Advanced Mobile Networks
Wi-Fi (IEEE 802.11 WLAN) Part 3

WS 2024/2025 Lecture

Max Riegel
(max.riegel@ieee.org)

WS 2024/2025 Wi-Fi Lecture topics overview

Part 0:

- Introduction and overview

Part 1:

- Wi-Fi Deployments
- Wi-Fi Network architecture
- Wi-Fi Stds & Certification
- Wi-Fi Spectrum
- Wireless Channel

Part 2:

- Wi-Fi PHY Layer
- Wi-Fi PHY Q&A

+ PHY Exercises

Part 3:

- Wi-Fi MAC Layer
- Wi-Fi QoS
- Wi-Fi MAC Q&A

+ MAC Exercises

Part 4:

- Wi-Fi Security
- Wi-Fi Mobility
- Wi-Fi Security Q&A

AMN – Wi-Fi Lecture dates and content (tentative)

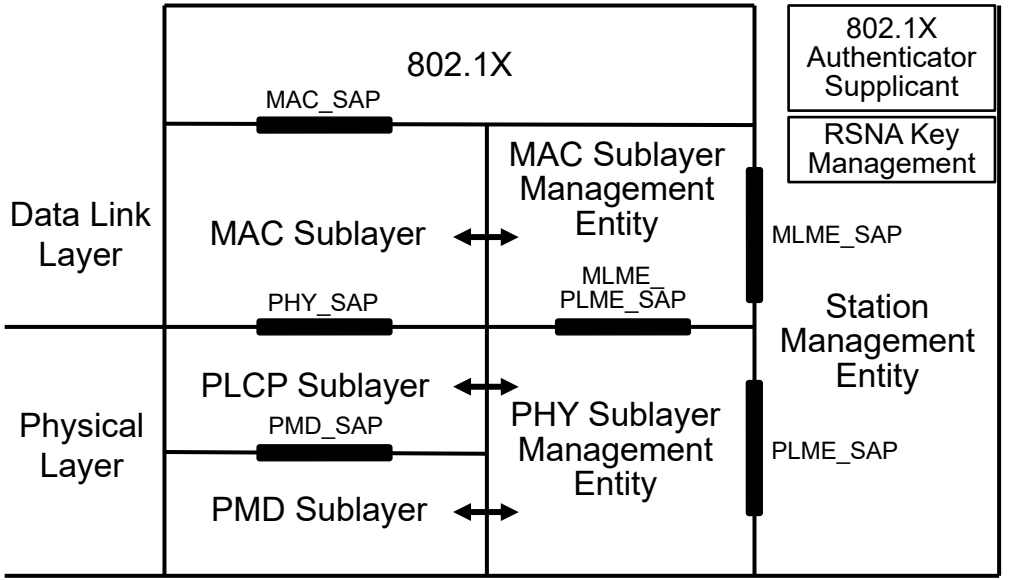
Thu, Nov. 28	Part 0	Thu, Jan 16th	Part 3
Tue, Dec. 10th	Part 1	Tue, Jan 21st	||
Thu, Dec 12th	||	Thu, Jan 23rd	||
Thu, Dec 19th	Part 2	Thu, Jan 30th	Part 4
Tue, Jan 7th	||	Tue, Feb 4th	||(partial)
Thu, Jan 9th	||	Thu, Feb 6th	????

Wi-Fi

IEEE 802.11 PROTOCOL ARCHITECTURE

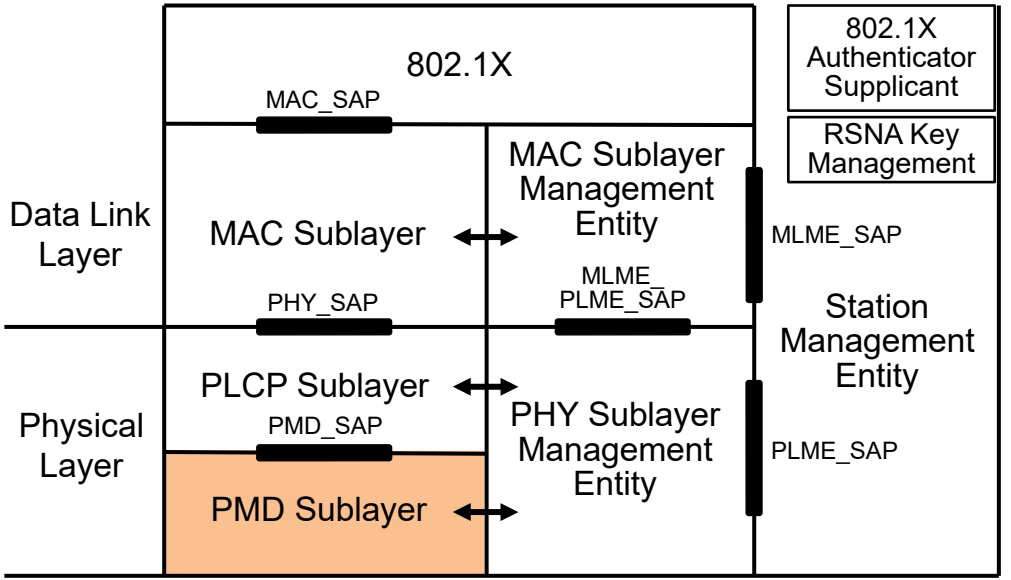
IEEE 802.11 Protocol architecture

- **802.1X**
  - Port Access Entity
  - Authenticator/Supplicant
- **RSNA Key Management**
  - Generation of Pair-wise and Group Keys
- **Station Management Entity (SME)**
  - interacts with both MAC and PHY Management
- **MAC Sublayer Management Entity (MLME)**
  - synchronization
  - power management
  - scanning
  - authentication
  - association
  - MAC configuration and monitoring
- **MAC Sublayer**
  - basic access mechanism
  - fragmentation
  - encryption
- **PHY Sublayer Management Entity (PLME)**
  - channel tuning
  - PHY configuration and monitoring
- **Physical Sublayer Convergence Protocol (PLCP)**
  - PHY-specific, supports common PHY SAP
  - provides Clear Channel Assessment signal (carrier sense)
- **Physical Medium Dependent Sublayer (PMD)**
  - modulation and encoding



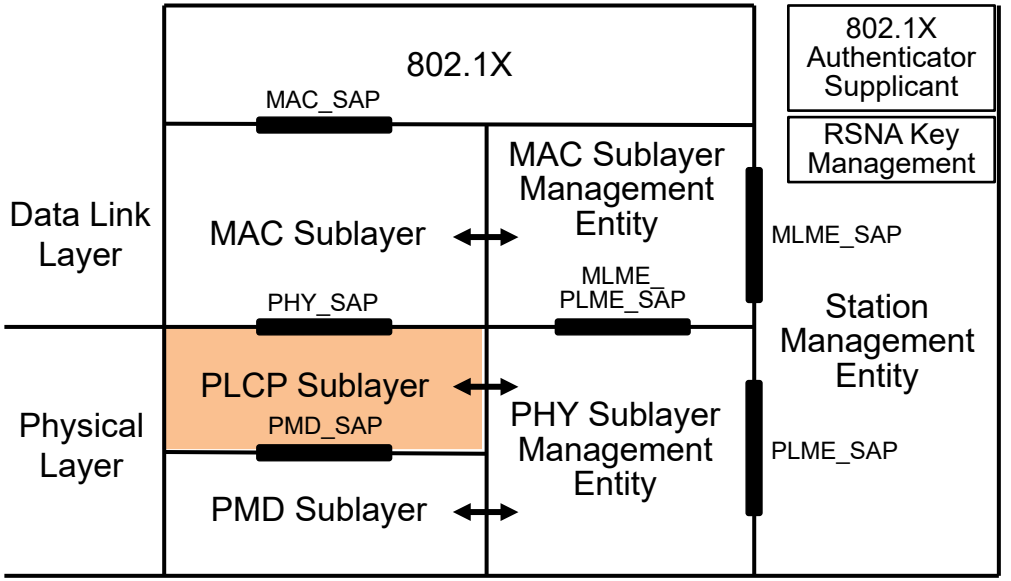
IEEE 802.11 Protocol architecture

- **802.1X**
  - Port Access Entity
  - Authenticator/Supplicant
- **RSNA Key Management**
  - Generation of Pair-wise and Group Keys
- **Station Management Entity (SME)**
  - interacts with both MAC and PHY Management
- **MAC Sublayer Management Entity (MLME)**
  - synchronization
  - power management
  - scanning
  - authentication
  - association
  - MAC configuration and monitoring
- **MAC Sublayer**
  - basic access mechanism
  - fragmentation
  - encryption
- **PHY Sublayer Management Entity (PLME)**
  - channel tuning
  - PHY configuration and monitoring
- **Physical Sublayer Convergence Protocol (PLCP)**
  - PHY-specific, supports common PHY SAP
  - provides Clear Channel Assessment signal (carrier sense)
- **Physical Medium Dependent Sublayer (PMD)**
  - modulation and encoding



