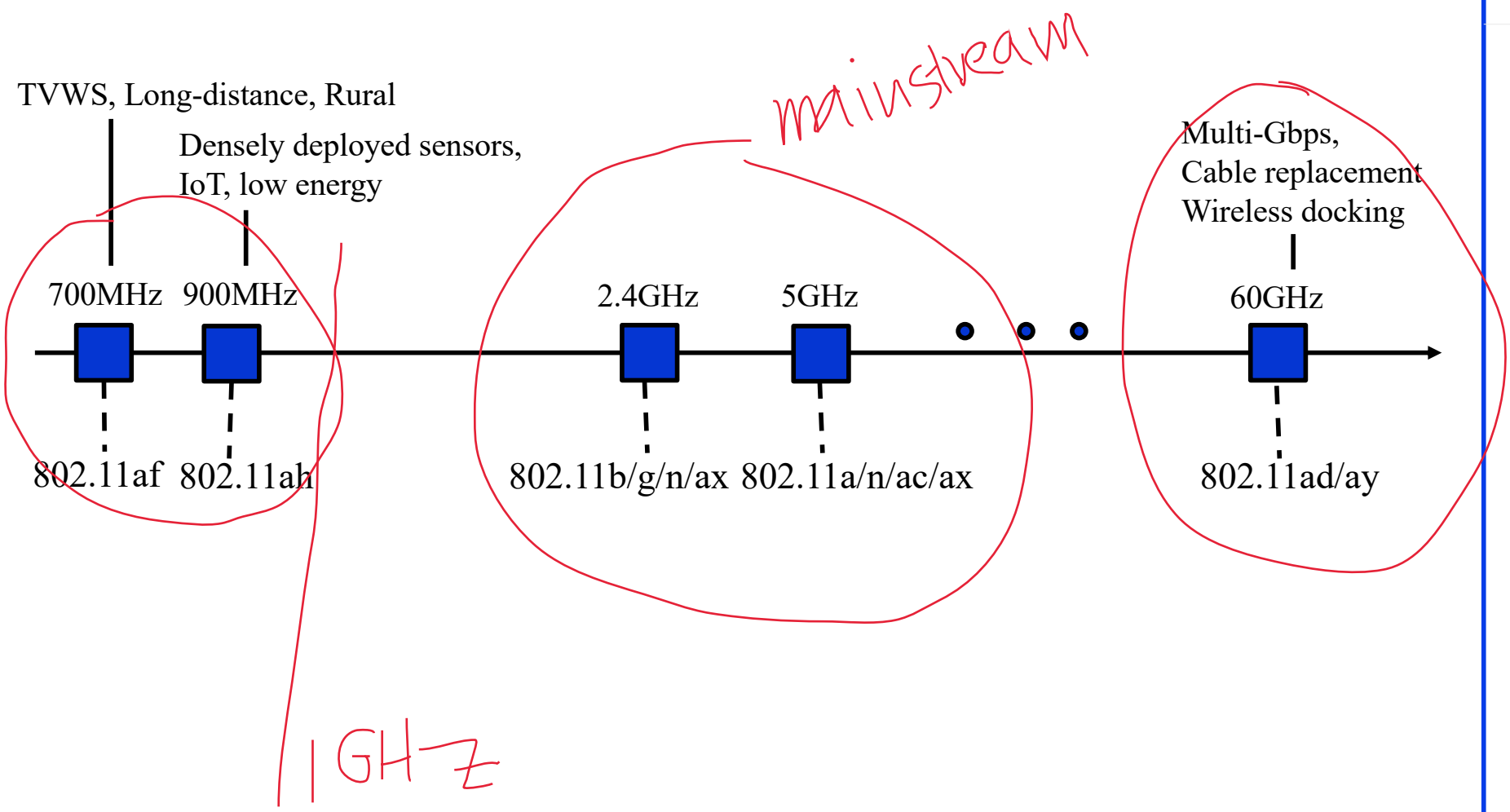
WiFi Part III

IEEE 802.11 for Niche Applications
802.11af/ah/ad/ay

Overview

- IEEE 802.11af
- IEEE 802.11ah
- IEEE 802.11ad
- IEEE 802.11ay

802.11 Standards

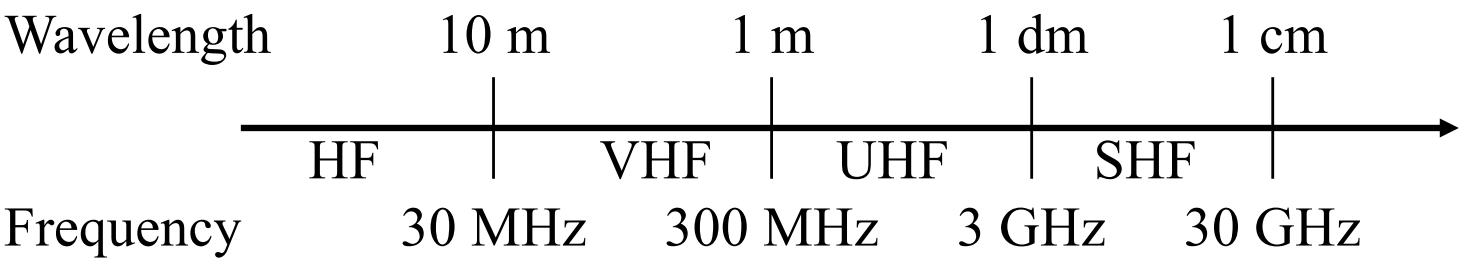


IEEE 802.11af-2014 (a.k.a. White-Fi)

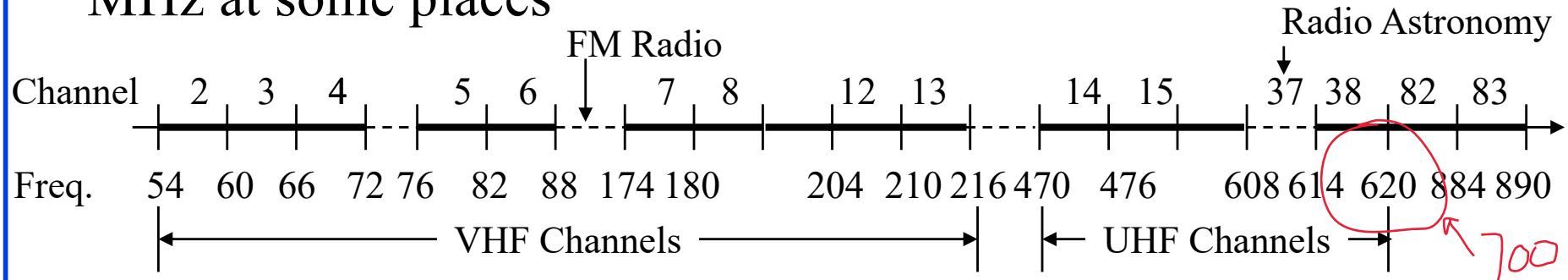
802.11af Overview

1. Television Channels
2. Software Defined Radios
3. Spectral White Spaces
4. FCC Rules for White Spaces
5. Data rates and MCS
6. Whitespace Database and Whitespace Access Protocol

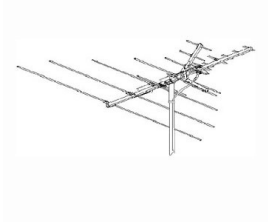
Over-the-Air Television Channels



- Television channels use Very High Frequency (VHF) and Ultra High Frequency (UHF) bands
- Each channel uses 6 MHz in USA, 8 MHz in Europe, and 7 MHz at some places



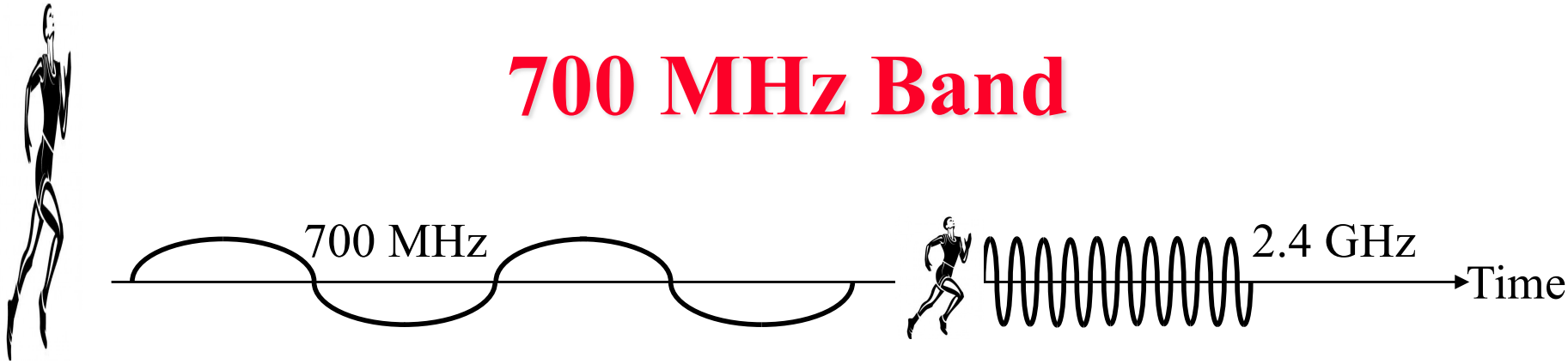
- At least one channel is skipped between two analog stations in neighboring areas to avoid interference



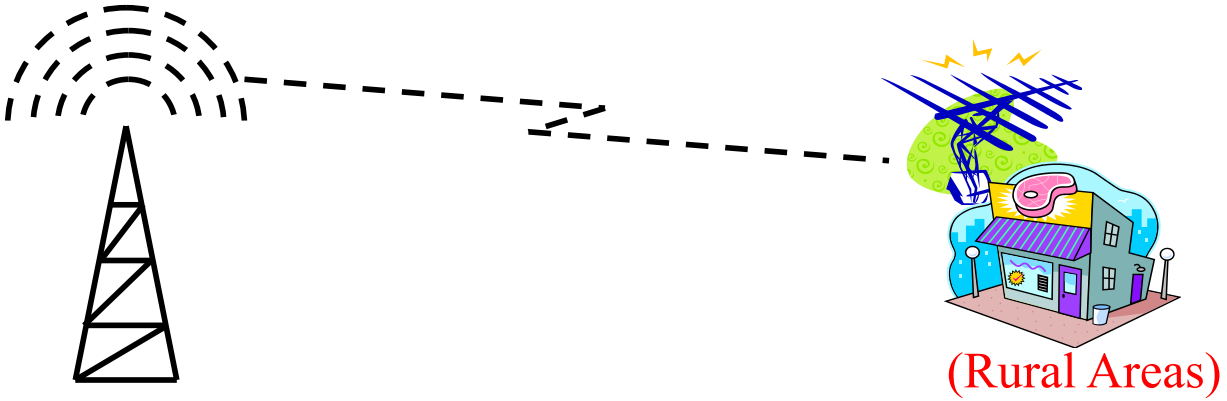
Digital Television

- Converting pixels to bits
  ⇒ Can easily encrypt, multiplex, mix with data
- Change Standard Definition (SD), High Definition (HD)
- Do not need empty channels between neighbors
- Need about 19 Mbps ⇒ Can transmit 6-8 channels in 6-8 MHz.
- US FCC stopped analog transmissions on June 12, 2009
- A lot of TV spectrum became available ⇒ **Digital Dividend**
- Big demand for this "new" spectrum in **700 MHz band**:
  - Cellular, Emergency Services, ISM, everyone wants it
  - Government raised $19.5 billion from auction to cellular companies and saved some for unlicensed use

700 MHz Band



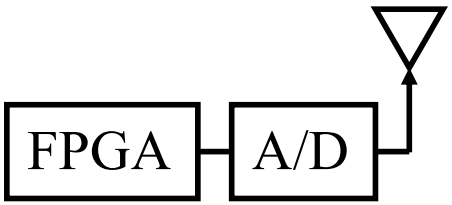
- Lower attenuation (1/7th to 1/9th of 1800/1900/2100 MHz)
  ⇒ Lower transmission power
  ⇒ Longer mobile battery life
- Larger Cell radius ⇒ Smaller number of towers
- Long distance propagation ⇒ Good for rural areas.



Ref: Adam LaMore, "The 700 MHz Band: Recent Developments and Future Plans,"
http://www.cse.wustl.edu/~jain/cse574-08/700mhz.htm

Software Defined Radio

- Analog radio circuits are specific to frequency, channel width, data rate, modulation (AM, FM), multiplexing (FDMA, TDMA, CDMA, OFDMA)
- Need multi-mode radios: Multiband, multi-channel, multi-carrier, multi-mode (AM, FM, CDMA), Multi-rate (samples per second) ⇒ Possible using digital computation
- Generally using Digital Signal Processing (DSP) or field programmable gate arrays (FPGAs)
- Signal is digitized as close to the antenna as possible. Logic reconfigured on demand.
- Software reconfigurable radio
- Flexibility, Upgradability, Lower cost (digital), Lower power consumption.
- **Software Defined Antenna**: Small pixel elements reconfigured by software for desired band.



