Οικονομικό Πανεπιστήμιο Αθηνών
Τμήμα Πληροφορικής

Ευφυή Κινητά Δίκτυα: IEEE 802.11

Χειμερινό Εξάμηνο 2024-25

Βασίλειος Σύρης

1

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

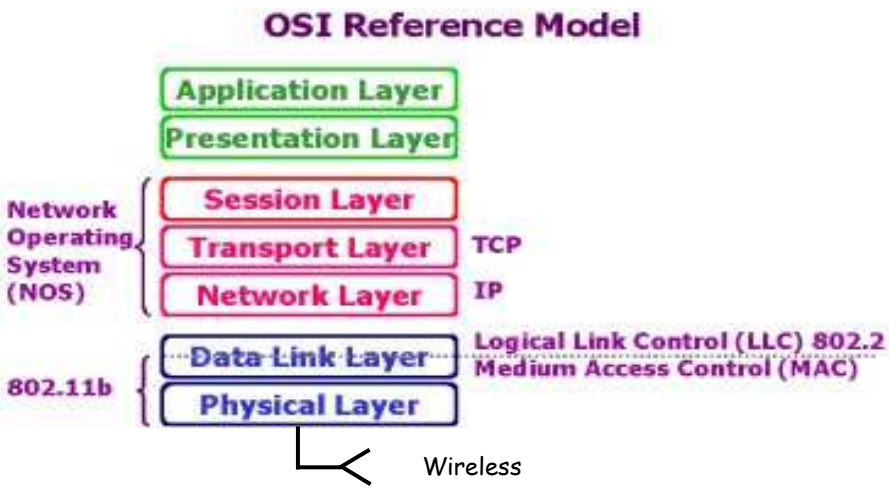
2

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

3

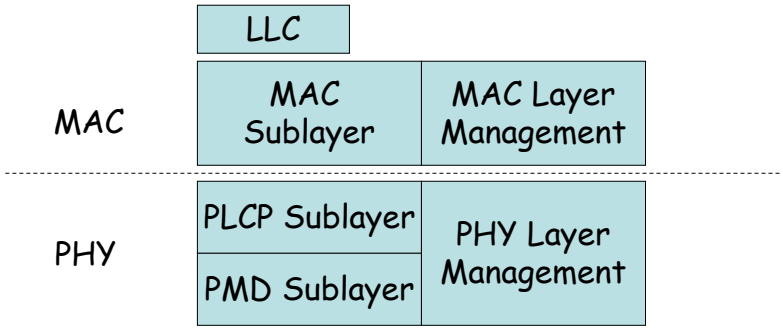
IEEE 802.11 and OSI model



4

802.11 scope & modules

- MAC and PHY specification for wireless connectivity for fixed, portable and moving stations in a local area



5

IEEE 802.11 standards

- 802.11b
  - 2.4 GHz unlicensed spectrum
  - up to 11 Mbps
- 802.11a
  - 5 GHz, OFDM (also in all later versions)
  - up to 54 Mbps
- 802.11g
  - 2.4, 5 GHz
  - up to 54 Mbps
- 802.11n: MIMO (x4), multiple channels (40MHz), 64 QAM
  - 2.4, 5 GHz
  - up to 450 Mbps (x3, 40MHz), 600 Mbps (x4, 40MHz)
- 802.11ac: MIMO (x8), multiple channels (160MHz), 256 QAM
  - 5 GHz
  - up to 3.4 Gbps (x8, 80MHz) – 1.7 Gbps in practice
- 802.11ad: beamforming
  - 60 GHz ISM band
  - 1-10 meters, up to 7 Gbps
- CSMA/CA for multiple access
- Access point and ad-hoc network versions

6

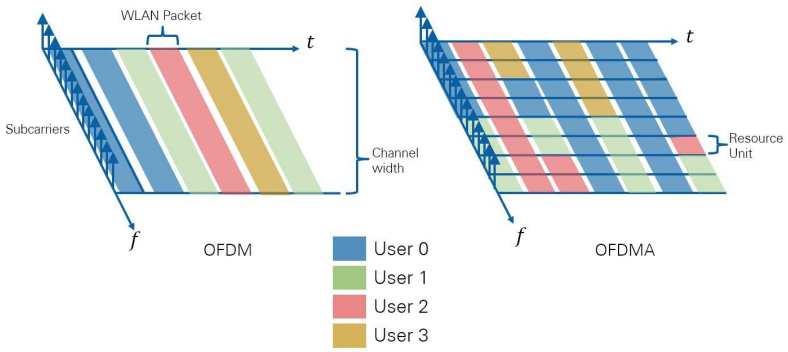
2019 Wi-Fi standard

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

7

802.11ax OFDMA

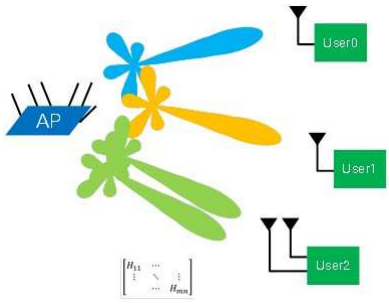


- 802.11ax can assign specific sets of subcarriers or Resource Units (RUs) to individual users

Source: Texas Instruments / Microwaves & RF

8

802.11ax multi-user MIMO

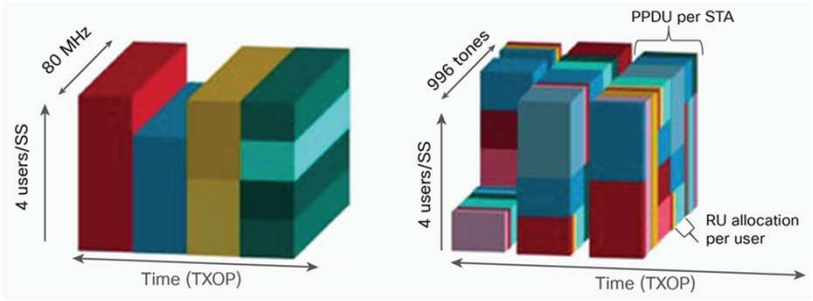


- Beamforming directs packets simultaneously to spatially diverse users
- Up to eight multi-user MIMO transmissions (spatial streams) at a time

Source: Texas Instruments / Microwaves & RF

9

802.11ax OFDMA: three dimensions of resource allocation



OFDM OFDMA

Source: Cisco

10

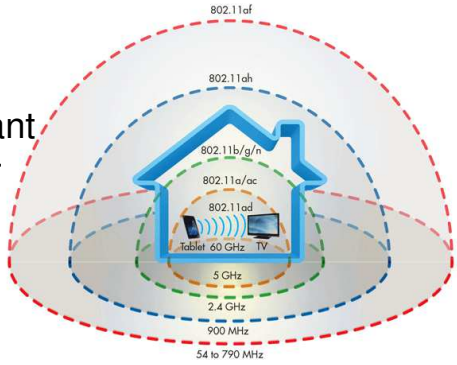
2019 Wi-Fi standards (cont.)

- 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)
  - 4 stream MIMO (44 Gbps per stream)
  - Higher order modulation (bits per symbol)

11

Both fast & long and slow & short

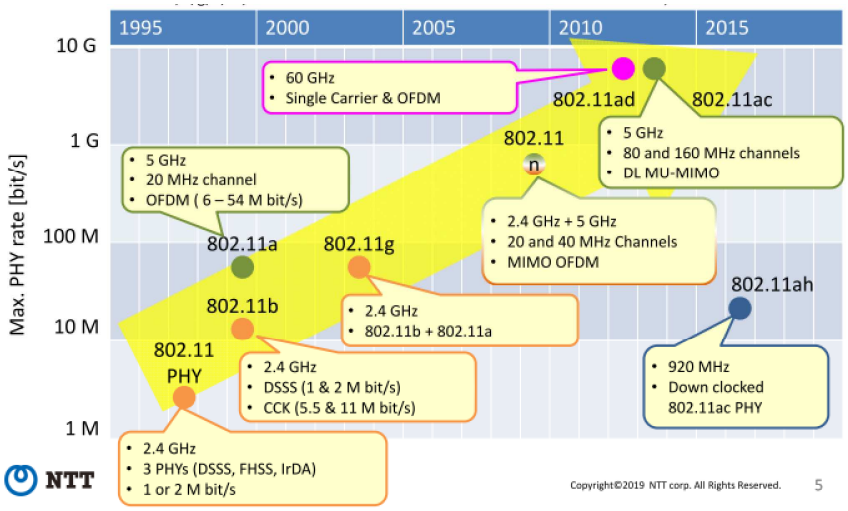
- Fast (higher speed) & long distance important
- Slow & short equally important
  - Longer battery lifetime, lower device cost, higher security
- Recent technologies:
  - IEEE 802.11ad (WiGig): 60 GHz, single room AP
  - IEEE 802.11af (White Wi-Fi), 802.11ah (low power Wi-Fi): <900MHz, long distance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



IoT (Internet of Things)