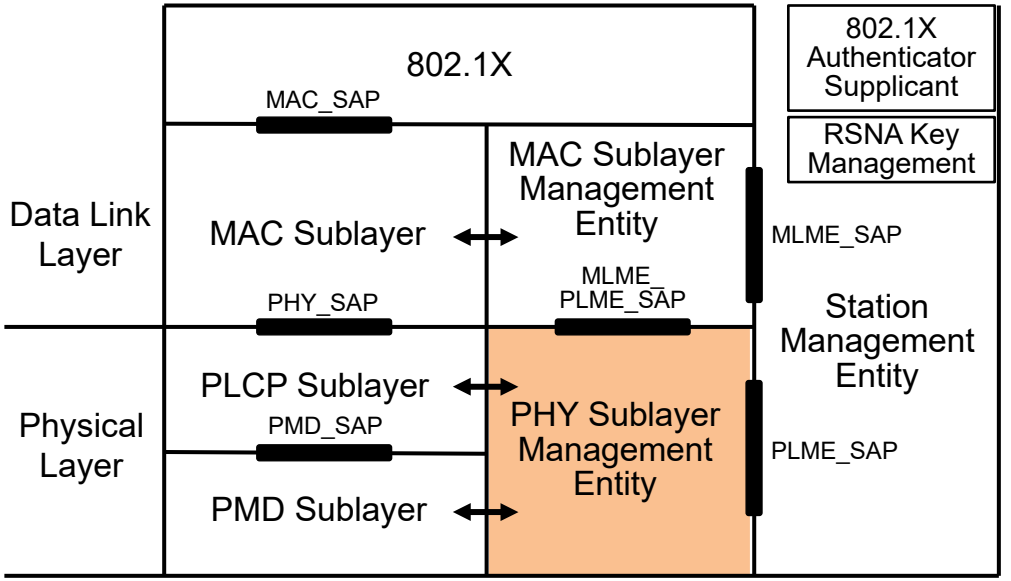
IEEE 802.11 Protocol architecture

- **802.1X**
  - Port Access Entity
  - Authenticator/Supplicant
- **RSNA Key Management**
  - Generation of Pair-wise and Group Keys
- **Station Management Entity (SME)**
  - interacts with both MAC and PHY Management
- **MAC Sublayer Management Entity (MLME)**
  - synchronization
  - power management
  - scanning
  - authentication
  - association
  - MAC configuration and monitoring
- **MAC Sublayer**
  - basic access mechanism
  - fragmentation
  - encryption
- **PHY Sublayer Management Entity (PLME)**
  - channel tuning
  - PHY configuration and monitoring
- **Physical Sublayer Convergence Protocol (PLCP)**
  - PHY-specific, supports common PHY SAP
  - provides Clear Channel Assessment signal (carrier sense)
- **Physical Medium Dependent Sublayer (PMD)**
  - modulation and encoding



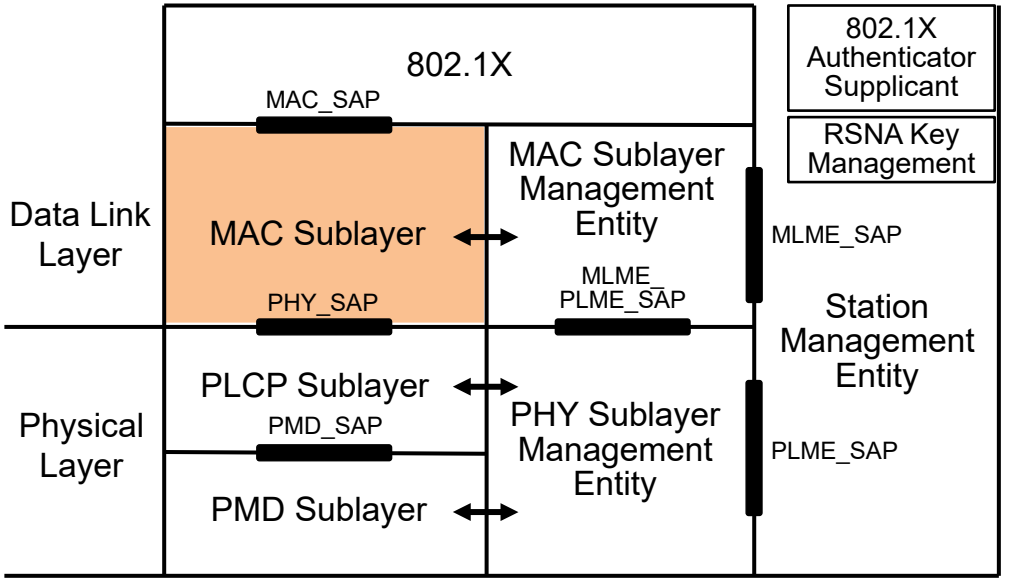
IEEE 802.11 Protocol architecture

- **802.1X**
  - Port Access Entity
  - Authenticator/Supplicant
- **RSNA Key Management**
  - Generation of Pair-wise and Group Keys
- **Station Management Entity (SME)**
  - interacts with both MAC and PHY Management
- **MAC Sublayer Management Entity (MLME)**
  - synchronization
  - power management
  - scanning
  - authentication
  - association
  - MAC configuration and monitoring
- **MAC Sublayer**
  - basic access mechanism
  - fragmentation
  - encryption
- **PHY Sublayer Management Entity (PLME)**
  - channel tuning
  - PHY configuration and monitoring
- **Physical Sublayer Convergence Protocol (PLCP)**
  - PHY-specific, supports common PHY SAP
  - provides Clear Channel Assessment signal (carrier sense)
- **Physical Medium Dependent Sublayer (PMD)**
  - modulation and encoding



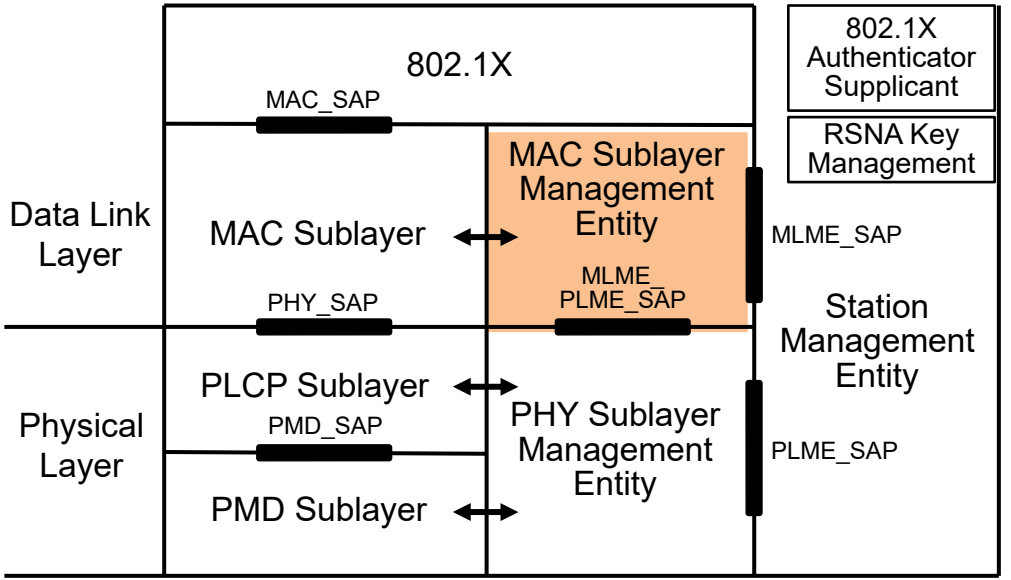
IEEE 802.11 Protocol architecture

- **802.1X**
  - Port Access Entity
  - Authenticator/Supplicant
- **RSNA Key Management**
  - Generation of Pair-wise and Group Keys
- **Station Management Entity (SME)**
  - interacts with both MAC and PHY Management
- **MAC Sublayer Management Entity (MLME)**
  - synchronization
  - power management
  - scanning
  - authentication
  - association
  - MAC configuration and monitoring
- **MAC Sublayer**
  - basic access mechanism
  - fragmentation
  - encryption
- **PHY Sublayer Management Entity (PLME)**
  - channel tuning
  - PHY configuration and monitoring
- **Physical Sublayer Convergence Protocol (PLCP)**
  - PHY-specific, supports common PHY SAP
  - provides Clear Channel Assessment signal (carrier sense)
- **Physical Medium Dependent Sublayer (PMD)**
  - modulation and encoding



