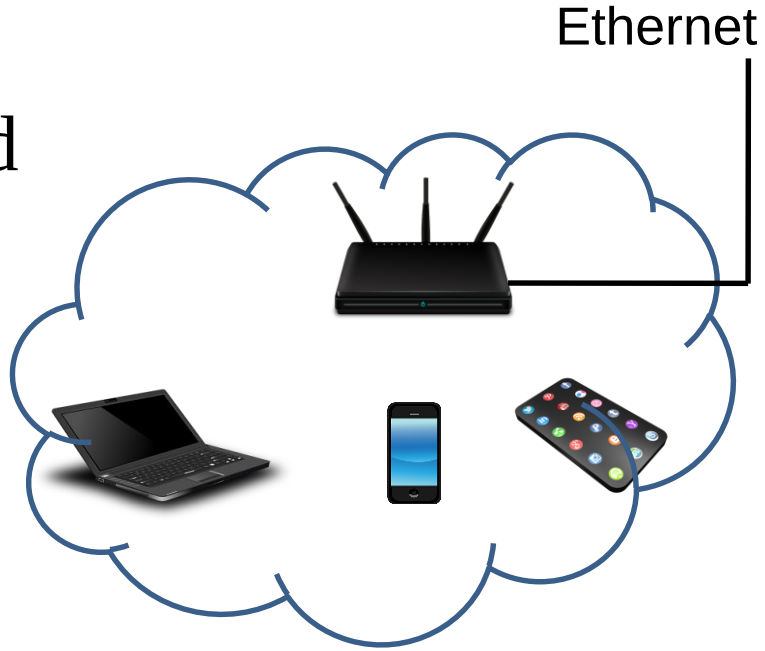
Working of WiFi: AP Selection -- 3

- Client acquires a list of APs via scanning
- Select “best” one
  - Based on signal strength
  - User preferences
  - Trust
  - Free or payment based



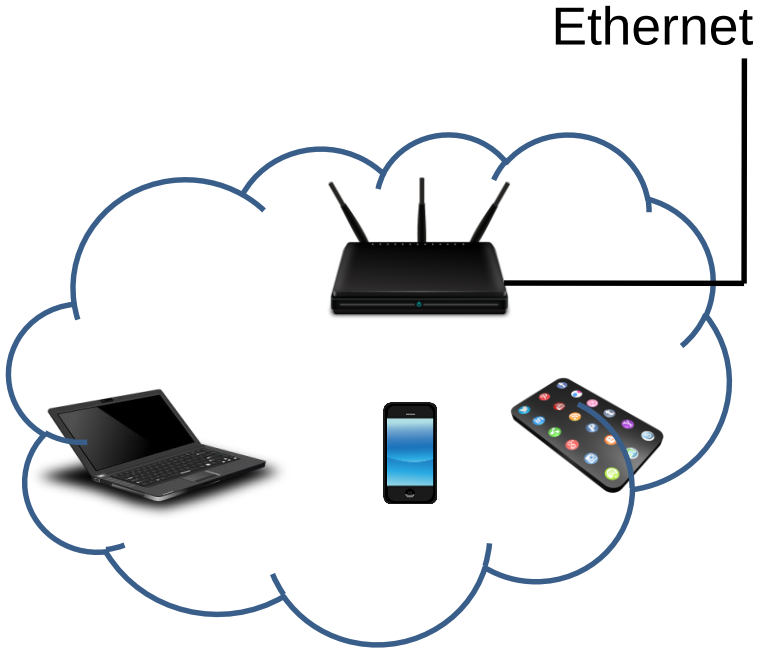
Working of WiFi: Authentication -- 4

- Allow only authorized clients to connect to AP
- Network security features defined by 802.11i
  - Apart from authentication, also provides data confidentiality
- A client can authenticate with multiple APs
  - Speeds up roaming



