Οικονομικό Πανεπιστήμιο Αθηνών
Τμήμα Πληροφορικής

Ευφυή Κινητά Δίκτυα: IEEE 802.11 - Μέρος Α

Γιάννης Θωμάς

Χειμερινό Εξάμηνο 2023-24

(Βασισμένο σε διαφάνειες του Βασίλειου Σύρη)

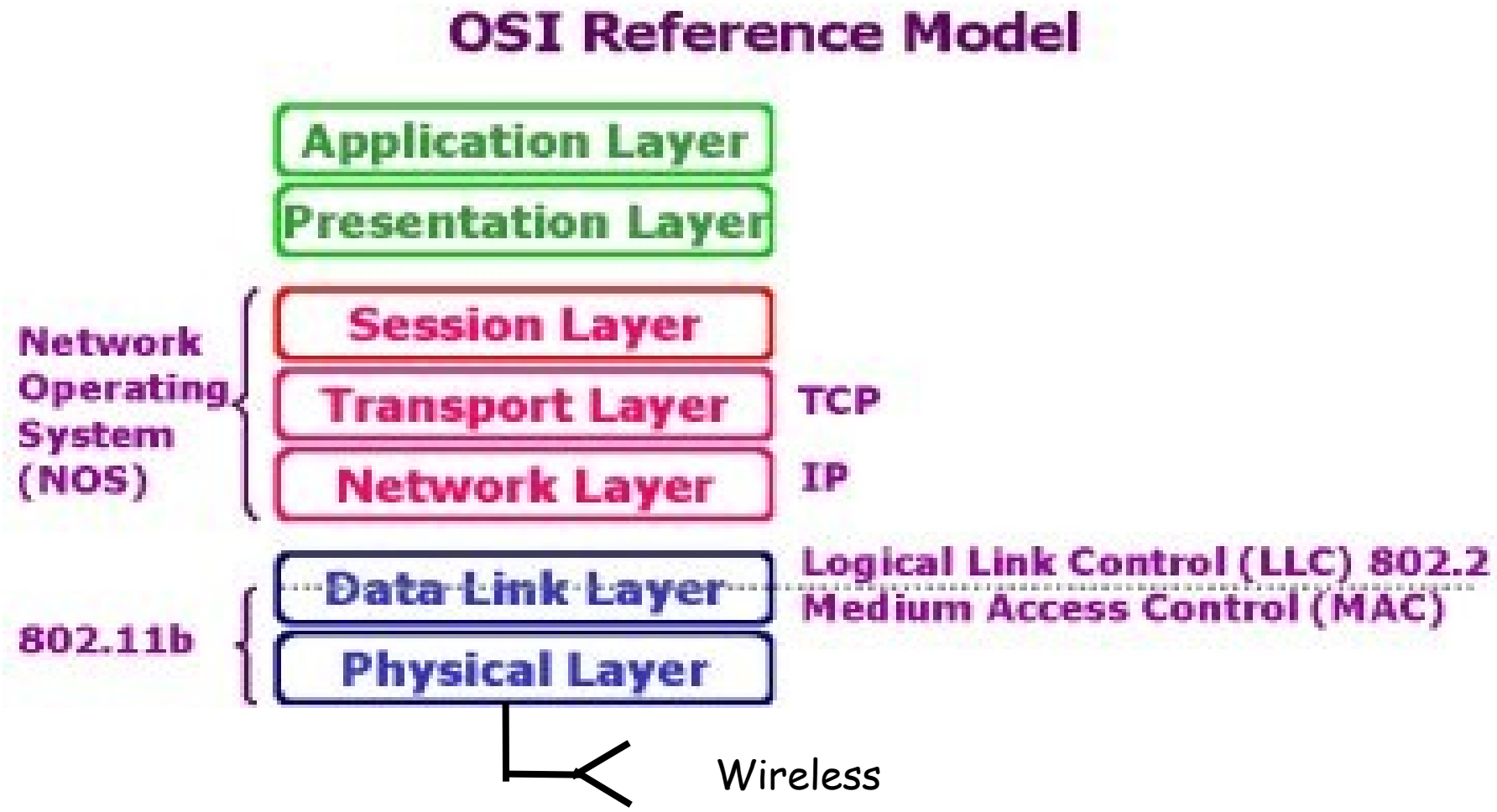
IEEE 802.11 Wireless LANs

- Architecture
- PHY specifications
- Components
- MAC mechanisms: DCF (CSMA/CA) and PCF
- Synchronization, Scanning/Roaming, Power management, transmission rate adaptation
- Recent advances: Wi-Fi 6 (802.11ax/ay), WiGig (60 GHz, 802.11ad), IoT support (< 1 GHz), etc
- Security

IEEE 802.11 - WiFi

- IEEE 802.11 working group formed 1990
- 802.11 used interchangeably with WiFi
  - WiFi=Wireless Fidelity
  - WiFi alliance: testing and certification of WLAN products
- IEEE 802.11/WiFi most popular and pervasive Wireless LAN (WLAN) standard
- Uses ISM (unlicensed) bands at 2.4 & 5 & 60 GHz, 54-790 MHz (white spaces, 802.11af), 900 MHz (ISM unlicensed band, 802.11ah)
  - initial standard also used 900 MHz

IEEE 802.11 and OSI model



IEEE 802.11 standards

- 802.11b (1999)
  - 2.4 GHz unlicensed spectrum
  - <11 Mbps
- 802.11a (1999)
  - 5 GHz,
  - up to 54 Mbps (OFDM)
- 802.11g (2003)
  - 2.4 GHz
  - <54 Mbps (20MHz, CSMA/CA)
- 802.11n (2008)
  - MIMO (x4), multiple channels (40MHz), 64 QAM
  - 2.4 & 5 GHz
  - <450 Mbps (x3, 40MHz), 600 Mbps (x4, 40MHz)
- 802.11ac (2014)
  - MIMO (x8), multiple channels (160MHz), 256 QAM
  - 5 GHz
  - <3.4 Gbps (x8, 80MHz) – 1.7 Gbps in practice
- 802.11ad (2012)
  - 60GHz
  - >Gbps, 2.16GHz BW

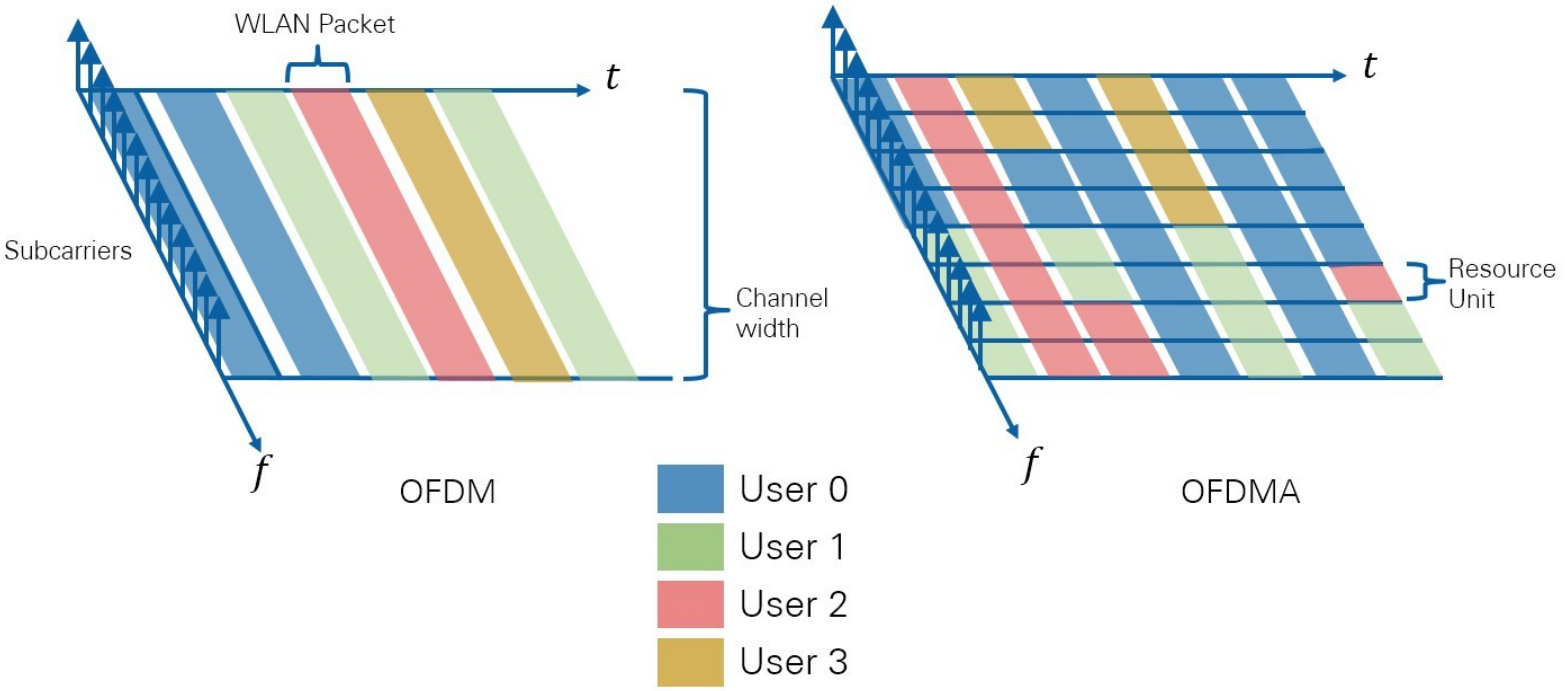
- CSMA/CA for multiple access
- Access point and ad-hoc network versions

2019 Wi-Fi standard

Wi-Fi 6: 802.11ax
Wi-Fi 5: 802.11ac
Wi-Fi 4: 802.11n

- IEEE 802.11ax / Wi-Fi 6
  - 1-6 GHz
  - Multi-user MIMO uplink & downlink (reception from multiple transmitters & concurrent transmission to multiple receivers)
  - OFDM**A** dynamic assignment of time-frequency Resource Units (RUs) by AP
  - Increased spatial reuse with dynamically adjusted transmit power and signal detection threshold
  - Target Wake Time (TWT): wake up at times other than beacon period – energy saving method

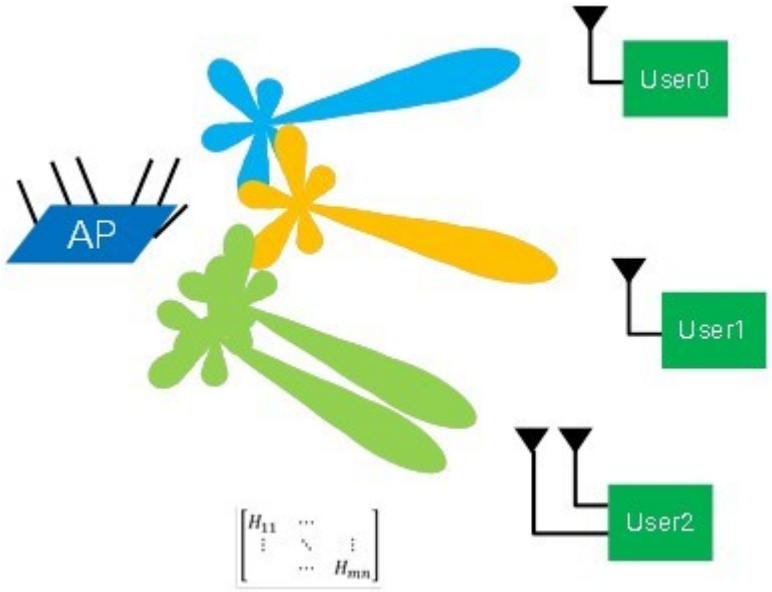
802.11ax OFDMA



- 802.11ax can assign specific sets of subcarriers or Resource Units (RUs) to individual users