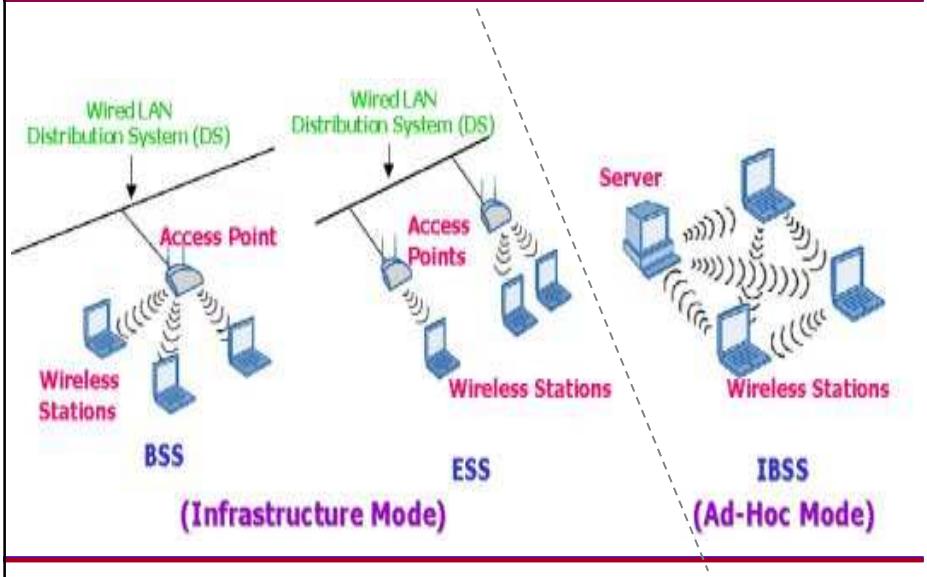
12

802.11 standards



13

802.11 architecture – two modes



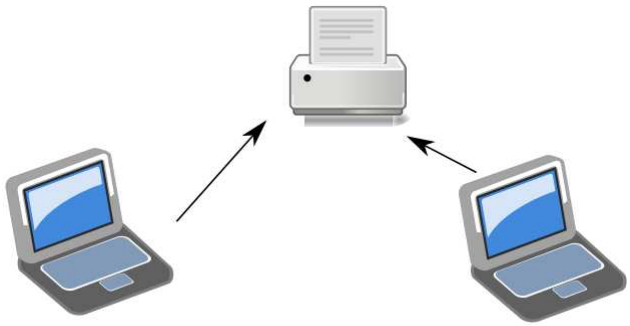
14

Wi-Fi P2P / Direct

- Wi-Fi peer-to-peer: technology, technical specification
- Wi-Fi direct: certification

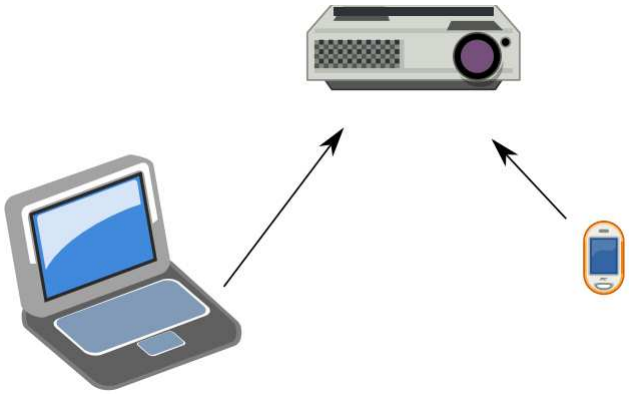
15

Wi-Fi Direct use cases



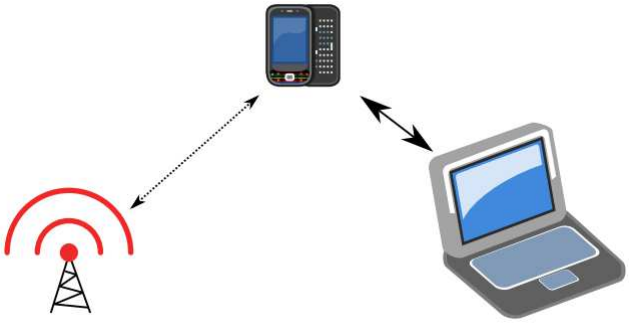
16

Wi-Fi Direct use cases



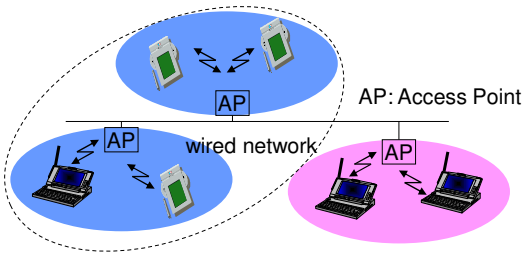
17

Wi-Fi Direct use cases



18

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

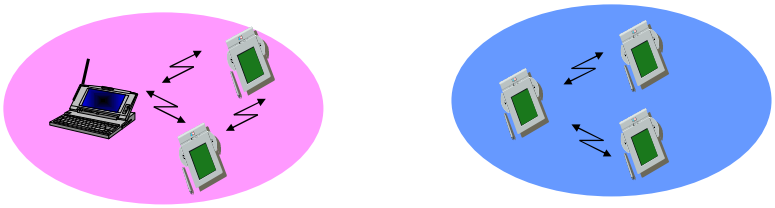
19

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

20

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

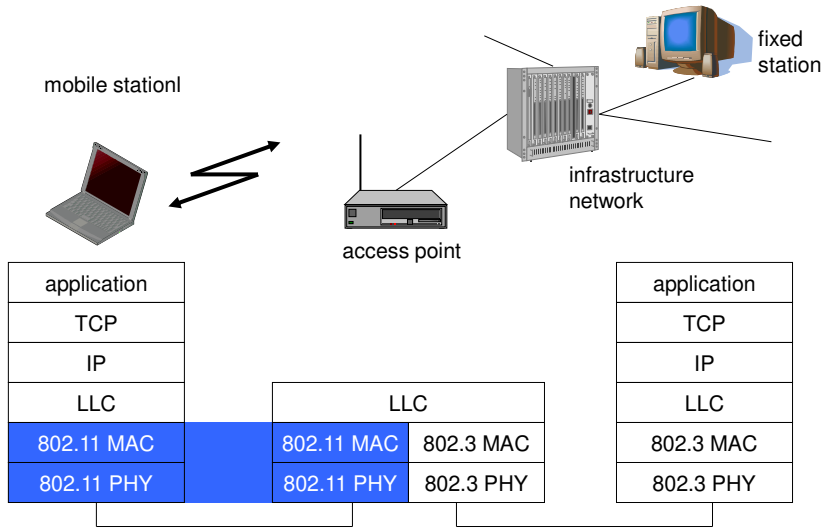
21

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

22

IEEE 802.11 architecture and layers



23

Original 802.11 PHY specification

- Direct-sequence spread spectrum
  - Operating in 2.4 GHz ISM band
  - Data rates: 1 and 2 Mbps
- Frequency-hopping spread spectrum
  - Operating in 2.4 GHz ISM band
  - Data rates: 1 and 2 Mbps
- Infrared
  - Wavelength between 850 and 950 nm
  - Data rates: 1 and 2 Mbps

24

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

25

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

26

2019 Wi-Fi standard

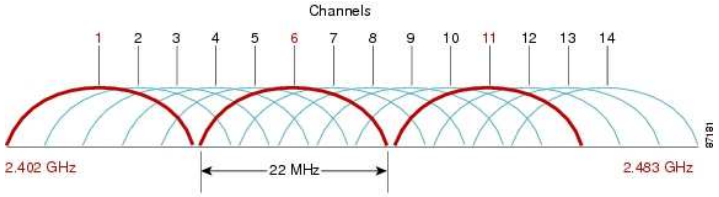
Wi-Fi 6: 802.11ax
Wi-Fi 5: 802.11ac
Wi-Fi 4: 802.11n

- 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

27

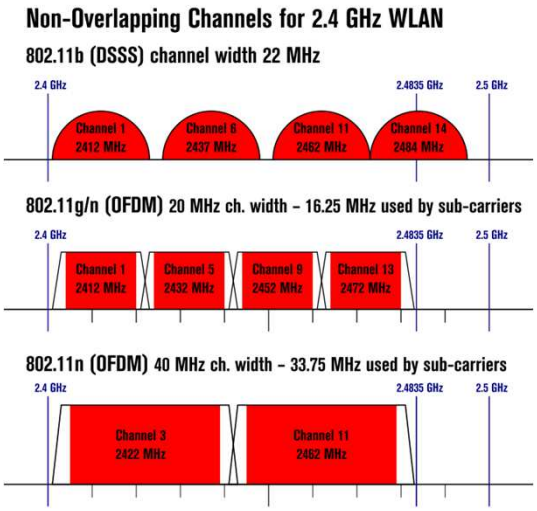
802.11b 2.4 GHz channels

- Available channels
  - FCC (North America): 11 channels
  - ETSI (EU): 13 channels
  - Overall bandwidth: 22 MHz
  - Center frequency separation only 5 MHz
- non-overlapping: 25 MHz apart
  - FCC: 1, 6, 11
  - ETSI: 1,6,11 or 2,7,12 or 3,8,13