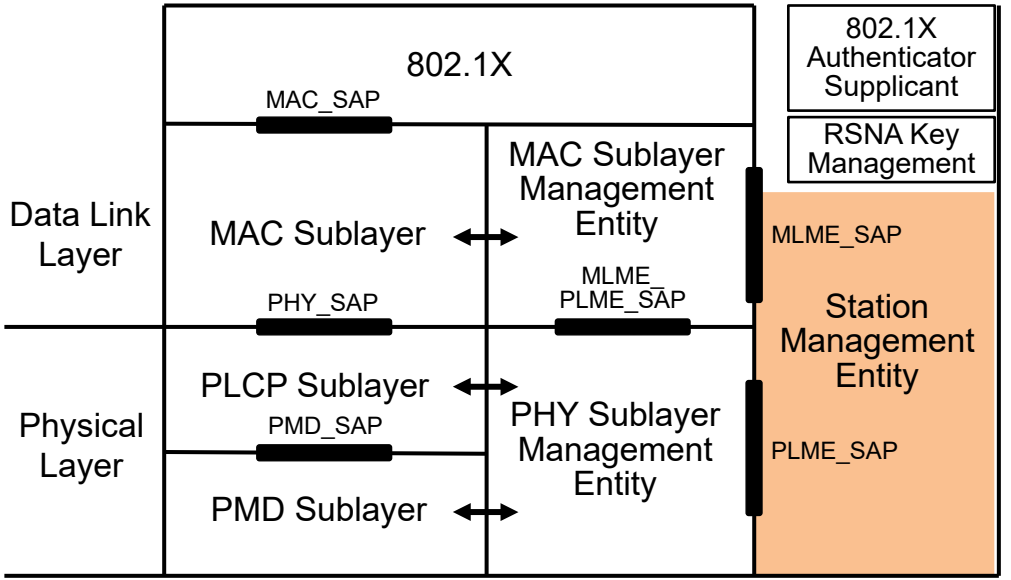
IEEE 802.11 Protocol architecture

- **802.1X**
  - Port Access Entity
  - Authenticator/Supplicant
- **RSNA Key Management**
  - Generation of Pair-wise and Group Keys
- **Station Management Entity (SME)**
  - interacts with both MAC and PHY Management
- **MAC Sublayer Management Entity (MLME)**
  - synchronization
  - power management
  - scanning
  - authentication
  - association
  - MAC configuration and monitoring
- **MAC Sublayer**
  - basic access mechanism
  - fragmentation
  - encryption
- **PHY Sublayer Management Entity (PLME)**
  - channel tuning
  - PHY configuration and monitoring
- **Physical Sublayer Convergence Protocol (PLCP)**
  - PHY-specific, supports common PHY SAP
  - provides Clear Channel Assessment signal (carrier sense)
- **Physical Medium Dependent Sublayer (PMD)**
  - modulation and encoding



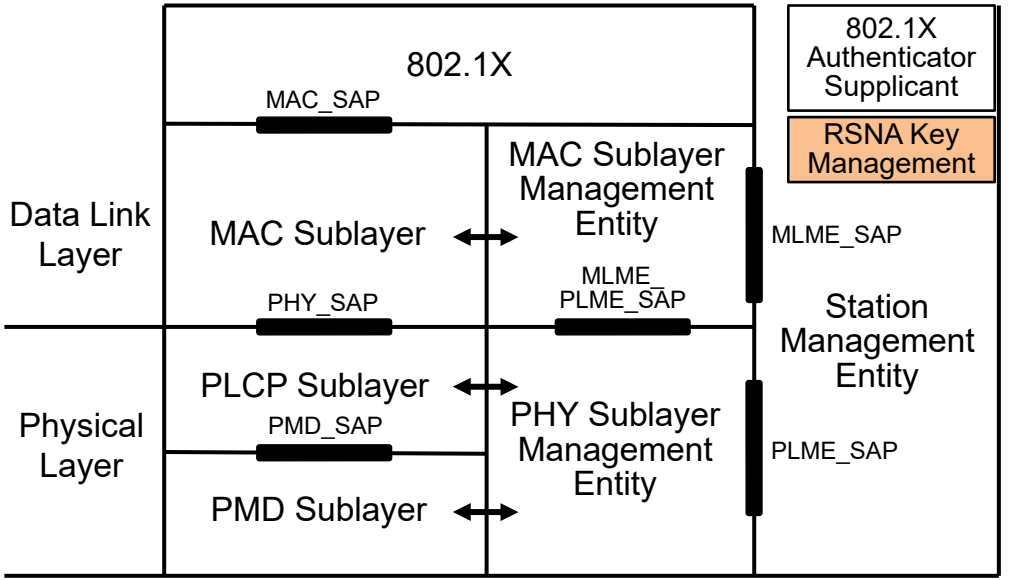
IEEE 802.11 Protocol architecture

- **802.1X**
  - Port Access Entity
  - Authenticator/Supplicant
- **RSNA Key Management**
  - Generation of Pair-wise and Group Keys
- **Station Management Entity (SME)**
  - interacts with both MAC and PHY Management
- **MAC Sublayer Management Entity (MLME)**
  - synchronization
  - power management
  - scanning
  - authentication
  - association
  - MAC configuration and monitoring
- **MAC Sublayer**
  - basic access mechanism
  - fragmentation
  - encryption
- **PHY Sublayer Management Entity (PLME)**
  - channel tuning
  - PHY configuration and monitoring
- **Physical Sublayer Convergence Protocol (PLCP)**
  - PHY-specific, supports common PHY SAP
  - provides Clear Channel Assessment signal (carrier sense)
- **Physical Medium Dependent Sublayer (PMD)**
  - modulation and encoding



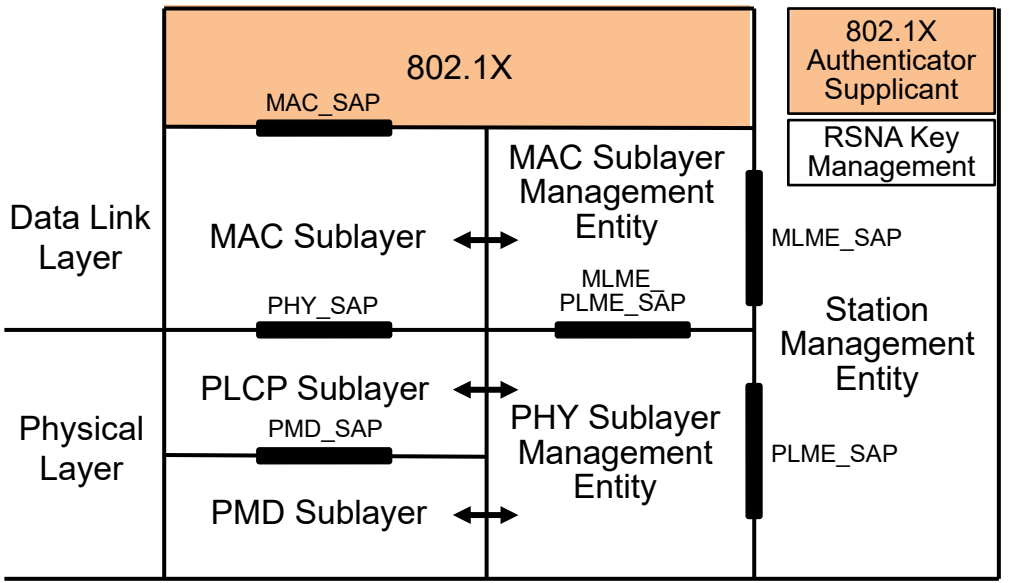
IEEE 802.11 Protocol architecture

- **802.1X**
  - Port Access Entity
  - Authenticator/Supplicant
- **RSNA Key Management**
  - Generation of Pair-wise and Group Keys
- **Station Management Entity (SME)**
  - interacts with both MAC and PHY Management
- **MAC Sublayer Management Entity (MLME)**
  - synchronization
  - power management
  - scanning
  - authentication
  - association
  - MAC configuration and monitoring
- **MAC Sublayer**
  - basic access mechanism
  - fragmentation
  - encryption
- **PHY Sublayer Management Entity (PLME)**
  - channel tuning
  - PHY configuration and monitoring
- **Physical Sublayer Convergence Protocol (PLCP)**
  - PHY-specific, supports common PHY SAP
  - provides Clear Channel Assessment signal (carrier sense)
- **Physical Medium Dependent Sublayer (PMD)**
  - modulation and encoding