Source: Texas Instruments / Microwaves & RF

802.11ax multi-user MIMO



- Beamforming directs packets simultaneously to spatially diverse users
- Up to eight multi-user MIMO transmissions (spatial streams) at a time

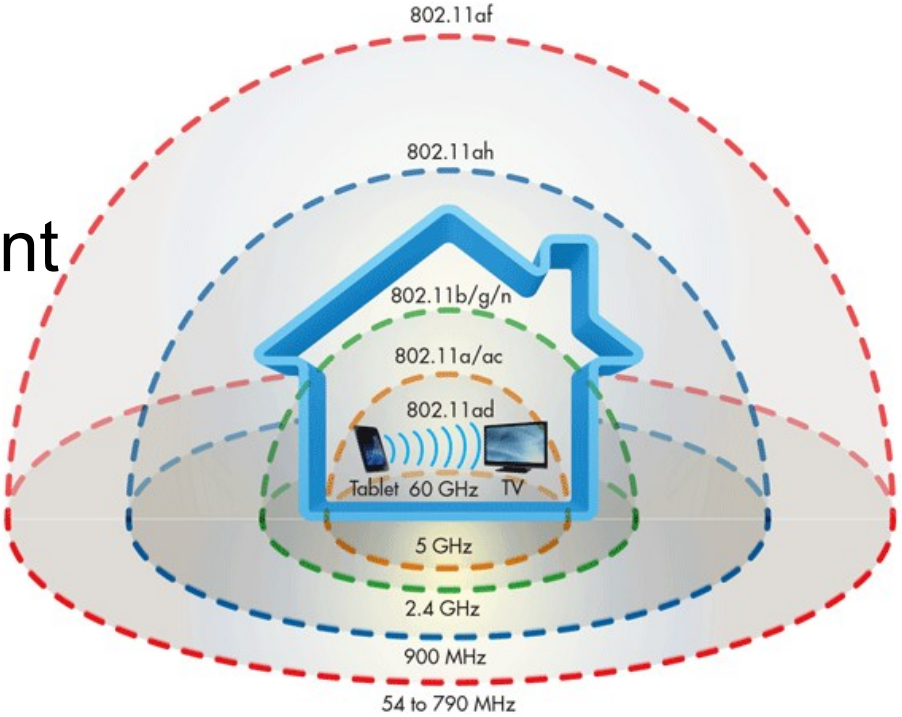
Source: Texas Instruments / Microwaves & RF

2019 Wi-Fi standards (cont.)

- IEEE 802.11ay
  - Improves IEEE 802.11ad
  - 60 GHz (as 802.11ad)
  - 20-40 Gbps, 300-500 meters
  - Channel bonding (max bandwidth 8.64 GHz)
    - Unifies 4 channels of 2.15GHz BW
  - 4 stream MIMO (44 Gbps per stream)
  - Higher order modulation (bits per symbol)
  - Ethernet alternative/replacement

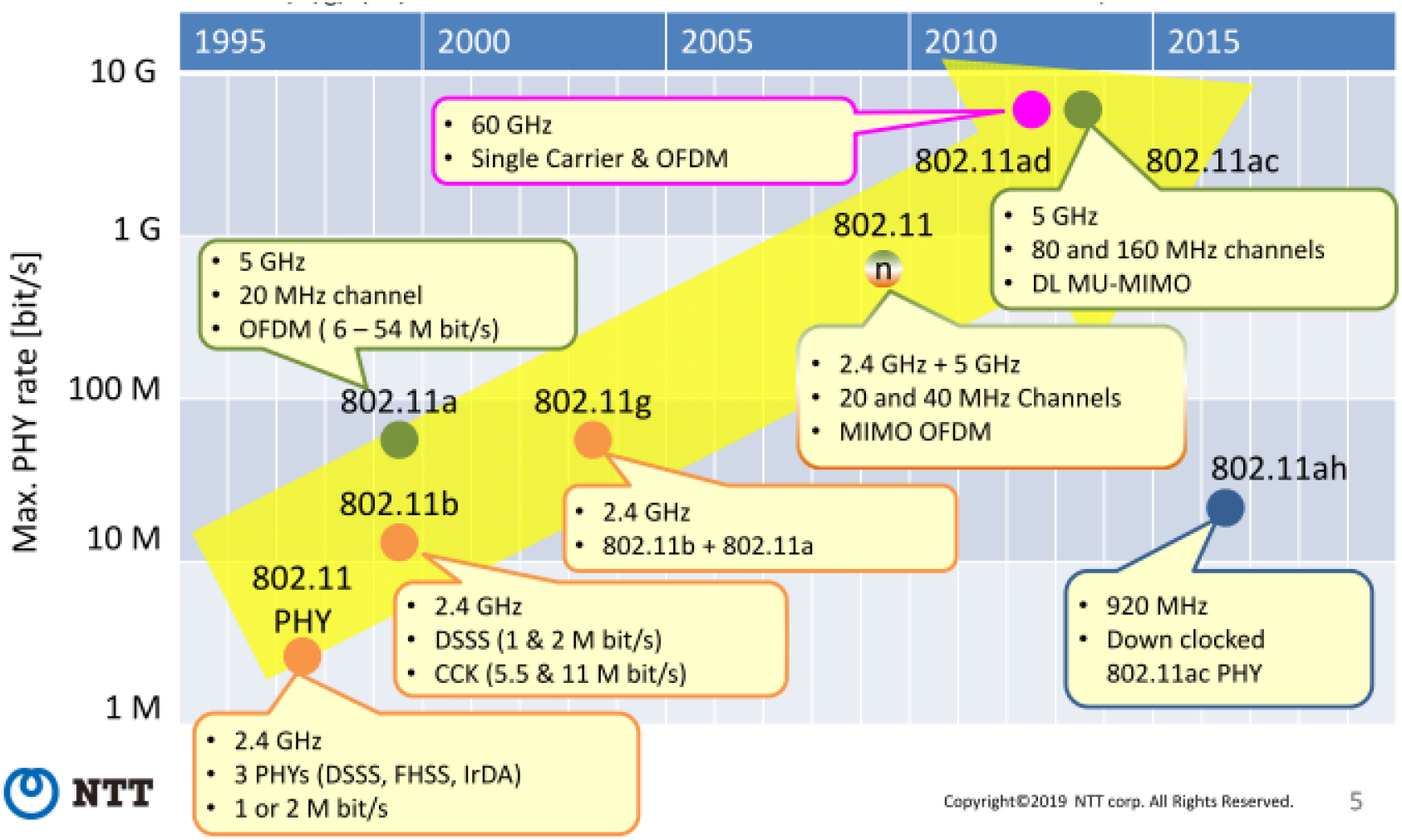
Both fast & long and slow & short

- Fast (higher speed) & long distance important
- Slow & short equally important
  - Longer battery lifetime, lower device cost, higher security
- Recent technologies:
  - IEEE 802.11ad (WiGig): 60 GHz, single room AP
  - IEEE 802.11af (White Wi-Fi), 802.11ah (low power Wi-Fi): <900MHz, long distance
  - 4G/LTE-M Rel-12/13: 1.4MHz, 0.2MHz (Broadband: 20MHz)



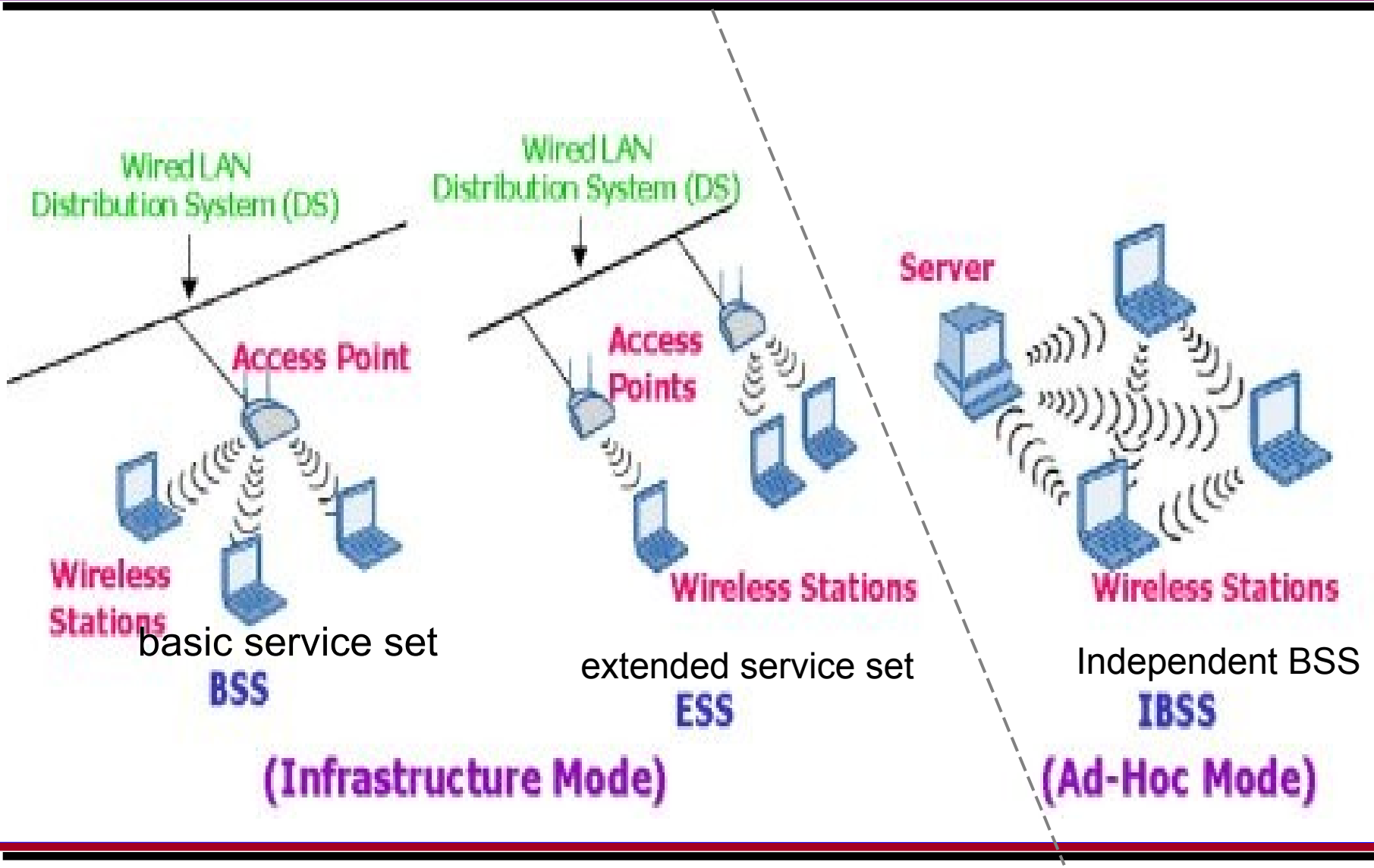
IoT (Internet of Things)