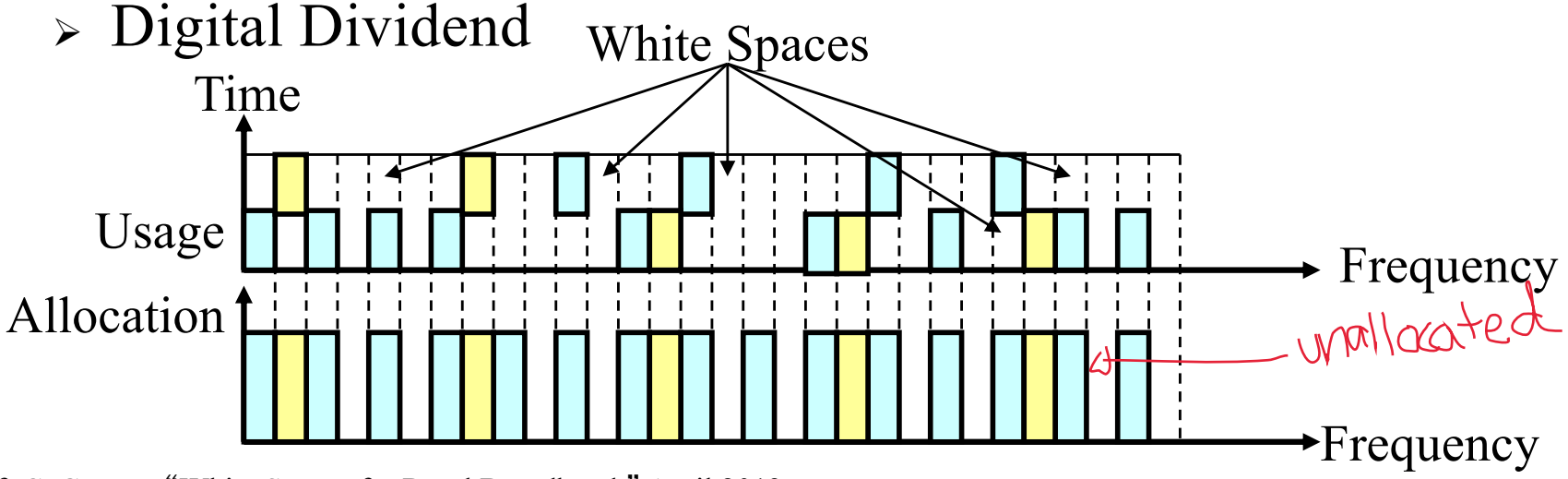
GNU Radio

- Open-source software defined radio toolkit
- Uses Python and C++ on Linux
- Performance critical signal processing in C++
- Universal Software Radio Peripheral (USRP): General purpose computer for SDRs.
  - Host CPU for waveform specific processing, like modulation, demodulation
  - High-Speed operations in Field Programmable Gate Arrays (FPGAs)

Ref: GNU Radio, http://gnuradio.org/redmine/,
http://en.wikipedia.org/wiki/GNU_Radio
http://en.wikipedia.org/wiki/Universal_Software_Radio_Peripheral
Ettus Research, "USRP Bus Series Products," https://www.ettus.com/product/category/

Spectral White Spaces

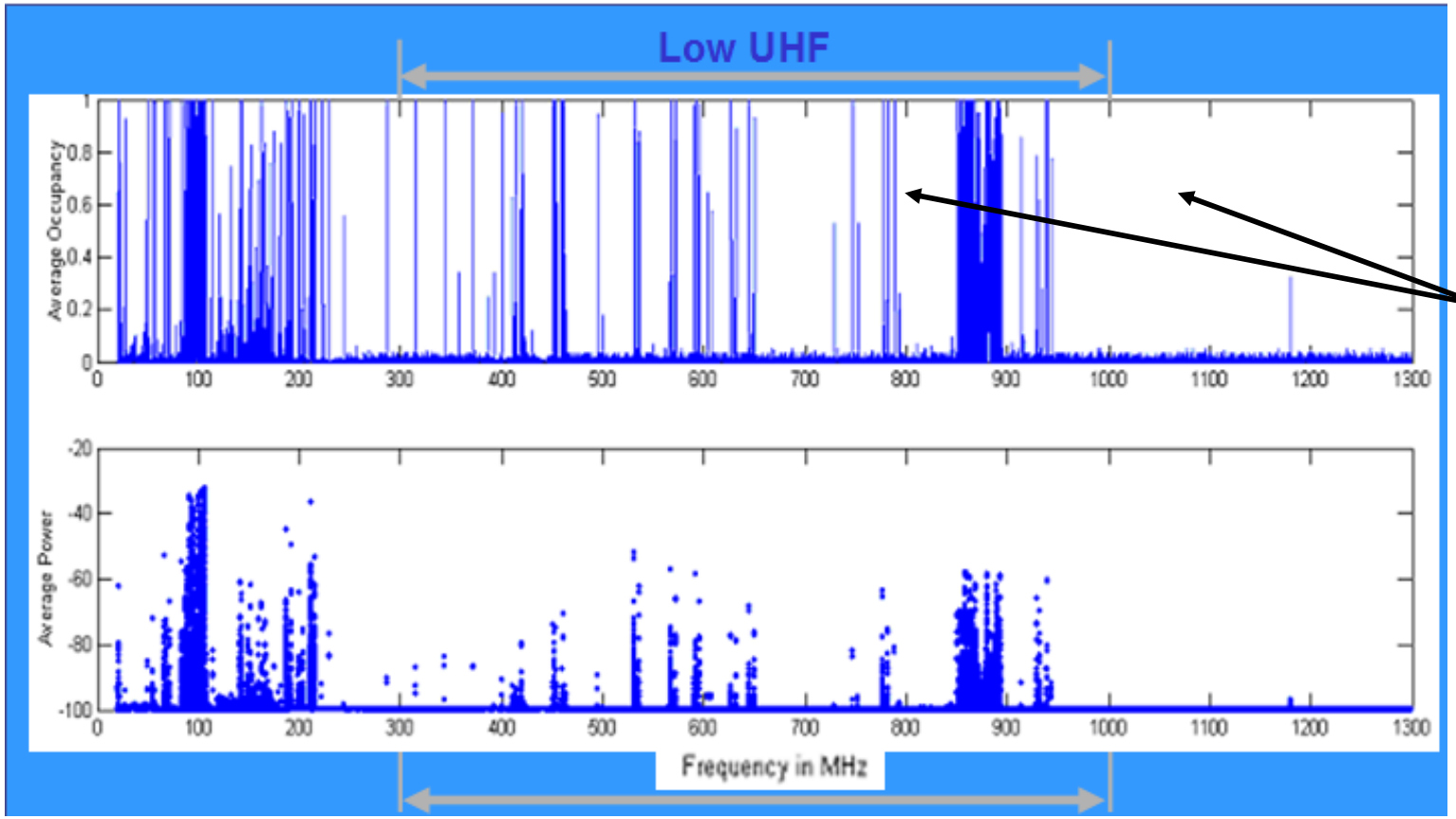
- Any spectrum at a given area at a given time available for use on a non-interfering basis:
  - Unallocated spectrum
  - Allocated but under-utilized
  - Channels not used to avoid interferences in adjacent cells
  - Digital Dividend



Ref: C. Gomez, "White Spaces for Rural Broadband," April 2013, http://www.itu.int/ITU-D/asp/CMS/Events/2013/PacificForum/ITU-APT-S3_Cristian_Gomez.pdf

Spectrum Usage Example

(Test conducted with antenna at a height of 22.1 metres above the ground in the rural sector west of Ottawa, Canada)



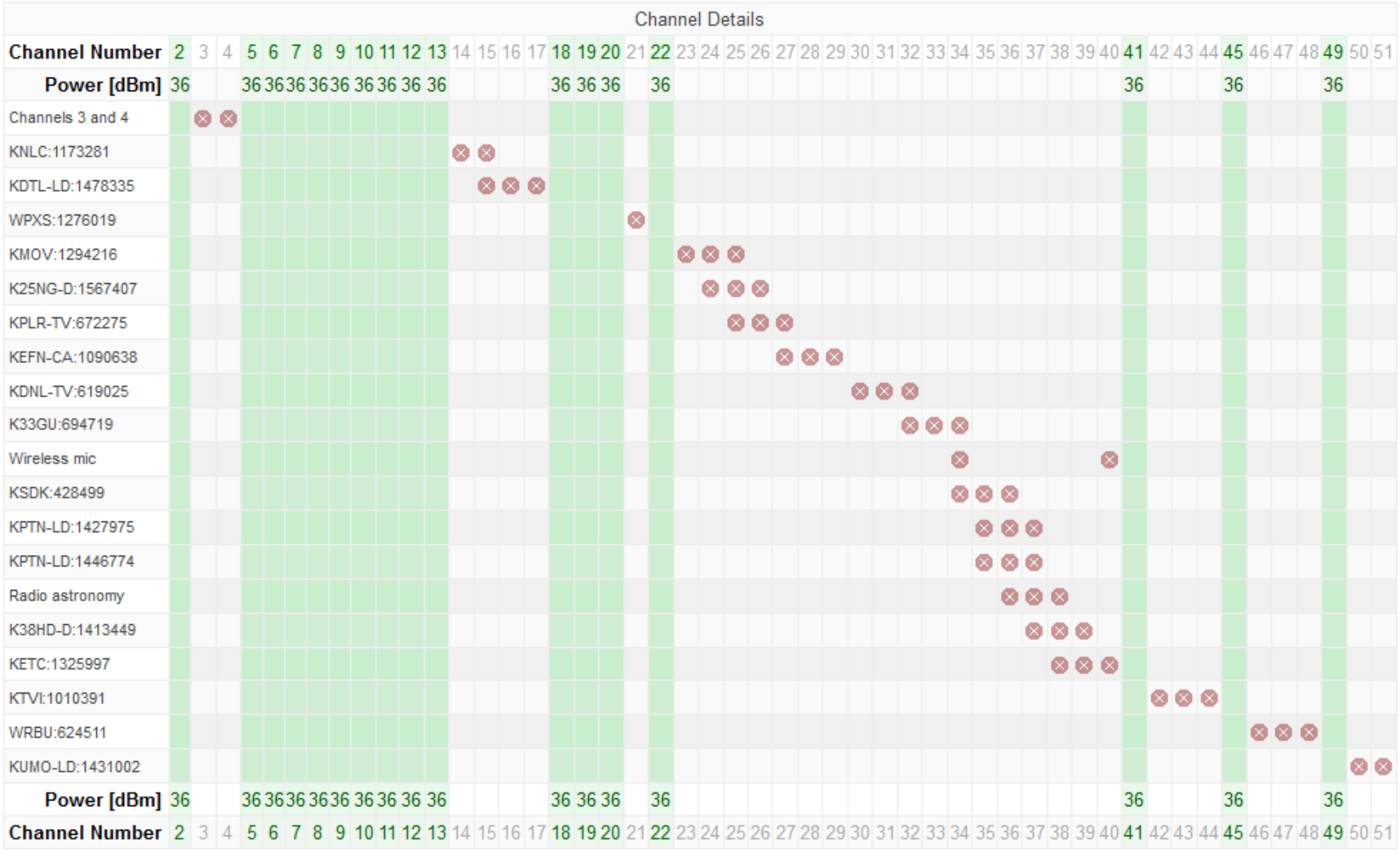
White Spaces

Ref: C. Stevenson, et al., "Tutorial on the P802.22.2 PAR for: *Recommended Practice for the Installation and Deployment of IEEE 802.22 Systems*" http://www.ieee802.org/802_tutorials/06-July/Rec-Practice_802.22_Tutorial.ppt

TVWS Databases

- FCC has authorized 10 companies to administer TVWS databases.
  - Get info from FCC database
  - Register fixed TVWS devices and wireless microphones
  - Synchronize databases with other companies
  - Provide channel availability lists to TVWS devices
- Europe requires devices to check every two hours

White Spaces Near WUSTL, St. Louis, USA

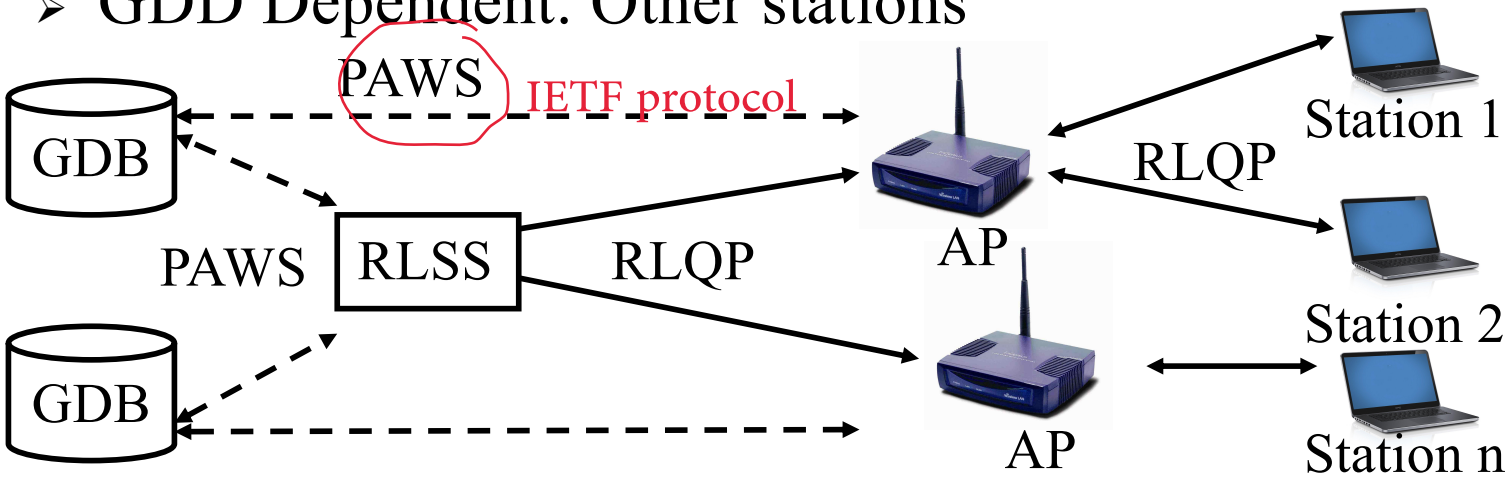


- 17 channels. Zipcode 63130.