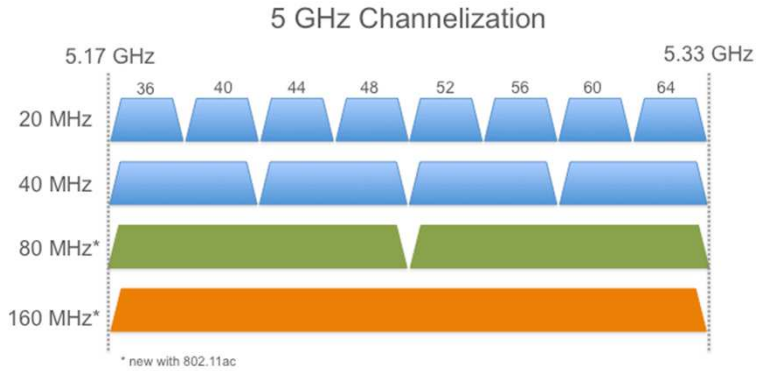
28

802.11b/g/n 2.4 GHz channels



29

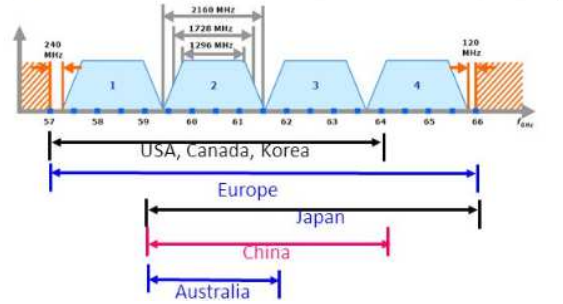
802.11ac 5 GHz channels

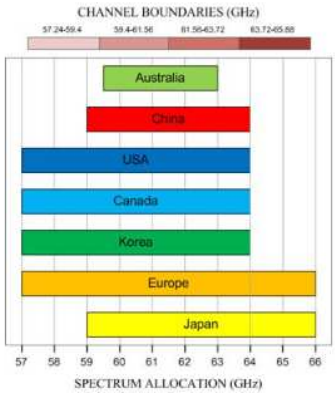


30

802.11ad 60 GHz

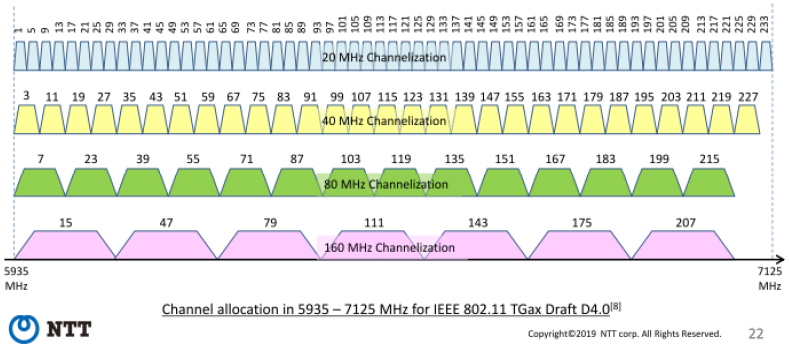
Channel Number	Low Freq. (GHz)	Center Freq. (GHz)	High Freq. (GHz)	3 dB BW (MHz)	Roll-Off Factor
1	57.240	58.320	59.400	1728	0.25
2	59.400	60.480	61.560	1728	0.25
3	61.560	62.640	63.720	1728	0.25
4	63.720	64.800	65.880	1728	0.25





31

802.11ax channels



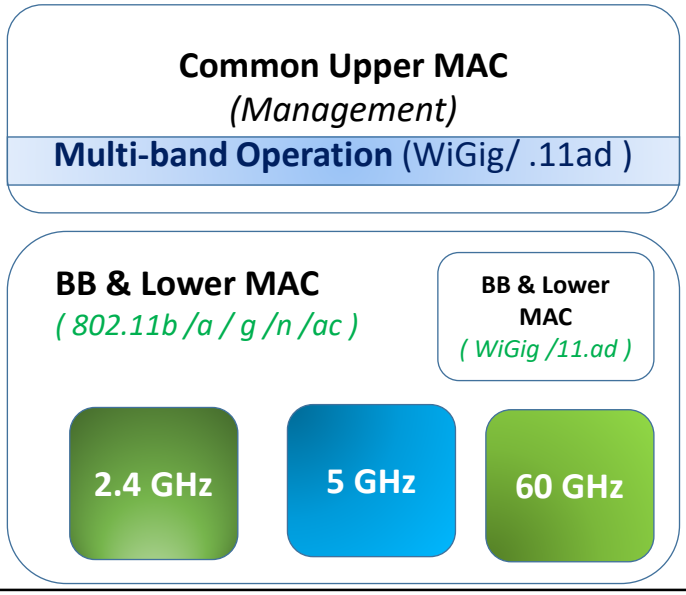
Channel allocation in 5935 – 7125 MHz for IEEE 802.11 TGax Draft D4.0[8]

NTT

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

32

2.4, 5, and 60 GHz coexistence



33

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. λ/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

34

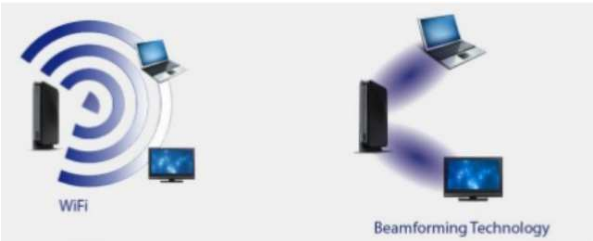
60GHz disadvantages

- Large Attenuation: Attenuation ∝ 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

35

Beamforming

- With beamforming each client focuses signal towards each client



36

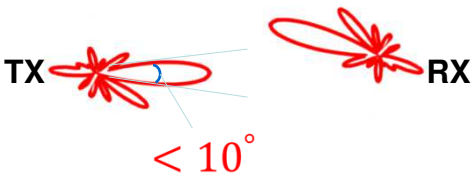
Challenges

- 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

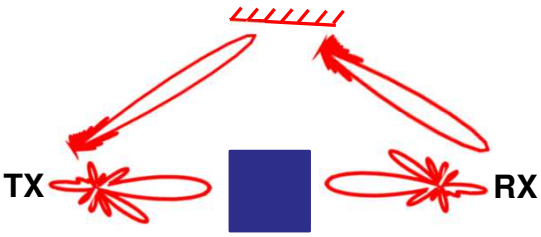
37

Beamforming challenges

- Alignment:



- Blockage:



38

Seamless multi-band operation

- Multi-band devices can continue accessing network when devices switches from a 60GHz to a lower frequency Wi-Fi channel

39

PHY Sublayers

- Physical layer convergence protocol (PLCP)
  - Provides common interface for MAC
    - Offers carrier sense status & CCA (Clear channel assessment)
    - Performs channel synchronization / training
- Physical medium dependent sublayer (PMD)
  - Functions based on underlying channel quality and characteristics
    - E.g., Takes care of the wireless encoding

40

PLCP (802.11b)

long preamble 192us

short preamble 96us (VoIP, video)

41

802.11 components

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

42

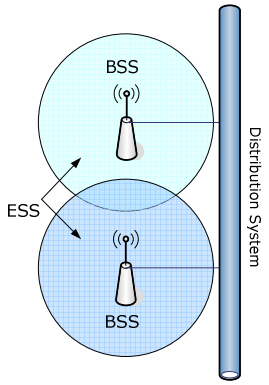
Basic Service Set (BSS)

- 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

43

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



44

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

45

802.11 and fixed network

- All mobile stations within ESS appear to outside networks as a single MAC-layer network where all stations are physically stationary
- Provides level of indirection to hide station mobility
- Allows existing network protocols (e.g., TCP/IP) to function properly within a WLAN where stations are mobile

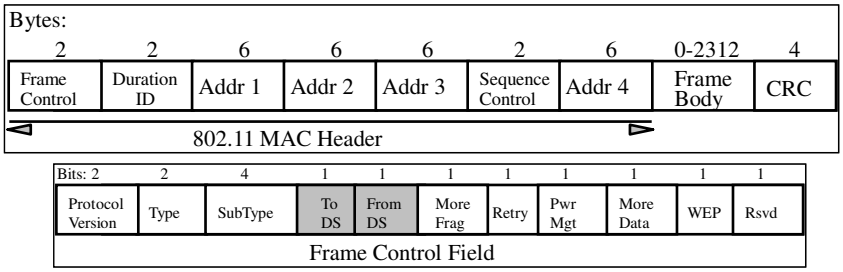
46

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

47

802.11 frame



MAC Header format differs per Type:

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

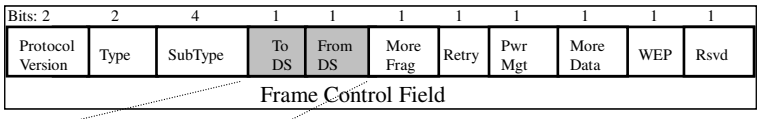
48

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

49

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

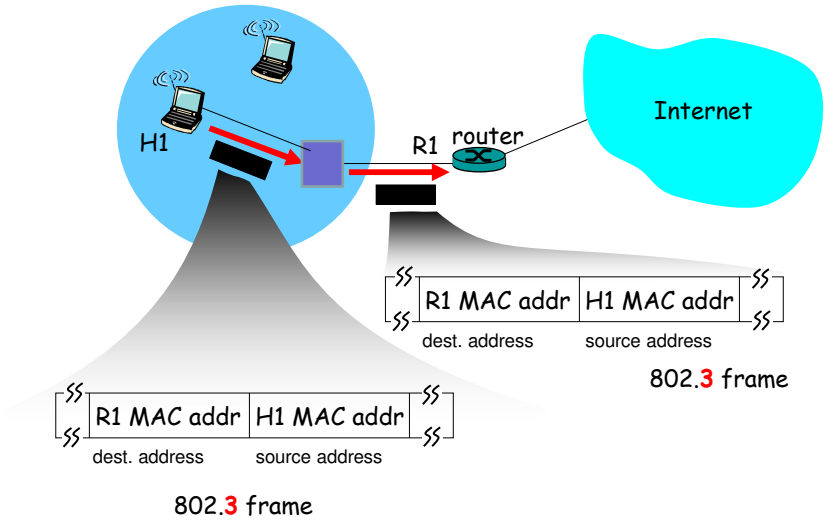
50

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

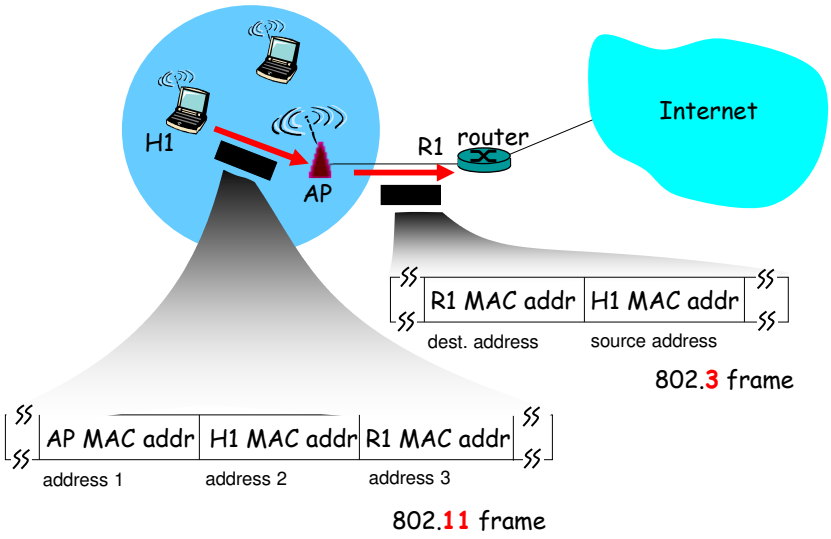
51

802.3 (Ethernet)