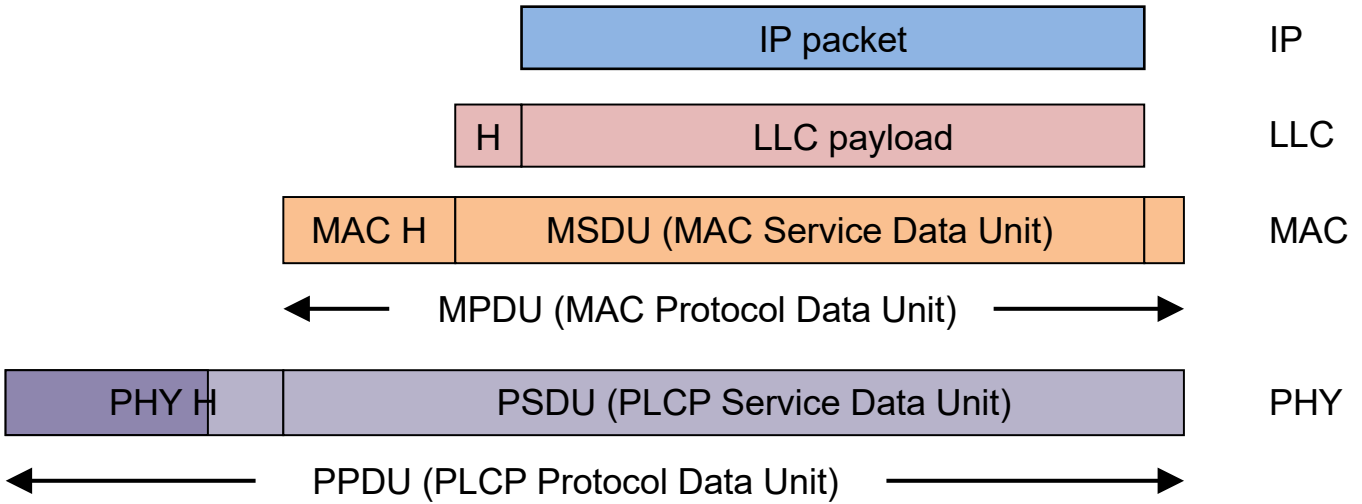
IEEE 802.11 Protocol architecture

- **802.1X**
  - Port Access Entity
  - Authenticator/Supplicant
- **RSNA Key Management**
  - Generation of Pair-wise and Group Keys
- **Station Management Entity (SME)**
  - interacts with both MAC and PHY Management
- **MAC Sublayer Management Entity (MLME)**
  - synchronization
  - power management
  - scanning
  - authentication
  - association
  - MAC configuration and monitoring
- **MAC Sublayer**
  - basic access mechanism
  - fragmentation
  - encryption
- **PHY Sublayer Management Entity (PLME)**
  - channel tuning
  - PHY configuration and monitoring
- **Physical Sublayer Convergence Protocol (PLCP)**
  - PHY-specific, supports common PHY SAP
  - provides Clear Channel Assessment signal (carrier sense)
- **Physical Medium Dependent Sublayer (PMD)**
  - modulation and encoding



IEEE 802.11 Protocol layering

- Each protocol layer deploys its own header for conveying the protocol information between peers



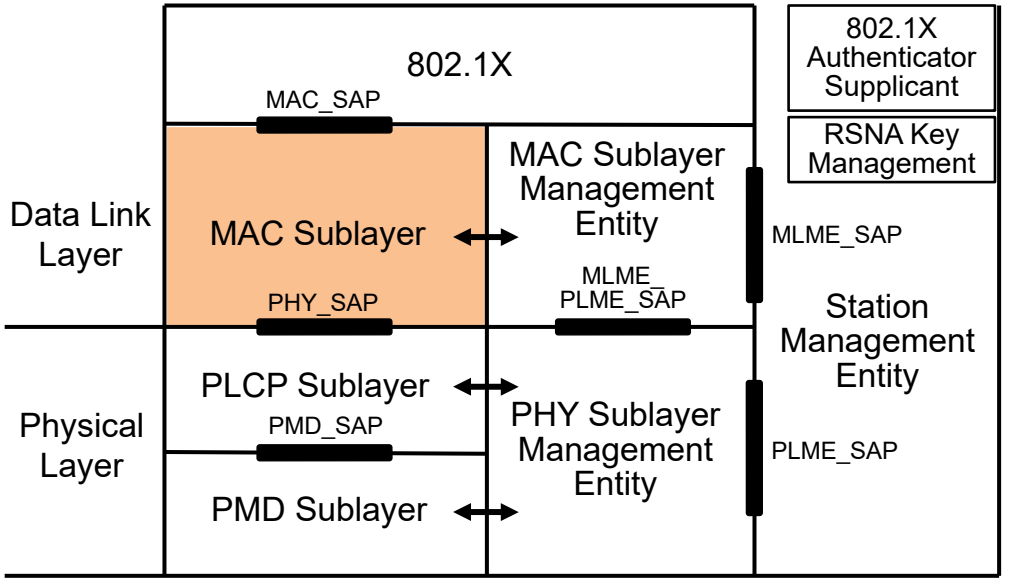
- Physical Layer Convergence Protocol (PLCP) provides a PHY independent Service Access Point (SAP) for higher layers
- One common MAC protocol for all different IEEE 802.11 PHYs

Wi-Fi

MAC SUBLAYER

Medium Access Functions in IEEE802.11 Architecture

- **802.1X**
  - Port Access Entity
  - Authenticator/Supplicant
- **RSNA Key Management**
  - Generation of Pair-wise and Group Keys
- **Station Management Entity (SME)**
  - interacts with both MAC and PHY Management
- **MAC Sublayer Management Entity (MLME)**
  - synchronization
  - power management
  - scanning
  - authentication
  - association
  - MAC configuration and monitoring
- **MAC Sublayer**
  - basic access mechanism
  - fragmentation
  - encryption
- **PHY Sublayer Management Entity (PLME)**
  - channel tuning
  - PHY configuration and monitoring
- **Physical Sublayer Convergence Protocol (PLCP)**
  - PHY-specific, supports common PHY SAP
  - provides Clear Channel Assessment signal (carrier sense)
- **Physical Medium Dependent Sublayer (PMD)**
  - modulation and encoding

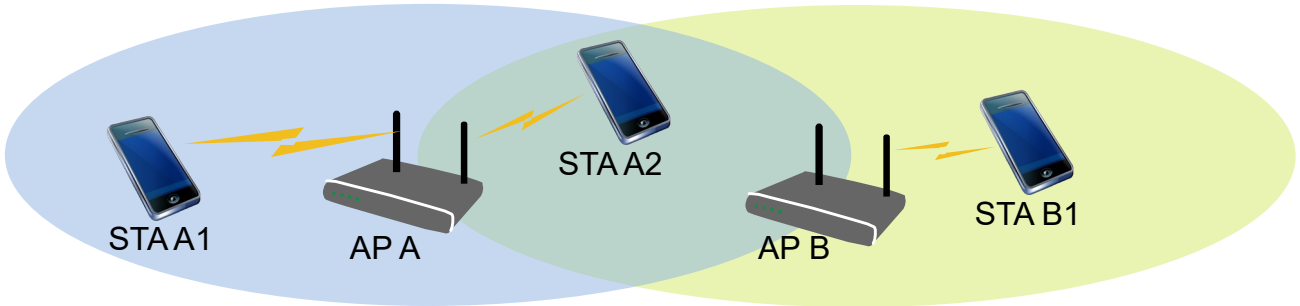


Topics covered in this section

- Medium access functions
  - Challenges
  - CSMA/CA
  - Distributed Coordination Function
  - RTS/CTS
  - Hidden node treatment
  - Fragmentation
  - Spatial reuse through BSS Coloring