Ref: Google Spectrum Database (not available anymore), https://www.google.com/get/spectrumdatabase/channel/

802.11af Database Operation

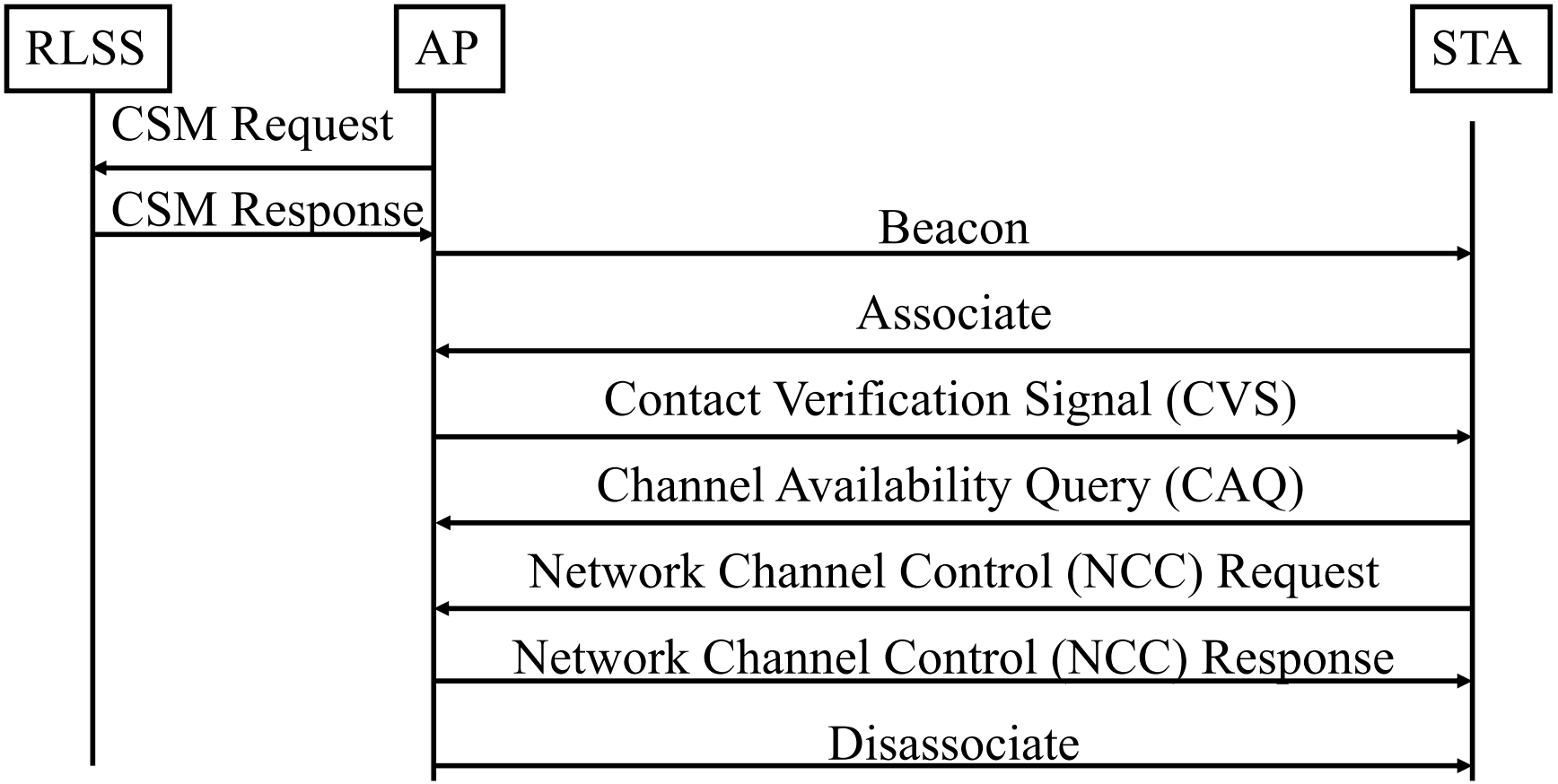
- Geolocation Database (GDB)
- Registered Location Secure Server (RLSS):
  - Provide faster response to access points (APs) locally in a campus.
  - May be Internet Service Provider (ISP) owned.
- Geolocation Database Dependent (GDD) entities:
  - GDD Enabling: Access Point
  - GDD Dependent: Other stations



Ref: A. Flores, et al., "IEEE 802.11af: A Standard for TV White Space Spectrum Sharing," http://networks.rice.edu/papers/FINAL_article_80211af.pdf

Registered Location Query Protocol (RLQP)

- Protocol for exchange of white space map (WSM) among RLSS, APs, and stations, aka, Channel Schedule Management (CSM)

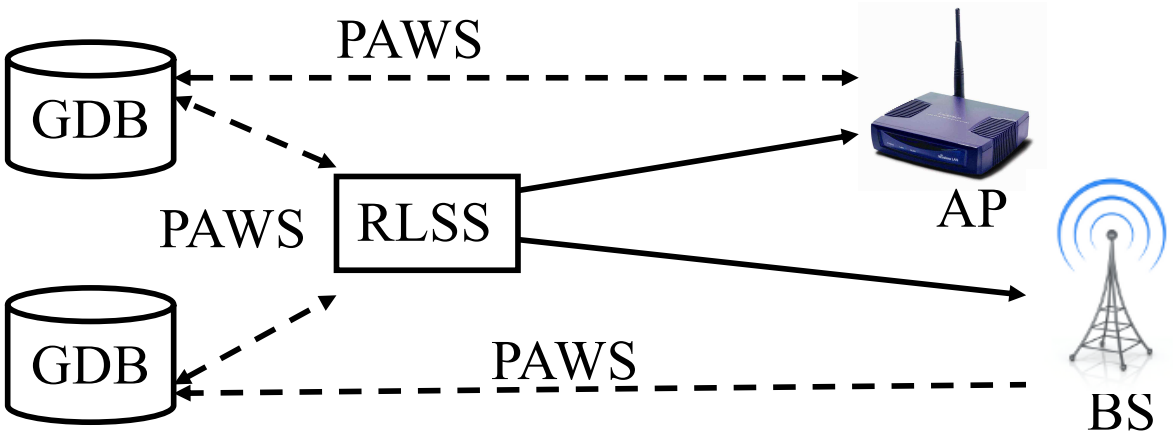


RLQP (Cont)

- CSM Request: APs ask other APs or RLSS about white space map
- APs broadcast beacons on all channels selected.
- Stations associate with the APs.
- Contact Verification Signal (CVS): APs tell their stations white space map and confirm that stations are still associated
- Contact Availability Query (CAQ): Stations ask AP, if they do not receive the map within a timeout interval
- CAQ Response
- Network Channel Control (NCC) Request: Sent by stations to APs requesting use of a channel. AP may forward to RLSS.
- NCC Response: Permission to transmit on requested channel
- Stations may be disassociated by APs if necessary

Protocol to Access White-Space (PAWS)

- IETF working group
- Mechanism to discover white space database
- Protocol to communicate with the database
- Interface Agnostic: 802.11af, 802.15.4m, 802.22, …
- Spectrum agnostic: 6 MHz, 7 MHz, 8 MHz, …
- Master Device: White-Space Device (WSD) connects to database
- Slave Device: WSD that get info from master devices



Ref: V. Chen, et al, ed. "Protocol to access White-Space (PAWS) Databases," Feb 2014, http://datatracker.ietf.org/doc/draft-ietf-paws-protocol/

PAWS (Cont)

- Stations should be able to discover WS Database, its regulatory domain. May be preconfigured similar to DNS or Certification Authorities.
- Listing Server: Web page listing all national database servers. Highly static ⇒ Can be cached by master
- Master may register with the database (model, serial, owner, …) of itself and its slaves
- Mutual authentication and authorization using certificates or passwords
- Master can then query the database
- The database should be able to push updates on channel availability changes
- Ensure security of discovery mechanism, access method, and query/response

Ref: A. Mancuso, Ed., at al, "Protocol to Access White-Space (PQWS) Databases: Use Cases and Requirements," IETF RFC 6953, May 2013, http://tools.ietf.org/pdf/rfc6953

PAWS (Cont)

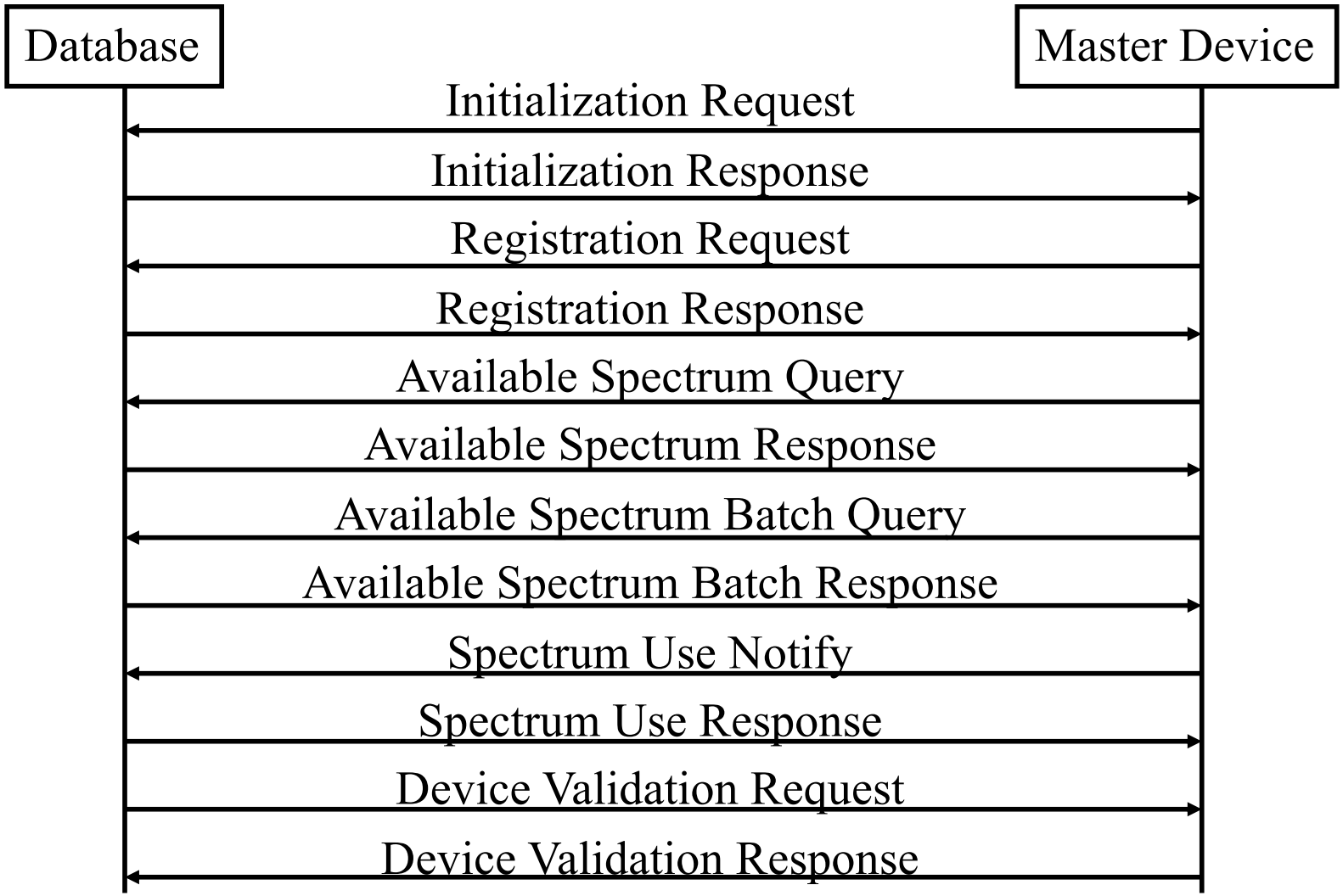
- Allows WSD to specify geolocation, height, serial number, Certificates, device class, radio access technology (RAT), antenna gain, maximum EIRP, radiation pattern, spectrum mask, owner contact information
- Allows database to specify available spectrum, available area, allowed power levels
- Allows WSD to register its selected spectrum for use
- Allows privacy to WSD (encryption)

Ref: V. Chen, et al, ed. "Protocol to access White-Space (PAWS) Databases," Feb 2014, http://datatracker.ietf.org/doc/draft-ietf-paws-protocol/

PAWS Messages (Cont)

- Listing Request/Response: To/from listing server (not shown)
- Initialization: Exchange capability, location, get rules
- Registration: Model, serial, antenna characteristics, owner, etc
- Available Spectrum: individual or batch request
- Spectrum Use: register used spectrum, location, antenna etc. Get time limits in response.
- Device Validation: Database may ask masters to authenticated slaves

PAWS Messages



802.11af-2014: White-Fi

- Basic Channel Unit (BCU): One TV Channel
  W = 6 MHz in USA
- Channel Bonding: Optional
  - Contiguous: 2W, 4W
  - Non-contiguous: W+W, 2W+2W