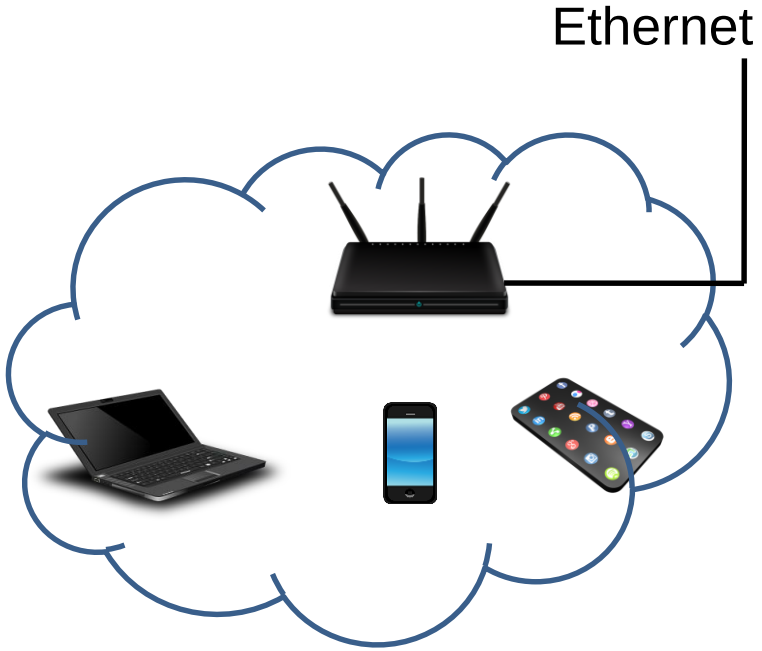
Working of WiFi: Association -- 5

- Any client must associate with an AP before data transfer
  - Can associate with only one AP at any time
  - Client packets are effectively routed
- Association request from client specifies its capabilities and SSID
- Association response from AP specifies accept or reject
- After association**, data transfer** can begin



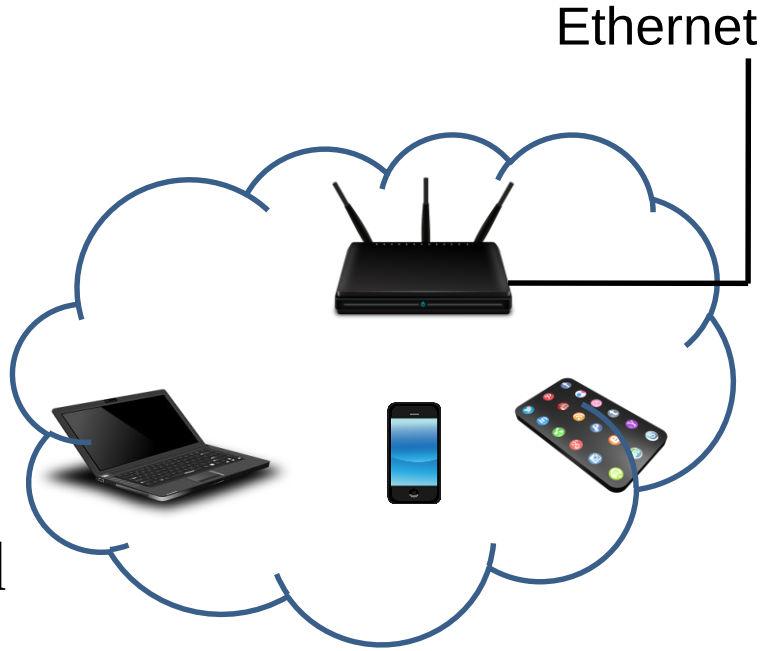
Working of WiFi: Re-Association -- 6

- Transfer association from current AP to new AP
  - E.g. poor signal strength
  - Supports layer-2 roaming
- Re-association algorithm is vendor specific
  - Only after link breaks
  - Active scanning (cannot receive frames when scanning)



