

Internet of Things: Protocols and Networks
(CSC2106)

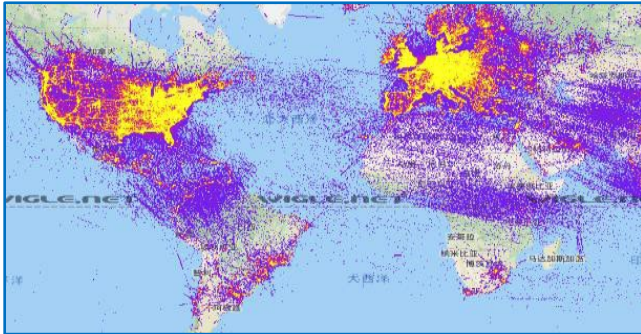
IEEE802.11ah aka “HaLow”

Recent Protocols for IoT

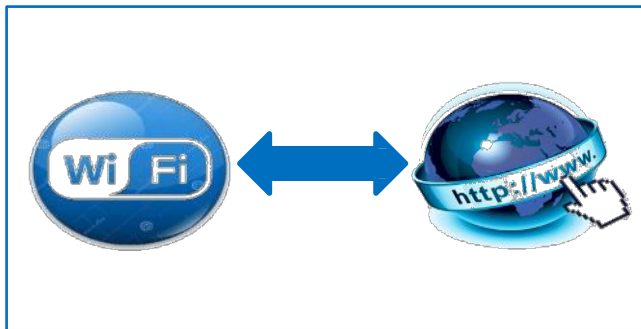
| | | | |
|----------|--|---|---|
| Session | MQTT, SMQTT, CoRE, DDS, AMQP , XMPP, CoAP, IEC,... | Security | Management |
| Network | Encapsulation 6LowPAN, 6TiSCH, 6Lo, Thread... | IEEE 1888.3, TCG, Oath 2.0, SMACK, SASL, EDSA, ace, DTLS, Dice, ... | IEEE 1905, IEEE 1451, IEEE 1377, IEEE P1828, IEEE P1856 |
| | Routing RPL, CORPL, CARP | | |
| Datalink | Wi-Fi, 802.11ah, Bluetooth Low Energy, Z-Wave, ZigBee Smart, DECT/ULE, 3G/LTE, NFC, Weightless, HomePlug GP, 802.15.4e, G.9959, WirelessHART, DASH7, ANT+, LTE-A, LoRaWAN, ISA100.11a, DigiMesh, WiMAX, NB-IoT , SigFox ... | | |

Wi-Fi: a prime Contender of IoT

Some low-power protocols do not currently enjoy ubiquitous access to the Internet