IEEE 802.11af OFDM Data Rates

- Modulation: 256-QAM highest
- Coding: 5/6 highest
- OFDM similar to 40 MHz in 802.11n down-clocked by 7.5x
- 6MHz channel: 144 total subcarriers, **108 Data**, 3 DC, 6 pilots, 36 Guard
- 7.5x down clocking
  - 0.4µs GI in 802.11n -→ 3µs in 802.11af (0.4x7.5=3)
  - 3.2µs data interval → 3.2x7.5 = 24µs
  - Total symbol interval = 24+3 = 27µs
- Data rate (single stream, single channel): 26.67 Mbps
- Max. Data rate (4 stream,4 channel): 26.67x16 = 426.7 Mbps

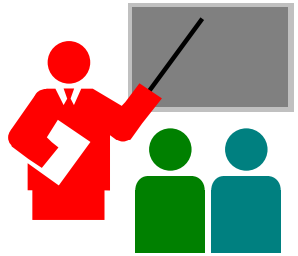
IEEE 802.11af Data Rates in Mbps (Single Stream)

			6 and 7 MHz channels	
MCS Index	Modulation	Rate	6 µs GI	3 µs GI
0	BPSK	2-Jan	1.8	2
1	QPSK	2-Jan	3.6	4
2	QPSK	4-Mar	5.4	6
3	16-QAM	2-Jan	7.2	8
4	16-QAM	4-Mar	10.8	12
5	64-QAM	3-Feb	14.4	16
6	64-QAM	4-Mar	16.2	18
7	64-QAM	6-May	18	20
8	256-QAM	4-Mar	21.6	24
9	256-QAM	6-May	24	26.7

0.8x7.5 = 6

2-jan = ½
4-mar = ¾
3-feb = 2/3
6-may = 5/6

Summary

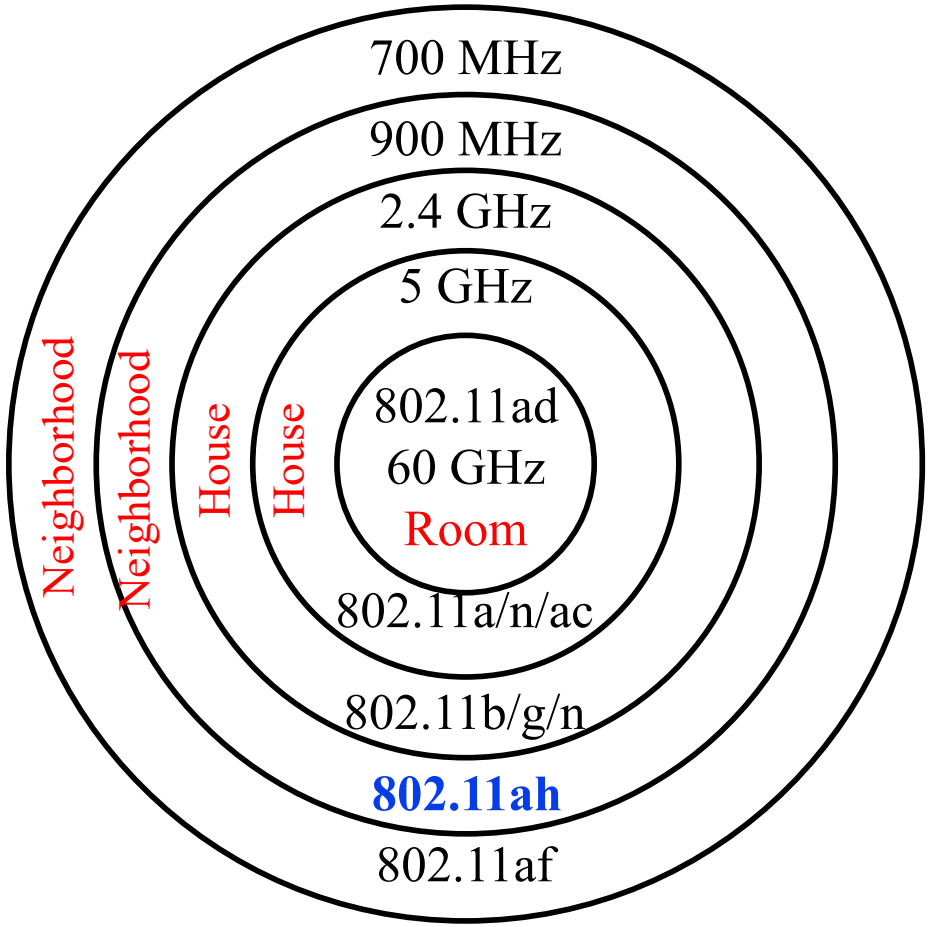


1. Analog to Digital conversion of TV channels has freed up spectrum in 700 MHz band ⇒ White Space.
2. 700MHz allows long-distance communication, useful for rural areas
3. FCC has allowed license-exempt use of some of the white space in TV bands. Requires software defined radio.
4. IEEE 802.11af White-Fi spec achieve up to 426.7 Mbps using OFDM, 4-stream MIMO, 256-QAM@5/6.
5. PAWS is the protocol for accessing white space databases.

IEEE 802.11ah-2017 (a.k.a HaLow)

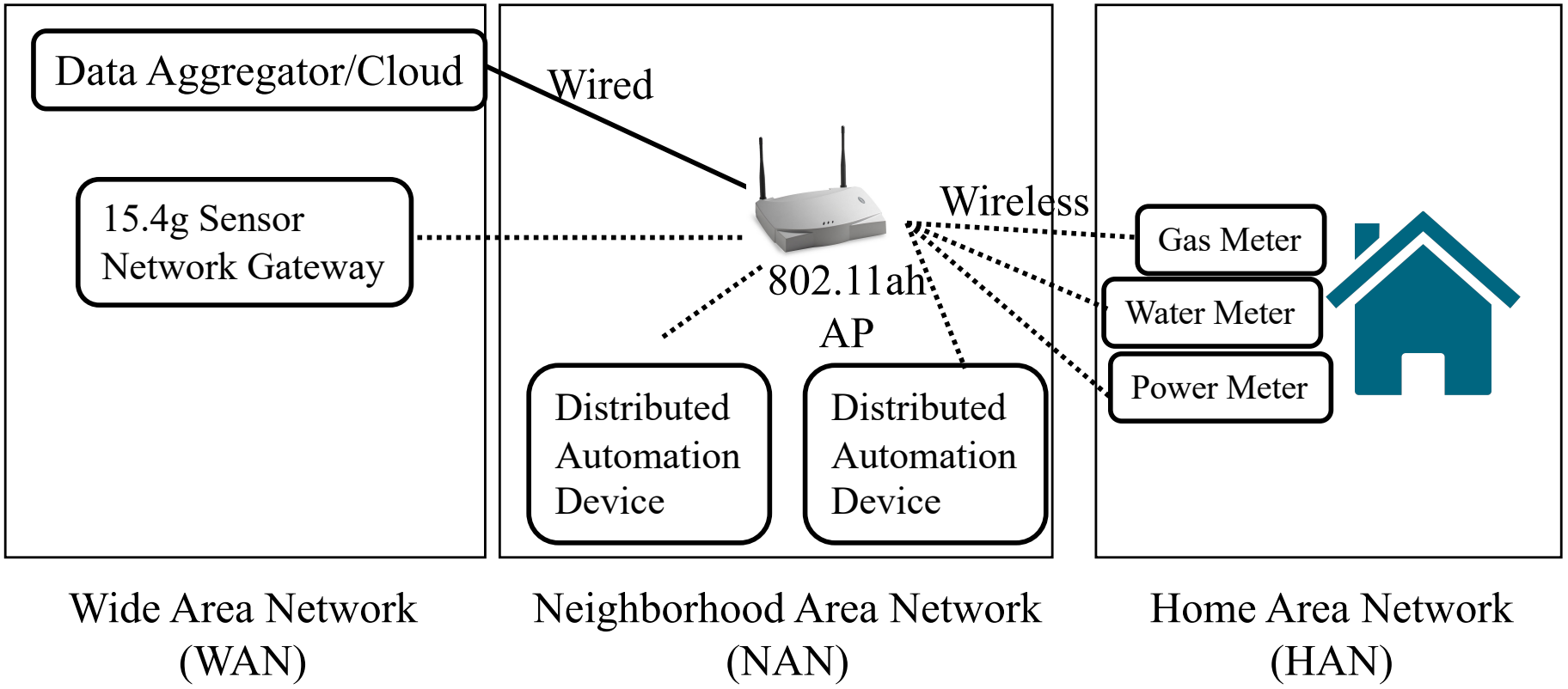
802.11 Standards: Ranges

- 150 kbps to 78 Mbps per spatial stream (up to 4 streams)



Ref: J. DeLisle, "What's the difference between 802.11af and 802.11ah," Microwave and RF, Oct 2015, http://mwrf.com/active-components/what-s-difference-between-ieee-80211af-and-80211ah

Sample Application



Ref: H. Wei, "Self-Organizing Energy Efficient M2M Communications," http://cc.ee.ntu.edu.tw/~ykchen/1123-HWei.pdf

802.11ah PHY

1. 802.11ac PHY **down clocked** by 10X
   - 2/4/8/16 MHz channels in place of 20/40/80/160 MHz in ac
   - 20 MHz 11ac and 2 MHz 11ah both have 64 FFT size and 48 data subcarriers + 4 pilots ⇒ $1/10^{th}$ inter-carrier spacing
     ⇒ 10X longer Symbols ⇒ Allows 10X delay spread
     ⇒ All times (SIFS, ACKs) are 10x longer
   - New 1 MHz PHY with 24 data subcarriers

many IoT devices require small bandwidth

2. **Adjacent channel bonding**: 1MHz+1MHz = 2 MHz
3. All stations have to support 1MHz and 2MHz
4. Up to **4 spatial streams** (compared to 8 in 11ac)
5. 1 MHz also allows a new MCS 10 which is MCS0 with 2x repetition ⇒ Allows 9 times longer reach than 2.4GHz
6. **Beam forming** to create sectors

Ref: W. Sun, M. Choi, and S. Choi, "IEEE 802.11ah: A Long Range 802.11 WLAN at Sub 1 GHz," River Journal, 2013, pp. 1-26, http://riverpublishers.com/journal/journal_articles/RP_Journal_2245-800X_115.pdf

Example

- If we reduce the clock speed of 802.11ac by a factor of 10, what would be the new symbol rate (symbols/s)?

802.11ac has a symbol duration of 3.6 μs (for 400 ns GI).

New symbol duration with a 10x slower clock = 36 μs

New symbol rate = $1/(36 \times 10^{-6}) = 27{,}777$ sym/s

Example

- In USA, 902-928 MHz has been allocated for 802.11ah. How many different channels can be used if 16 MHz channel option is used?

902-928 MHz has a total bandwidth of 26 MHz. There is *only one (non-overlapping)* 16 MHz channel possible out of 26 MHz.

802.11 MAC

- **Large number of devices** per Access Point (AP)
  - Hierarchical Association Identifier (AID)
- **Relays** are used to allow connectivity outside the coverage area. Limited to 2-hops.
- **Power Savings Enhancements**:
  - Allows stations to sleep and save energy.
  - AP negotiates a Target Wake Time (TWT) for individual stations
- **Speed frame exchange** allows stations to exchange a sequence of frames for a TXOP.

Ref: E. Khorov, et al., "A survey on IEEE 802.11ah: An enabling networking technology for smart cities," Computer Communications, 2014, http://dx.doi.org/10.1016/j.comcom.2014.08.008

MAC Protocol Versions

- Protocol Version 0 (PV0) is same as that for b/a/g/n/ac
- Protocol version 1 (PV1) is optimized for IoT
  - Short headers
  - Null Data packets
  - Speed frame exchange
  - Improved channel access

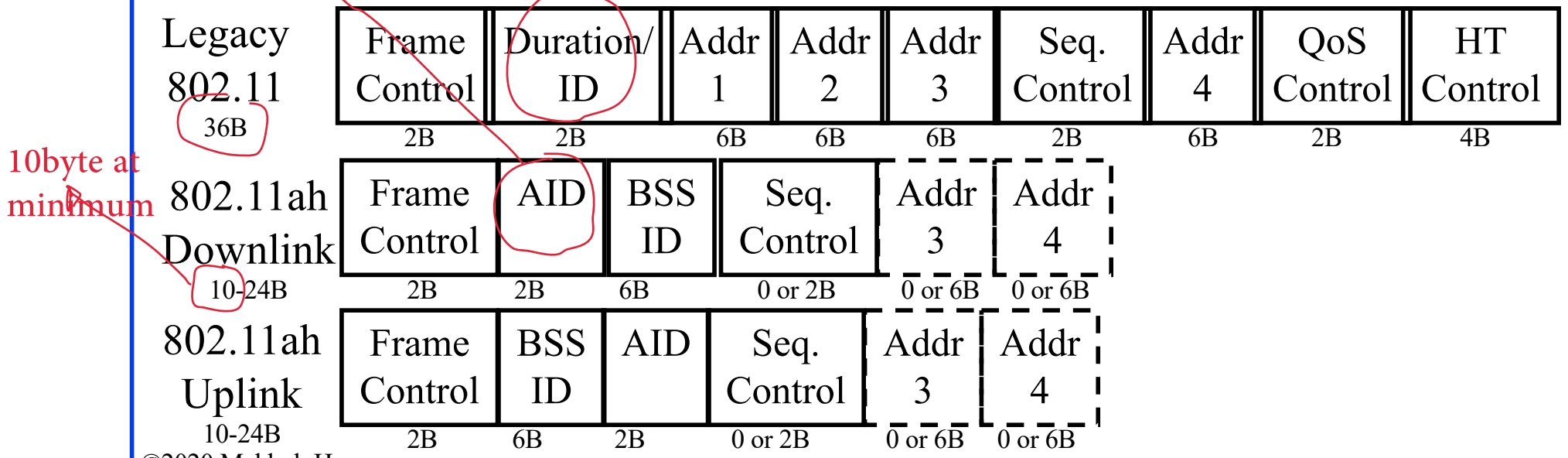
Short MAC Header

- MAC Header shortened by 12-26 Bytes:
  - Removed: High throughput control, QoS, Duration field (No virtual carrier sensing)
  - Optional: 3rd address
  - 2-byte AID in place of some 6-byte addresses
  - Frame Control indicates what protocol version is being used
  - Sequence field indicates if 3rd /4th addresses are present

local addressing

is now gone

10byte at minimum



Example

- A garbage bin sensor uses 802.11ah to upload 10 bytes of bin-fill-level data once every hour. Compared to legacy 802.11 (a/b/g/n/ac), the bin sensor has to upload how many less bytes per day?