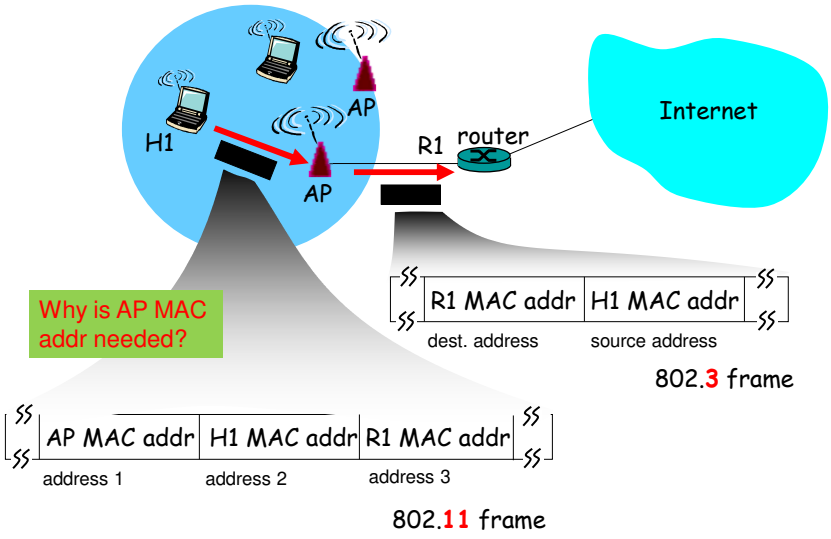
52

802.11 addressing: To DS



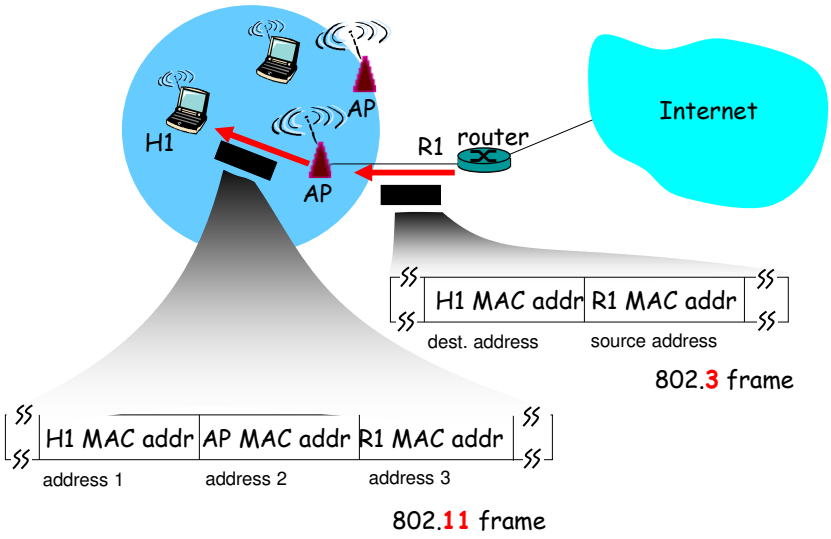
53

802.11 addressing: To DS



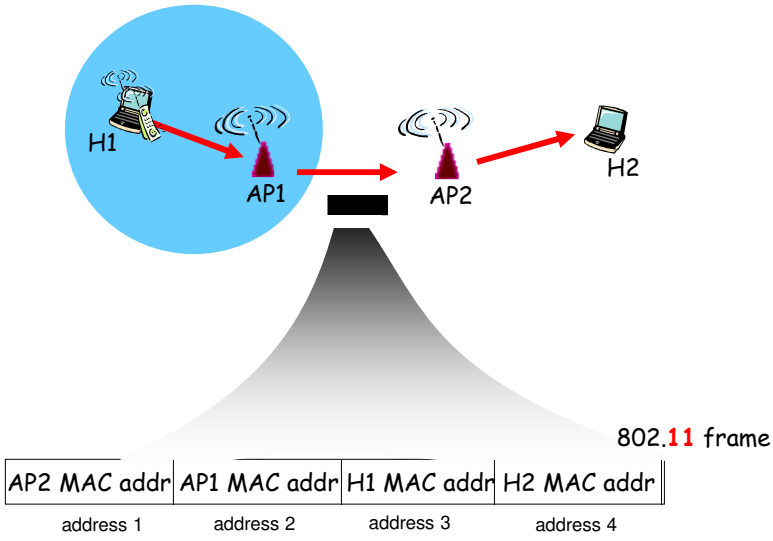
54

802.11 addressing: From DS



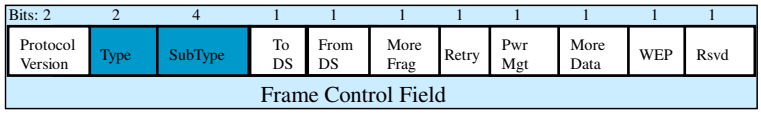
55

802.11 addressing: From & To DS



56

Frame types



Type and subtype identify the function of the frame:

- Type=00 Management Frame
  - Beacon
  - Probe
  - Power Management
  - (Re)Association
  - (De)Authentication
- Type=01 Control Frame
  - RTS/CTS
  - ACK
- Type=10 Data Frame

57

802.11 MAC

- The basic services provided by the MAC layer are the mandatory **asynchronous data service** and an optional **time-bounded service**.
- IEEE 802.11 offers only the asynchronous data service in ad-hoc network mode
- Both service types can be offered using an infrastructure-based network together with the access point coordinating medium access.
- The asynchronous service supports broadcast and multicast packets, and packet exchange is based on a “best-effort” model
  - no delay bounds can be given for transmission
  - cannot guarantee a maximum access delay or minimum transmission bandwidth

58

802.11 MAC (cont)

- Three basic access mechanisms have been defined for IEEE 802.11
  - CSMA/CA (mandatory)
  - Optional method avoiding the hidden terminal problem
  - A contention-free polling method for time-bounded service
    - access point polls terminals according to a list
- The first two methods are also summarized as **distributed coordination function (DCF)**
- The third method is called p**oint coordination function (PCF)**
- DCF only offers asynchronous service, while PCF offers both asynchronous and time-bounded service, but needs an access point to control medium access and to avoid contention.

59

802.11 MAC (DCF)

- CSMA/CA based
  - Carrier Sense=Listen before you talk
  - Uses exponential backoff
  - Different from CSMA/CD (used in wireline MAC) – why ??
- Robust for error and interference control
  - More efficient to deal with errors at the MAC level than higher layer (such as TCP)
  - MAC layer ACKnowledgment for unicast frames
  - MAC level loss recovery through finite retransmissions
  - No ACKs for broadcast frames
- Physical carrier sense
  - Sense medium for certain time to ensure channel free
  - uses Clear Channel Assessment signal detection
- Optional RTS/CTS offers Virtual Carrier Sensing
  - RTS/CTS include transmission duration (Network Allocation Vector – NAV)
  - Addresses hidden terminal problems

60

Wireless collision detection

- typically wireless adapters have single radio that either transmits or receives at any time
- collision detection in wireline networks based on signal strength
- wireless channel attenuation
  - transmitters might not hear each other (hidden terminal) – collision inferred by lost ACK
  - destination might hear one transmitter (false collision

61

Inter-frame Spacing

- IFS: minimum time channel must be sensed idle prior to transmission
  - **Short inter-frame spacing (SIFS)**
    - the shortest waiting time for medium access
    - defined for short control messages (e.g., ACK of data packets)
  - **DCF inter-frame spacing (DIFS)**
    - the longest waiting time used for asynchronous data service within a contention period
    - SIFS + two slot times
  - **PCF inter-frame spacing (PIFS)**
    - an access point polling other nodes only has to wait PIFS for medium access (for a time-bounded service)
    - SIFS + one slot time
- Different IFS values allow differential access to wireless channel
- Delay values in slot time
  - slot time=maximum time to detect a transmitting station (20 μsec in 802.11b

62

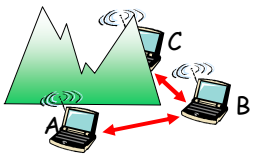
CSMA/CA

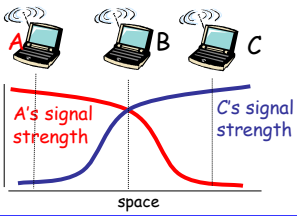
- The mandatory access mechanism of IEEE 802.11 is based on Carrier Sense Multiple Access with Collision Avoidance (***CSMA/CA***)
  - random access scheme with carrier sense and collision avoidance through random back-off
- The standard defines also two control frames:
  - RTS: Request To Send
  - CTS: Clear To Send

63

CSMA/CA: carrier sensing but no collision detection

- avoid collisions: >=2 nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
  - don't collide with ongoing transmission by other node
- 802.11: *no* collision detection!
  - difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
  - can't sense all collisions in any case: hidden terminal, fading
  - goal: *avoid collisions:* CSMA/C(ollision)A(voidance)





64

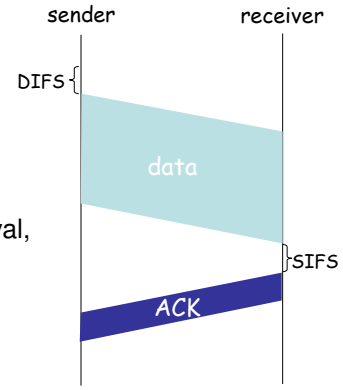
CSMA/CA

802.11 sender

1. if sense channel idle for **DIFS** then
   transmit entire frame (no CD)
2. if sense channel busy then
   start random backoff time
   timer counts down while channel idle
   transmit when timer expires
   if no ACK, increase random backoff interval, repeat 2