802.11 standards



NTT

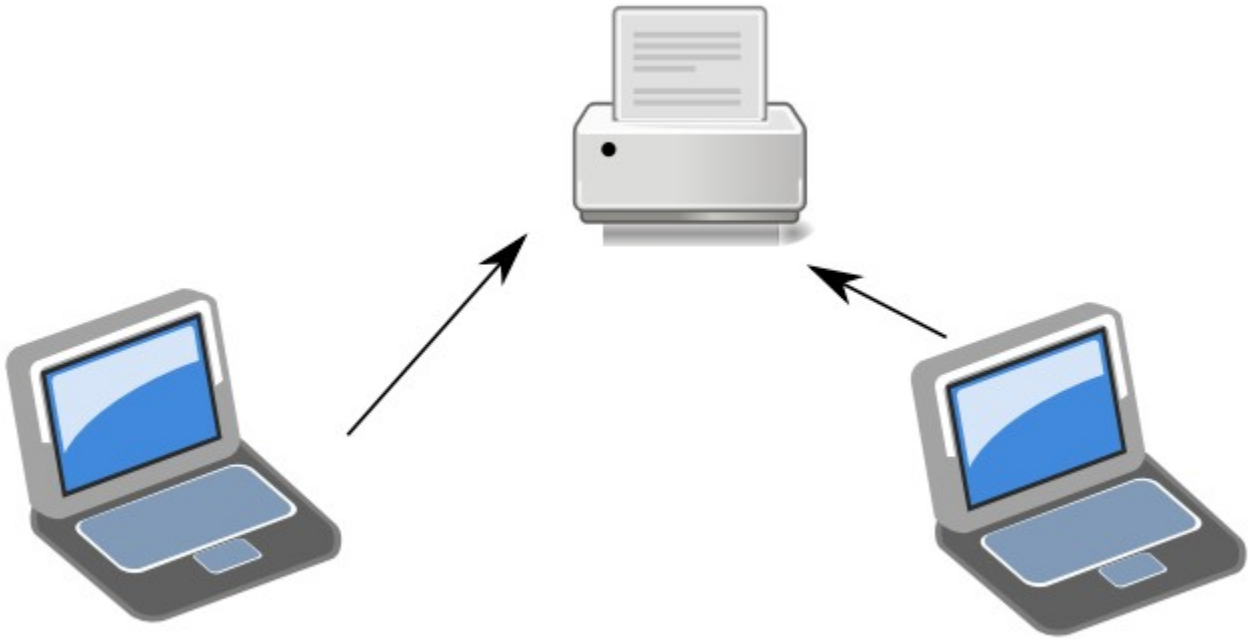
802.11 architecture – two modes



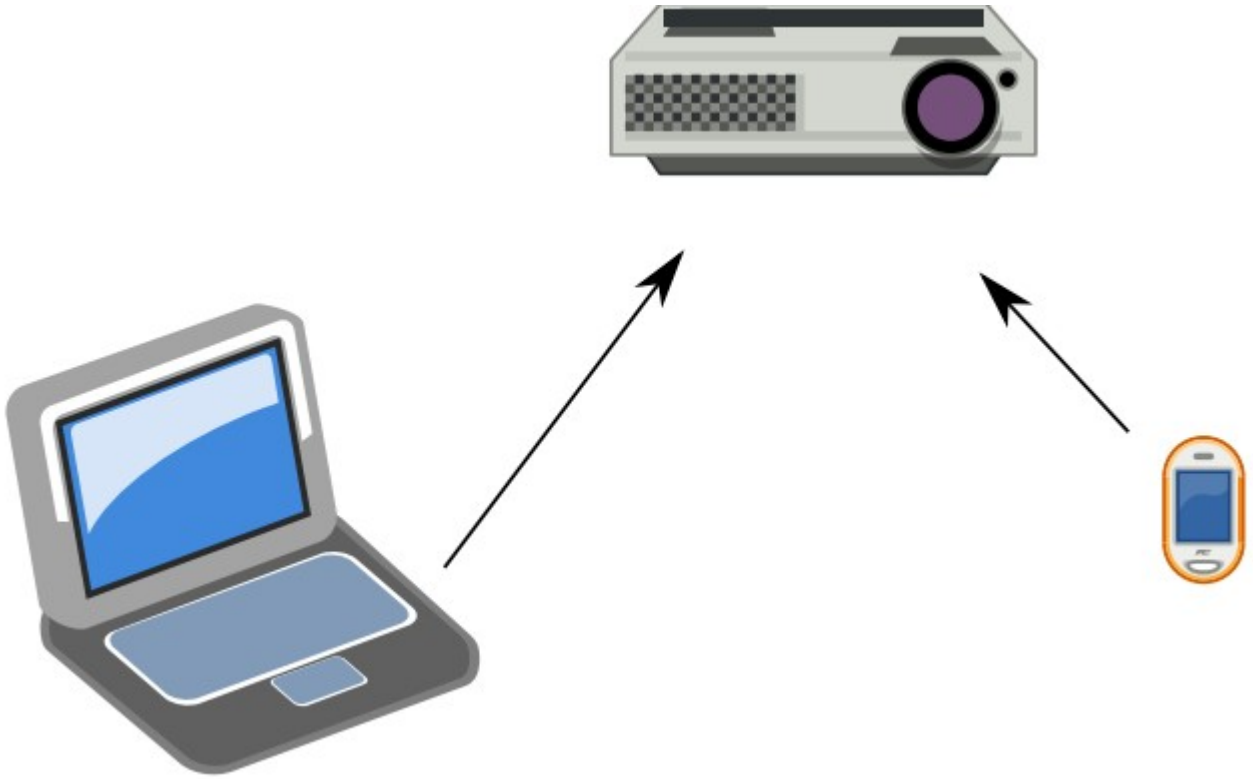
Wi-Fi P2P / Direct

- Wi-Fi peer-to-peer: technology, technical specification
- Wi-Fi direct: certification
- Like Wi-Fi ad-hoc (IBSS) but without packet relaying

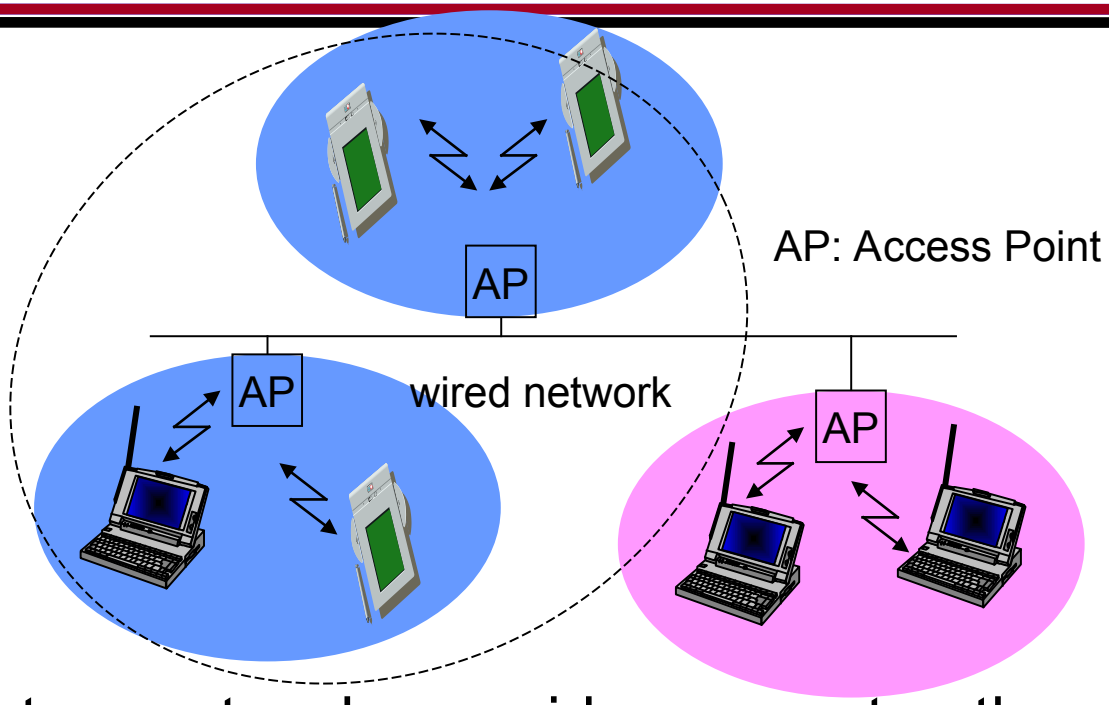
Wi-Fi Direct use cases



Wi-Fi Direct use cases



Infrastructure-based wireless network

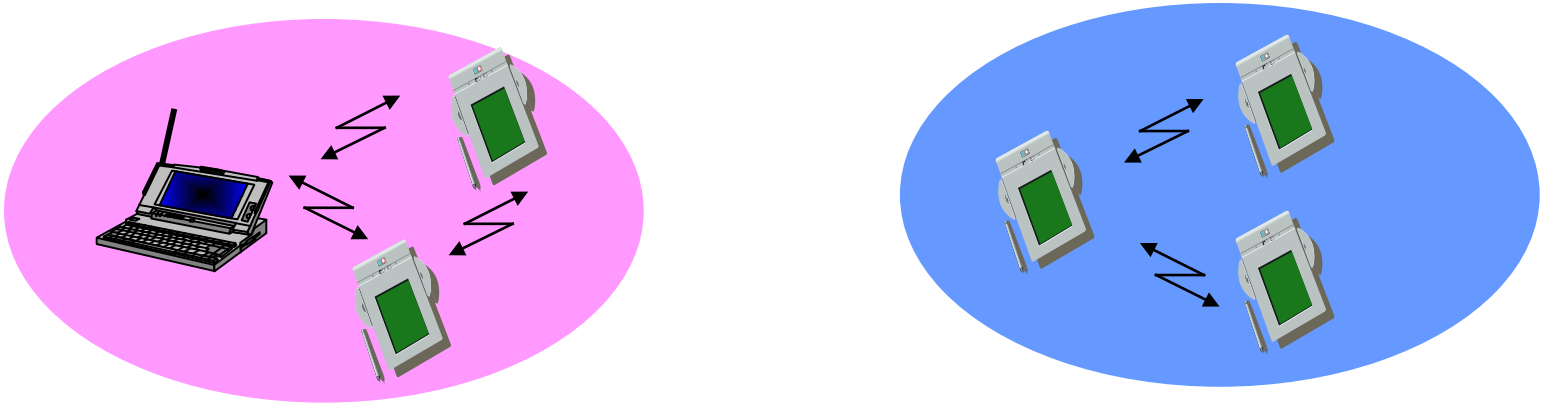


- Infrastructure networks provide access to other networks
- Communication typically takes place only between the wireless nodes and the access point (AP), but not directly between the wireless nodes
- AP not only controls medium access, but also acts as bridge to other wireless or wired networks

Infrastructure-based wireless network (cont.)