Legacy 802.11 MAC header length = 36 byte

Total bytes uploaded with legacy 802.11 = 24x(10+36) = 1104 bytes/day

Total bytes uploaded with 802.11ah = 24x(10+10) = 480 bytes/day (min)

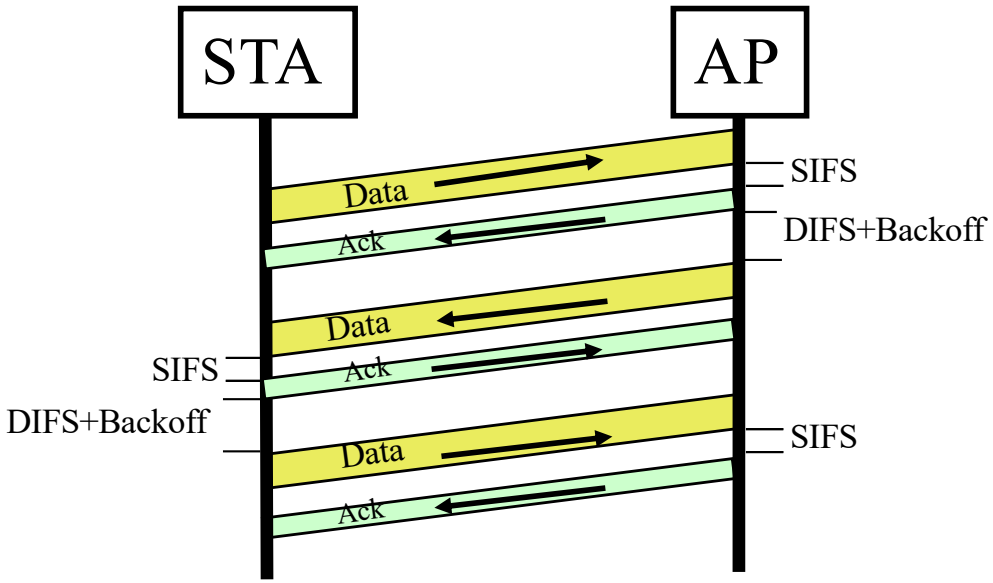
1104 - 480 = 624 less bytes per day

Null Data Packet (NDP)

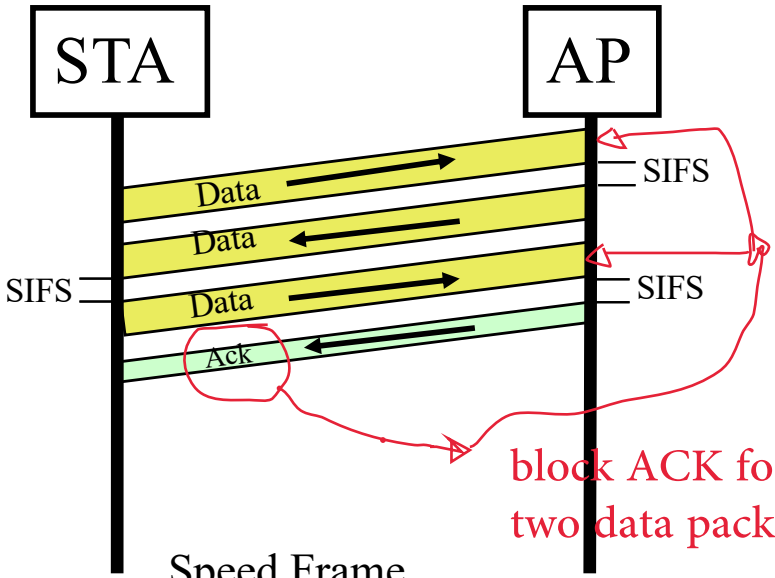
- RTS/CTS/ACK has no data, but consumes too much MAC overhead
- 802.11ah removes the entire MAC header for these packets and identifies these packets via the *modulation and coding* (MCS) scheme at the PHY
- ACK, Block ACK, CTS, etc, all use different MCS

Speed Frame Exchange

- Also called "**Bi Directional Transmit** (BDT)"
- Initiator sends a frame with response indicator set to "long response"
  - Receiver can send data instead of ACK within a SIFS
  - Frames are sent until there are no more frames; block ACK at end



Legacy 802.11



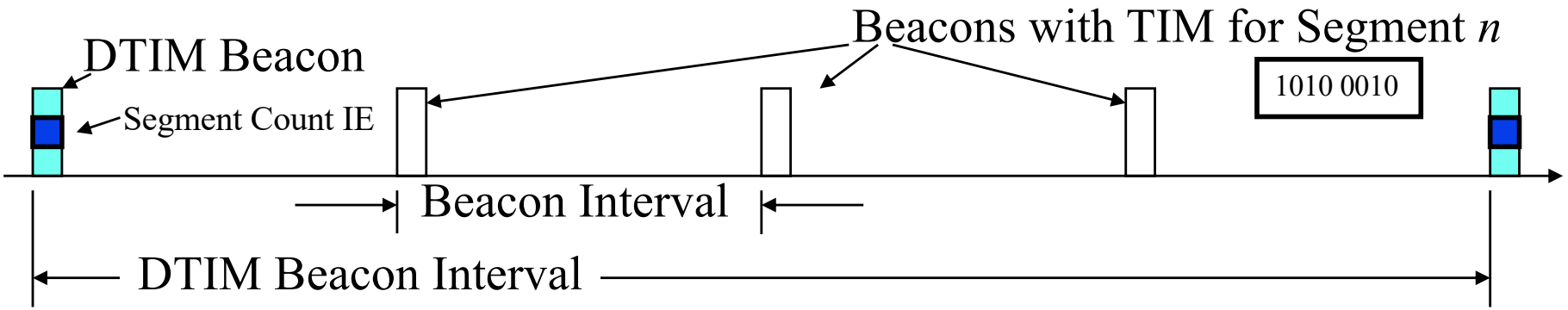
Speed Frame Exchange in 802.11ah

Types of Stations

- **High-Traffic**: Listens to Traffic Indication Map (TIM) in beacons and transmit accordingly within a restricted access window ⇒ *TIM Stations*
  - *Remain awake all the time to monitor all beacons*
- **Periodic Low-Traffic**: Negotiate a transmission time allocated in a periodic restricted access windows. Do not listen to beacons ⇒ *Non-TIM Stations*
- **Very Low-Traffic**: Send a poll to AP and get a transmission opportunity in response ⇒ *Unscheduled Stations*

Page Segmentation

- Announcing all buffered frames in each beacon
  $\Rightarrow$ 8096 bits would be wasted per beacon interval
- AP segments the TIM stations in segments and announces only one segment at a time.
- Every Delivery TIM (DTIM) interval, AP announces which segments have pending data and downlink, uplink periods.



Channel Access for TIM

- Each station knows what segments they belong to.
- Stations wake up every "*DTIM*" interval and find out which beacon they should listen to. The beacon has detailed map indicating which station has pending traffic and when stations can contend for access
- If the map indicates, AP has buffered packets for a station, the station uses DCF (distributed coordination function) to send a PS-poll to get the packet
- If a station has a packet to send, it listens to the map and uses DCF to send RTS in the allocated slot (two or more stations may be allocated to the same slot → collision is possible)
- Small number of stations per slot reduces chances of collisions
- Under low load, it becomes TDMA

Response Indication Deferral (RID)

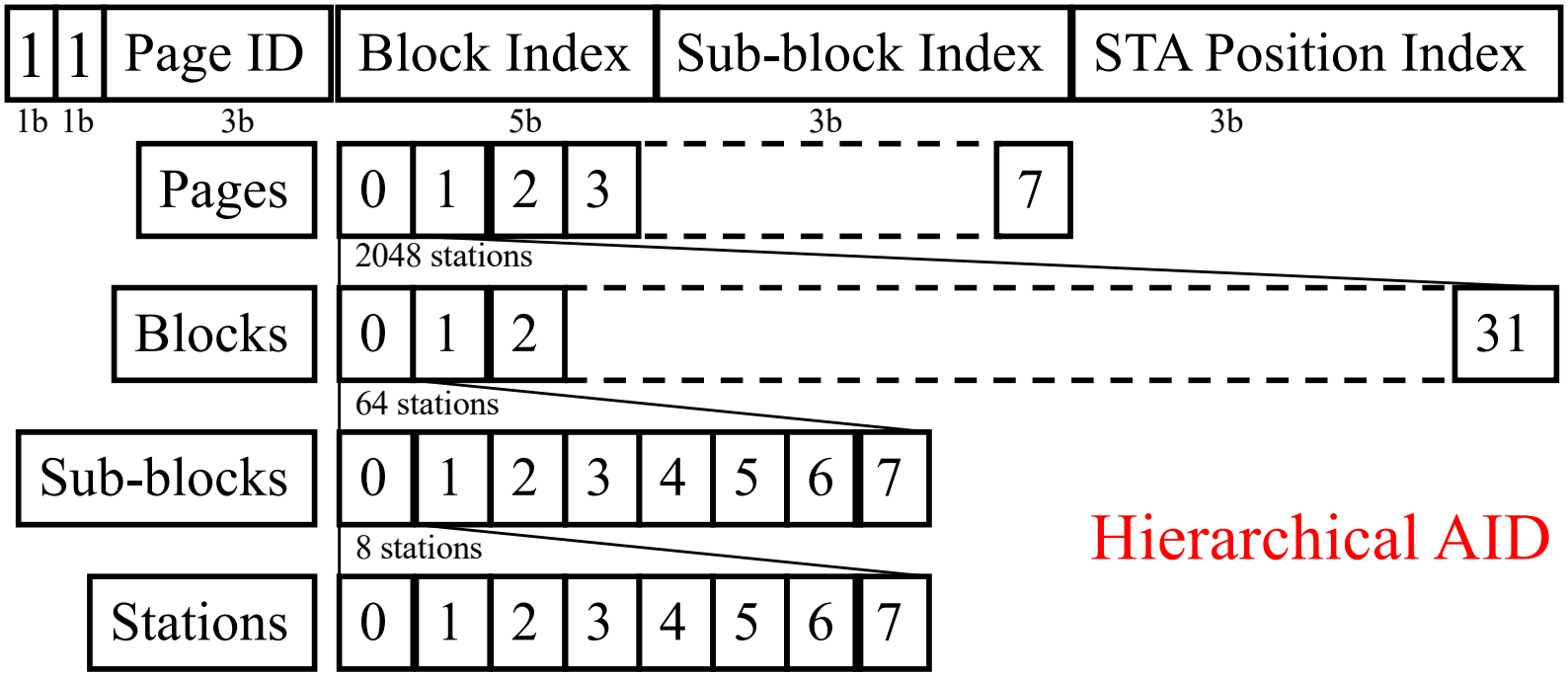
- New virtual carrier sense mechanism replacing NAV (Network Allocation Vector)
- Can not use NAV since there is no duration field
- RID is also a time count down mechanism similar to NAV
  - NAV is MAC-based, RID is PHY-based
- RID is set after reception of PHY header
  NAV is set after reception of complete MAC frame
- RID is set based on the 2-bit response indication field in the PHY header (2 bits → 4 combinations)
  - Normal Response: RID ← SIFS + Ack or Block Ack time
  - NDP Response: RID ← SIFS + NDP Frame time
  - No Response (Broadcast frames): RID ← 0
  - Long Response: RID ← SIFS + Longest transmission time
    (Used with Speed Frame Exchange)

Power Enhancements

- Page Segmentation
- Restricted Access Window
- Target Wake Time

Association Identifier

- 802.11 b/g/n/ac use 11-bit identifier ⇒ 2007 stations
  - 2000+ bits required in "Traffic Indication Map (TIM)"
- 802.11ah uses 16-bit identifier ⇒ 8X stations
  - 8 pages of ~2^{11} stations each. Actually 2007 stations.
    Currently only page 0 is allowed. Page 1-7 are reserved.
    First 2 bits should be 11 to distinguish AID from duration and others.



Restricted Access Window (RAW)

- Allows a set of slot to be restricted to a group of stations (pages/blocks/subblocks)
  ⇒ Reduces contention
- A TIM station can be allocated slots during restricted access window (RAW) to transmit/receive packets
- RAW is a part of "Contention Free Period"
- Access may granted for transmission, reception, polling, etc for one or a group of stations
- A RAW schedule is transmitted at the beginning of RAW interval
- A station can tell AP that it has a frame to transmit using a Uplink Data Indication (UDI) bit
  - Helps AP to workout which stations need access in the next round
- Dividing stations into groups and dividing time into slots for each group increases the efficiency under heavy load.
  - At 100% load: RAW gives close to 100%. Regular EDCF gives 0%.