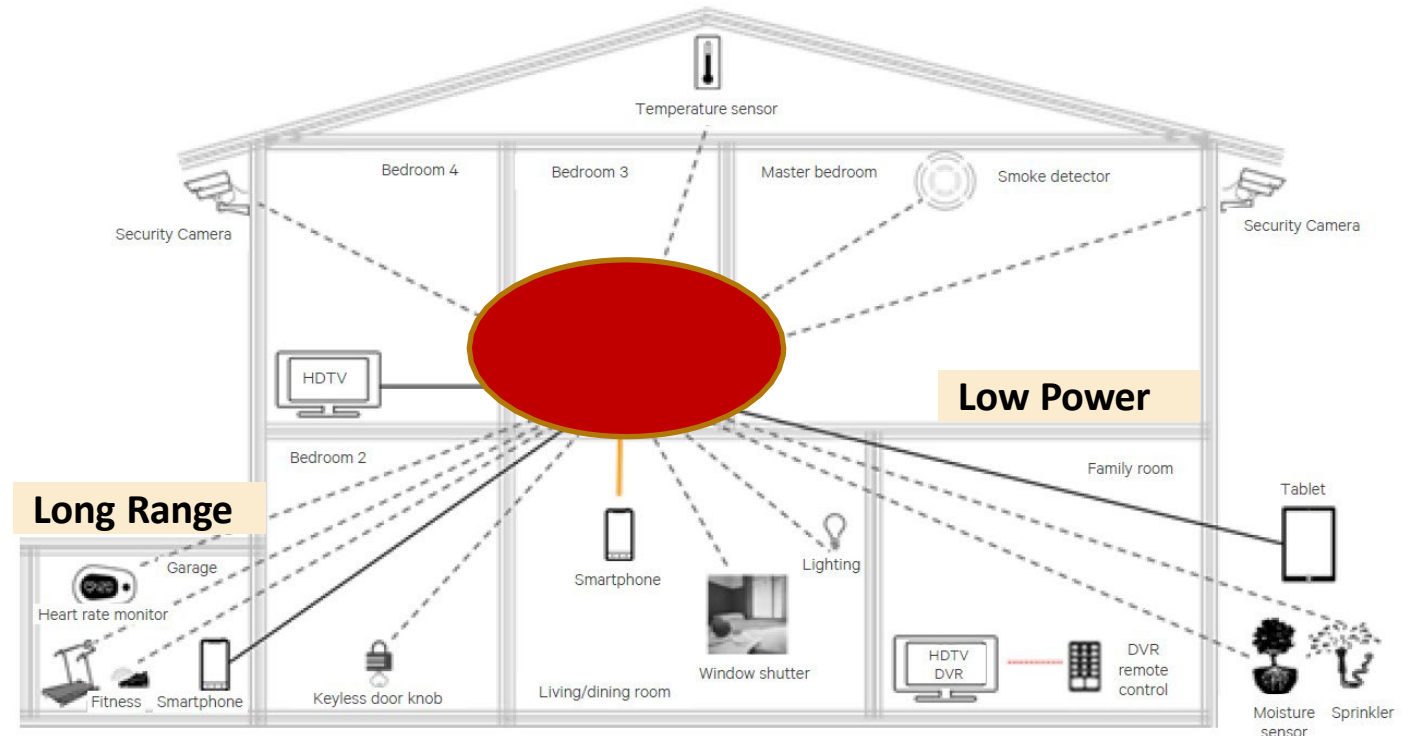


Wide deployments

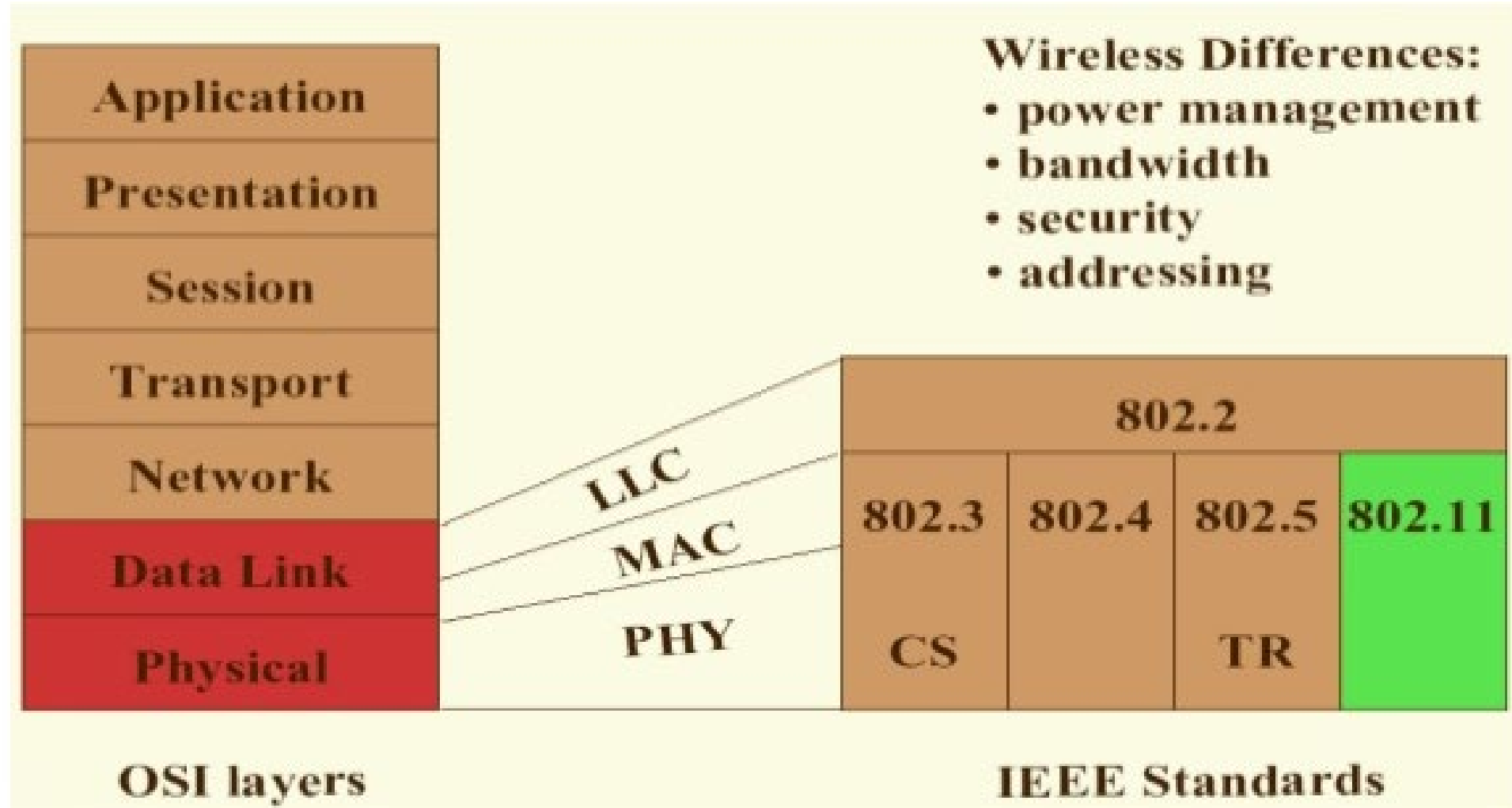


Compatibility with Internet

IoT Wi-Fi (home) Vision



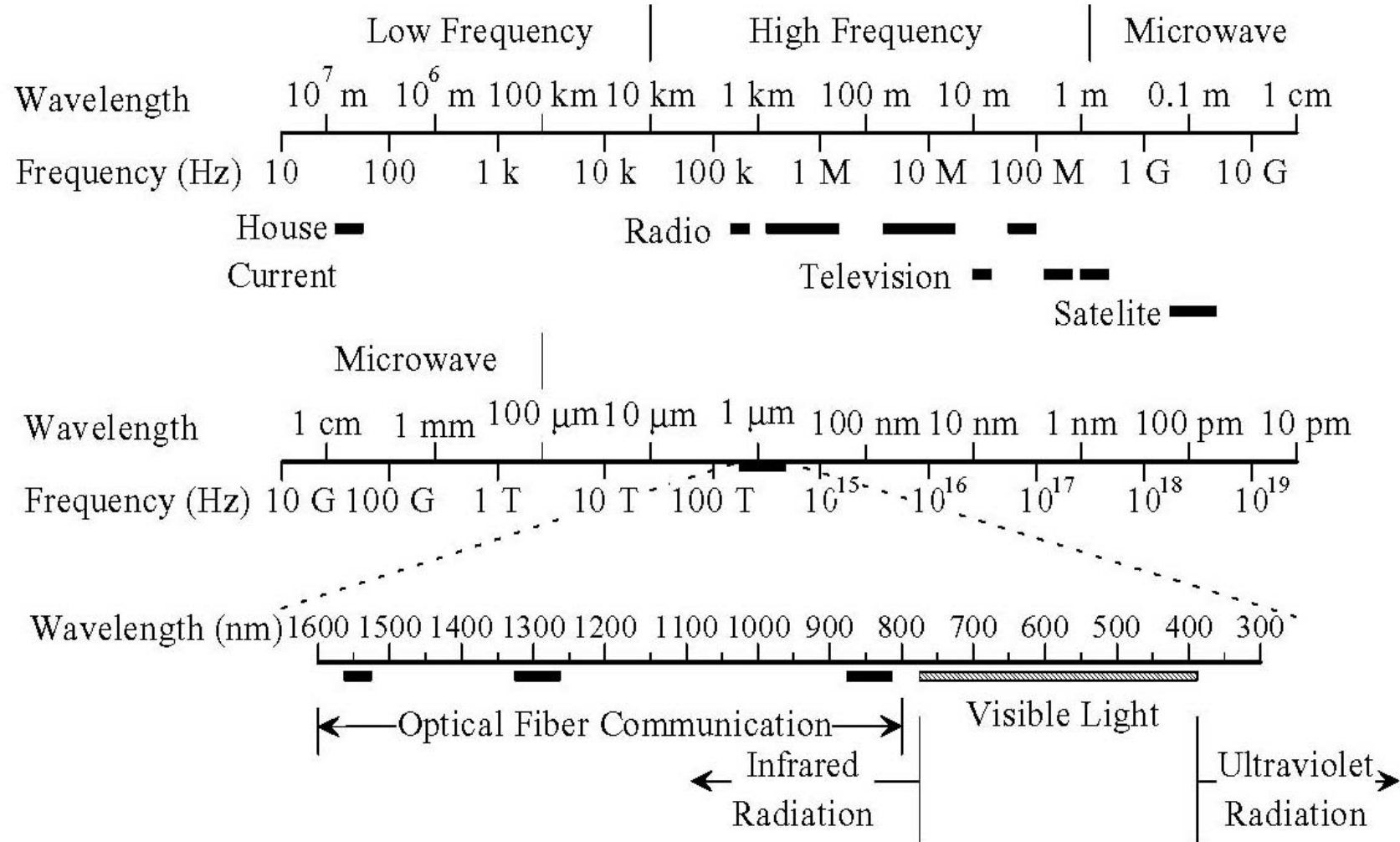
Protocols for the 'Data Link' and 'Physical' Layers of OSI Reference Model: Ethernet and Wi-Fi



IEEE 802.11 vs. Wi-Fi

- IEEE 802.11 is a standard
 - Wi-Fi = “Wireless Fidelity” is a trademark
 - Fidelity = Compatibility between wireless equipment from different manufacturers
 - Wi-Fi Alliance is a non-profit organization that does the compatibility testing (WiFi.org)
 - 802.11 has many options and it is possible for two equipment based on 802.11 to be incompatible.
 - All equipment with “Wi-Fi” logo have selected options such that they will interoperate.
-

Electromagnetic Spectrum



IEEE 802.11 Physical Layers

- First version in 1997: IEEE 802.11
 - Includes MAC layer and three physical layer specifications
 - Two in 2.4-GHz band and one infrared
 - All operating at 1 and 2 Mbps
 - No longer used
- Two additional amendments in 1999:
 - IEEE 802.11a-1999: 5-GHz band, 54 Mbps/20 MHz, **OFDM**
 - IEEE 802.11b-1999: 2.4 GHz band, 11 Mbps/22 MHz
- Fourth amendment:
 - IEEE 802.11g-2003 : 2.4 GHz band, 54 Mbps/20 MHz, **OFDM**

IEEE 802.11 Physical Layers

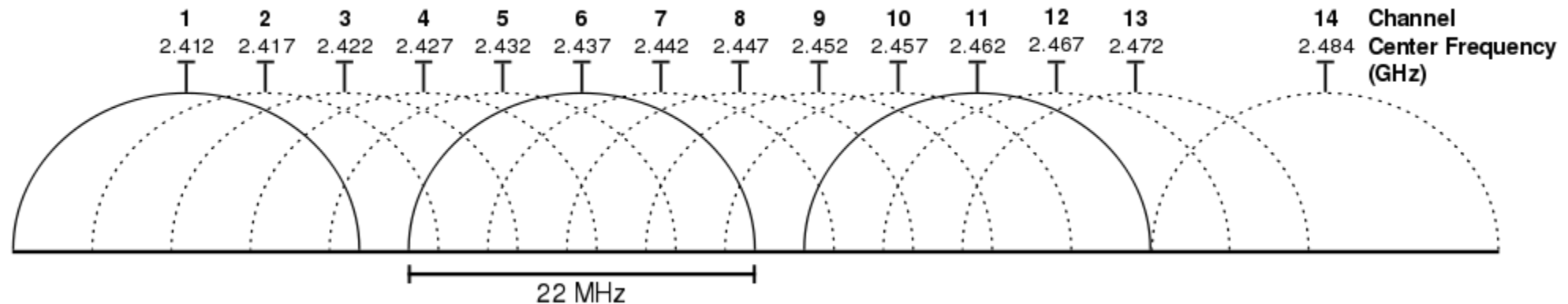
- WiFi 4
 - Based on IEEE 802.11n-2009 standard
 - Operates in 2.4GHz or 5GHz band
 - First WiFi to introduce MIMO (Multiple Input Multiple Output)
 - Maximum Data rate: 72Mbps/20MHz, 600Mbps/40MHz, uses OFDM
- WiFi 5
 - Based on IEEE 802.11ac-2023 standard
 - Operates in 5GHz band
 - Uses MIMO, Multiuser-MIMO and OFDM
 - Possible to use 256 QAM i.e. grouping 8 bits into one symbol.
 - Overall throughput can reach up to 1.1 Gbps/80MHz
 - Also has the option to use 160MHz but not compulsory to implement