Working of WiFi: Re-Association -- 6

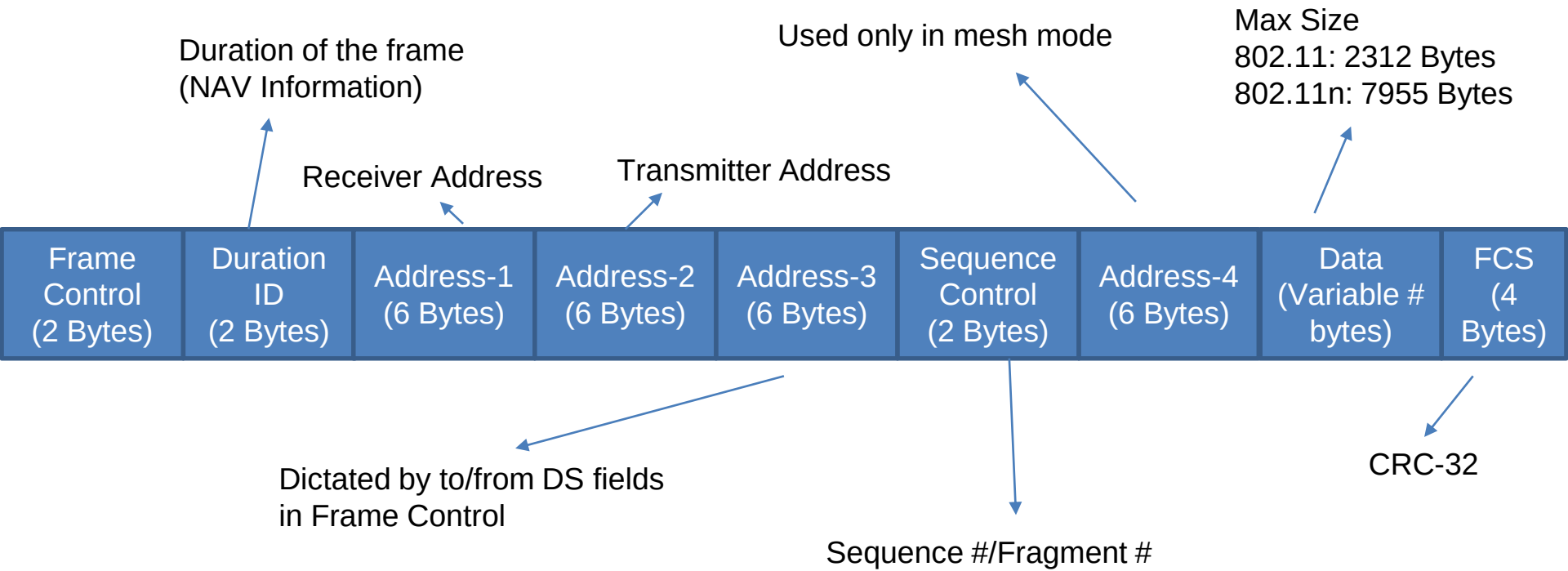
- Client sends association request to new AP
  - Also specifies old AP's id
- New AP accepts or rejects request
- If accept, new AP contacts old AP to get buffered packets
  - Coordination between APs defined by 802.11f



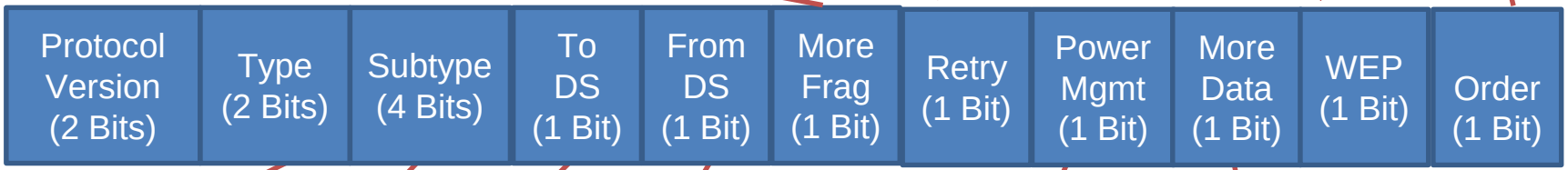
Types of Frames

- Management: Help maintain communication
  - Authentication, Association, Beacons, Probe request/response
- Data: Carry higher layer data (email, web traffic etc)
- Control: Facilitate exchange of data frames
  - ACK, RTS (Request to Send), CTS (Clear to Send)

Frame Format



Frame Control



Indicates if all received frames are to be processed in order

Is it a retransmission?

Indicates if the frame is protected

more fragments belonging to the same frame are to follow

Management, Control or 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?