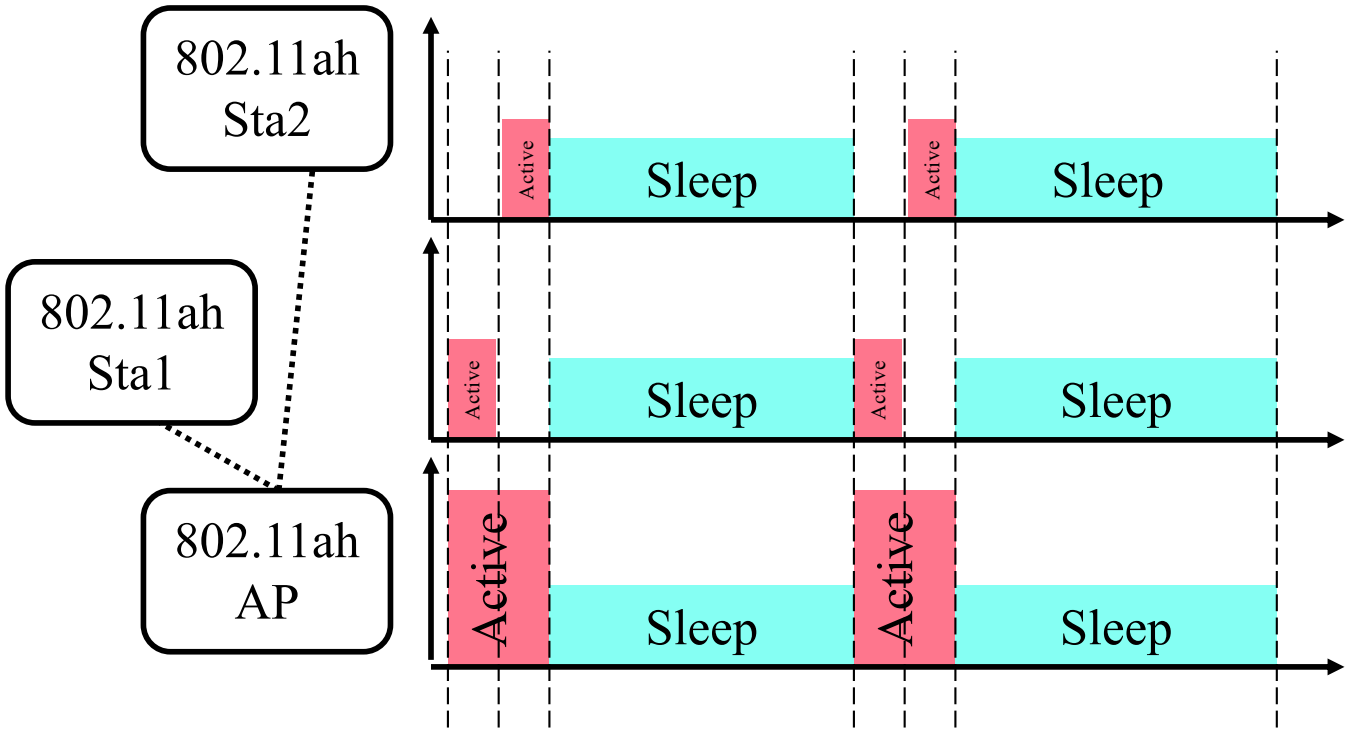
because of high collision and backoff

Other RAWs

- **Periodic RAW**: Period and duration of PRAW are announced by AP for *periodic* stations
- **Sounding RAW**: used for sector sounding
- **AP Power Management RAW**: used by AP to announce the time when it will be sleeping
- **Non-TIM RAW**: Protects transmission of non-TIM stations
  - Prevents TIM stations from hogging the channel
- **Triggering Frame RAW**: Used to allow stations to send PS-poll frames indicating their need to transmit

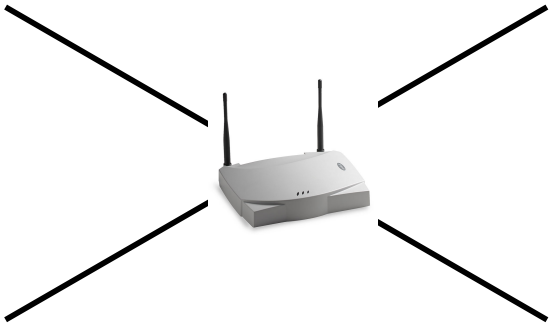
Target Wake Time (TWT)

- Non-TIM stations may sleep for a long time → waste for AP to include their buffer information in every beacon
- Non-TIM stations can provide a Target Wake Time (TWT), so the AP does not worry about these stations during their long sleeps
- Because sleeps can be very long, it is difficult to precisely provide waking tie in ms and sec. -→ three parameters: Target-Wake-Time, Minimum-Wake-Duration, and Wake Interval mantissa.
- AP sends a "Null Data Packet (NDP)" to a station at its target wake up time containing buffering status. A station can then send a PS-poll and get its frames.
- AP can also sleep if all stations are sleeping



Sectorization

- AP can divide the space in sectors
  Each station is told which sector it belongs to.
- Beacon announces which sectors can transmit in this sector interval
- Some sector intervals may be for omni-directional transmissions
  Some may be for only some sectors
- Allows spatial reuse and increase throughput



802.11ah: Summary

1. 802.11ah runs at 900 MHz band ⇒ Longer distance
2. 802.11ah is 802.11ac down by 10x.
   It uses OFDM with 1/2/4/8/16 MHz channels.
   Longer symbols ⇒ Can handle longer multi-path
3. MAC is more efficient by reducing header, aggregating acks, null data packets, speed frame exchanges → good for short M2M communications
4. Saves energy by allowing stations and AP to sleep longer using Target Wakeup Time, Restricted Access Window

Wireless LAN III

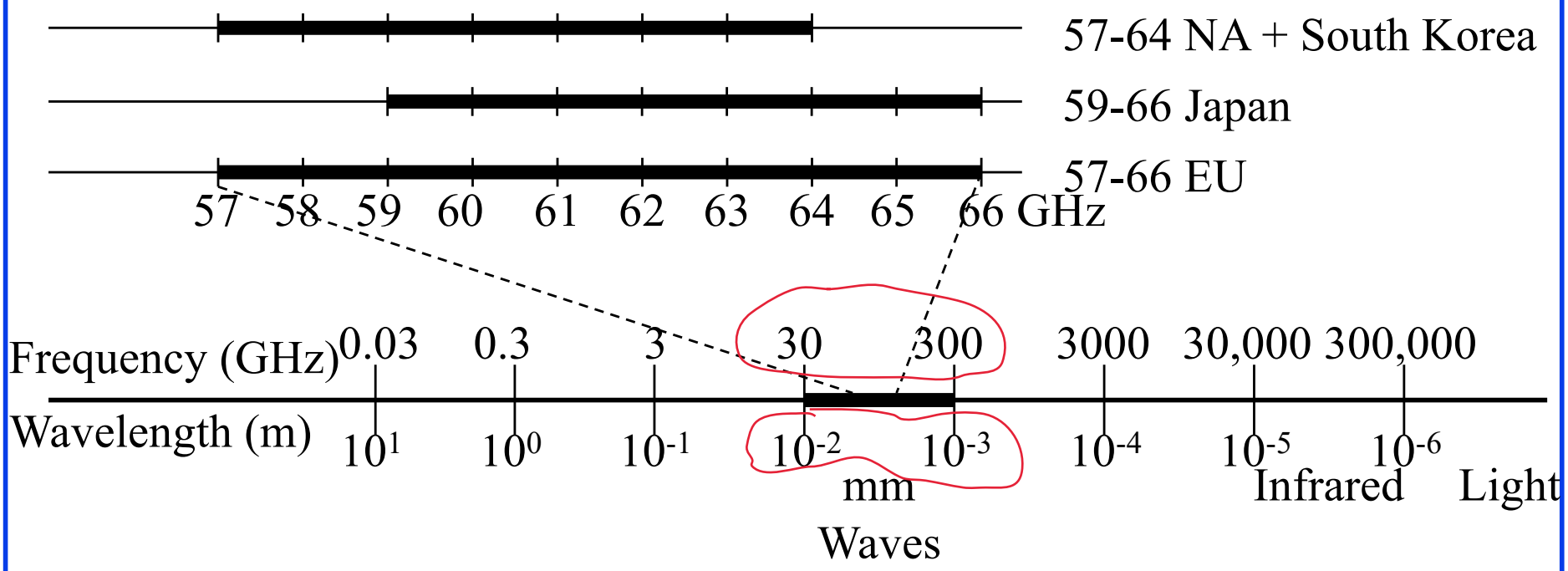
IEEE 802.11ad-2012 (a.k.a WiGig)
60 GHz WLAN

Overview

1. 60 GHz Frequency Allocations and characteristics
2. IEEE 802.11ad
   - PHY data rates
   - Network topology and MAC
   - Beamforming
   - Spatial Frequency Sharing

60 GHz Frequency Allocations

- 7-9 GHz in 57-66 GHz (**millimeter** waves 30GHz-300GHz)
- 4 Channels of ~ 2 GHz
- Significant activity after FCC made 57-64 GHz license-exempt



Ref: FCC, "Part 15 Rules for Unlicensed Operation in the 57-64 GHz Band," FCC13-112, August 2013, http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-13-112A1.pdf

Advantages of 60 GHz Band

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

Disadvantages of 60 GHz Band

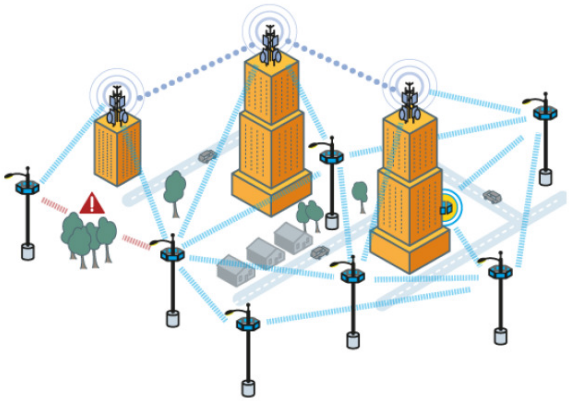
1. **Large Attenuation**: Attenuation / frequency^2
   - Strong absorption by Oxygen
   - Need larger transmit power
   - Need high antenna gain ⇒ directional antennas
   - Short Distance ~ 10m

focusing all energy to one direction

2. **Directional Deafness**: Can't hear unless aligned
   - Carrier sense not possible
   - RTS/CTS does not work
   - Multicast Difficult
3. **Easily Blocked**: By a human/dog
   Need a relay

Multi-Gigabit Wireless Applications

- **Cable Replacement**: High-Definition Uncompressed streaming video
- Interactive **gaming**
- High-speed file transfer
- Wireless Mesh **Backhaul** (200-400m)



802.11ad OFDM PHY

- Total 355 subcarriers at inter-carrier spacing of 5.15626MHz
  ➔ 1830.47MHz channel bandwidth
- 336 data subcarriers (16 pilots, 3 DC)
- Guard interval = ¼ of the data symbol interval
  - GI = 1/5 of the total symbol interval = data interval+GI
- Symbol interval = ~242ns (=336/1386)
- Guard interval = ~48.4ns
- Modulation: QPSK, 16-QAM, 64-QAM
- Coding rates: ½, ¾, 5/8, 13/16
- Only single stream allowed

802.11ad OFDM Data Rates (Mbps)

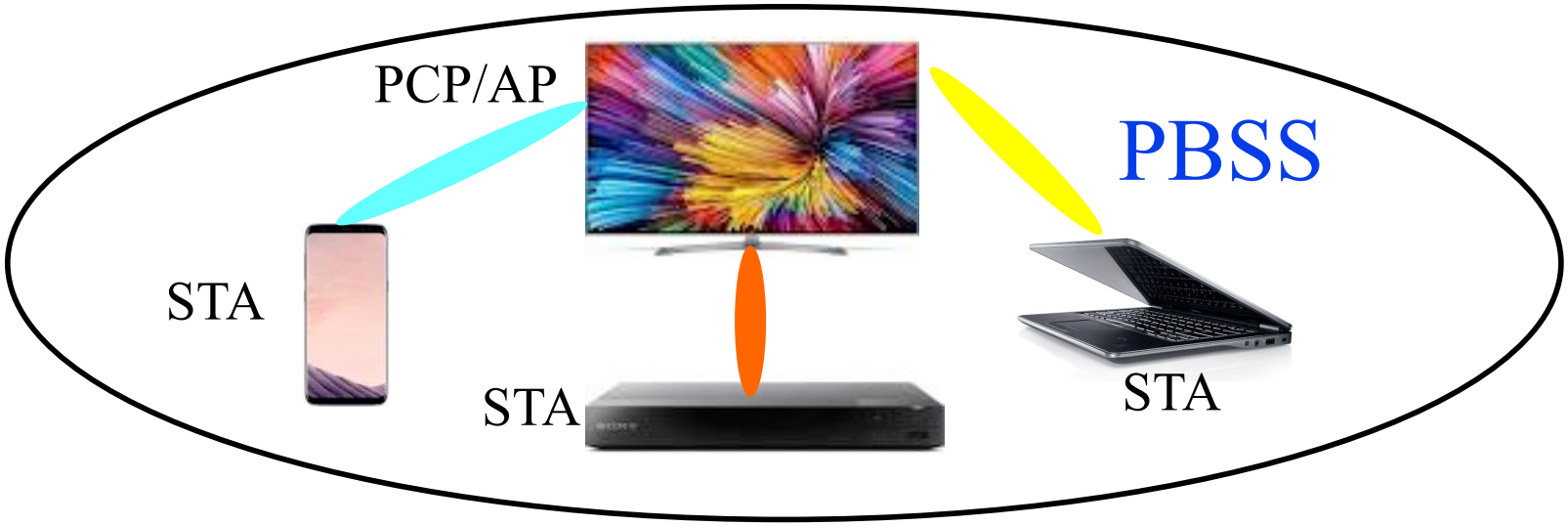
MCS.	Modulation	Coding	Data Rate
13	SQPSK	1/2	693.00
14	SQPSK	5/8	866.25
15	QPSK	1/2	1386.00
16	QPSK	5/8	1732.50
17	QPSK	3/4	2079.00
18	16-QAM	1/2	2772.00
19	16-QAM	5/8	3465.00
20	16-QAM	3/4	4158.00
21	16-QAM	13/16	4504.50
22	64-QAM	5/8	5197.50
23	64-QAM	3/4	6237.00
24	64-QAM	13/16	6756.75