IEEE 802.11 Physical Layers

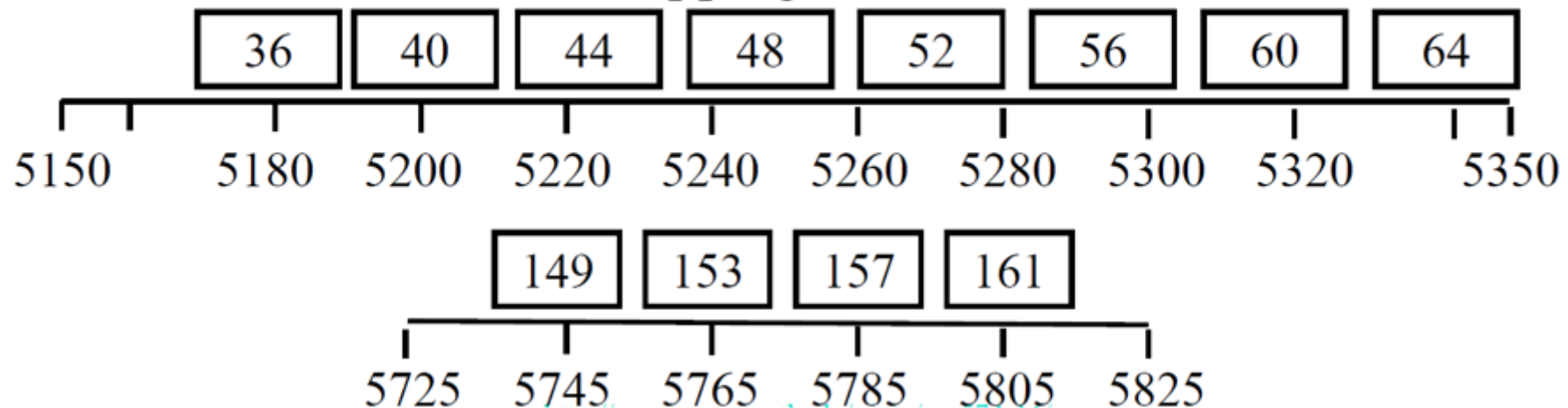
- WiFi 6/WiFi 6E (adopted in 2019)
 - Based on IEEE 802.11ax
 - Operates in 2.5GHz, 5GHz and 6GHz bands
 - Introduced OFDMA for supporting multiple users in a single band
 - Bandwidth up to 160MHz, Data rates up to 10Gbps
 - Enhancements like 1024QAM exist in this standard i.e. grouping 10 bits into one symbol
- WiFi 7 (will be finalized in 2024)
 - Based on IEEE 802.11be
 - Operates in 2.5GHz, 5GHz and 6GHz bands
 - Data rates up to 46Gbps
 - Enhancements like 4096QAM exist in this standard i.e. grouping 12 bits into one symbol
 - Enhanced resource allocation in OFDMA
 - Contiguous and non-contiguous 320/160+160 MHz and 240/160+80 MHz bandwidth
- WiFi 8 (yet to start, based on IEEE 802.11bn)

Wi-Fi Channels

2.4 GHz Band: 100 MHz between 2400 MHz to 2500 MHz, 14 5-MHz channels, **only 3 non-overlapping**



5 GHz Band: 12 non-overlapping channels



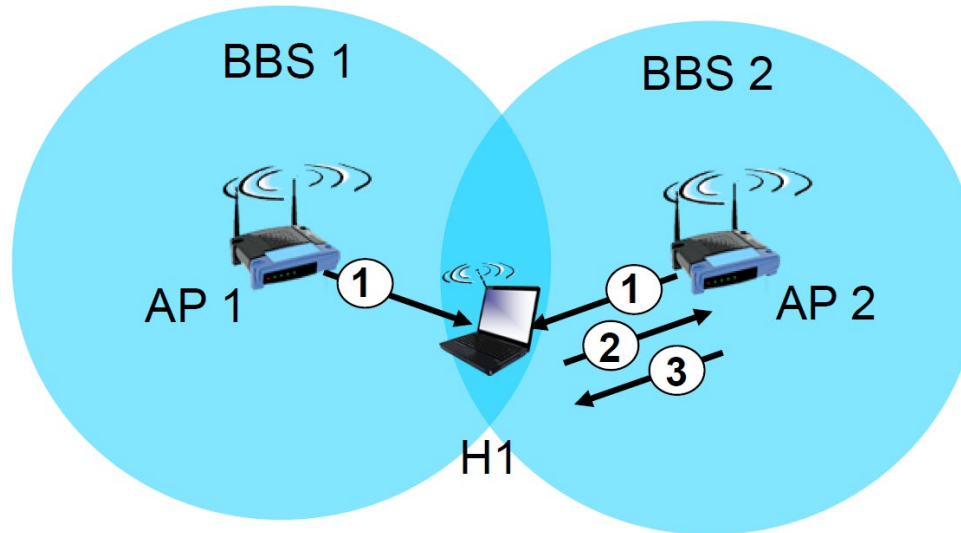
IEEE 802.11 Components

- **Station:** the component (or the device) that connects to the wireless medium.
 - **Basic Service Set (BSS)**
 - Infrastructure BSS: A BSS with a set of stations associated with one AP
 - Independent BSS: A BSS with a set of stations that communicate with one another. IBSS is typically short-lived network, with a small number of stations, that is created for a particular purpose (Example: Ad-hoc networks).
 - **Extended Service Set (ESS):** An ESS is a set of infrastructure BSSs, where the APs communicate among themselves to forward traffic from one BSS to another and to facilitate the movement of mobile stations from one BSS to another.
 - **Distribution System (DS):** The distribution system (DS) is the mechanism by which one AP communicates with another to exchange frames for stations in their BSSs, forward frames to follow mobile stations from one BSS to another, and exchange frames with wired network.
-
-

How does a station join a BSS?

Passive Scanning

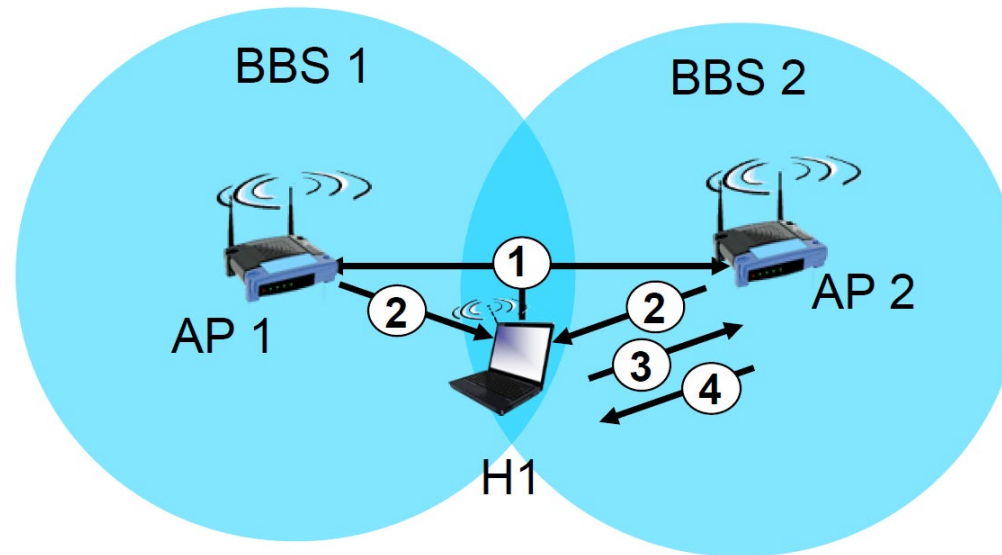
1. Beacon Frames sent from APs
2. Association Request frame sent from the H1 selected AP
3. Association Response frame sent from selected AP to H1
4. When mobile stations associate with an access point, the access point assigns a value called the Association ID (AID) from the range 1-2007



How does a station join a BSS?

Active Scanning: →

1. Probe Request frame broadcast from H1
2. Probe Response frames sent from APs
3. Association Request frame sent: H1 to selected AP
4. Association Response frame sent from selected AP to H1

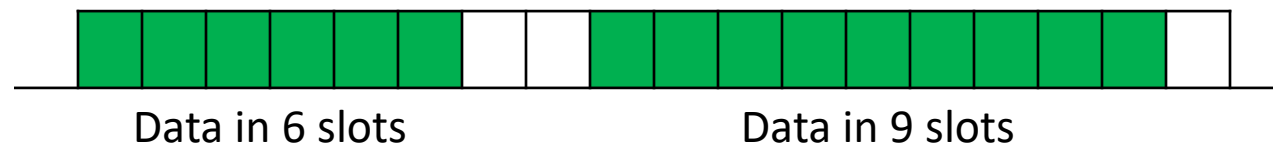


What data rate?

- Modulation and Coding Scheme (MCS)
 - MCS is a technique used in wireless communication to improve the data transmission rate by manipulating the way data is transmitted over the airwaves.
 - MCS is a combination of modulation and coding techniques that work together to increase the data transmission rate while maintaining the quality of the received signal.
 - The MCS technique has been widely used in different wireless communication technologies such as Wi-Fi, 4G LTE, 5G, and others.
- MCS works by selecting the most appropriate modulation and coding scheme for a given transmission channel based on the signal quality.
 - The selection process is based on the channel's signal-to-noise ratio (SNR), which is the ratio of the signal power to the noise power in the channel.
 - The higher the SNR, the more data can be transmitted over the channel without errors.
- Various modulation schemes and coding rates are defined by the standard, which also assigns an arbitrary number to each.
 - This number is the modulation and coding scheme index, or MCS index.

Channel Access

- Nodes have random access to the channel
 - They can transmit whenever they need to.
 - Data is transmitted in frames.
 - This will also lead to collisions.
- What is a collision?
 - Two nodes transmitting at the same time.
 - Signal received at the AP is a mixture of the signals transmitted by the nodes.
 - Makes it difficult to decode and leads to wastage of resources.
- Parameters that will be used often:
 - A SLOT time: defined in the 802.11 standard
 - Frame: Data transmitted (could be anything) spread over different SLOTS.