802.11 receiver

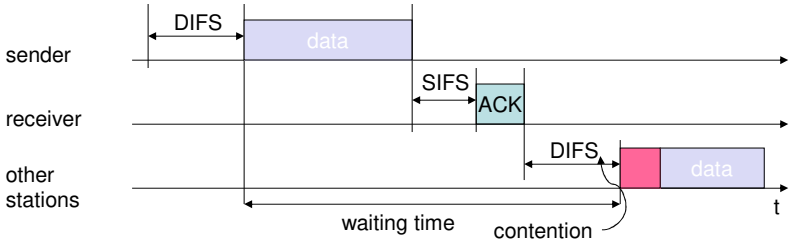
- if frame received OK
  return ACK after **SIFS** (ACK needed due to hidden terminal problem)



65

CSMA/CA: another view

- Unicast data transfer



  - station has to wait for DIFS before sending data
  - receivers acknowledge after waiting for a duration of a Short Inter-Frame Space (SIFS), if the packet was received correctly

66

Collision Avoidance

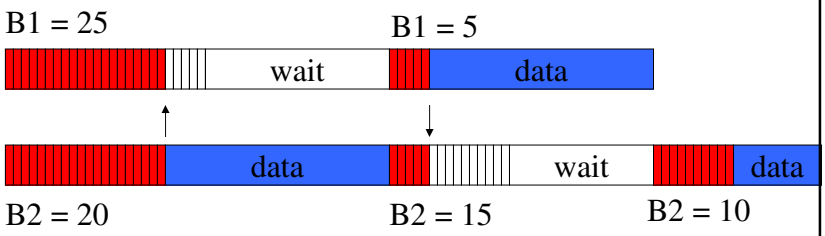
- Collision avoidance mechanism: When transmitting a packet, choose a backoff interval in the range [0,cw]
  - cw is contention window

- Count down the backoff interval when medium is idle
- When backoff interval reaches 0, transmit

67

Collision Avoidance: Example

Timer decremented only in RED periods



cw = 31

B1 and B2 are backoff intervals at nodes 1 and 2

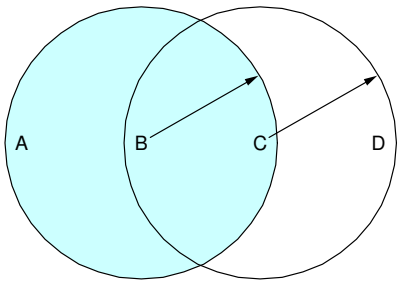
68

Collision Avoidance: Exponential Backoff

- Initial value of CW is CWmin
- For each collision, double the contention window CW
- Maximum value of CW is CWmax
- After successful transmission set contention window to CWmin

69

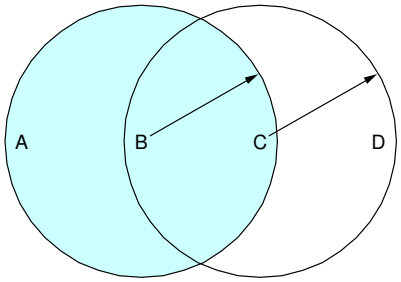
Hidden Node Problem



- A and C want to communicate with B
- Signal from A cannot reach C and vice-versa
- Carrier sensing does not work!

70

Exposed Node Problem



- B wants to send to A & C wants to send to D
- C senses B's transmission, hence doesn't transmit
- But, B->A and C->D both possible !
- Carrier sensing does not work!

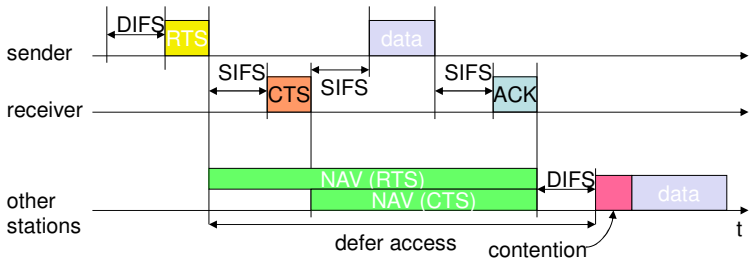
71

4-way handshake using RTS/CTS

- Sender "reserves" channel prior to transmitting data frames
  - First transmits *small* request-to-send (RTS) packets to BS using CSMA
  - RTSs may still collide (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

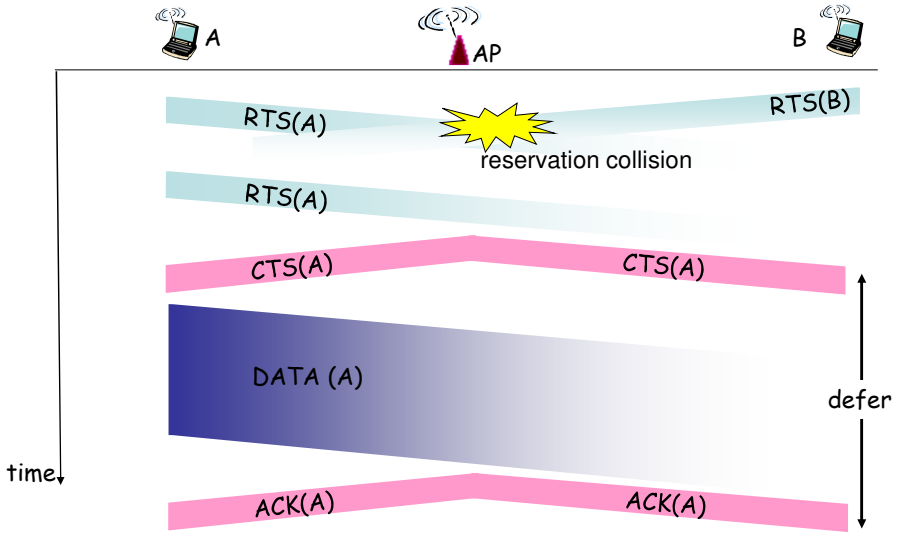
72

♦ Sending unicast packets with RTS/CTS control frames



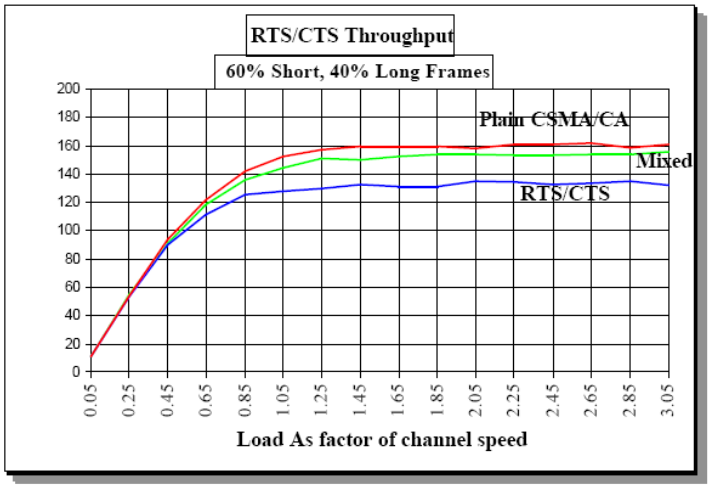
– station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium and the ACK related to it). Every node receiving this RTS now has to set its net allocation vector – it specifies the earliest point at which the node can try to access the medium again
– acknowledgement via CTS after SIFS by receiver (if ready to receive)
– sender can now send data at once, acknowledgement via ACK
– Other stations store medium reservations distributed via RTS and CTS

73



74

RTS/CTS overhead impact



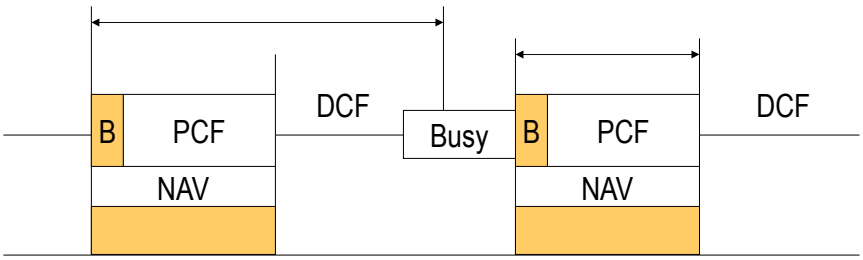
75

802.11 Point Coordination Function (PCF)

- AP polls stations
- polls may include data
- stations respond with data or ACKs
- Only one AP should operate PCF periods in each channel
- PCF periods alternate with DCF periods

76

DCF and PCF operation



NAV: Network Allocation Vector
PCF: Point Coordination Function
DCF: Distributed Coordination Function
B: Beacon Frame

77

802.11 MAC management

- **Synchronization**
  - Finding and staying with a WLAN
    - Uses TSF timers and beacons
- **Power Management**
  - Sleeping without missing any messages
    - Periodic sleep, frame buffering, traffic indication map
- **Association and Reassociation**
  - Joining a network
  - Roaming, moving from one AP to another
  - Scanning

78

Synchronization

- **Timing Synchronization Function (TSF)**
  - Enables synchronous waking/sleeping
  - Enables switching from DCF to PCF
  - Enables frequency hopping in FHSS PHY
    - Transmitter and receiver has identical dwell interval at each center frequency
- **Achieving TSF**
  - All stations maintain a local timer.
  - AP periodically broadcasts beacons containing timestamps, management info, roaming info, etc.
    - Not necessary to hear every beacon
  - Beacon synchronizes entire BSS
    - Applicable in infrastructure mode ONLY
  - Distributed TSF (for Independent BSS) more difficult

79

802.11 power management

- Station-to-AP: “I am going to sleep until next beacon frame”
  - AP knows not to transmit frames to this station
  - Station wakes up before next beacon frame
- Beacon frame: contains list of stations with packets waiting in AP buffer
  - station stays awake as long as AP has frames to send it; otherwise sleeps again until next beacon frame
  - if AP has packets for it, station polls AP
- Broadcast packets can also be buffered

80

- **Battery powered devices require power efficiency**
  - LAN protocols assume idle nodes are always ON and thus ready to receive.
  - Idle-receive state key source of power wastage
- **Devices need to power off during idle periods**
  - Yet maintain an active session – tradeoff power Vs throughput
- **Achieving power conservation**
  - Allow idle stations to go to sleep periodically
  - APs buffer packets for sleeping stations
  - AP announces which stations have frames buffered when all stations are awake – called **Traffic Indication Map (TIM)**
    - TSF assures AP and Power Save stations are synchronized
    - TSF timer keeps running when stations are sleeping

81

802.11 association and roaming

Questions

- How does station find AP?
- How does station associate with AP?
- How does station roam to another AP?