- Several wireless networks can form one logical network
  - APs together with the wired/wireless network in between can connect several wireless networks to form larger network beyond actual radio coverage
- Network connectivity functionality lies in APs, and wireless clients can remain quite simple
- Different access schemes with or without collision
  - Collisions may occur if medium access from wireless stations and AP is not coordinated.
  - Collisions avoided If only AP controls medium access
    - Useful for quality of service guarantees (e.g. minimum bandwidth)
    - AP polls stations for uplink data transmission

Ad hoc wireless network

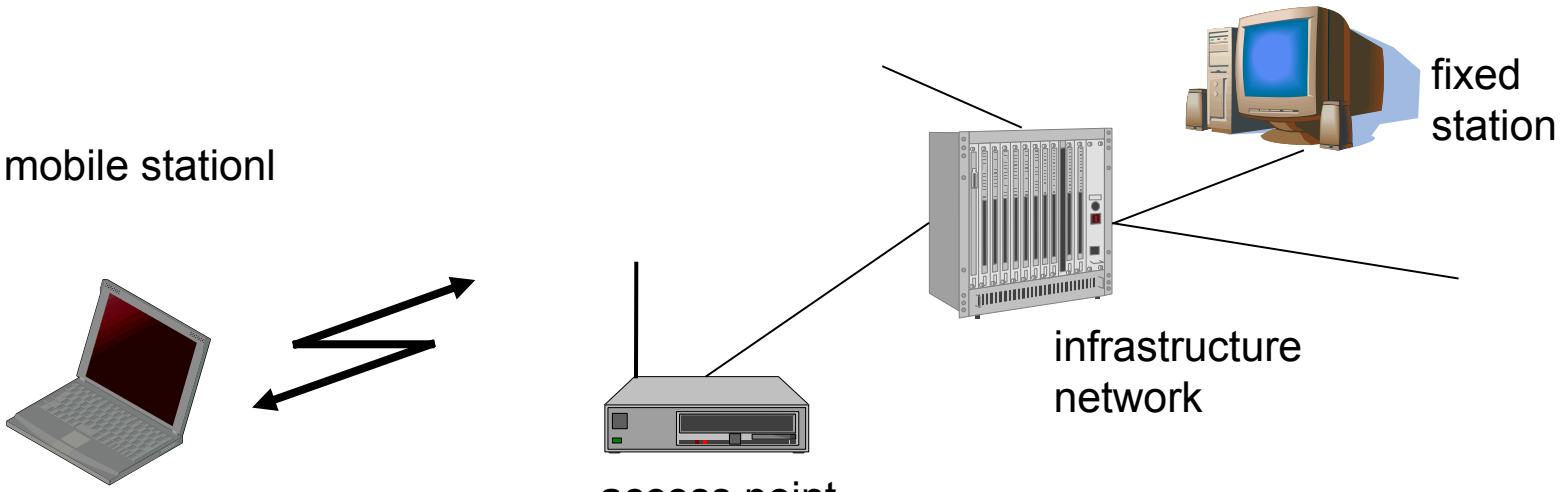


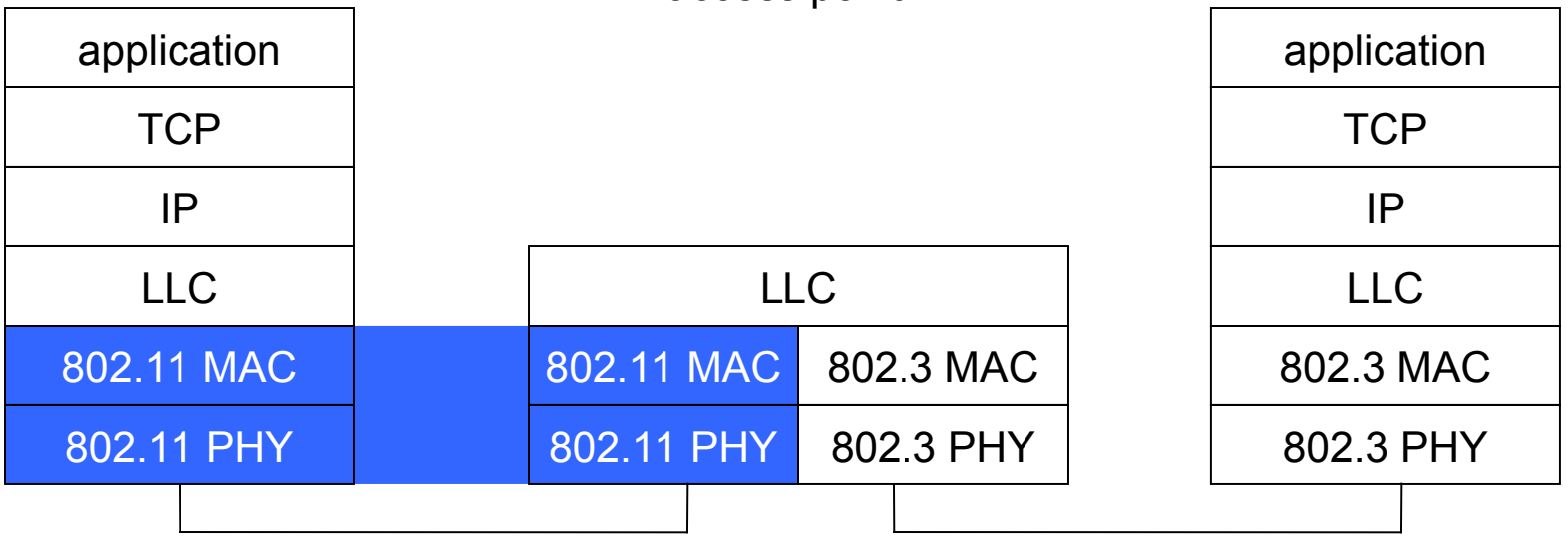
- No need of a priori infrastructure
- Nodes communicate directly with other nodes
  - AP for medium access not necessary
  - Complexity of each node higher: data forwarding

Ad hoc wireless network (cont)

- Nodes within an ad-hoc network can communicate if
  - they are within each other's radio range
  - other nodes can forward frames
- IEEE 802.11 and HiperLAN2 are typically infrastructure-based networks, which additionally support ad-hoc networking
- Bluetooth is a typical wireless ad-hoc network

IEEE 802.11 architecture and layers





802.11 PHY specifications

- IEEE 802.11a
  - 5 GHz band, 20 MHz channel bandwidth
  - Data rates: 6, 9 , 12, 18, 24, 36, 48, 54 Mbps
  - Orthogonal frequency division multiplexing (OFDM)
  - Subcarrier modulated using BPSK, QPSK, 16-QAM or 64-QAM
- IEEE 802.11b
  - 2.4 GHz band, 20 MHz channel bandwidth
  - Data rate: 5.5 and 11 Mbps
  - Fall back to 1 and 2 Mbps to interoperate with 802.11
  - DSSS, Complementary code keying (CCK) modulation scheme

802.11 PHY specifications

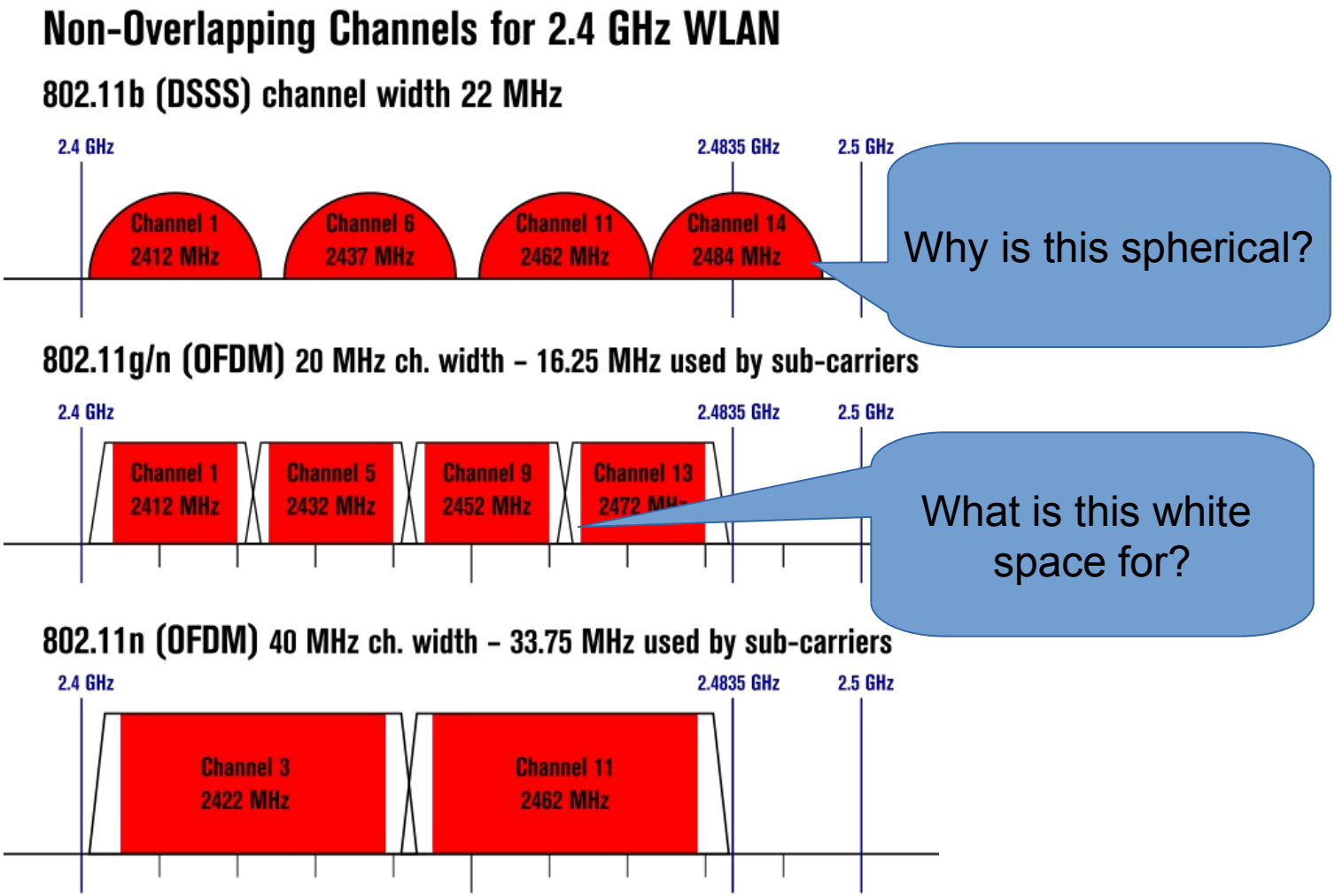
- IEEE 802.11g
  - Uses 2.4 GHz band, 20 MHz channel bandwidth
  - Provides rates of 6, 9 , 12, 18, 24, 36, 48, 54 Mbps
  - Similar to 802.11a, but operates in 2.4 GHz band
  - Also backward compatible with 802.11b, legacy
- IEEE 802.11n – WiFi 4
  - Uses 2.4GHz or 5GHz, 40 MHz channel bandwidth
  - MIMO up to 4 spatial streams to achieve much higher data rates than previous 802.11 standards
  - Data rates up to 540 Mbps, 50m
- IEEE 802.11ac – WiFi 5
  - 5 GHz, **up to** 160 MHz channel bandwidth
  - MIMO up to 8 spatial streams
  - Data rates up to 3.4 Gbps