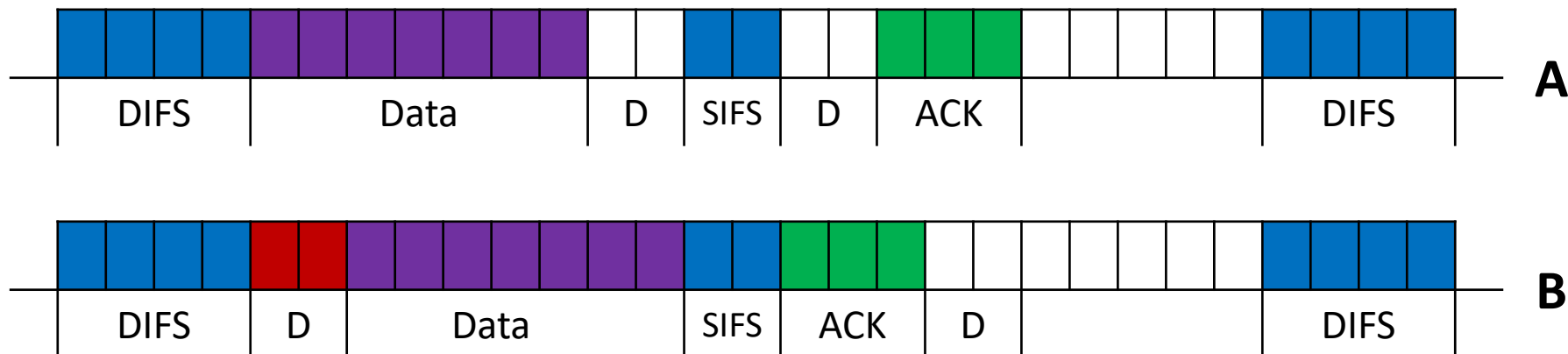
Channel Access: DCF

- To avoid collisions, we include some rules
 - Referred to as the Distributed Coordination Function (DCF)
 - Based on Carrier Sense Multiple Access (CSMA).
 - Nodes listen to the channel and transmit only if they sense it to be “idle”.
 - The channels needs to be “idle” for a time equal to DCF Inter Frame Space (DIFS)



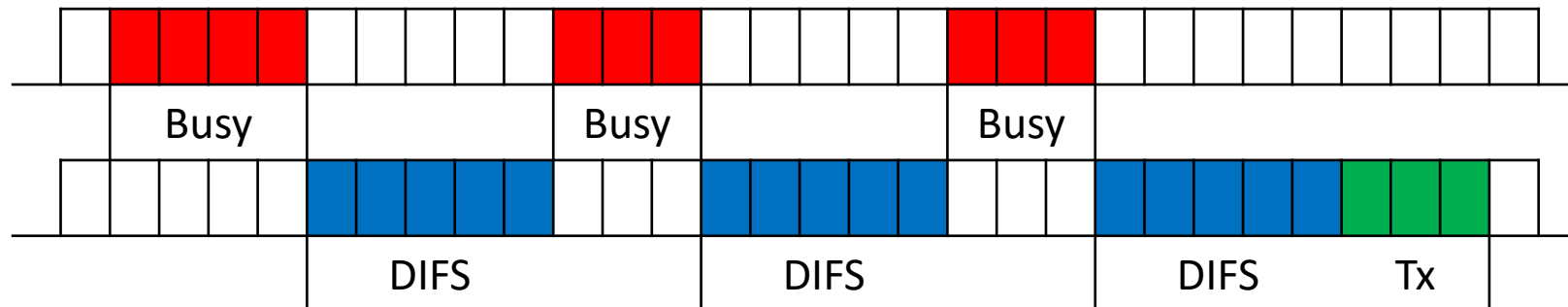
Channel Access: CSMA

- A node/station **A** is transmitting to the AP **B**.
 - DIFS: DCF Inter Frame Space
 - SIFS: Short Inter Frame Space. Required for switching from Rx to Tx.
 - $DIFS = SIFS + 2 \text{ slot time}$ (slot time is defined in standard)
 - Propagation Delay **D**
 - A positive ACK is necessary to ensure that the frame has been successfully received. Frames may be lost due to channel errors or collisions (To confirm collision either a NACK is sent or nothing).



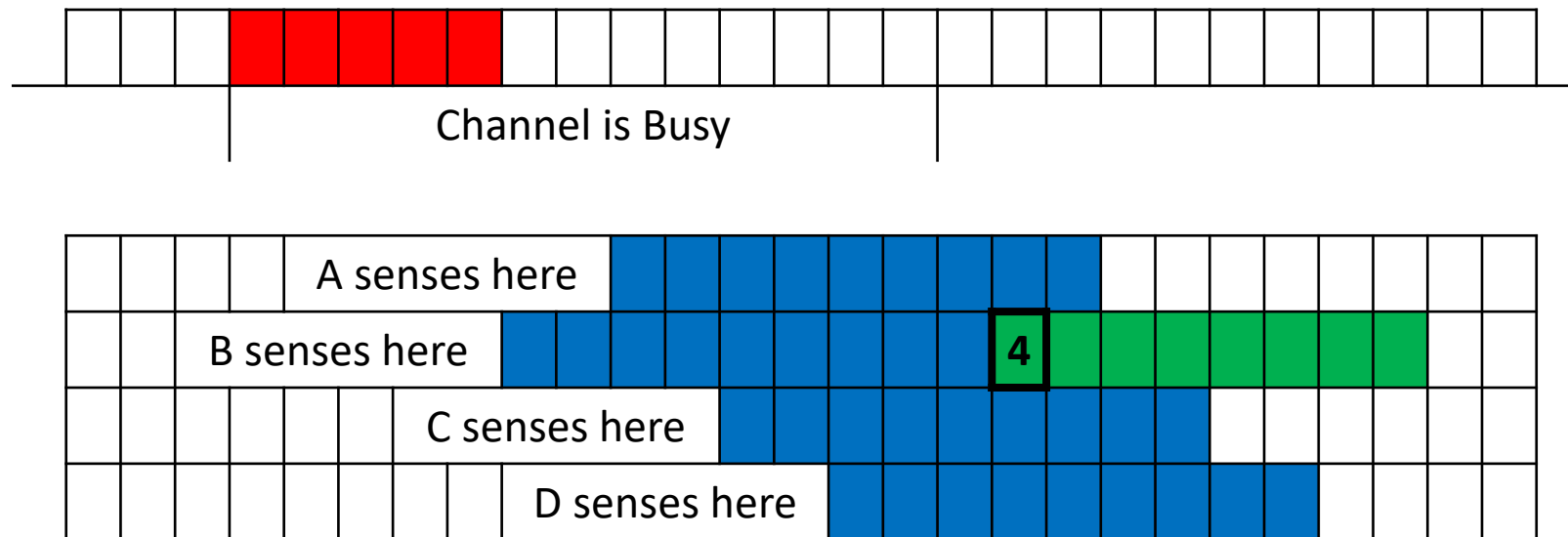
Virtual Carrier Sense

- Every frame has a “Duration ID” which indicates how long the medium will be busy.
 - The busy channels includes Data, SIFS and ACK
- All stations keep a “Network Allocation Vector (NAV)” timer in which they record the duration of each frame they hear.
- Stations do not need to sense the channel until NAV becomes zero.



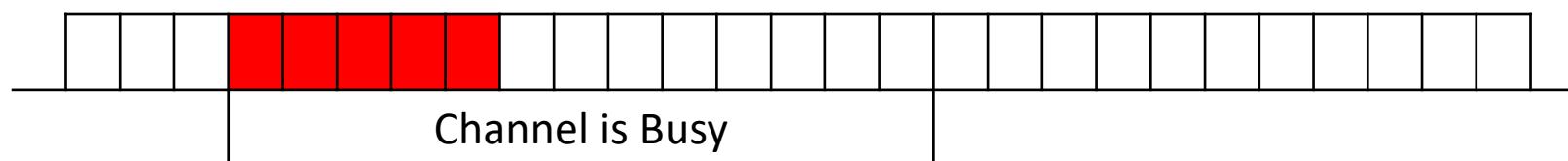
Channel Access: CSMA

- Which device will transmit? In which slot will it start transmitting?
 - Node **B** will transmit, and rest again wait for their slot.
 - Starts transmitting in slot 4.