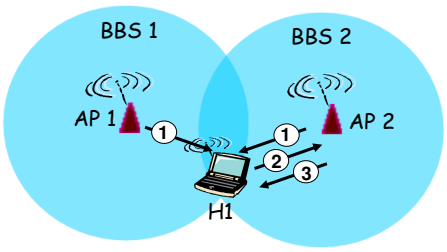
82

802.11 channels and association

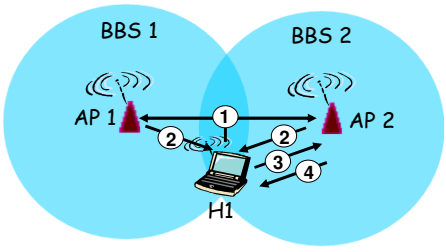
- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  - AP admin chooses AP channel
  - interference possible: channel can be same as that chosen by neighboring AP!
- Stations association with an AP
  - scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address (BSSID)
  - selects AP to associate with
    - based on beacon signal strength
  - may perform authentication
  - will typically run DHCP to get IP address in AP's subnet

83

Passive vs. active scanning



Passive Scanning:
(1) beacon frames sent by APs
(2) association Request frame sent by H1 to selected AP
(3) association Response frame sent by selected AP to H1



Active Scanning:
(1) Probe Request frame broadcasted from H1
(2) Probes response frame sent from APs
(3) Association Request frame sent from H1 to selected AP
(4) Association Response frame sent from selected AP to H1

84

Authentication and association

- Three 802.11 connection states
  - No authentication and no association
  - Authenticated but not associated
  - Authenticated and associated
- Original 802.11 authentication occurred before association
  - 802.1X/802.11i authentication follows
- Association allows the AP/router to record each mobile device so frames are properly delivered
  - Association involved agreeing on bit rates and security parameters (for 802.1X/802.11i authentication)
  - After successful association, AP sends station an Association ID used

85

802.11 roaming

- No or bad connection? Then perform:
- Scanning
  - scan the environment, i.e., listen into the medium for beacon signals or send probes into the medium and wait for an answer
- Reassociation Request
  - station sends a request to one or several AP(s)
- Reassociation Response
  - success: AP has answered, station can now participate
  - failure: continue scanning
- AP accepts Reassociation Request
  - signal the new station to the distribution system
  - the distribution system updates its data base (i.e., location information)
  - typically, the distribution system now informs the old AP so it can release resources
- Roaming support robustness/redundancy and mobility

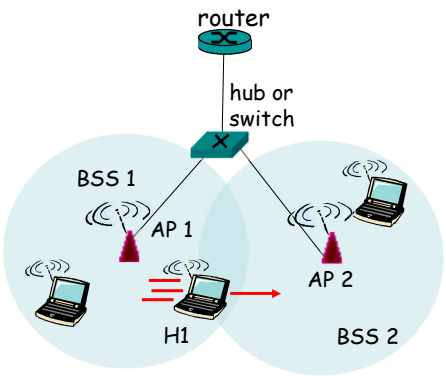
86

802.11 roaming (cont)

- L2 handover
  - If handover from one AP to another belonging to the same subnet, then handover is completed at L2
- L3 handover
  - If new AP is in another domain, then the handover must be completed at L3, due to the assignment of an IP belonging to the new domain – hence routing to the new IP.
    - Mobile IP deals with these issues – more later

87

- H1 remains in same IP subnet: IP address can remain same
- switch: which AP is associated with H1?
  - self-learning: switch will see frame from H1 and "remember" which switch port can be used to reach H1



88

Reactive and proactive scanning

- Reactive: scan when connection lost
- Proactive: periodically scan for better AP
  - higher performance but higher overhead
- not standardized by 802.11
  - vendor/implementation specific

89

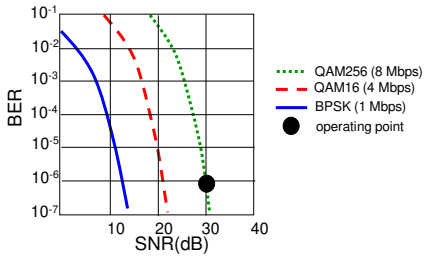
IEEE 802.11 Wireless LANs

- 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

90

802.11 rate adaptation

- base station, mobile dynamically change transmission rate (physical layer modulation technique)
- Key questions:
  - what to measure
  - when to change rate
  - what rate to change to



1. SNR decreases, BER increase as node moves away from base station

2. When BER becomes too high, switch to lower transmission rate but with lower BER

91

MAC management frames

- Beacon
  - Timestamp, Beacon Interval, Capabilities, ESSID, Supported Rates, parameters
  - Traffic Indication Map
- Probe
  - ESSID, Capabilities, Supported Rates
- Probe Response
  - Timestamp, Beacon Interval, Capabilities, ESSID, Supported Rates, parameters
  - same for Beacon except for TIM
- Association Request
  - Capability, Listen Interval, ESSID, Supported Rates
- Association Response
  - Capability, Status Code, Station ID, Supported Rates

92

MAC management frames (cont)

- Reassociation Request
  - Capability, Listen Interval, ESSID, Supported Rates, Current AP Address
- Reassociation Response
  - Capability, Status Code, Station ID, Supported Rates
- Disassociation
  - Reason code
- Authentication
  - Algorithm, Sequence, Status, Challenge Text
- Deauthentication Reason

93

Extended Distributed Channel Access (EDCA)

- DIFS (AIFS in 802.11e)
- CWmin
- CWmax
- Transmission Opportunity (TXOP)

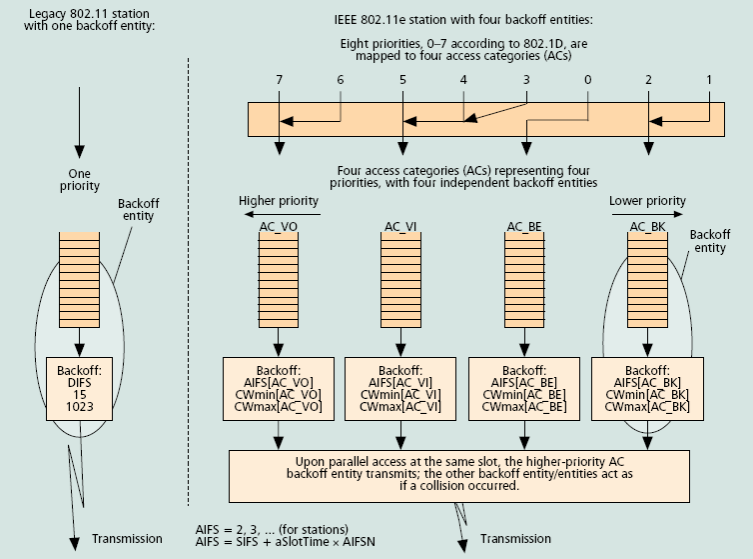
} Supported by EDCA

Can also differentiate:

- Persistence Factor (PF): CW increase after collision

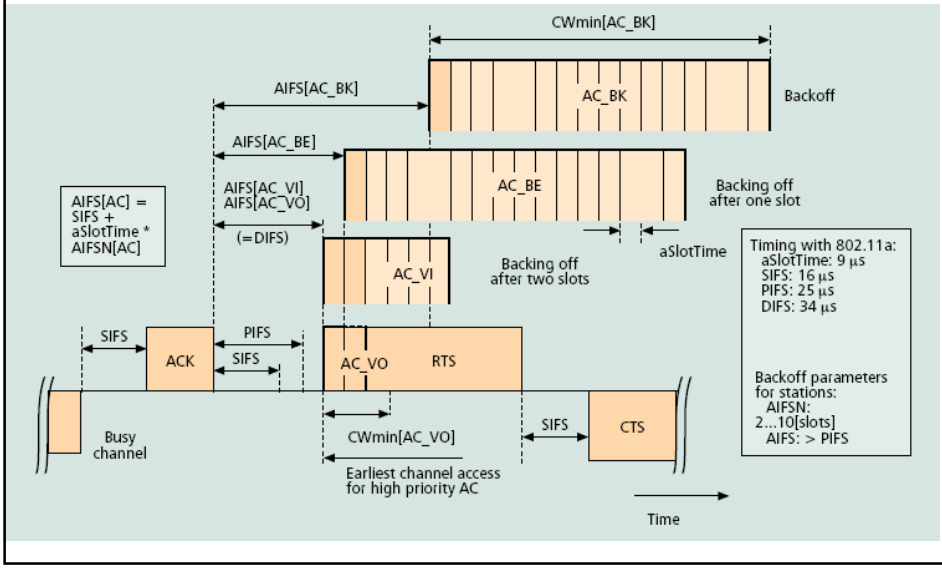
94

802.11e Access Categories



95

802.11e multiple backoff entities



96

802.11 security

- Authentication: ensure station is allowed to associate to partiular AP
- Privacy: prevent outsiders from eavesdropping
- 802.11: contains mechanisms to support both, but many aspects are vendor specific