MAC Challenges for 60 GHz

- High path loss at 60 GHz
  - 28 dB higher than 2.4 GHz WLAN, 22 dB higher than 5 GHz WLAN
- Stations must have high antenna gain to overcome high path loss → directional antenna/beamforming
  - The narrower the beam, the higher the antenna gains
- Directional communication complicates MAC design
  - AP can talk to a STA only if their beams point to each other
  - Similarly, two STAs must point their beams to each other before they can exchange data
- MAC must always facilitate all stations to find the right beam directions
  - Different beam directions for different destinations
  - Beam directions change with mobility
  - Becomes challenging with many stations in a network

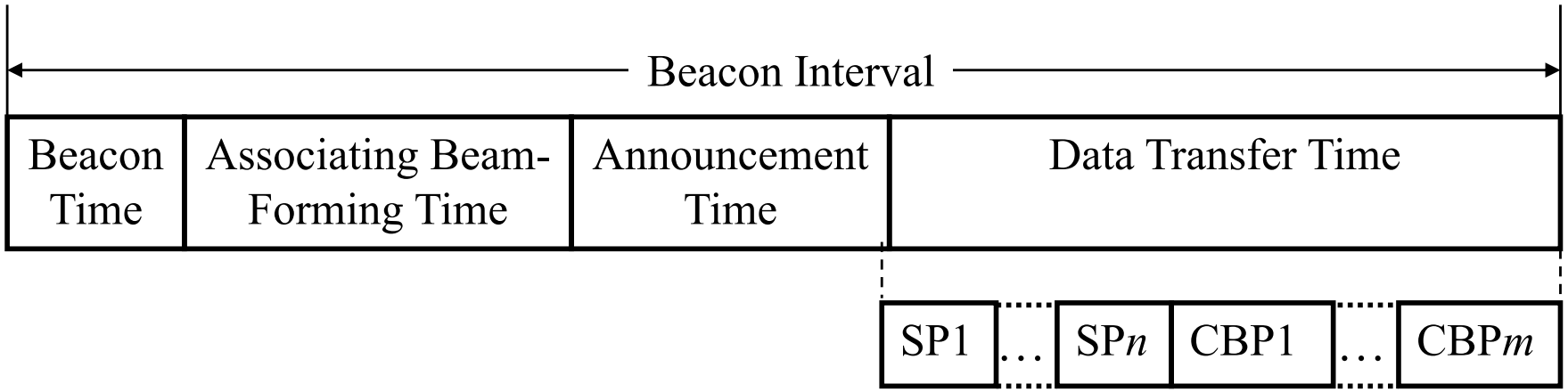
IEEE 802.11ad Network Topology

- **Personal Basic Service Set (PBSS):**
  Group of stations that communicate
- **PBSS Central Point (PCP)** provides scheduling and timing using beacons
  - Dedicated AP not needed, PCP function can be assumed by any 802.11ad device, such as a TV in the room can be PCP/AP
- **1 PCP/AP per PBSS, 1-254 non-PCP stations (STA)**



802.11ad MAC – Beacon Interval

- Each super-frame called "**Beacon Interval**" is divided into 4 *access periods*: Beacon Time (**BT**), Associating Beamforming Training (**A-BFT**), Announcement Time (**AT**), and Data Transfer Time (**DTT**)

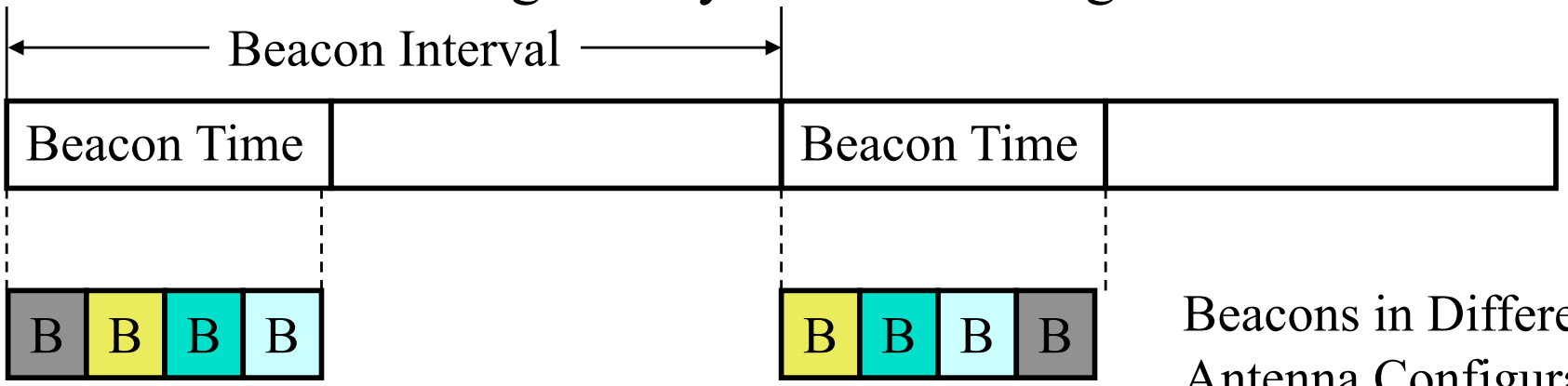


Access Periods in 802.11ad Beacon Interval

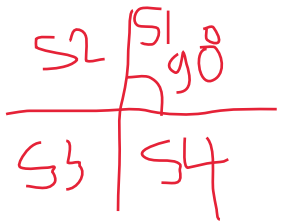
- BT: Only PCP can send a beacon during beacon time; PCP starts beamforming training in BT by sending training frames; STAs cannot transmit
- A-BFT: PCP performs antenna training with its members (STAs)
- AT: PCP polls members and receives non-data responses (STAs can request *service periods or SPs* to be scheduled during DTT)
- DTT: STA-to-STA exchange happens. All stations exchange data frames in a dedicated **service period (SP)** or by **contention in contention-based period (CBP)**
  - CBP uses Distributed Coordination Function (DCF); SP uses Hybrid Coordination Function (HCF)

IEEE 802.11ad Beacon

- Beacon transmissions are omni-directional ⇒ One beacon is transmitted through every antenna configuration/sectors



Example 1



- A 802.11ad PCP/AP has a four-sector antenna with every sector covering 90 degrees. During a Beacon Time (BT), how many beacons the AP should transmit?

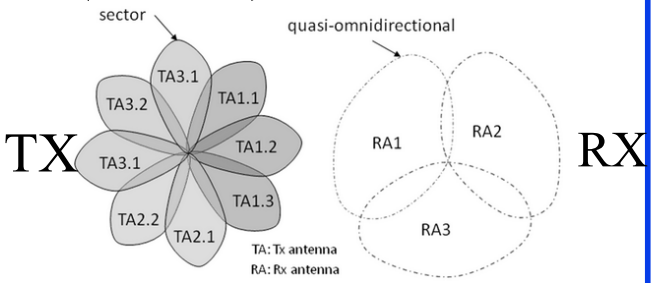
Beacons must be transmitted in omni-direction, so all STAs receive it. 360 degree coverage is achieved by four sectors (each sector covers 90 degrees). The AP therefore will send four beacons, one per sector.

Beamforming Options

- The goal of beamforming is to choose the best beam direction pair that gives the highest gain
- Exhaustive search: exhaustively examine all beam pairs
  - E.g., 64 pairs for 8x8, 1024 pairs for 32x32 → O(B1xB2)
  - Time and energy consuming

# of sectors in device 1

#of sectors on device 2



- Searching with omni-directional antenna
  - Transmitter transmits on all beam directions (B1 transmissions)
  - Receiver uses omni-directional antenna to record RSS for all beam directions of the transmitter
  - Receiver selects the highest RSS as the best beam for the transmitter
  - The pair takes turn to find each others best beam direction (B2 transmissions) → O(B1+B2)

Example 2

- Two 802.11ad devices, STA1 and STA2, want to beamform. STA1 has 32 different antenna configurations (i.e., capable of steering the beam to 32 different directions). STA2 has only 4 beam directions. For Exhaustive Search, how many training frames are transmitted in total by these two devices before they discover the optimum beam pairs for communication?

Total combinations of antenna configurations between the two stations is 32x4 = 128. Therefore, 128 training frames are transmitted, one per specific pair of antenna configurations, before the best combination (pair) is finally selected.

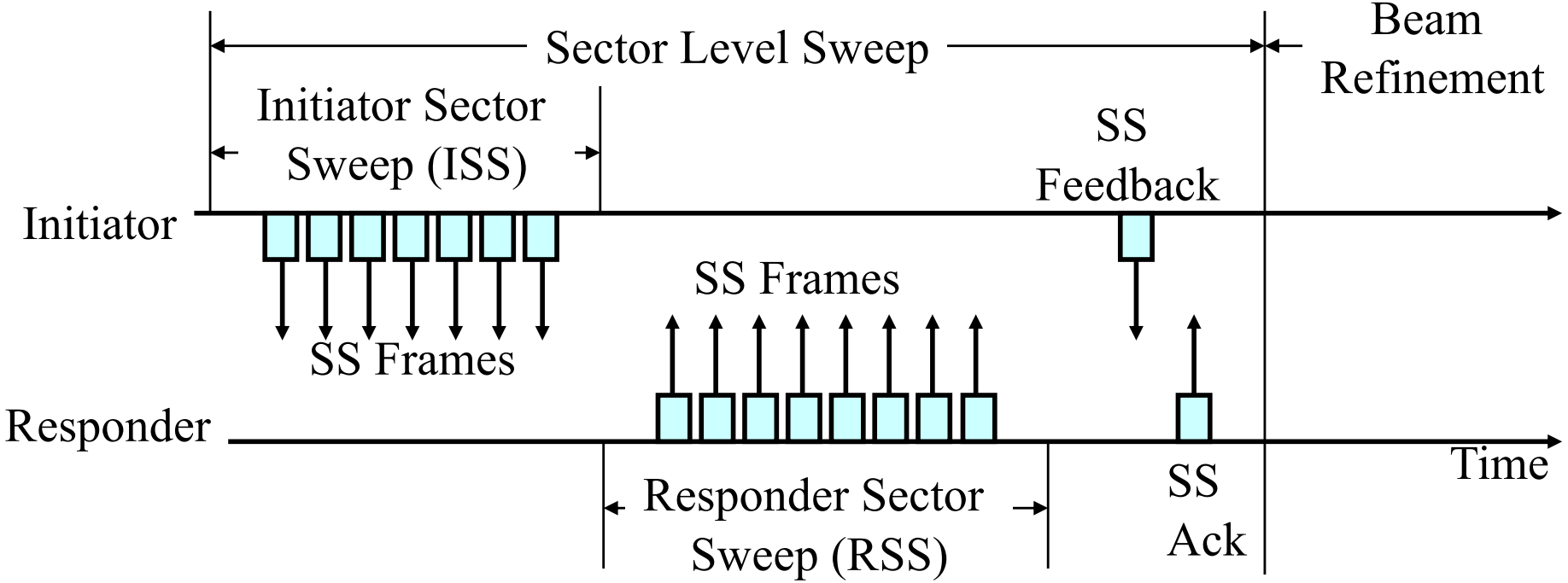
Example 3

- Two 802.11ad devices, STA1 and STA2, want to beamform. STA1 has 16 different antenna configurations (i.e., capable of steering the beam to 16 different directions). STA2 has only 4 beam directions. For Omni-direction Antenna approach, how many training frames are transmitted in total by these two devices before they discover the optimum beam pairs for communication?

STA1 first transmits 16 training frames while STA2 is listening in omni-direction. Then STA2 transmits 4 frames while STA2 is listening. Total frames transmitted = 16+4 = 20.