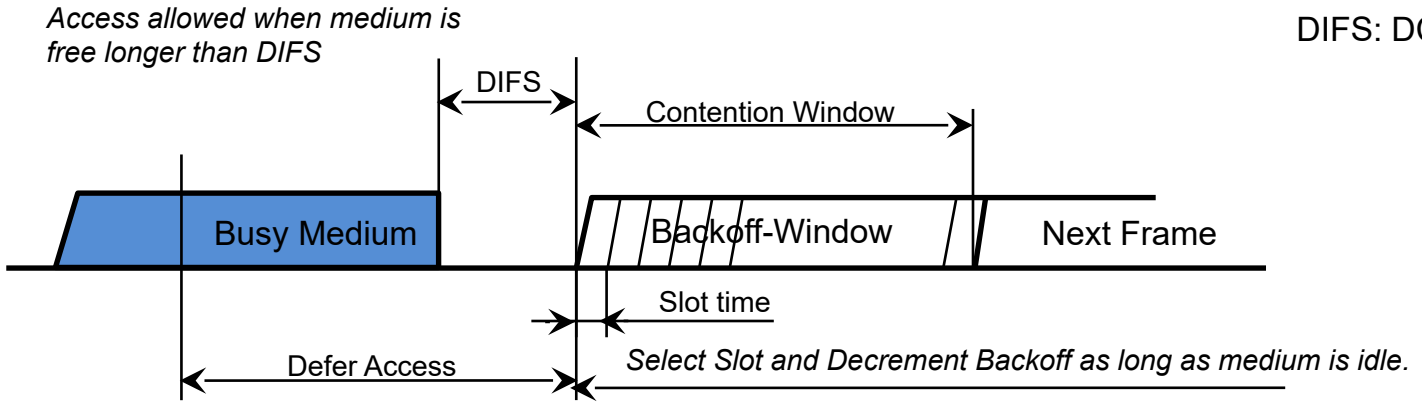
Shared Spectrum Medium Access Challenges

- Multiple concurrent transmissions in the same channel might collide.



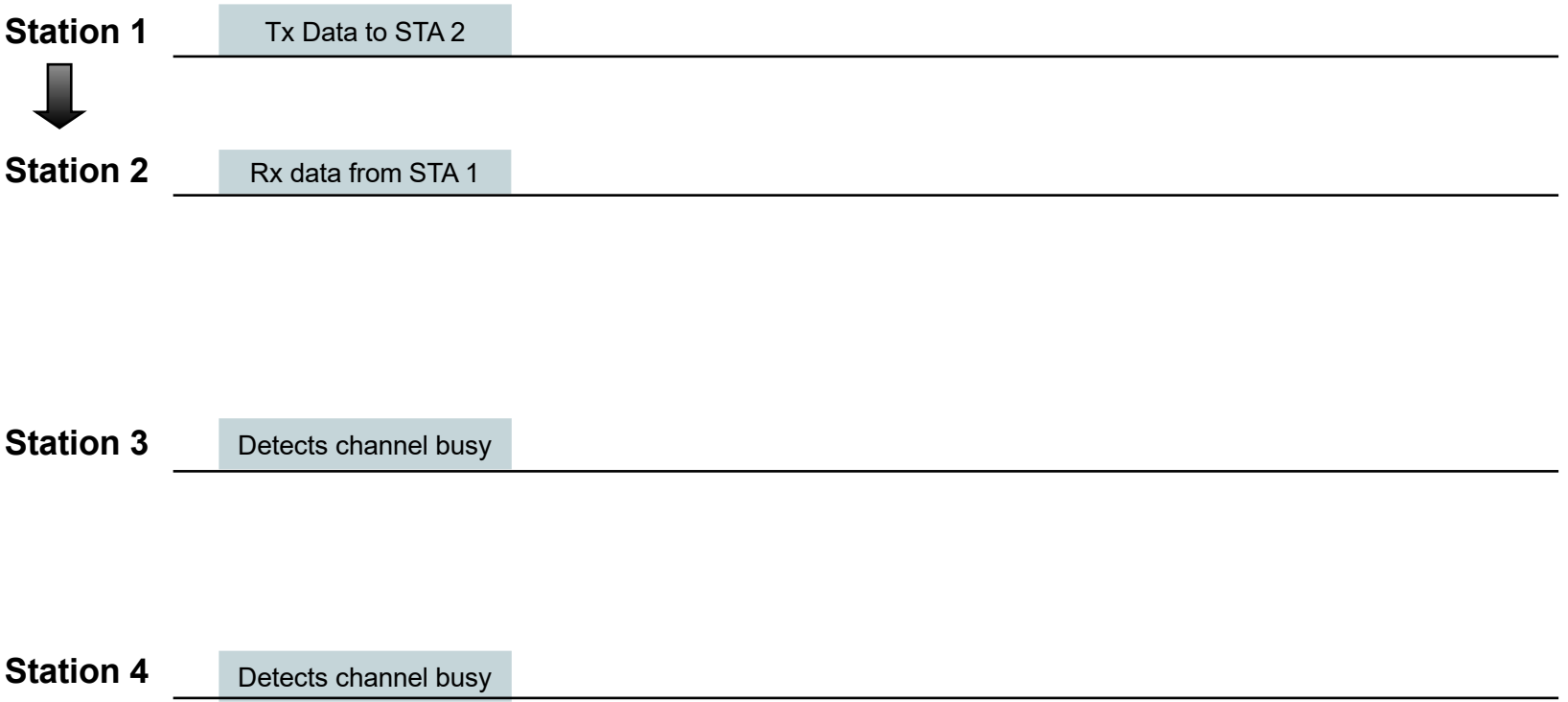
- No wireless issue only; same issue exists in shared wired medium as well
- (Legacy) Ethernet introduced CSMA/CD to avoid collisions.
  - CSMA/CD (Carrier Sense Multiple Access/Collision Detection) denotes method that potential transmitters first listen to the medium to ensure that no other transmission is ongoing before starting own transmission. When collision is detected, transmitter immediately stops.
  - Same behaviour that humans are usually applying when taking to each other.
- Wireless medium is somewhat more difficult.
  - During ongoing transmissions the transmitter can't detect collisions occuring elsewhere in the shared domain.