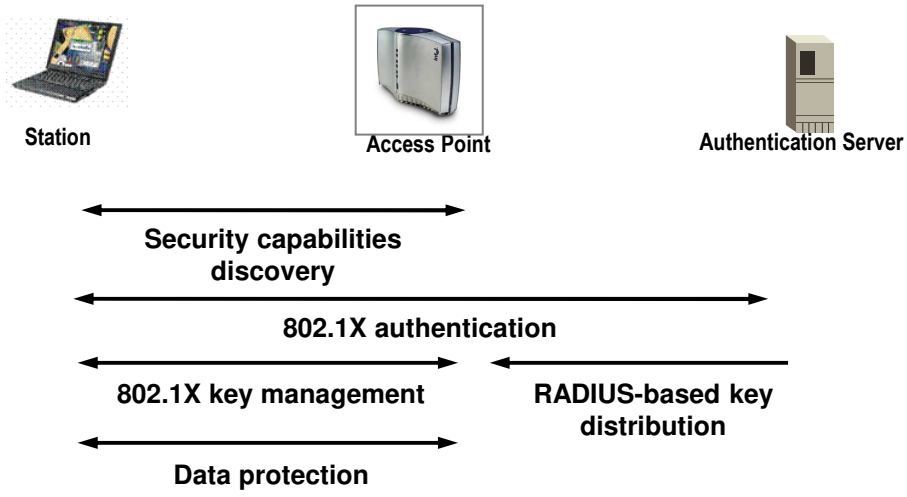
97

WEP: Wired Equivalent Privacy

- Provide security similar to wired 802 networks
- Encryption over wireless hop (not end-to-end)
  - only data payload
  - based on RC4 stream cipher
  - 64-bit WEP (40 bit key), 128-bit WEP (26 hexadecimal – 106 bit key)

98

802.11i – Operational Components



99

Actions of each phase

- Discovery
  - Determine promising parties with whom to communicate
  - AP advertises network security capabilities to STAs
- 802.1X authentication
  - Centralize network admission policy decisions at the AS
  - STA determines whether it does indeed want to communicate
  - Mutually authenticate STA and AS
  - Generate Master Key as a side effect of authentication
  - Use master key to generate session keys = authorization token

100

Actions of each phase (cont)

- RADIUS-based key distribution
  - AS moves (not copies) session key (PMK) to STA's AP
- 802.1X key management
  - Bind PMK to STA and AP
  - Confirm both AP and STA possess PMK
  - Generate fresh operational key (PTK)
  - Prove each peer is live
  - Synchronize PTK use

101

Data transfer

- 802.11i defines 2 protocols to protect data transfer
  - TKIP – for legacy devices only
  - CCMP – better security for new devices
- Two protocols instead of one due to politics

102

Data transfer requirements

- Never send or receive unprotected packets
- Message origin authenticity — prevent forgeries
- Sequence packets — detect replays
- Avoid rekeying — 48 bit packet sequence number
- Eliminate per-packet key – don't misuse encryption
- Protect source and destination addresses
- Use one strong cryptographic primitive for both confidentiality and integrity
- Interoperate with proposed quality of service (QoS) enhancements (IEEE 802.11 TGe)

103

Other 802.11 enhancements

- 802.11f: inter-AP communication
- 802.11h: dynamic frequency selection and power control
- 802.11i: enhanced security
- 802.11k: Radio measurements
- 802.11p
  - WAVE: wireless access for vehicular environments
- 802.11r: reduction of handoff latency
- 802.11s
  - Mesh networking

104

802.11 standards

IEEE Standard	Year Adopted	Frequency	Max. Data Rate	Max. Range	
802.11a	1999	5 GHz	54 Mbps	400 ft.	
802.11b	1999	2.4 GHz	11 Mbps	450 ft.	
802.11g	2003	2.4 GHz	54 Mbps	450 ft.	
802.11n	2009	2.4/5 GHz	600 Mbps	825 ft.	
802.11ac	2014	5 GHz	1 Gbps	1,000 ft.	
802.11ac Wave 2	2015	5 GHz	3.47 Gbps	10 m.	Typically combined with 802.11n
802.11ad	2016	60 GHz	7 Gbps	10 m.	
802.11af	2014	54 - 790 MHz	26.7 Mbps – 568.9 Mbps (depending on channel)	1,000 m.	TV white spaces
802.11ah	2016	900 MHz	347 Mbps	1,000 m.	unlicensed
802.11ax	2019 (expected)	2.4/5 GHz	10 Gbps	1,000 ft.	
802.11ay	late 2019 (expected)	60 GHz	100 Gbps	300-500 m.	
802.11az	2021 (expected)	60 GHz	Device tracking refresh rate 0.1-0.5 Hz	Accuracy <1m to <0.1m	

Sep 2019

105

Latest 802.11 standards

- 802.11ax (02/2021): next “normal” Wi-Fi
  - Also called Wi-Fi 6 (Wi-Fi Alliance), while Wi-Fi 5: 802.11ac, Wi-Fi 4: 802.11n
  - Backward compatible with Wi-Fi 5 (802.11ac)
  - Combine 2.4 & 5 GHz
  - OFDMA versus OFDM
- 802.11ay: next Wi-Gig. Compared to 802.11ad:
  - Channel bonding: 4 channels of 2.16 GHz: 8.64GHz => 44Gbps
  - MIMO with 4 streams => 4x44Gbps=176Gbps

106

802.11ax major features

802.11ax major features

1. Downlink and uplink OFDMA
2. Downlink* and uplink multi-user MIMO
3. Higher order modulation
4. Advanced OFDM and coding
5. Outdoor operation
6. Reduced power consumption
7. Spatial re-use
8. Transmit beamforming*
9. Single-user operation*

(* not new in 802.11ax)

802.11ax source: Aruba 802.11ax White Paper

107

Wi-Fi standards progression

2021

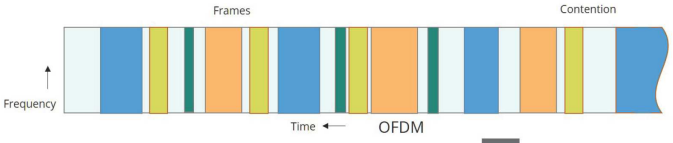
802.11n (2008):	802.11ac (2012):	802.11ax (2018):	Goals of the 802.11ax project:
• 2.4 and 5 GHz supported • Wider channels (40 MHz) • Better modulation (64-QAM) • Additional streams (up to 4) • Beam forming (explicit and implicit) • Backwards compatibility with 11a/b/g	• 5 GHz only • Even wider channels (80, 160 MHz) • Better modulation (256-QAM) • Additional streams (up to 8) • Beam forming (explicit) • MU-MIMO • Backwards compatibility with 11a/b/g/n	• 2.4 GHz and 5 GHz supported • OFDMA uplink and downlink • Extends and generalizes OFDM • Introduces the concept of Resource Units (RU's) • Massive parallelism • Better modulation (1024-QAM) • Uplink MU MIMO • Spatial re-use (BSS color) • Backwards compatibility with 11a/b/g/n/ac	• Enhance operation in 2.4 & 5 GHz bands (802.11ac was only 5 GHz) • Increase average throughput per station by at least 4x in a dense deployment scenario (802.11ac specified aggregate throughput without a specific scenario) • For outdoor and indoor networks • Scenarios include wireless corporate office, outdoor hotspot, dense residential apartments, stadiums • Maintain or improve power efficiency of client devices

108

802.11ax OFDMA

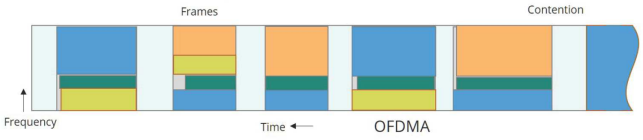
Single user OFDM:

Different colors correspond to different users



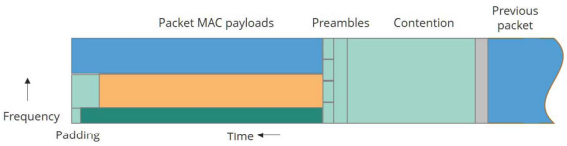
- Each frame is transmitted across the whole channel width.
- Each transmit opportunity requires contention, losing spectral efficiency.
- Low-rate transmissions can block the channel for others, increasing latency and jitter.

- As each transmit opportunity can be shared across a number of frames, there is less contention overhead.
- Low data-rate traffic can reduce its contention and header overhead.
- Traffic requiring lower latency or jitter can be allocated more frequent transmit opportunities.



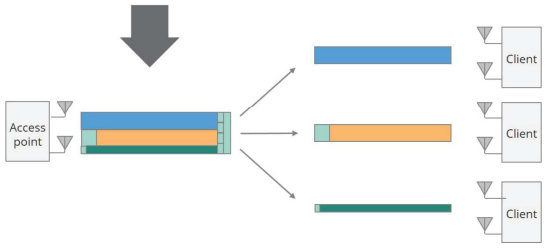
109

802.11ax OFDMA in downlink



- Access point performs contention to gain a single transmit opportunity.
- Transmits a single preamble across all frequencies, followed by individually-addressed frames in each chosen OFDMA sub-channel.
- Padding ensures all frames have the length of the longest.

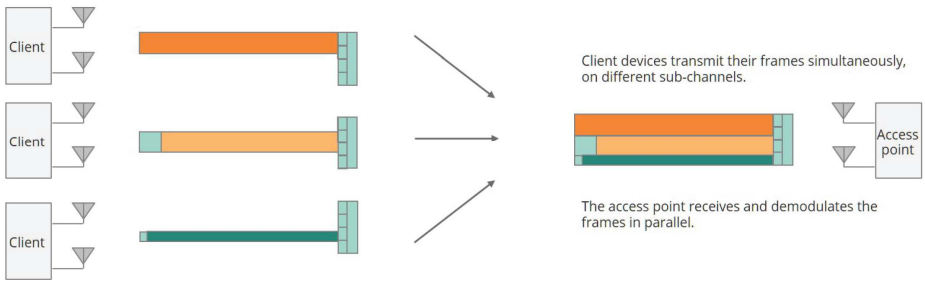
- Access point transmits in one transmit opportunity, packing frames to different clients into different OFDMA sub-channels.
- Sub-channels can have different widths (in frequency dimension).