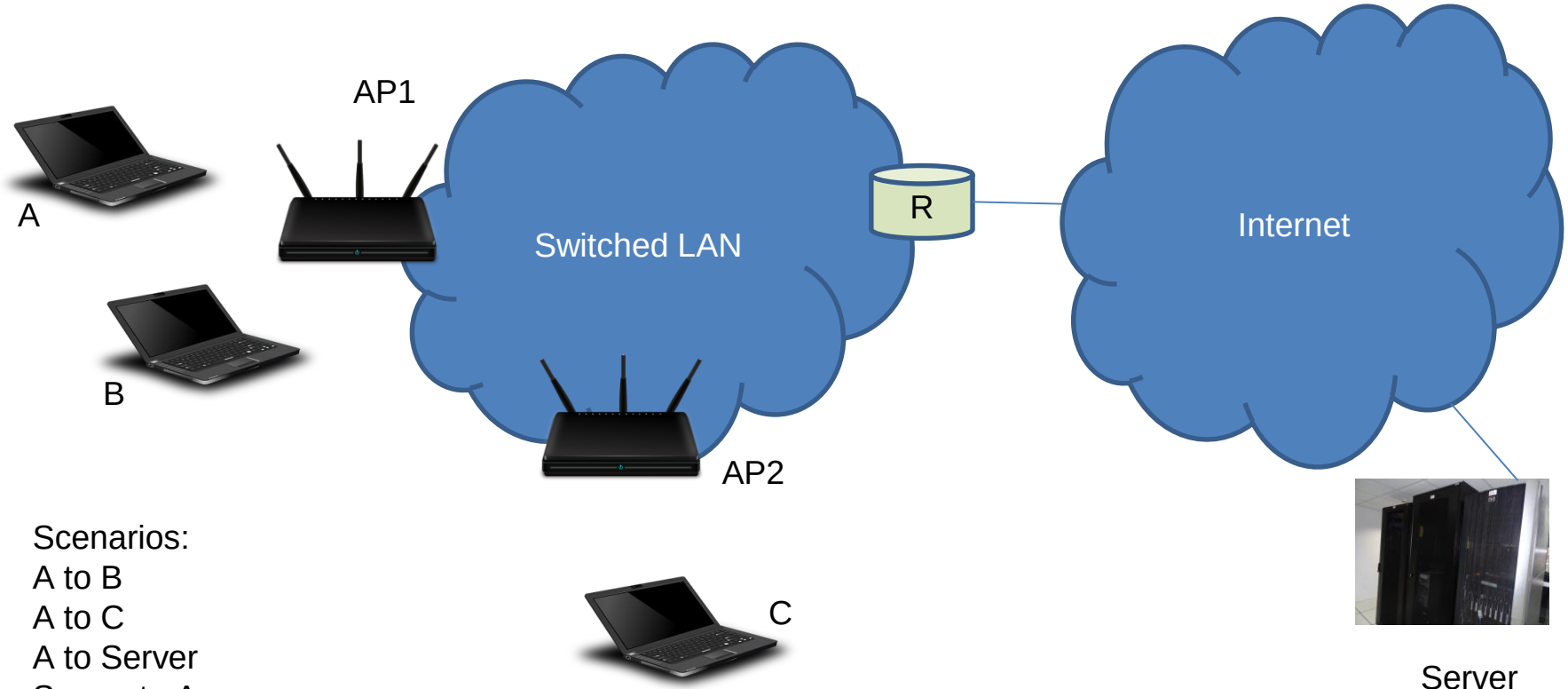
Used by client to indicate to AP that it is going into power save mode

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

To DS	From DS	Direction	Address1	Address 2	Address 3	Address 4
0	0	Data frame from STA to another STA in IBSS; All mgmt. and control frames	DA	SA	BSSID	n/a
0	1	AP to STA	DA	BSSID	SA	n/a
1	0	STA to AP	BSSID	SA	DA	n/a
1	1	One AP to another AP in same DS	RA	TA	DA	SA

RA: Receiver Address
TA: Transmitter Address
DA: Destination Address
SA: Source Address

802.11 based communication



Scenarios:
A to B
A to C
A to Server
Server to A

Summary

- 802.11: Extremely successful technology with many variants
- Looked at 802.11 terminology, modes of operation
  - AP, STA, BSSID, DS, SSID etc
  - Infrastructure and adhoc mode
- Understood how clients connect to APs and the frame structure employed
- Homework: Understand (using wireshark and ping) how 802.11 stations communicate with each other and with outside entities