Carrier Sense Multiple Access with Collision Avoidance

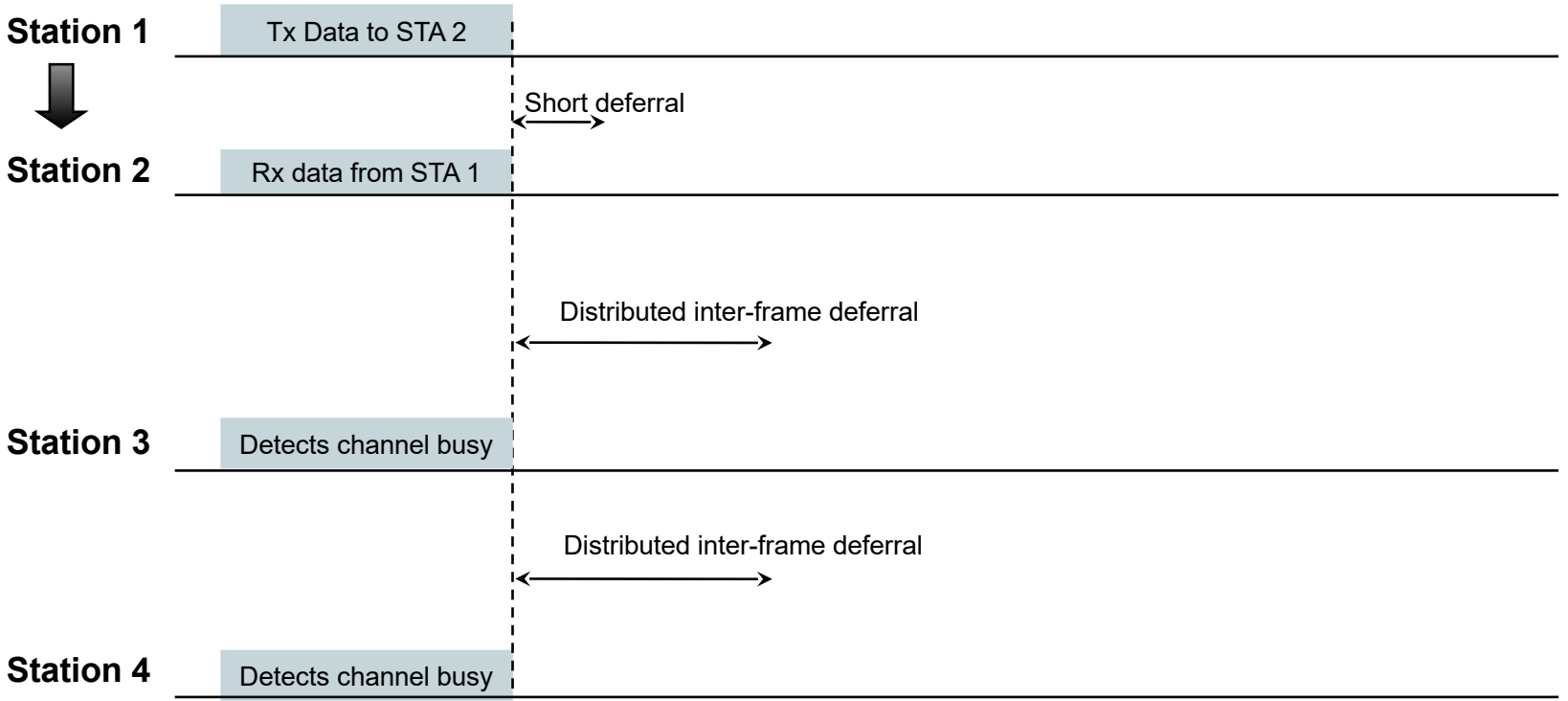


- CSMA/CA reduces collision probability in wireless medium.
  - Stations (also APs) are waiting for medium to become free.
  - Random backoff is used after a defer, resolving contention to avoid collisions.
    - Random backoff is an equally distributed value in the range 0..CWmin; CWmin = 15
  - Exponential backoff is used in the case of retransmissions.
    - $CW = (2^k - 1)$ with k = n+4 with n= number of retransmission; CWmax = 1023
    - Efficient Backoff algorithm stable at high loads.
  - Backoff timer elapses only when medium is idle.
- The method is denoted as Distributed Coordination Function (DCF) in IEEE 802.11

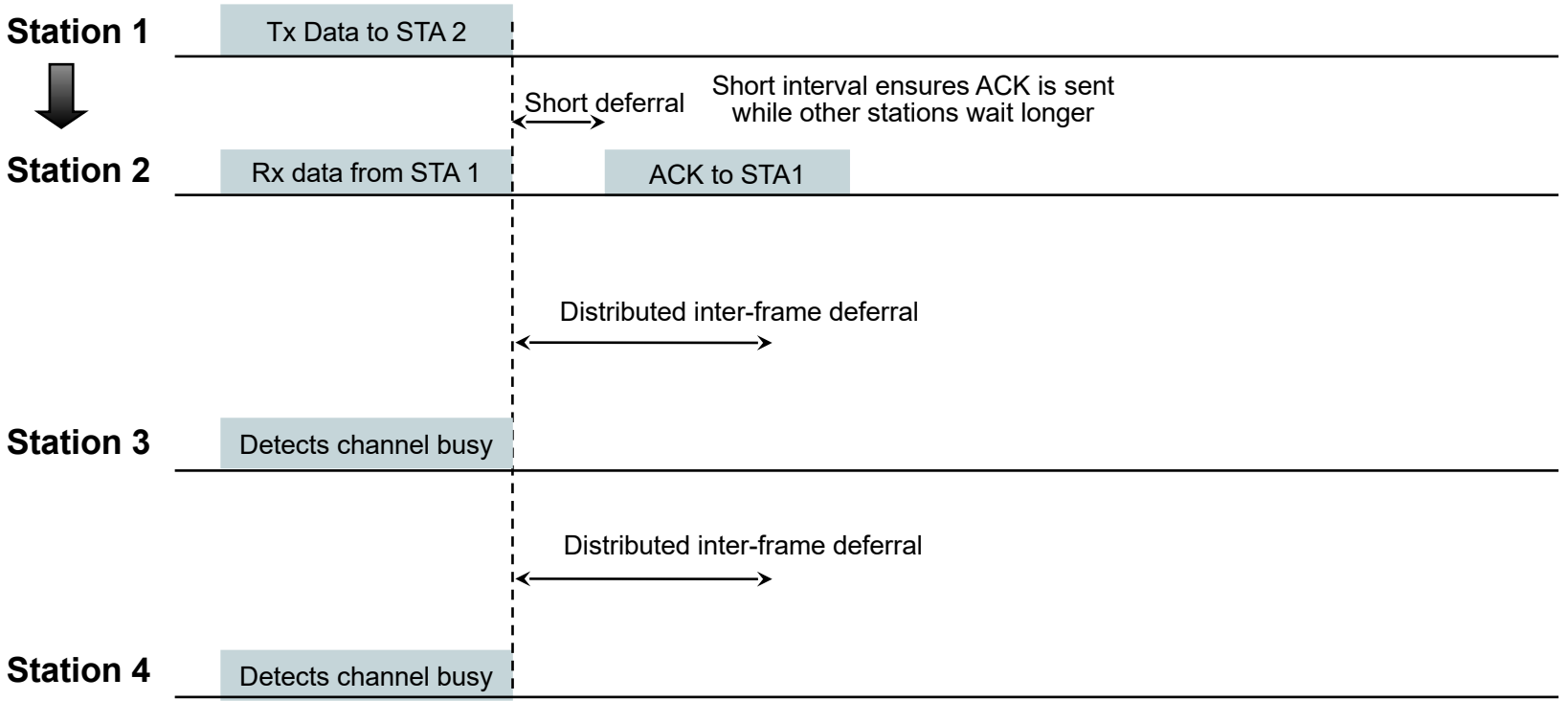
Distributed Coordination Function (DCF)



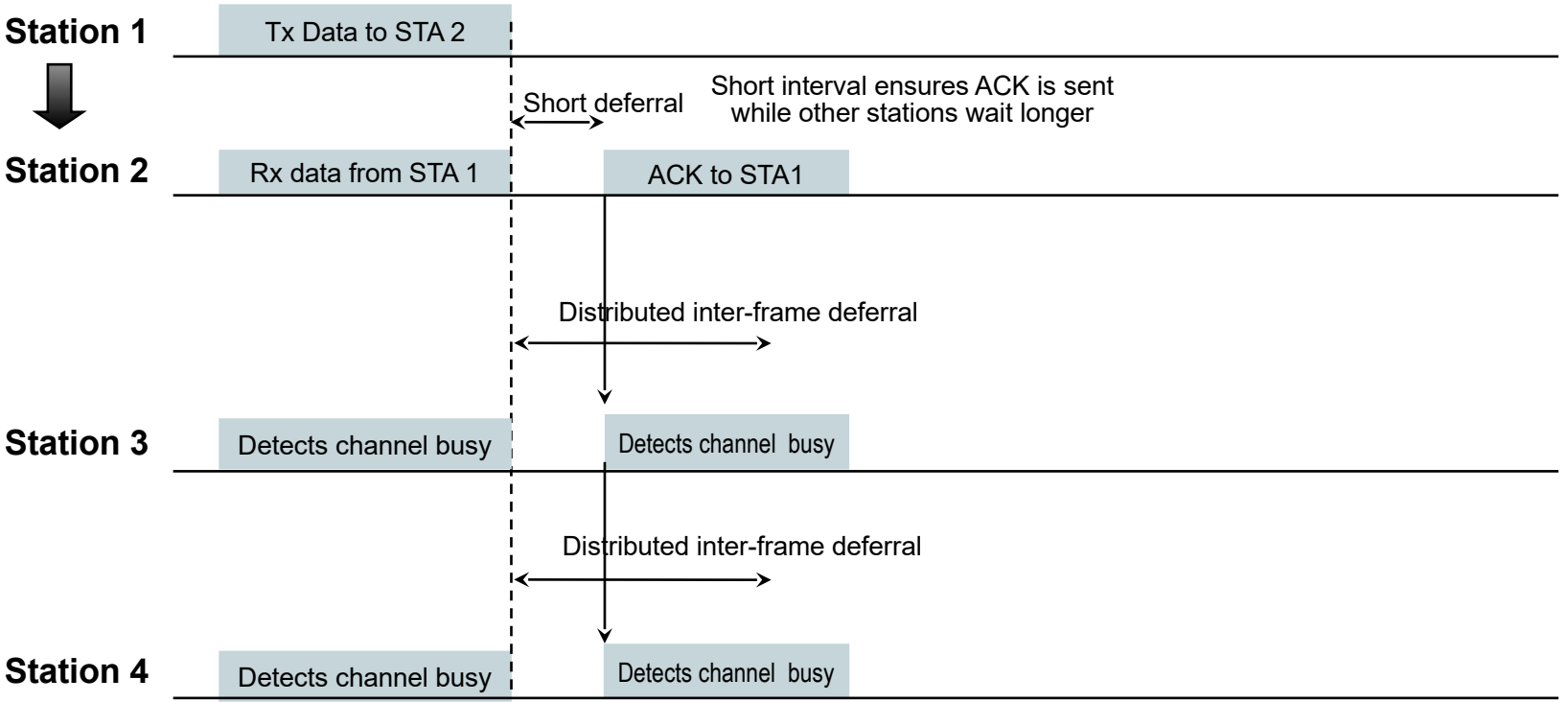
Distributed Coordination Function (DCF)