2019 Wi-Fi standard

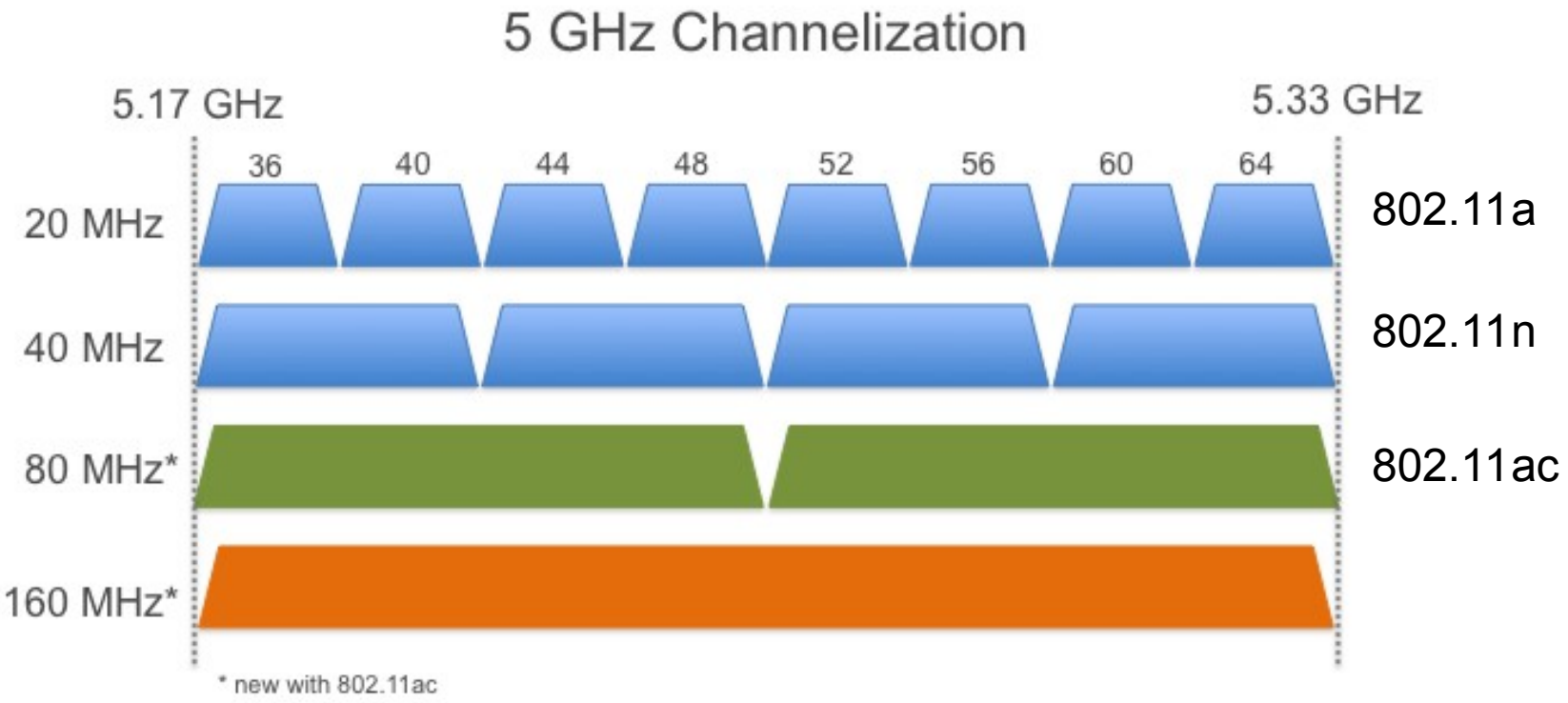
Wi-Fi 6: 802.11ax
Wi-Fi 5: 802.11ac
Wi-Fi 4: 802.11n

- IEEE 802.11ax / Wi-Fi 6
  - 1-6 GHz
  - Multi-user MIMO uplink & downlink (reception from multiple transmitters & concurrent transmission to multiple receivers)
  - OFDMA dynamic assignment of time-frequency Resource Units (RUs) by AP
  - Increased spatial reuse with dynamically adjusted transmit power and signal detection threshold
  - Target Wake Time (TWT): wake up at times other than beacon period

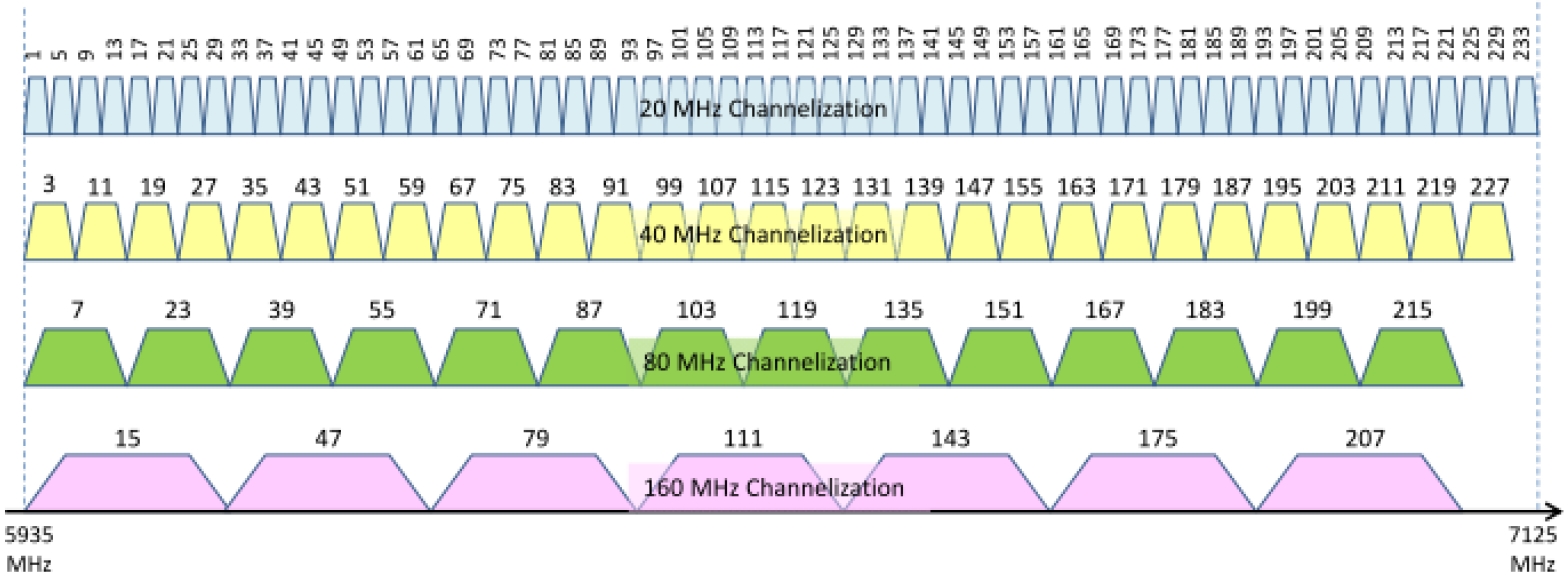
802.11b/g/n 2.4 GHz channels



802.11ac 5 GHz channels



802.11ax channels

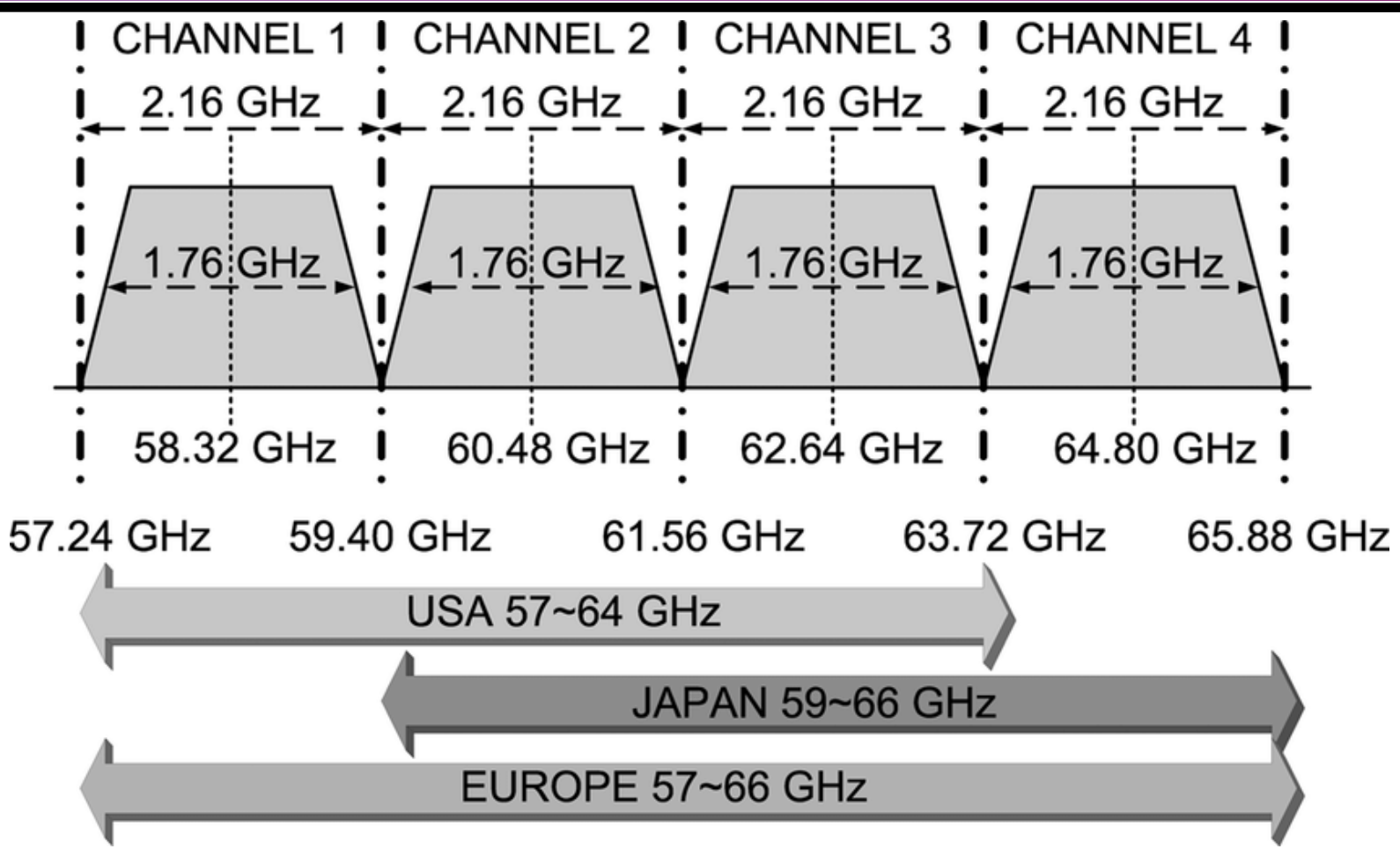


Channel allocation in 5935 – 7125 MHz for IEEE 802.11 TGax Draft D4.0[8]

NTT

- 802.11ax will also use 6 GHz band allocated to ISM
  - In addition to 2.4 and 5 GHz