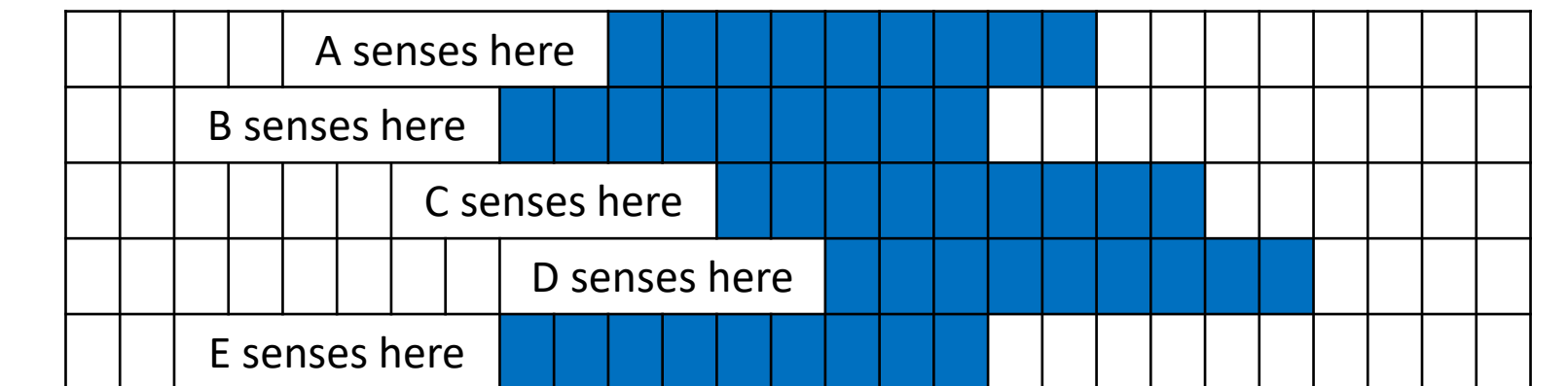


Channel Access: CSMA

- Have we completely evaded the collision problem?
 - Not completely. Collisions can still happen!

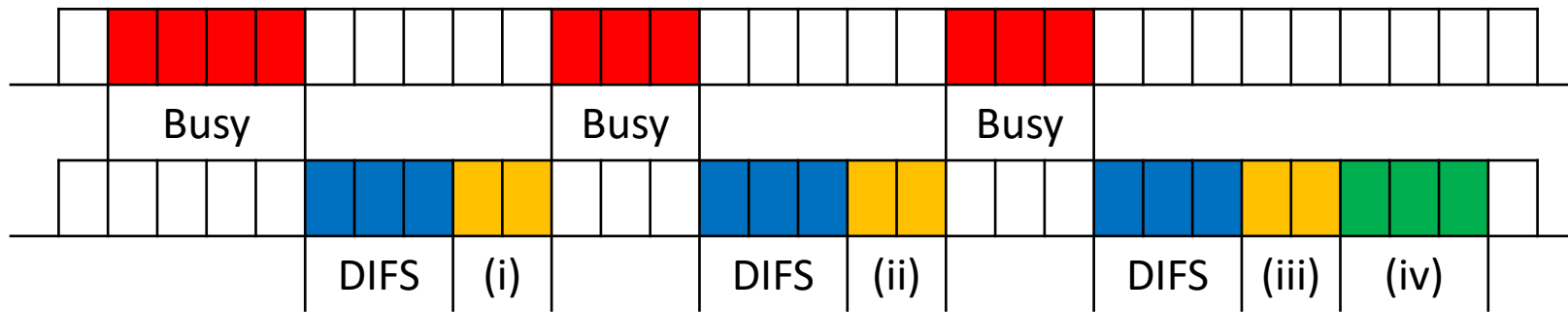


- Nodes **B** and **E** would end up colliding!



Channel Access: CSMA/CA

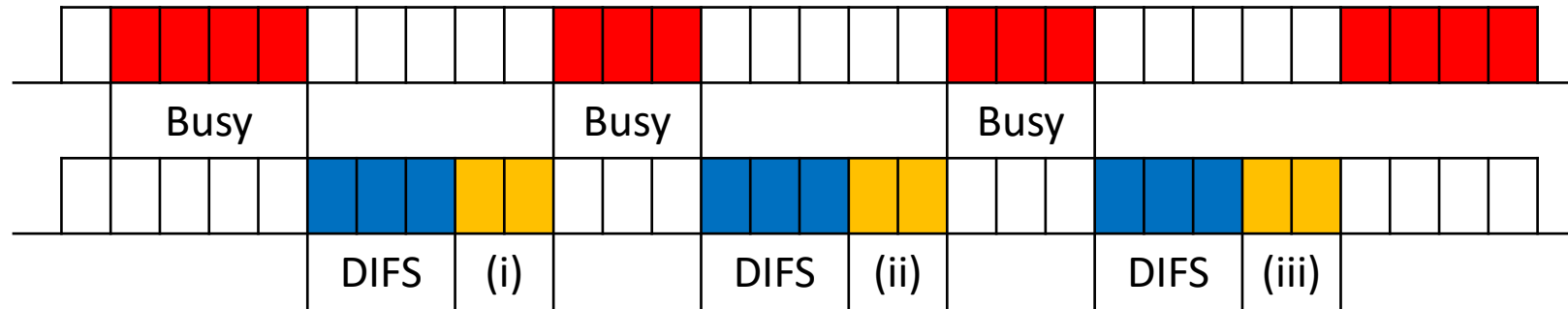
- To avoid such collisions, we use something called Exponential Backoff. This will further decrease the number of collisions.
 - Each node selects a random number CW (defined as Contention Window).
 - For example, say the node selected CW equal to 6 slots.



- The backoff counter is decremented by 2, $CW = 4$
- The backoff counter is decremented by 2, $CW = 2$
- The backoff counter is decremented by 2, $CW = 0$
- The node transmits data and resets CW back to its original value

Channel Access: CSMA/CA

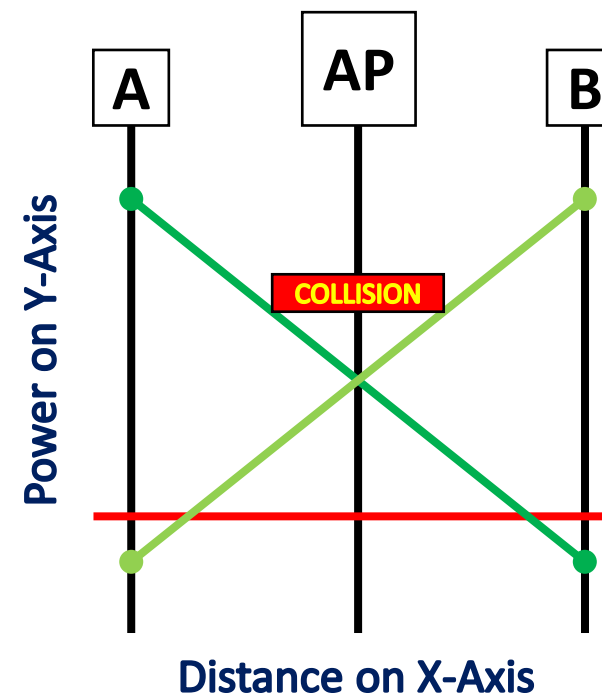
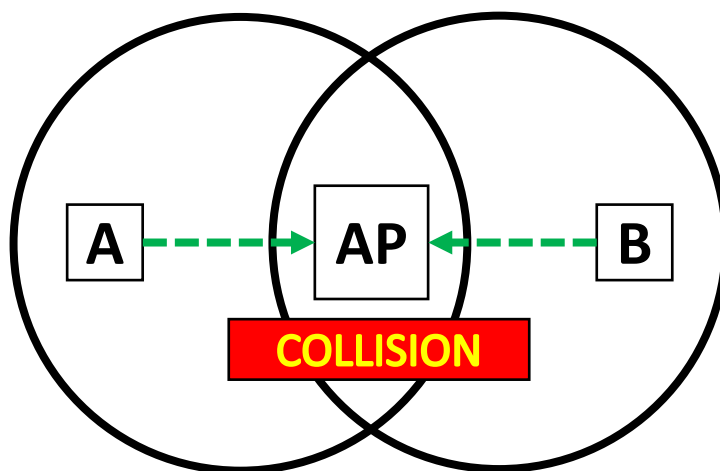
- What happens if the channel is still not available after CW becomes zero?



- (i) The backoff counter is decremented by 2, $CW = 4$
- (ii) The backoff counter is decremented by 2, $CW = 2$
- (iii) The backoff counter is decremented by 2, $CW = 0$
- (iv) CW gets updated $\Rightarrow CW = \min\{2CW + 1, CW_{\max}\}$

IEEE 802.11: Hidden Node Problem

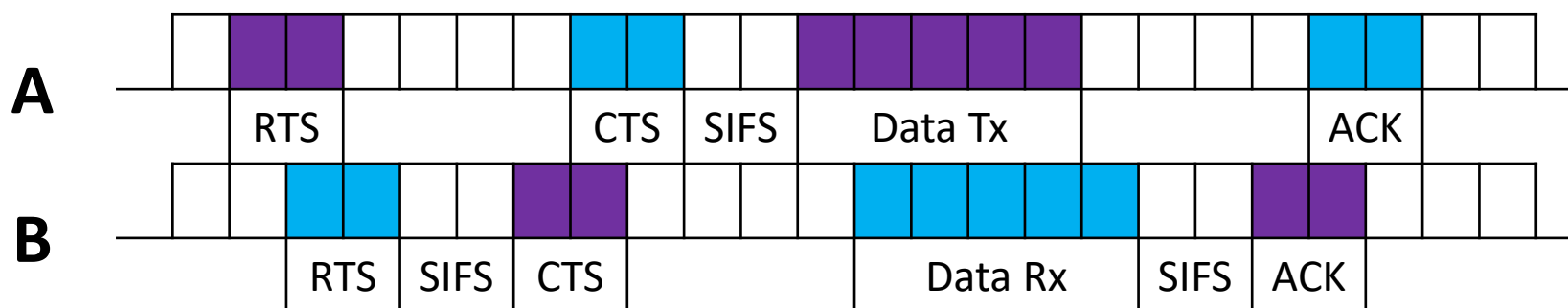
- Does this solve the problem?
 - Nope! There are hidden nodes
- What is a hidden node?