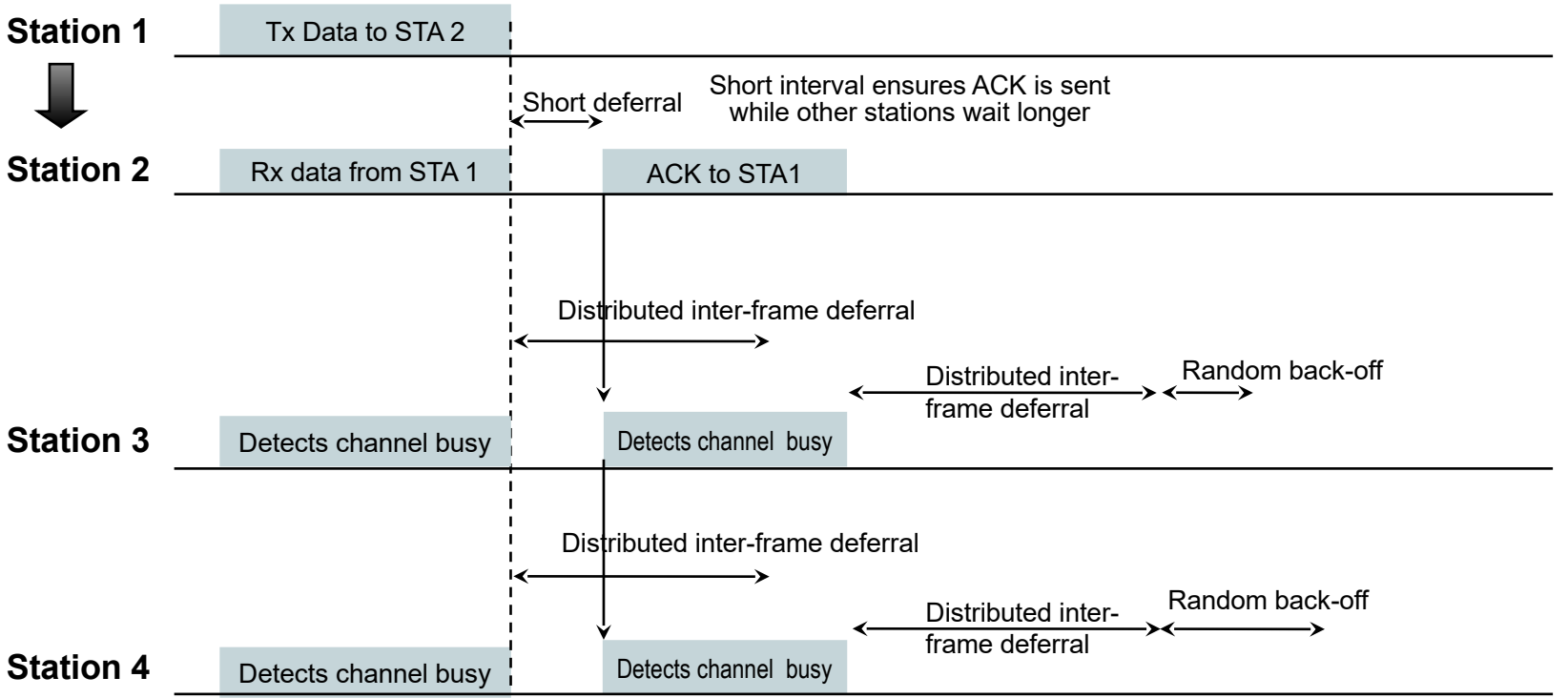
Distributed Coordination Function (DCF)



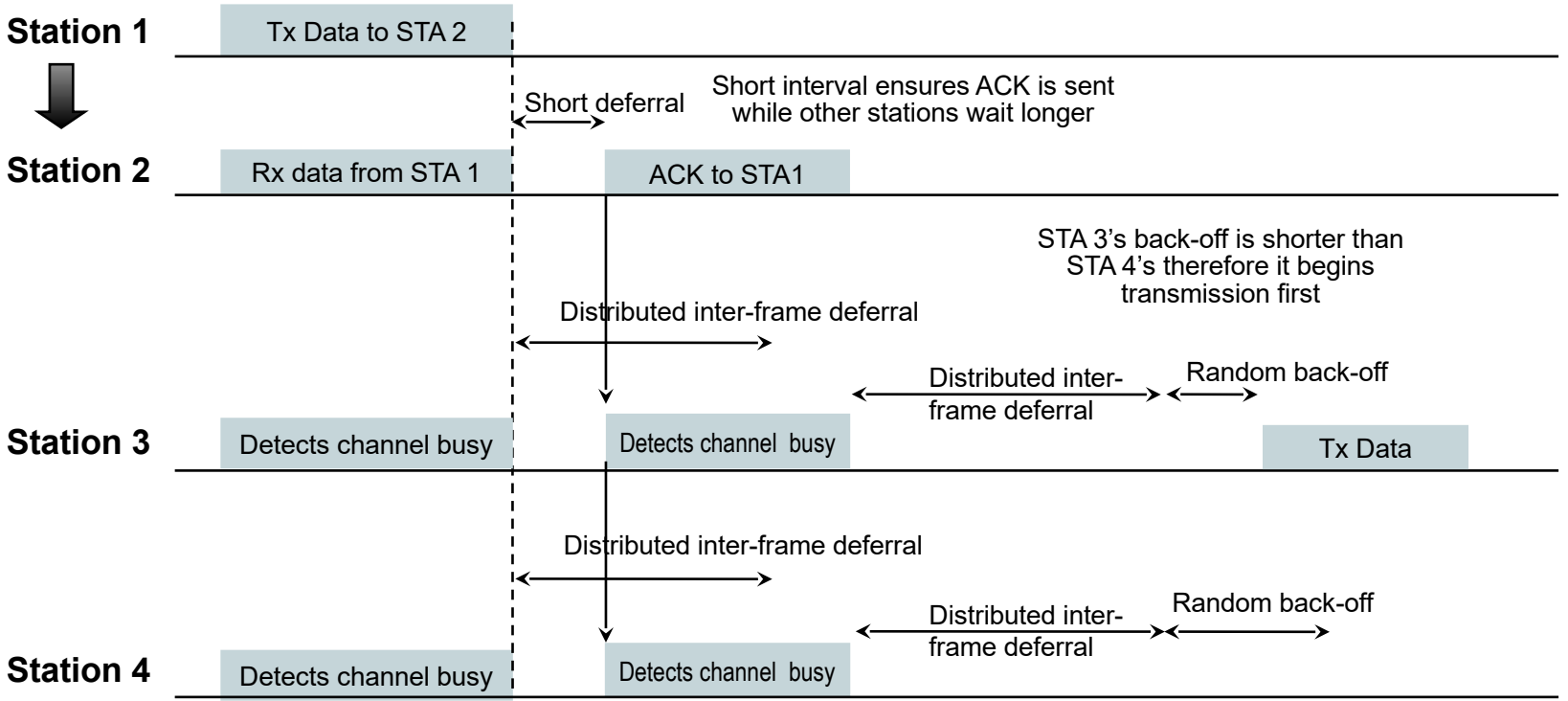
Distributed Coordination Function (DCF)