802.11ad 60 GHz



Src: https://www.researchgate.net/profile/Hao-Yu-56/publication/250304851/figure/fig21/AS:613954397155344@1523389543673/Channelization-of-60-GHz-high-data-rate-wireless-communication-system-under-IEEE.png

60GHz advantages

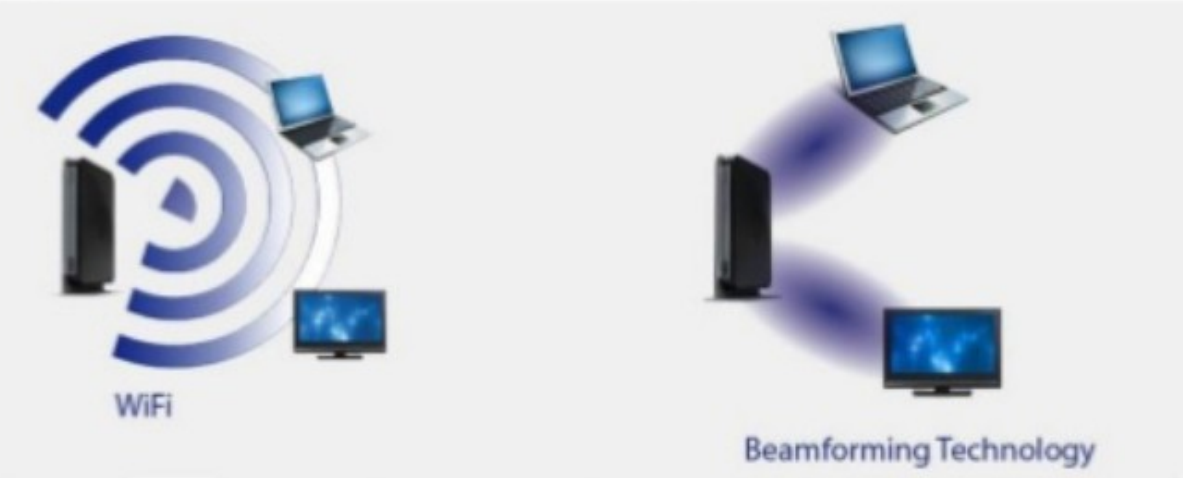
- Large spectrum: 7 GHz
  - 7 Gbps requires only 1 b/Hz (BPSK ok).
  - Complex 256-QAM not needed
- Small Antenna Separation:
  - 5 mm wavelength. $\lambda/4$=1.25 mm
- Easy Beamforming: Antenna arrays on a chip.
- Low Interference:
  - Does not cross walls.
  - Good for urban neighbors
- Directional Antennas: Spatial reuse is easy
- Inherent security: Difficult to intercept
- Higher power transmission

60GHz disadvantages

- Large Attenuation: Attenuation $\propto$ frequency^2
  - Strong absorption by Oxygen
  - Need larger transmit power: 10W allowed in 60GHz
  - Need high antenna gain => directional antennas
  - Short Distance ≈ 10m
- Directional Deafness: Can't hear unless aligned
  - Carrier sense not possible
  - RTS/CTS does not work
  - Multicast Difficult
- Easily Blocked: By a human/dog
  - Need a relay

Beamforming

- With beamforming each client focuses signal towards each client

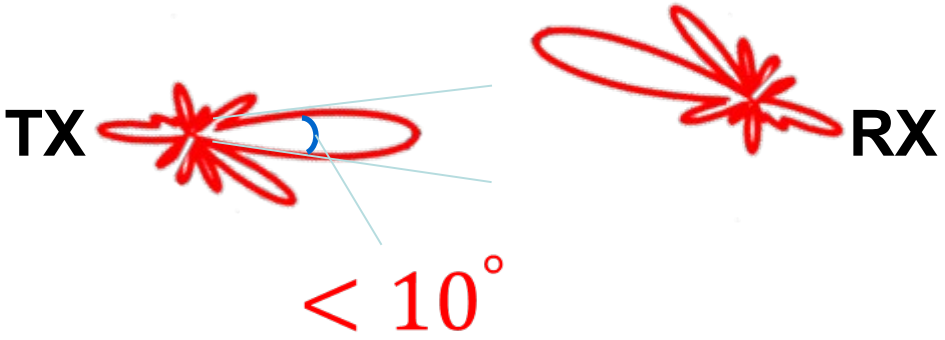


Challenges

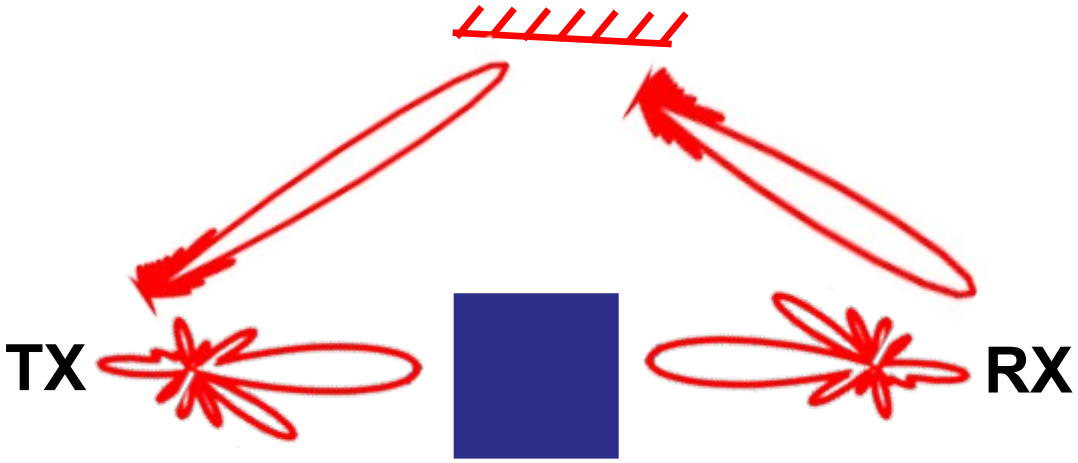
- Shorter wavelengths, higher attenuation
  - ~1000x higher attenuation than WiFi or LTE
- Beemforming: Highly directional, electronically steerable phased-arrays overcome propagation loss
  - But, introduce new challenges: alignment, blockage

Beamforming challenges

- Alignment:



- Blockage:



802.11 components

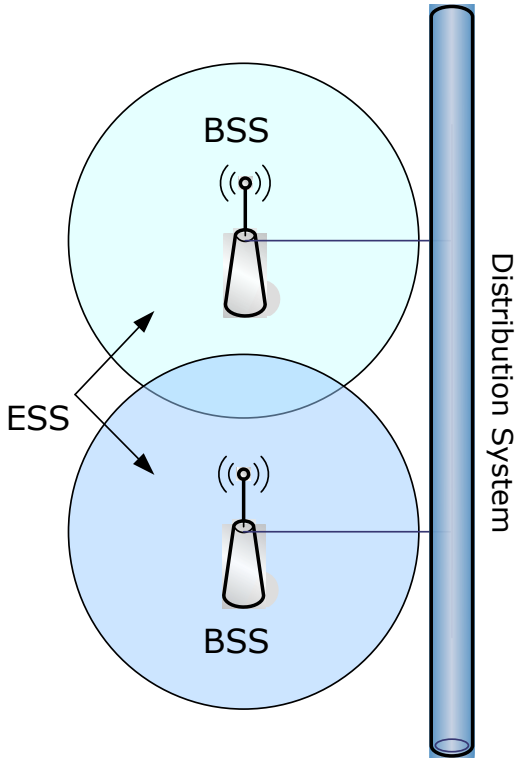
- Stations (STA)
- Access point (AP)
- Basic service set (BSS)
- Extended service set (ESS)
- Distribution system (DS)

Basic Service Set (BSS)

- Set of stations that communicate with each other
- Independent BSS (IBSS)
  - When all stations in a BSS are mobile and there is no connection to a wired network
  - Typically short-lived with a small number of stations
  - Ad-hoc in nature
  - Stations communicate directly with one another
- Infrastructure BSS (BSS)
  - Includes an Access Point (AP)
  - All mobiles communicate directly to AP
    - AP provides connection to wired LAN and relay functionality

Extended Service Set (ESS)

- Set of infrastructure BSS's
  - AP's communicate with each other
  - Forward traffic from one BSS to another
  - Facilitate movement of stations from one BSS to another
- Extends range of mobility beyond reach of a single BSS
- ESS looks like a single virtual LAN and single subnet



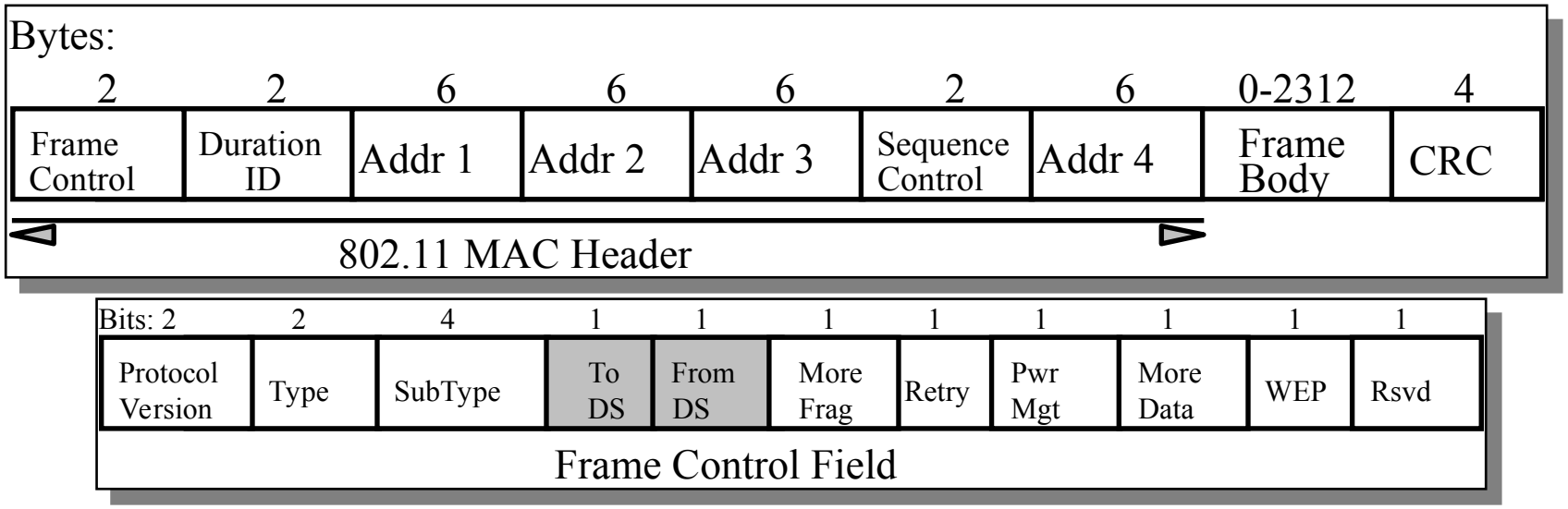
Distribution System (DS)

- Mechanism that allows APs to communicate with each other and wired infrastructure (if available)
- Backbone of the WLAN
- May contain both wired and wireless networks
- Functionality in each AP that determines where received packet should be sent
  - To another station within the same BSS
  - To the DS of another AP (e.g., sent to another BSS)
  - To the wired infrastructure for a destination not in the ESS
- When DS of AP receives packet, it is sent to station in BSS