IEEE 802.11ad Beamforming Training

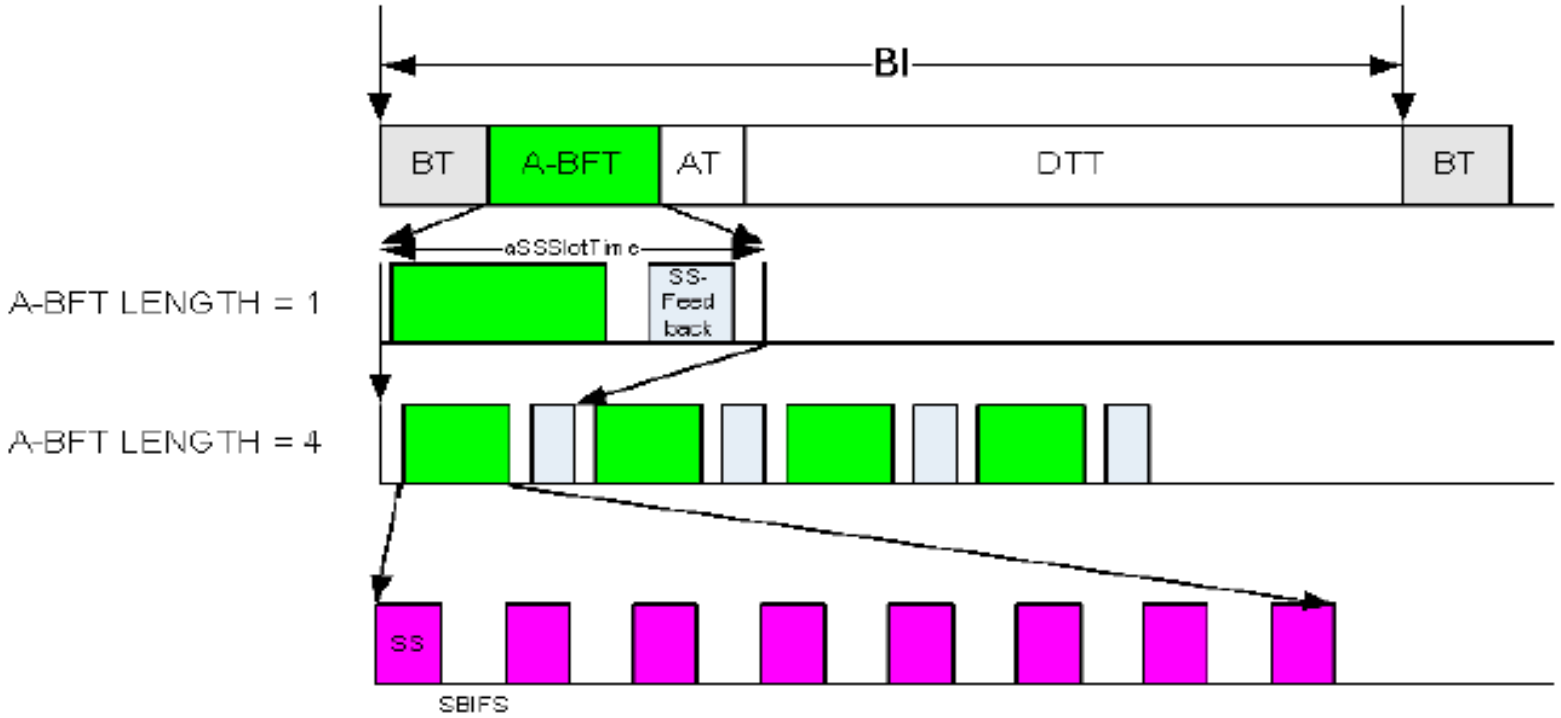
- Each station finds the optimal antenna configuration with its recipient using a two-stage search --- SLS followed by BRP
- **Sector Level Sweep (SLS):** Sends in all sectors and finds the optimal *sector pair*
  - Sector → coarse direction (there can be several sharper beams within a sector)
  - Low data rate with sector-level beamforming
- **Beam Refinement Protocol (BRP):** Searches through the optimal sector to find the optimal parameters in that sector (identify a narrower beam)
  - Higher data rate (multi-gigabit) with beam refinement



AP-STA Beamforming

- Takes place during BT and A-BFT durations
- During BT, AP transmits training frames on all its sectors; all STAs listen in omni-direction mode
- A-BFT duration is slotted; each STA selects a slot randomly and transmits training frames on all its sectors; AP listens in omni-direction mode
- Random slot selection may lead to collision. No feedback from AP to the STA if collision; STA tries in next beacon interval
- Only SLS is completed in BT and A-BFT; BFP is optional and may take place in DT duration

SLS in A-BFT



Example: consider that the A-BFT LENGTH = 8 and 3 mSTAs A, B and C are competing. All mSTAs choose a random value between [0,7]. mSTA A chooses value = 2, while mSTAs B and C choose a value = 5 which may result in a collision.

Akhtar and Ergen, "Efficient Network Level Beamforming Training for IEEE 802.11ad WLANs", SPECTS 2015

Example 4

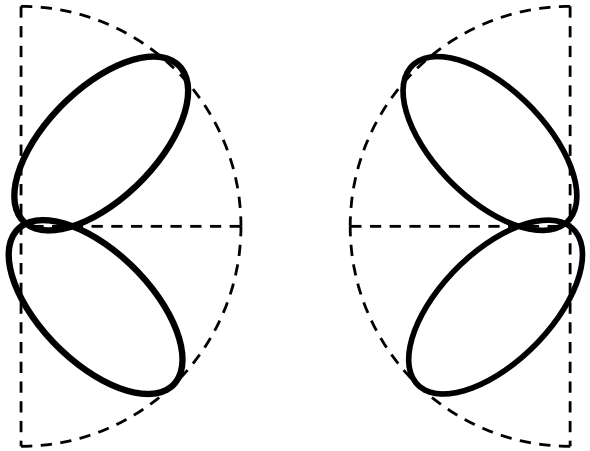
- The table shows the received signal strength (RSS) at the responder for each transmitted training frame from the beam training initiator during SLS. There are four sectors for both initiator and responder, and the number after the station letter denotes the sector number. For example, row 1 shows the frame transmitted by station A on its sector 1. What is the optimum beam (sector) pair discovered after the SLS?

Transmitted Training Frame	RSS at Responder
A.1	-70 dBm
A.2	-62 dBm
A.3	-50 dBm
A.4	-64 dBm
B.1	-49 dBm
B.2	-71 dBm
B.3	-75 dBm
B.4	-80 dBm

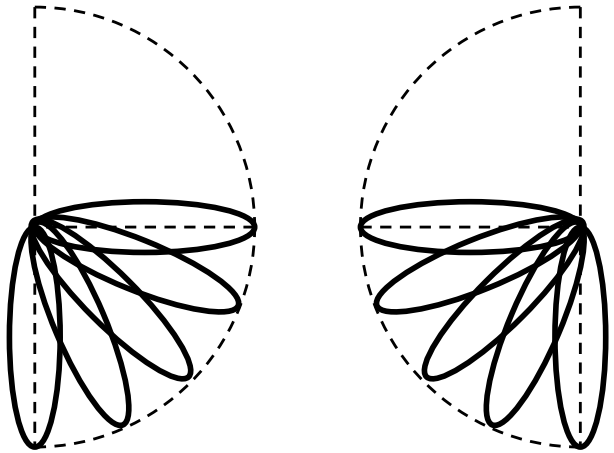
The sector that produces the strongest signal is selected as the best sector. For A, the strongest sector is 3 (-50 dBm). For B, sector 1 produces the strongest signal at A (-49 dBm). The optimum beam pair for (A,B) therefore is (3,1).

SLS vs. Beam Refinement

- SLS uses “coarse” (wider) beams
  - Quick, but low gain and hence low data rate
- Beam refinement finds narrower beams within the same sector
  - Increases gain and data rate, but takes additional time before communication can begin



Sector-Level Sweep



Beam Refinement

Spatial Frequency Sharing (SFS)

- Multiple transmissions may be scheduled on the same frequency at the same time if they don't interfere
- PCP asks stations to send results of any STA-STA beamforming training outcomes. PCP then has the complete knowledge of beam pairing among the stations within its PBSS. PCP then can work out which station pairs can share the same slot (will not interfere).

Example 6

- In a given PBSS, all stations have 12 antenna sectors with 30 degree transmission angle. The table shows the beam pairs learned from beam training among 6 stations, A to F. For example, the first row of the table shows that A would use its beam #1 to communicate with B while B would use its beam #7 to communicate with A. If a communication, SP1, between A and B has already been scheduled, can SP2, a new communication between E and F, be spatially shared with SP1, i.e., be allocated during the same time slots without interference?

a.k.a. sector pair

STA Pair	Beam Pair
(A,B)	(1,7)
(A,E)	(4,12)
(B,E)	(7,2)
(B,F)	(9,10)
(C,D)	(10,4)
(A,F)	(2,7)
(E,F)	(3,7)

No. During SP1, B will transmit on its beam #7, which is the same beam number found to be optimum to communicate with E (Row 3 in the table). Therefore B's transmissions to A during SP1 will affect E. SP2 therefore cannot be spatially shared with SP1 without interference.

Summary

1. 60 GHz, a.k.a. mm wave, has large bandwidth, small antenna separation allows easy beamforming and gigabit speeds but short distance due to large attenuation
2. Tri-band Wireless LAN devices with 2.4 GHz, 5.8GHz, and 60GHz are coming
3. 802.11ad LAN uses a PBSS central control point (PCP)
4. In all cases antenna alignment and tracking is required.
5. **Centralized** scheduling. Only **PCP** can send beacons. It sends beacons in all sectors.
6. Superframe (**Beacon Interval**) consists of Beacon Time, Associating Beamforming Training, Announcement Time, and Data Transfer Time
7. Announcement time is used for collecting requests from STAs
8. Data transfer can be pre-allocated or by contention
9. **Antenna training** is a 2-phase process. Sector selection and beam refinement.
10. Multiple transmission can take place on the same frequency at the same time (**Spatial Frequency Sharing**).

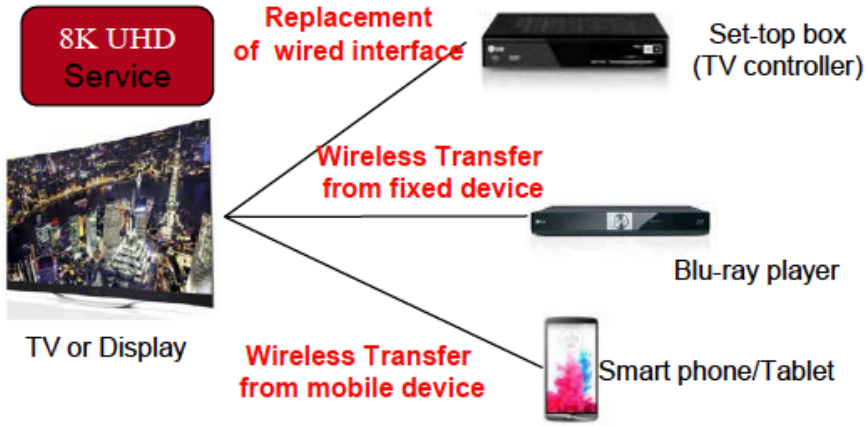
IEEE 802.11ay-2020 (expected)
Faster 60 GHz WLAN

802.11ay

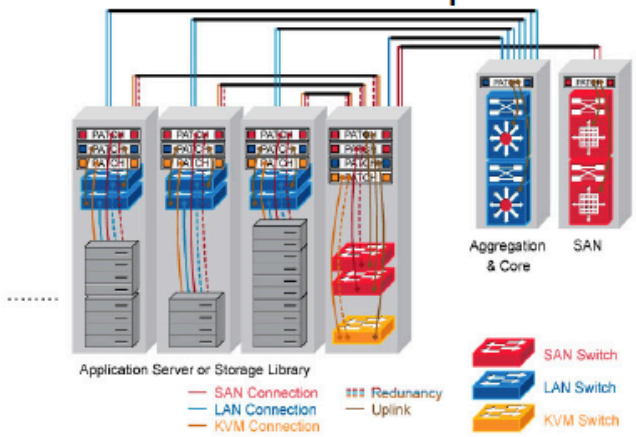
- 60GHz like 802.11ad, but faster than 802.11ad
  - 802.11ad is single stream and cannot bond channels (channel = 2.16GHz)
  - Single channel, single stream max speed: ~7Gbps
- 802.11ay expects to support 4 streams and bond multiple channels
  - 4 channels = 8.64GHz bandwidth
  - Max speed (4 channel, 4 stream) 170+ Gbps
- 802.11ay also offers longer range: up to 500m
- Expected in 2020

802.11ay projected use cases

Wireless Video

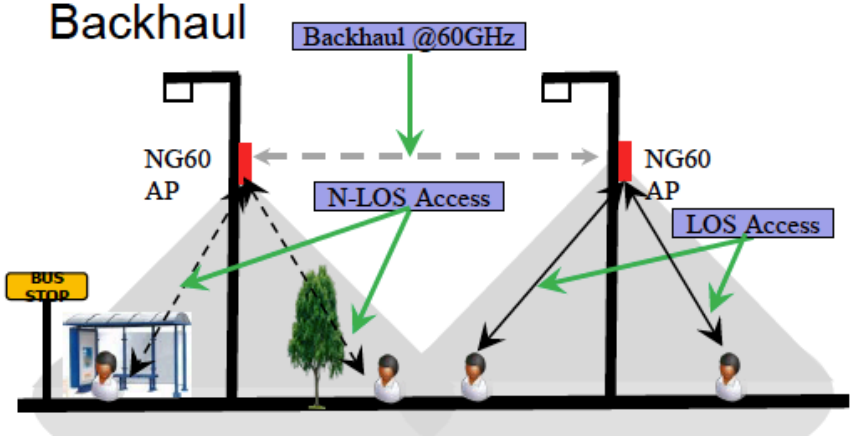


Data Center backup connection



VR/AR

Backhaul



Source: KEYSIGHT Technologies

Summary: Niche WiFi

- Mainstream WiFi operates in 2.4/5GHz band: hugely popular and used in many consumer products: mobile phone, tablets, laptops, …
  - IEEE 802.11a/b/g/n/ac/ax (11n=WiFi4, 11ac=WiFi5, 11ax=WiFi6)
- Niche WiFi: both sub-GHz and 60GHz
- Sub-GHz: 802.11af (700 MHz TV Whitespace: long-distance) and 802.11ah (900 MHz: IoT, sensors networks, home automation, large number of connections)
- 60GHz: 802.11ad (7Gbps; already penetrated some niche products) and 802.11ay (upcoming; 100+Gbps cable replacement, backhaul, …)