IF Power goes below the red line
THEN Transmission **cannot** be heard

Hidden Node: RTS-CTS Mechanism

- The hidden node problem can be addressed using RTS (Request To Send) and CTS (Clear To Send) packets
- Sender first transmits RTS packets to AP using CSMA
 - RTSs may still collide with each other (but they're short)
- AP broadcasts CTS in response to RTS
- CTS is heard by all nodes
 - Sender transmits data frame
 - Other stations defer transmissions using NAV

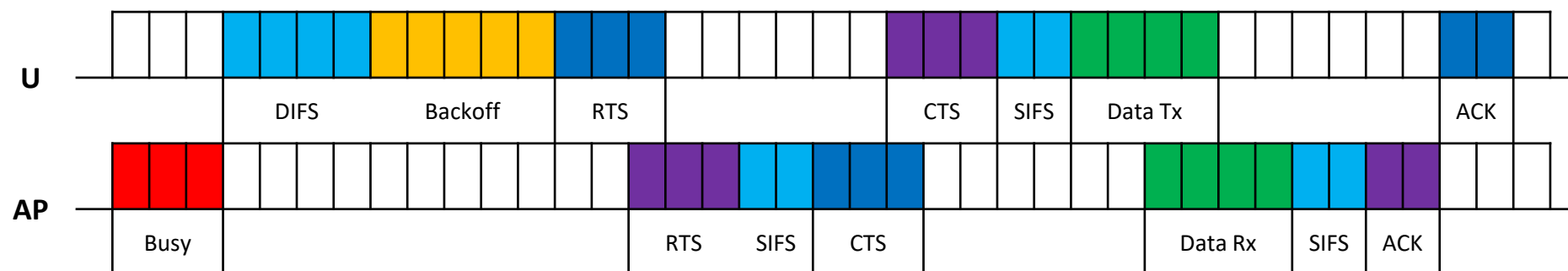


RTS-CTS Mechanism

- RTS alerts all stations that are within reception range of the source that an exchange is under way; these stations refrain from transmission in order to avoid a collision between two frames transmitted at the same time.
- Similarly, the CTS alerts all stations that are within reception range of the destination that an exchange is under way.
- RTS and CTS portion of the exchange is a required function of the MAC but may be disabled.

Overall Look of the Channel Access

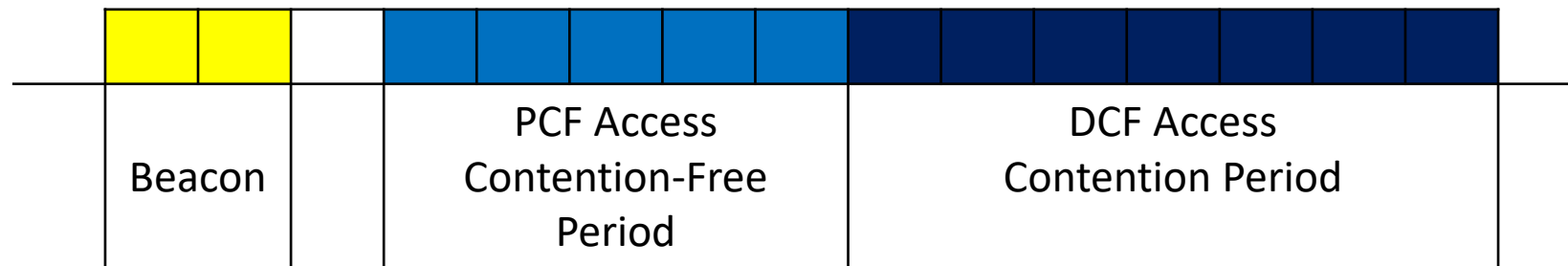
- Consider a node **U** transmitting information to an Access Point **AP**.



- What could be the propagation delay?
 - Answer as the number of slots: **2 slots**

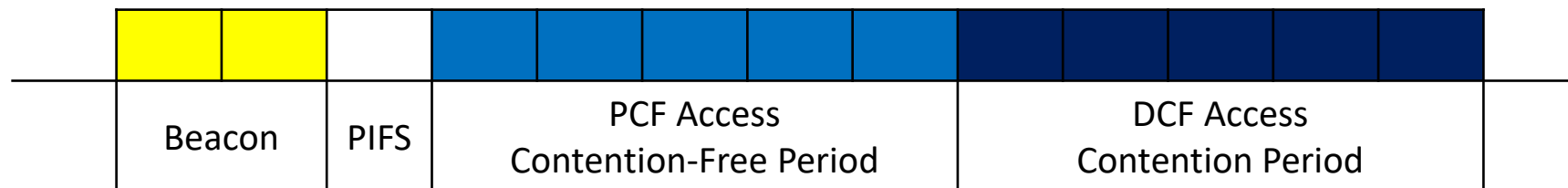
Point Coordination Function (PCF)

- Time critical services use Point Coordination Function
- Point coordinator (AP) polls devices
 - To give them permission to send on a schedule that the point coordinator (AP) determines
- Optional mechanism built on top of DCF



Point Coordination Function (PCF)

- AP transmits a beacon frame at regular intervals.
 - In the beacon frame, the AP announces a contention free period (CFP) where the usual DCF operation will be preempted.
- All MSs that use only DCF will set NAV to indicate that the medium will be busy for the duration of the CFP.
- The nodes which require PCF access, request the AP accordingly. Nodes are assigned slots in the PCF window to transmit (like cellular architecture).
- The time between the beacon and PCF window is PIFS (PCF Inter Frame Space)

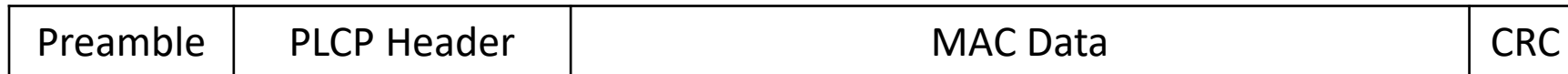


Power Management

- Key idea of numerous power management mechanisms used in IEEE 802.11 networks is based on alternating between two states: **awake** and **doze**.
 - In the awake state, a station can receive and transmit frames.
 - In the doze state, a station switches off radio module and can neither receive nor transmit.
 - A station can work in two modes: in power save (PS) mode, it alternates between these states, while in active mode it is always awake.
- In infrastructure networks, a station shall notify the AP before it changes the mode. If the station is in the PS mode, the AP buffers all frames (except for some kinds of management frames) destined for this station.
 - To notify PS stations about buffered packets, the AP includes Traffic Indication Map (TIM) in each beacon. TIM indicates the presence of packets destined for each station.
 - A PS station periodically wakes up to receive a beacon. It does not need to listen to each TIM element, so it can sleep for Listen Interval which can be much longer than Beacon Period.
 - Although the standard does not require it, in practice, PS stations wake up just before DTIM beacon.
 - If no buffered packets are destined for the station, it returns to the doze state just after the beacon.
- Alternatively, the station sends a PS-Poll frame after groupcast transmission. As a response to PS-Poll, the AP sends buffered frames.

Types of Frames

- Three types of frames:
 - Data Frames: which are used for data transmission
 - Control Frames: which are used to control access to the medium (RTS, CTS and ACK)
 - Management Frames: Frames transmitted the same way as the data frames but are not forwarded to the upper layers.
- Components of an 802.11 Frame (PHY headers):



- Components of an 802.11 MAC Header



WiFi: Can it support all IoT devices?

- Need to support all traffic demands
- Symmetrical design is very inefficient
 - Example: Use the same sampling rates for packet receiving
- Legacy Wi-Fi is originally designed to offer high throughput to a limited number of stations located indoor at a short distance between each other.