802.11 identifiers

- Service Set Identifier (SSID)
  - “Network name”
  - 32 octets long
  - One network (ESS or IBSS) has one SSID
- Basic Service Set Identifier (BSSID)
  - “cell identifier”
  - 6 octets long (MAC address format)
  - One BSS has one SSID
  - BSSID same as MAC address of the radio in Access-Point

802.11 frame



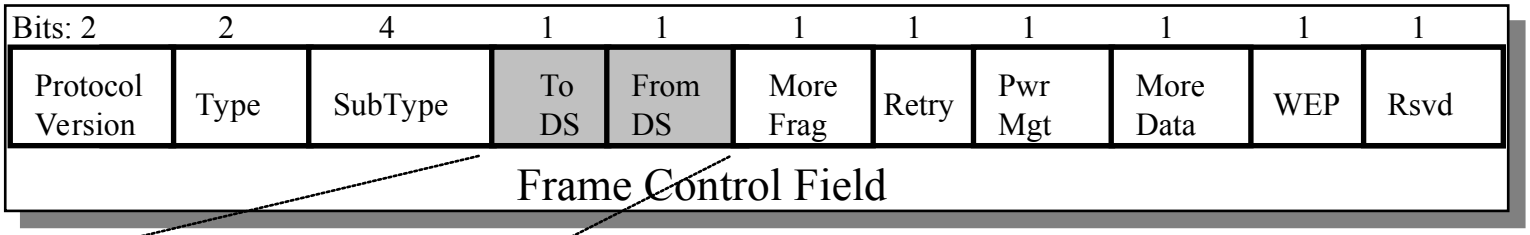
MAC Header format differs per Type:

- Control Frames (several fields are omitted)
- Management Frames
- Data Frames

Addresses

- Destination Address (DA): MAC address of the final destination to receive the frame
- Source Address (SA): MAC address of the original source that initially created and transmitted the frame
- Receiver Address (RA): MAC address of the next immediate STA on the wireless medium to receive the frame
- Transmitter Address (TA): MAC address of the STA that transmitted the frame onto the wireless medium

Address fields



To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Addr. 1 = Receiver Address. All stations filter on this address

Addr. 2 = Transmitter Address (TA), Identifies transmitter to address the ACK frame to (wireless transmitter)

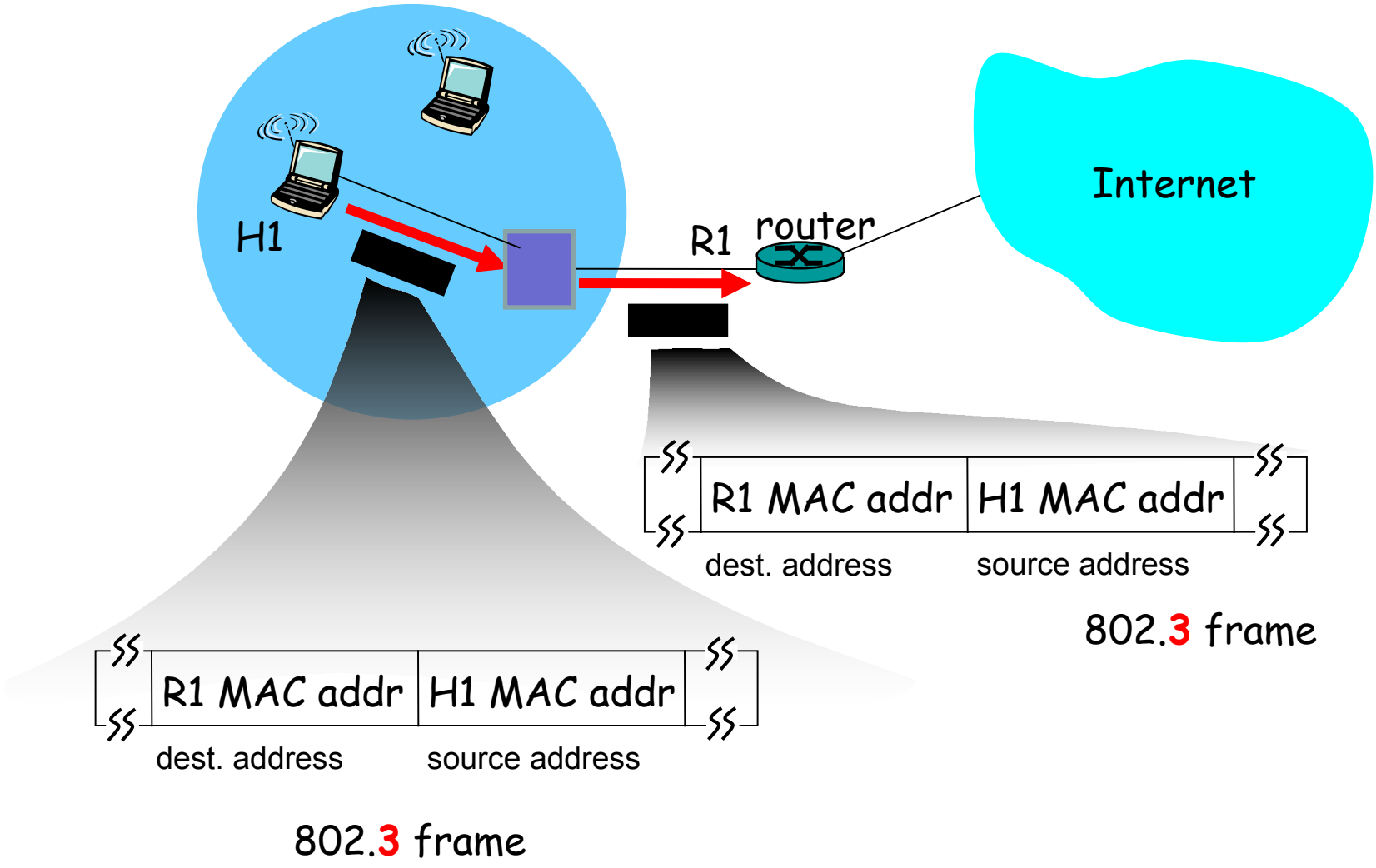
Addr. 3 = Dependent on *To* and *From DS* bits

Addr. 4 = Only needed to identify the original source of WDS (*Wireless Distribution System)* frames

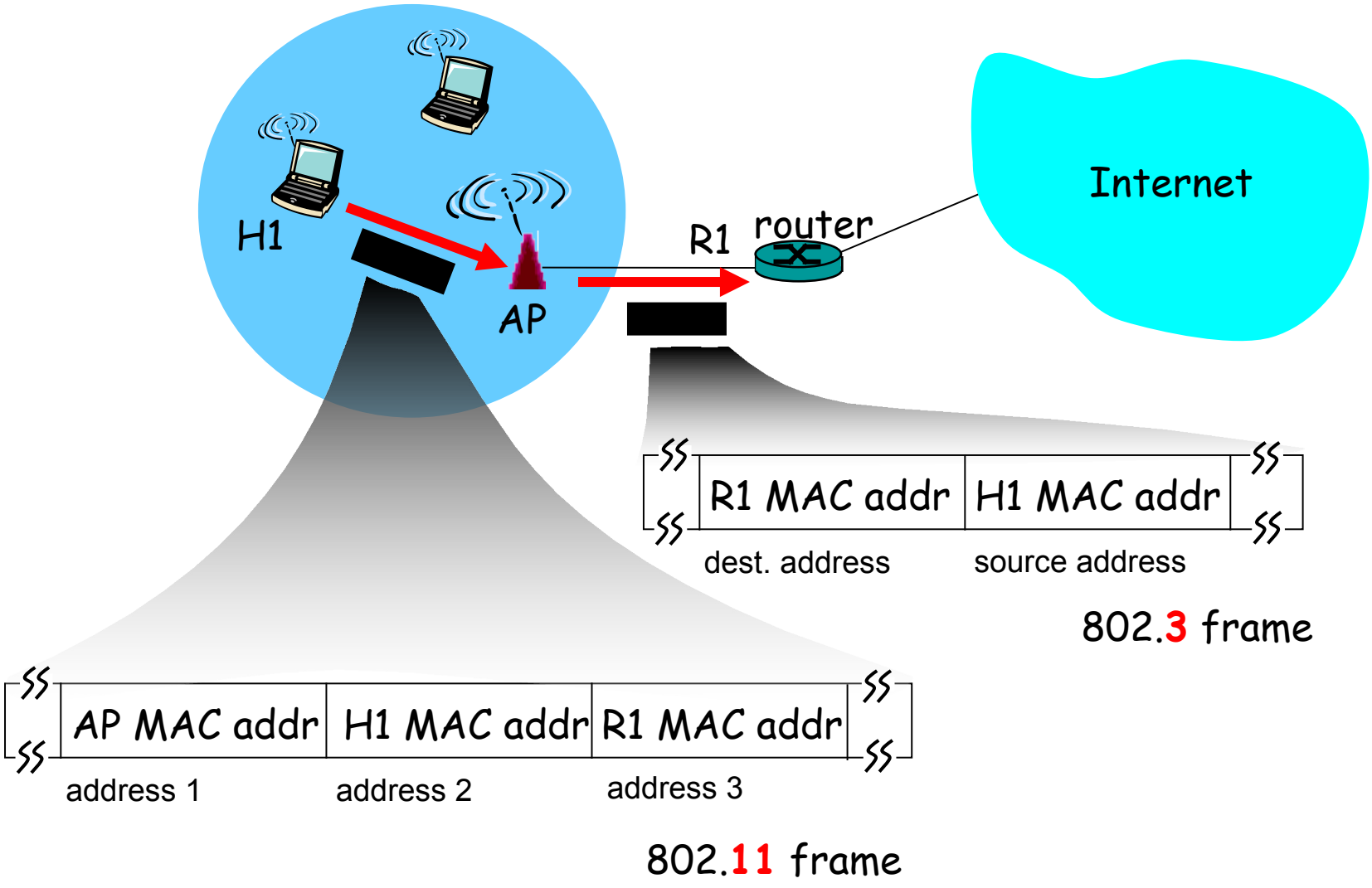
To/From DS bit

- **To DS bit is set** – Frame is coming from a wireless station to the wired network
- **From DS bit is set** – Frame is coming from the wired network, or possibly the AP itself and is destined for a wireless station
- **From DS and To DS are cleared** – Frame is from an Ad-hoc network
- **From DS and To DS are set** – Frame is from a WDS network and is destined for wired network. Example: wireless link between buildings