- AP contends for channel access
- Assembles number of frames to different clients on different subcarriers

110

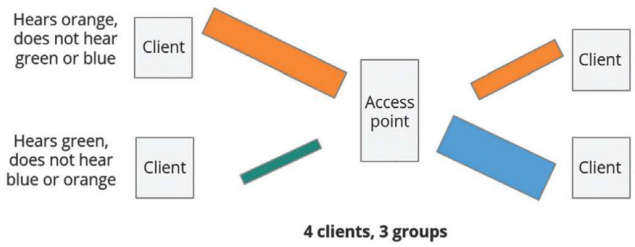
802.11ax OFDMA in uplink



- AP needs to calculate best grouping of clients

111

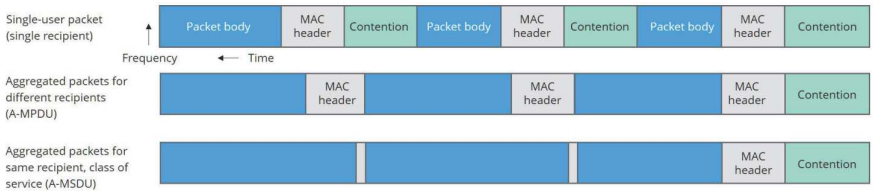
Downlink MU-MIMO



- Exploits space diversity
- Supported in 802.11ac
- AP sends null frames on all antennas to clients
  - clients return responses with matrices of the measured receive levels for each AP-antenna to client-antenna pair
- Clients return receive levels on all antennas

112

Packet aggregation (from 802.11n)



- Avoid contention for transmissions from AP
  - Gains for video streaming
- MAC header only for packets to different stations
- Single MAC header for packets to same station
- 802.11ax: combines packet aggregation with MU-MIMO and OFDMA

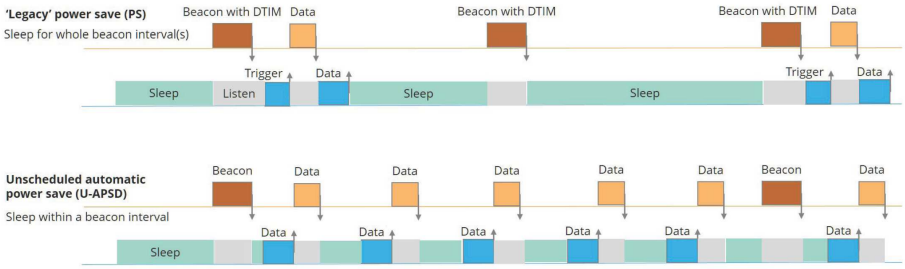
113

Multi-User modes

- Two multi-user modes:
  - MU-MIMO
  - OFDMA
- Supported in downlink and uplink
- Downlink: only AP sends
- Uplink: AP needs to poll clients for requirements
- AP performs scheduling in both directions

114

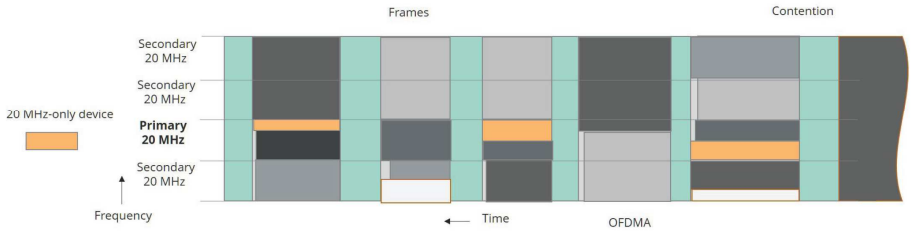
802.11ax power save mode TWT (Target Wait Time)



- Legacy 802.11: Clients can sleep between AP beacons (or multiples of beacons), waking when they have data to transmit and for beacons containing the delivery traffic information map (DTIM)
- 802.11ax: allows more flexible, long-term, multi-client sleeping arrangements
  - A negotiation between the client and AP sets up an agreed schedule for client to wake and communicate.
  - Schedule is often periodic, with a long, multi-beacon interval (minutes, perhaps hours or days) between activities

115

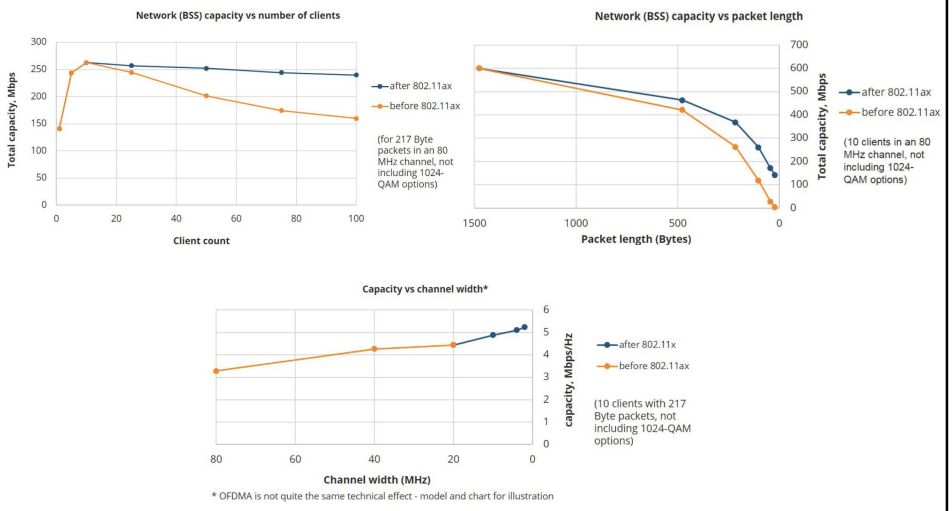
20 MHz IoT devices



- 20 MHz-only devices of operating in either 2.4 or 5 GHz band
  - OFDMA also allows such devices to transmit and receive on much smaller sub-channel
- Access points must support full standard

116

802.11ax support for large # clients, small packets & small channel width



802.11ax Aruba White Paper

117

802.11ax major features summary

Access Point	
Mandatory	Optional
Downlink OFDMA transmit	
Uplink OFDMA receive	
Downlink MU-MIMO transmit (if 4+ SS)	Downlink MU-MIMO transmit (if < 4 SS)
Transmit beamforming (if 4+ SS)	
SU MIMO transmit & receive with up to 2x SS	SU MIMO with 3+ SS
20, 40, 80 MHz operation if supporting 5 GHz	
20 MHz operation if supporting 2.4 GHz	
20 MHz-only operation in wideband OFDMA	
Individual TWT	
BSS coloring	Spatial re-use
Transmit & Receive operating mode	
	MCS 8, 9, 10, 11 (256 & 1024-QAM)
	160 MHz operation (if supporting 5 GHz)

Client	
Mandatory	Optional
Downlink OFDMA receive	
Uplink OFDMA transmit	
Downlink MU-MIMO receive (up to 4x SS)	
Receive beamforming	
SU MIMO transmit & receive	
20, 40, 80 MHz operation if supporting 5 GHz	
20 MHz operation if supporting 2.4 GHz	
	Individual TWT
BSS coloring	Spatial re-use
Transmit & receive operating mode	

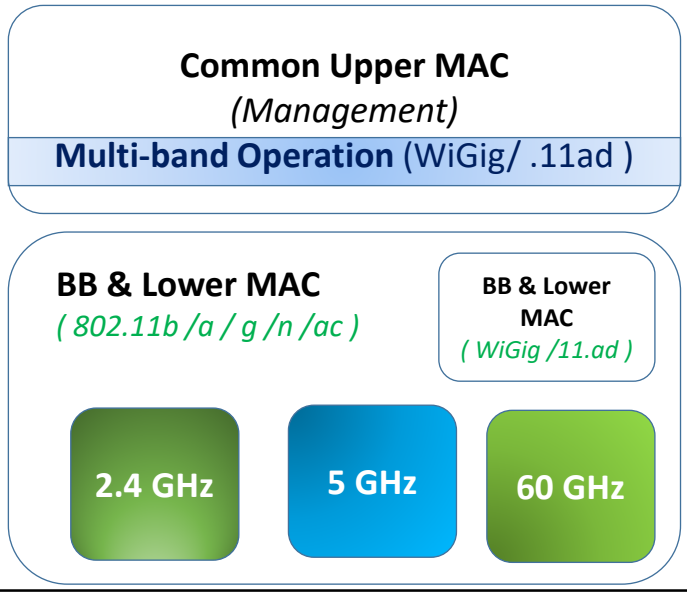
118

802.11ax wave 1 and 2

Wave 1	Wave 2
Downlink and uplink OFDMA	Uplink multi-user MIMO
Downlink MU-MIMO	
Target Wait Time (TWT)	
BSS Coloring	Spatial re-use
20 MHz-only	
	Long-range 802.11ax

119

802.11ad: 2.4, 5, and 60 GHz coexistence



120

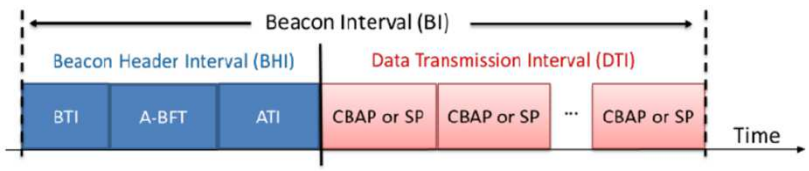
802.11ad: Network Architecture

- PBSS (Personal Basic Service Set): allow nodes to communicate in ad-hoc manner
  - Similarities with WiFi direct: one participating node has role of PBSS Control Point (PCP)
- Topology: Simultaneously support for infrastructure and P2P connections
- Multiple AP/PCP coexistence
  - One AP serves as synchronization AP
- PCP handover: addresses PCP outages

121

802.11ad MAC: Beacon interval and Framing

- All nodes synchronized in beacon intervals
- Beacon interval (BI) = BHI + DTI
  - BHI: training, signaling; DTI: data transmission
- Two modes of data transmission
  - CBAP: contention-based access periods
  - SP: Service periods (TDMA)



122

IEEE 802.11ad MAC

- Contention-based medium access: IEEE 802.11 EDCA
  - Challenges due to directionality of 60 GHz signals
  - Virtual carrier sensing with RTS/CTS & NAV
- Dynamic channel time allocation
  - Polling-based mechanism
  - Extension of 802.11 PCF (Point Coordination Function)
- Pseudo-static TDMA channel time allocation
  - AP sends time slot allocations to all associated stations

123

IEEE 802.11ad beamforming training

- Transmit and receive training

- Sector Level Sweep (SLS) in two phases: coarse-grain and refined
  - Allows implementation customization

124