Heavy traffic
High end



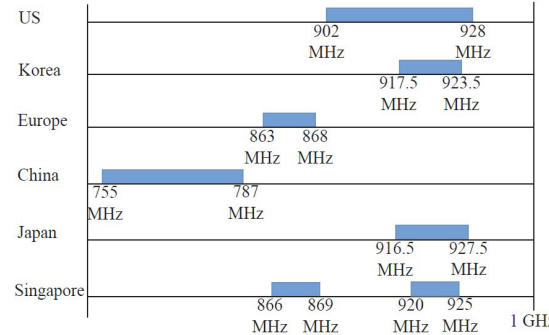
Moderate
traffic



Light traffic
Energy constrained






Introducing Wi-Fi 802.11ah

- aka “**Wi-Fi HaLow**” by WiFi Alliance.
- IEEE spec for Low-rate long-range IoT applications.
- Spectrum: **Sub-Giga Hertz** license-exempt spectrum. Not including TV white spaces (700 MHz for 802.11af).
 - 902-928 MHz (USA)
 - 863-868.6 MHz (Europe)
 - 916.5-927.5 MHz (Japan)
 - 755-587 MHz (China)
 - 917.5-923.5 MHz (Korea)
- Sub-GHz frequency \Rightarrow **Longer range than 2.4 GHz**, Less congested, better penetration
- Low bit rate for IoT, Short data transmissions, Power savings, Efficient MAC
- Goal: Support at least **4X devices per AP** than legacy 802.11
- 802.11ah PHY **down clocked by 10X** when compared to 802.11ac
 - 2/4/8/16 MHz channels in place of 20/40/80/160 MHz in ac


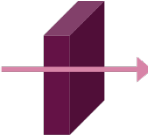




Wi-Fi CERTIFIED HaLow™ for IoT

Features

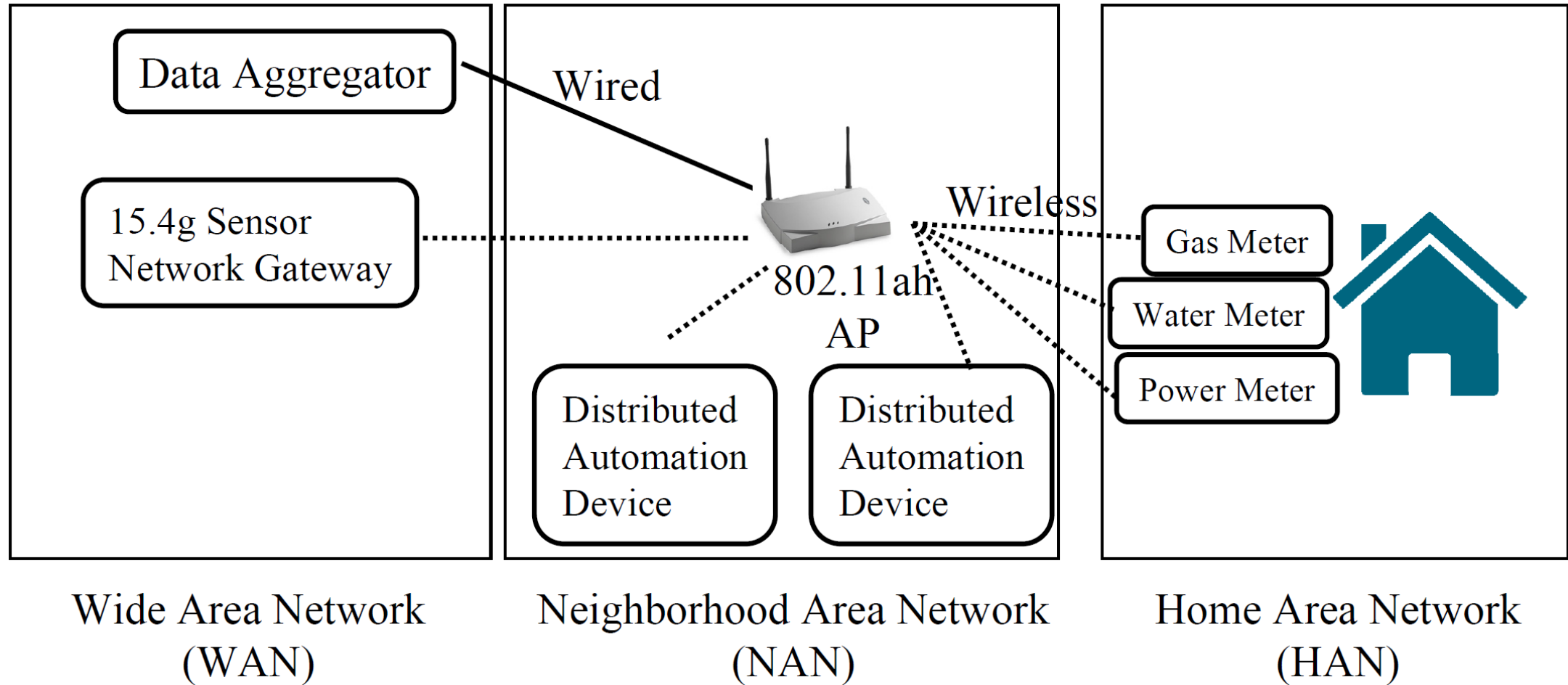
-  Sub-1 GHz spectrum operation
-  Narrow band OFDM channels
-  Several device power saving modes
-  Native IP support
-  Latest Wi-Fi® security

Benefits

-  Long range: approximately 1 km
-  Penetration through walls and other obstacles
-  Supports coin cell battery devices for months or years
-  No need for proprietary hubs or gateways

Source: Wi-Fi Alliance®

Sample Application



How is it different from the legacy Wi-Fi?

- IEEE 802.11ah PHY layer is inherited from .11ac and adopted to Sub 1GHz band.
 - The channels used in .11ah are 10 times narrower than those in .11ac: 1, 2, 4, 8 and 16 MHz.
 - Only 1 and 2 MHz channels are mandatory.
- Uses OFDM for transmission
 - For 1MHz: 24 subcarriers available for data transmission
 - For 2MHz: 52 subcarriers available for data transmission

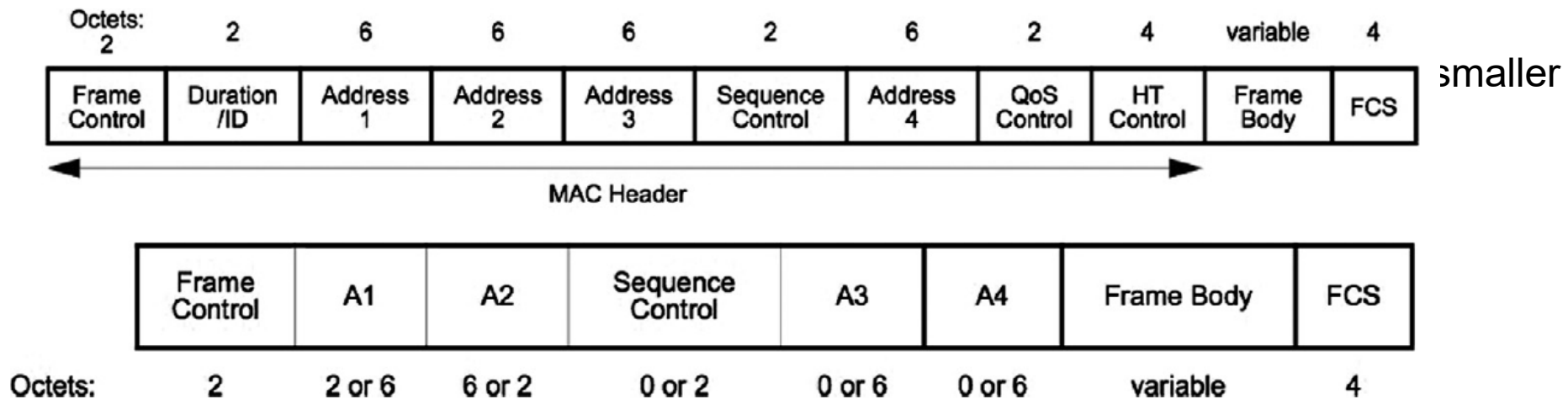
| MCS | 1 MHz | 2 MHz | 4 MHz | 8 MHz | 16 MHz |
|-------|-------|-------|-------|--------|--------|
| MCS0 | 0.3 | 0.65 | 1.35 | 2.925 | 5.85 |
| MCS1 | 0.6 | 1.30 | 2.70 | 5.850 | 11.70 |
| MCS2 | 0.9 | 1.95 | 4.05 | 8.775 | 17.55 |
| MCS3 | 1.2 | 2.60 | 5.40 | 11.700 | 23.40 |
| MCS4 | 1.8 | 3.90 | 8.10 | 17.550 | 35.10 |
| MCS5 | 2.4 | 5.20 | 10.80 | 23.400 | 46.80 |
| MCS6 | 2.7 | 5.85 | 12.15 | 26.325 | 52.65 |
| MCS7 | 3.0 | 6.50 | 13.50 | 29.250 | 58.50 |
| MCS8 | 3.6 | 7.80 | 16.20 | 35.100 | 70.20 |
| MCS9 | 4.0 | – | 18.00 | 39.000 | 78.00 |
| MCS10 | 0.15 | – | – | – | – |

How is it different from the legacy Wi-Fi?

- Legacy Wi-Fi: Maximum AID is 2007
 - Limits the number of devices to a little over 2k
 - IEEE 802.11ah Task Force Group increased the same to 8191 thereby enabling support for more devices.
- Header Reduction
 - In legacy .11 infrastructure networks, the length of the MAC header containing 3 addresses is 30 bytes, see Fig. 3. Frame Check Sequence (FCS) gives another 4 bytes.
 - Thus, for a 100-byte payload (messages), MAC header overhead exceeds 30%. For smaller messages, the overhead is even higher.
 - A significant change is that the short header contains no Duration/ID field required for NAV, a legacy virtual carrier sense mechanism, which made .11ah group to develop a novel channel access mechanism called Response Indication Deferral (RID).
 - The difference between RID and NAV is that RID is set just after reception of the PHY header, while NAV requires the whole frame to be successfully received.
 - RID estimates the duration based on the type of response stored in the 2-bit Response Indication field of the PHY header of the recently received frame

How is it different from the legacy Wi-Fi?