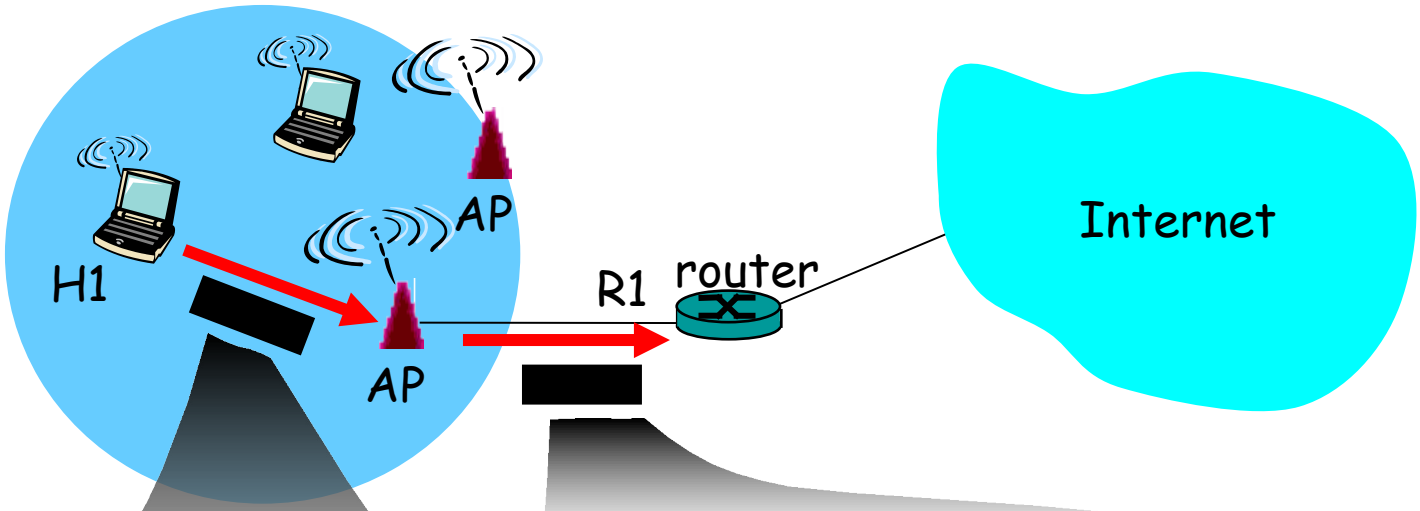
802.3 (Ethernet)



802.11 addressing: To DS



802.11 addressing: To DS



Why is AP MAC addr needed?

R1 MAC addr	H1 MAC addr

dest. address source address

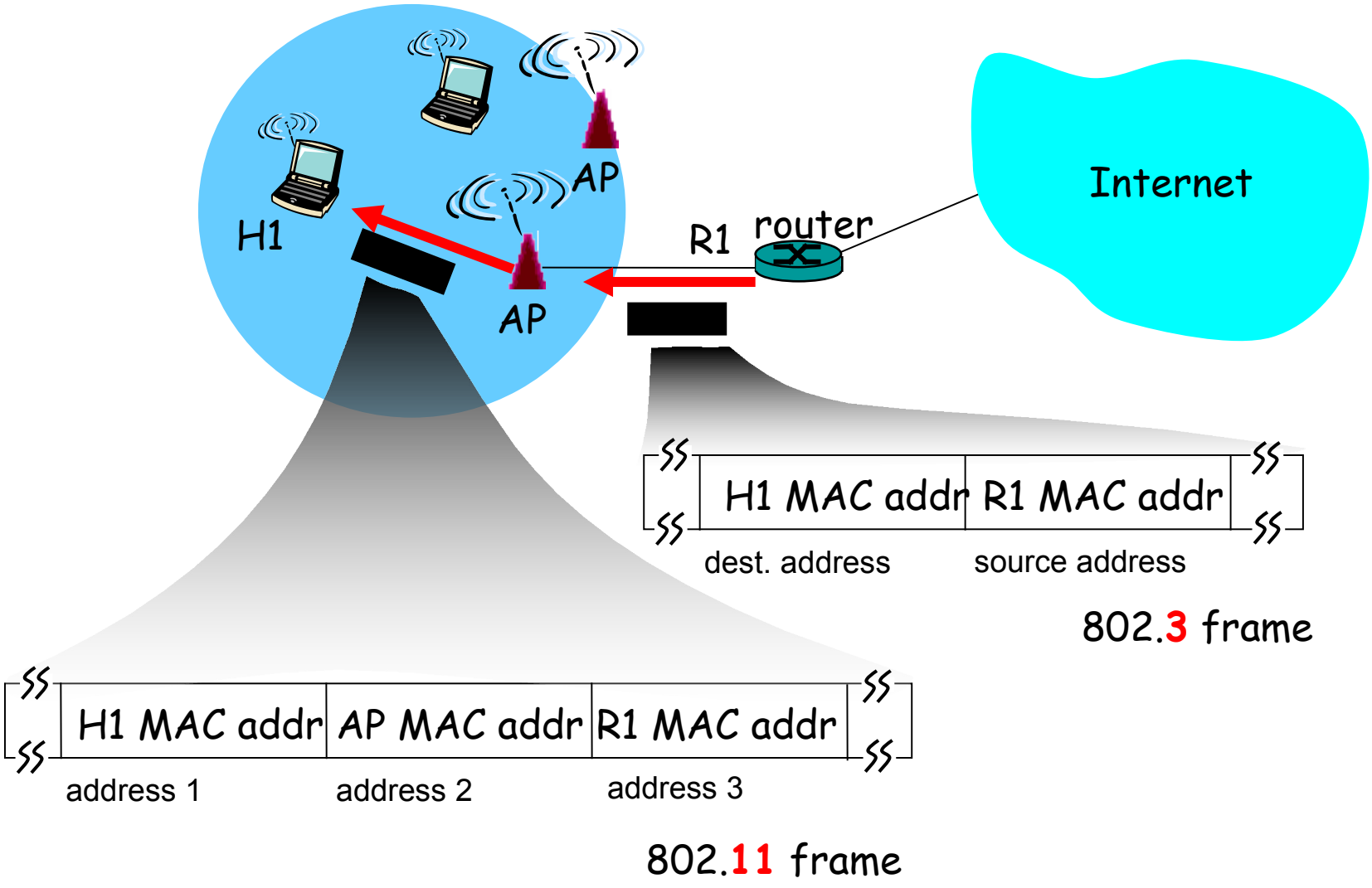
802.3 frame

AP MAC addr	H1 MAC addr	R1 MAC addr

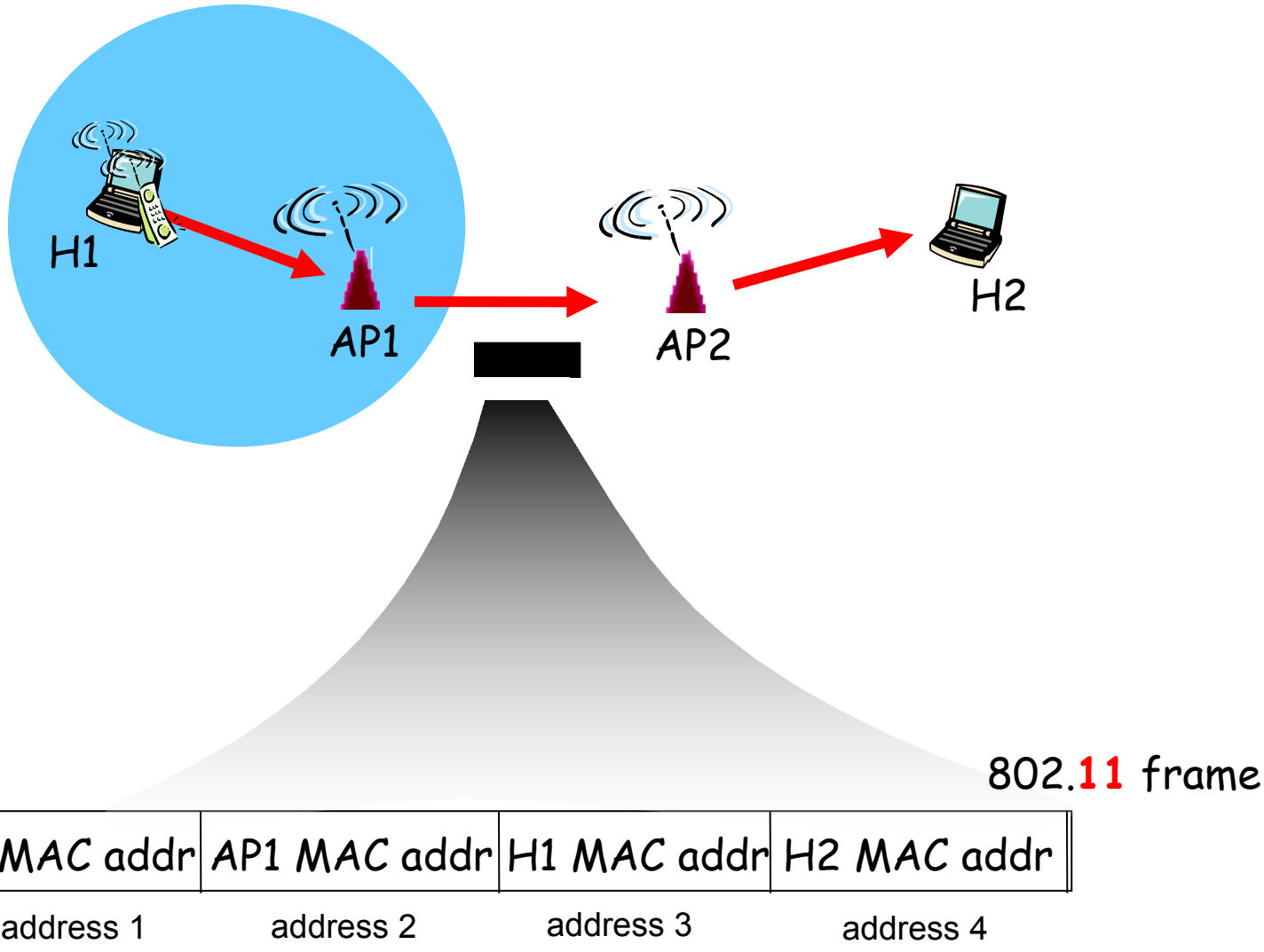
address 1 address 2 address 3

802.11 frame

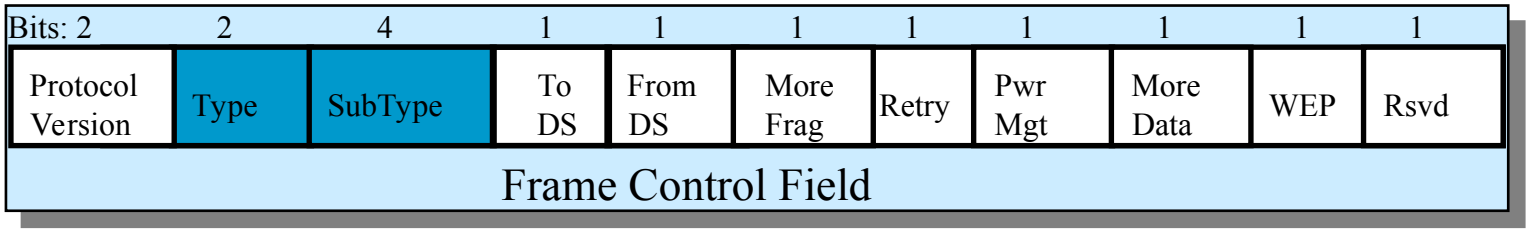
802.11 addressing: From DS



802.11 addressing: From & To DS



Frame types



Type and subtype identify the function of the frame:

- Type=00 Management Frame

  Beacon (Re)Association

  Probe (De)Authentication

  Power Management

- Type=01 Control Frame

  RTS/CTS ACK

- Type=10 Data Frame