- Legacy Wi-Fi: Maximum AID is 2007
 - Limits the number of devices to a little over 2k
 - IEEE 802.11ah Task Force Group increased the same to 8191 thereby enabling support for more devices.
- Header Reduction
 - In legacy .11 infrastructure networks, the length of the MAC header containing 3 addresses is 30
- Th
me:



Legacy MAC header (top) and short MAC header (bottom)

How is it different from the legacy Wi-Fi?

- NDP MAC Frames:
 - Frames such as ACK, CTS, etc. do not transmit any useful information (except for the Duration field), just indicating frame reception, channel access, or other event.
 - However, they cause overhead, especially high in case of short transmissions.
 - To reduce overhead, .11ah develops a novel frame format called Null Data Packet (NDP) MAC frames
 - NDP frames were included in .11ac as short frames used for channel calibration.
 - .11ah extends this concept, allowing to include useful information in the SIG field of the PHY header.
- Short Beacons
 - Another source of excessive overhead is beacon. In infrastructure BSS, beacons are periodically sent by the AP. Beacon content depends on the mode in which the AP is operating, and typically its length may exceed 100 bytes
 - To reduce medium occupancy and power consumption for both the AP transmitting the beacon and sensor stations receiving it, .11ah uses 2 types of beacons: full and short.
 - Some fields like destination addresses, sequence control, etc. are omitted in short beacons
 - Some field like timestamp, SSID, etc. are shortened.

How is it different from the legacy Wi-Fi?

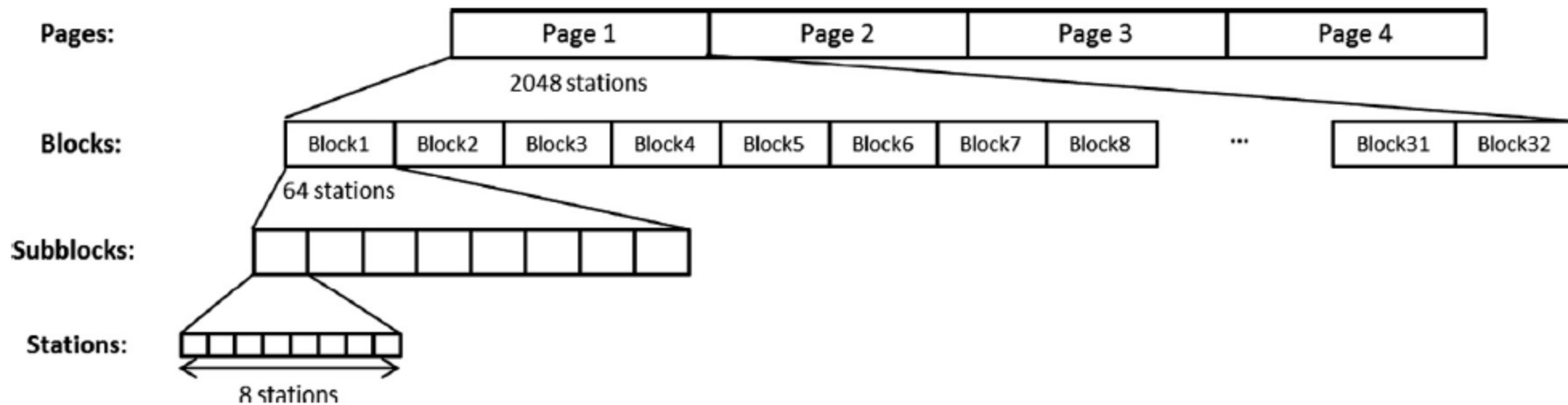
- More number of devices: High Collision Probability!
 - How does .11ah deal with it?
 - .11ah developed Restricted Access Window (RAW) to limit the set of stations accessing the channel and to spread their access attempts over a long period of time.
 - In other words, RAW divides stations into groups and splits the channel into slots. Then it assign each slot to a group. Stations can transmit only in their slots.
- Fast association and authentication
 - How to handle 6000 stations authenticating at the same time?
 - Two ways to solve: Centralized and Distributed Authentication Control
 - Centralized: When AP sends the beacon, it includes a control threshold. The device generates a random value between $[0,1022]$. If this value is less than the threshold, authentication is attempted.
 - Distributed authentication control: Each station generates two values: l and m . l is uniformly distributed at $[0,L]$ where L is the number of whole slots in a beacon interval. m is uniformly distributed at $[0,TI]$ where Tl is the transmission interval initialized to Tl_{min} . The station initiates authentication request in beacon interval m and slot l . If unsuccessful, Tl is increased similar to binary exponential backoff.

How is it different from the legacy Wi-Fi?

- Increased Doze state duration.
 - In legacy Wi-Fi: The value of Max idle period is chosen by the AP and transmitted to stations during their association in a 16-bit field as a number of 1.024 ms time units.
 - .11ah develops 2 solutions modifying Max idle period usage.
 - The first one is the use of two the most significant bits of the Max idle period field as a scaling factor. Values 00, 01, 10, 11 represent scaling factors 1, 10, 1000, 10,000 respectively. This way maximal value of Max idle period is 2500 times greater.
 - The second one allows the AP to set different Max idle period for various stations. Moreover, a station can request specific Max idle period in its association request.
- .11ah defines three modes of BSS operation:
 - Sensor Only BSS,
 - Non-sensor only BSS, containing only non-sensor networks,
 - Mixed mode, when the AP supports both sensors and non-sensors.
 - BSS of various types can be separated spatially or by assigning different channels, limiting the influence of non-sensor stations on the sensor ones.

How is it different from the legacy Wi-Fi?

- What about buffered frames?
 - TIM segmentation mechanism allows to split information transmitted in TIM into several segments and to transmit TIM segments separately.
 - How is this done? Grouping stations with similar characteristics into pages, blocks and subblocks.

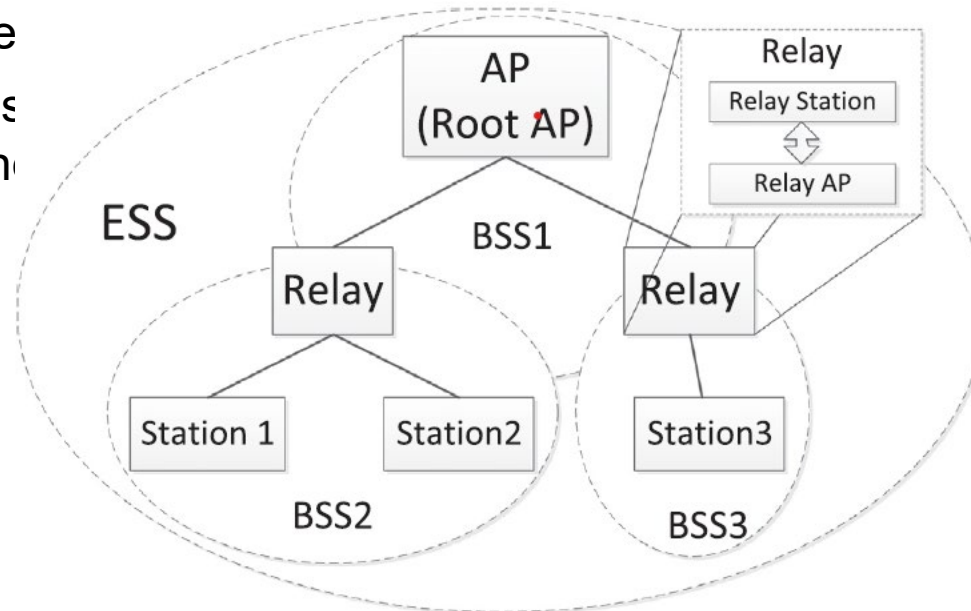


How is this different from legacy Wi-Fi?

- To improve efficiency of data transmission in the use cases IEEE 802.11ah extends a hot-spot Wi-Fi network containing an AP and several non-AP stations with Relays.
 - Relays forward frames between the stations associated with the Relay and the parent AP (called Root AP, as being the root node in the network topology).
 - Relays extend the distance between the Root AP and edge stations and improve reliability of data transmission in scenarios with obstructions.
 - Another benefit of Relays is reducing energy consumed by stations in two ways.
 - Since a station is closer to the Relay than to the Root AP, it can transmit frames (i) at lower power and (ii) at higher data rate making the transmission shorter.

How is this different from legacy Wi-Fi?

- To improve efficiency of data transmission in the use cases IEEE 802.11ah extends a hot-spot Wi-Fi network containing an AP and several non-AP stations with Relays.
 - Relays forward frames between the stations associated with the Relay and the parent AP (called Root AP, as being the root node in the network topology).
 - Relays extend the distance between the Root AP and edge stations and improve reliability of data transmission in scenarios with obstructions.
 - Another benefit of Re
 - Since a station is close power and (ii) at high



in two ways.
smit frames (i) at lower

Summary

- Transmission in legacy 802.11 networks
- Different 802.11 networks and their specifications/features
- How to handle IoT devices?
 - 802.11ah is introduced
 - We specifically saw how 802.11ah handles some problems
 - There are more features that are unexplored in this lecture.
 - Refer to the document below for more information:

Ref: Khorov, Evgeny, Andrey Lyakhov, Alexander Krotov, and Andrey Guschin. "A survey on IEEE 802.11 ah: An enabling networking technology for smart cities." Computer communications 58 (2015): 53-69.

END