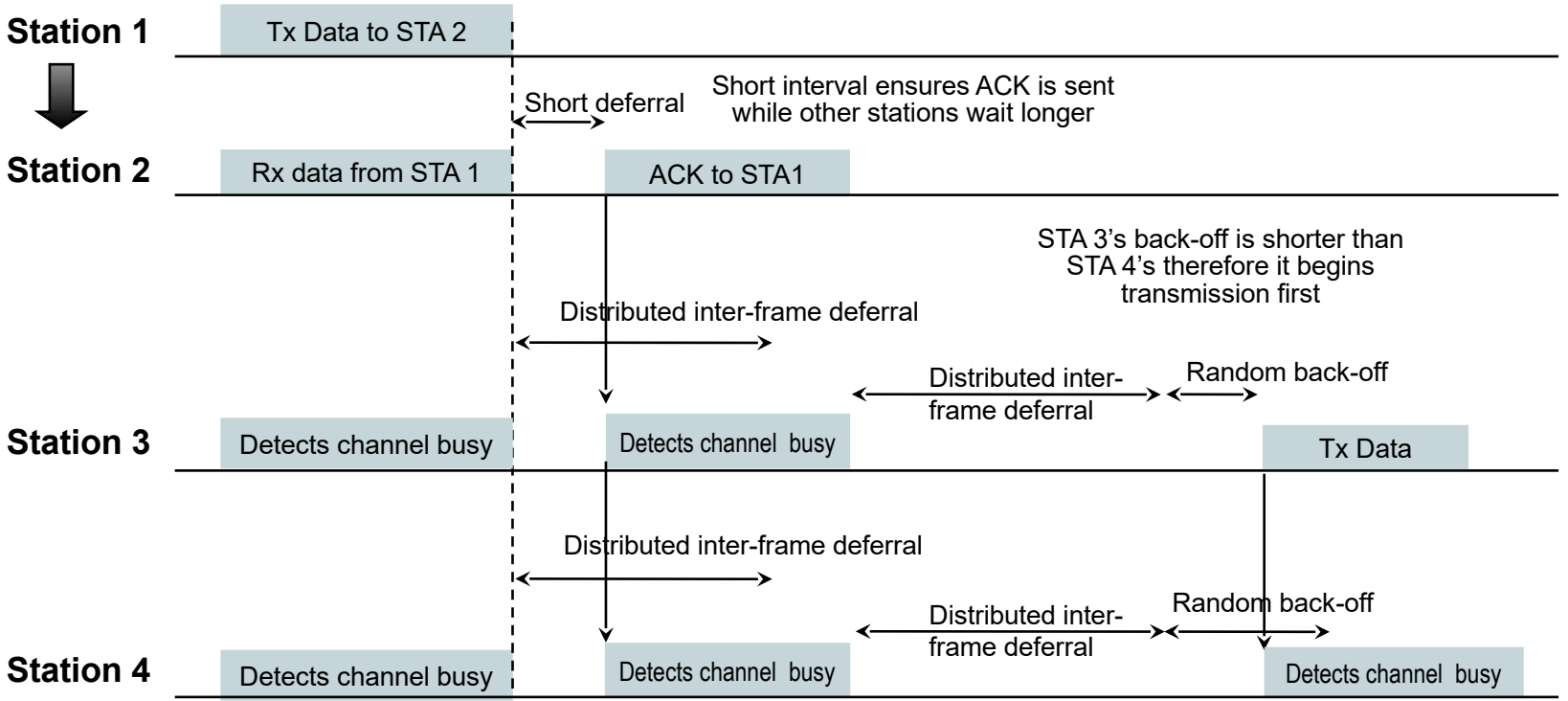
Distributed Coordination Function (DCF)



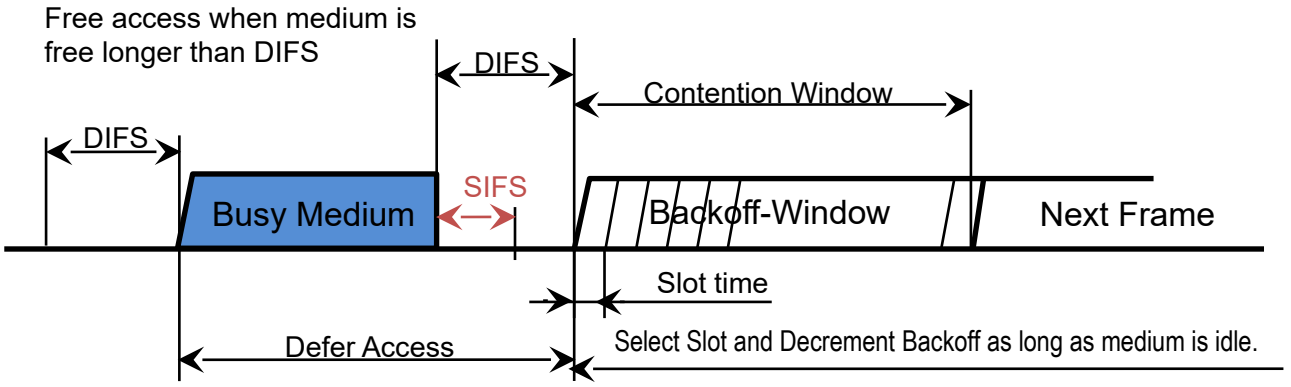
Distributed Coordination Function (DCF)



Distributed Coordination Function (DCF)



Physical carrier sensing: Clear Channel Access (CCA)



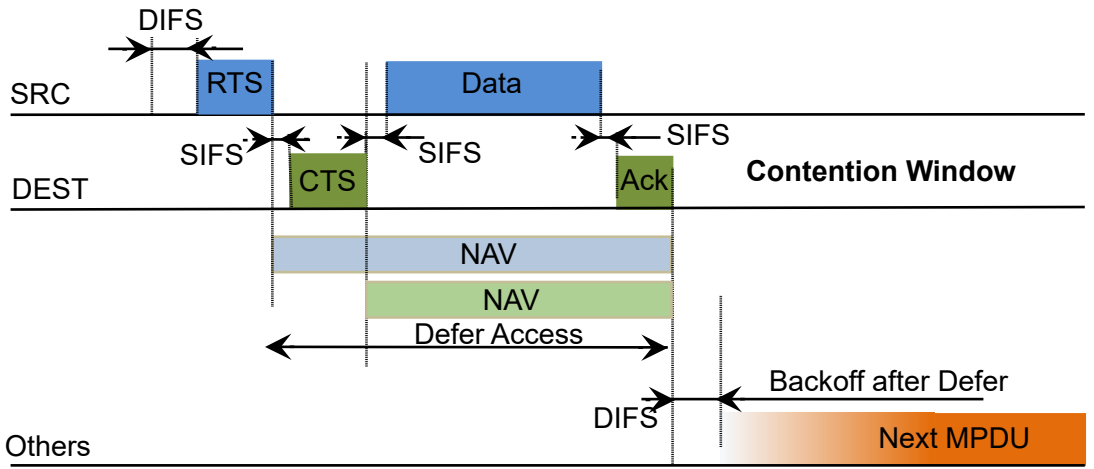
Standard	Slot time (µs)	DIFS (µs)
IEEE 802.11b	20	50
IEEE 802.11a/n/ac/ax/be	9	34
IEEE 802.11g/n/ax/be	9	28

SIFS: Short Inter Frame Space
PIFS: PCF Inter Frame Space
DIFS: DCF Inter Frame Space
DIFS = SIFS + 2x Slot time

- Energy in the channel is sensed for detection of idle channel.
- Two different thresholds are used for sensing in Wi-Fi
  - Regulatory requires that the medium has to be considered as occupied when an **energy level** higher than – 62 dBm/20MHz can be detected.
  - For better coverage, Wi-Fi deploys a more sensitive detection of neighbour Wi-Fi systems through **preamble detection** at a level of – 82dBm/20MHz.
- In 6 GHz band, regulatory defines a single detection threshold of – 72dBm/20 MHz.

Virtual carrier sensing: Timer values control the access.

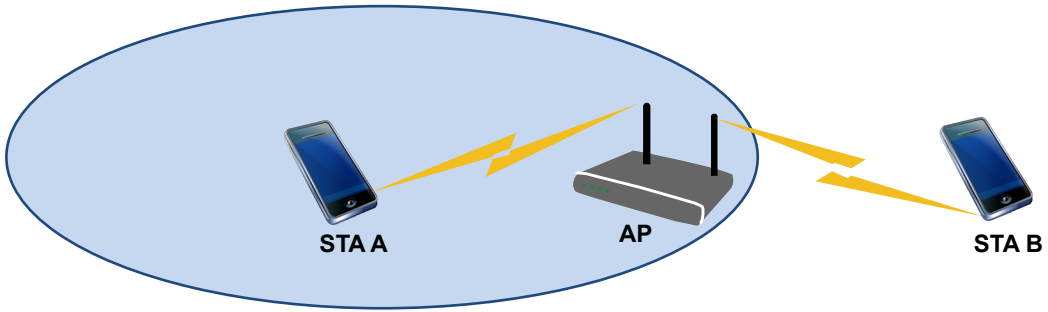
- Defer access based on Carrier Sense happens
  - either physical through CCA (Clear Channel Assessment) from PHY,
  - or virtual through NAV (Network Allocation Vector).



- Medium is blocked when indicated so by NAV. Others defer access until NAV expired and medium is free for at least DIFS.

Hidden Node Problem

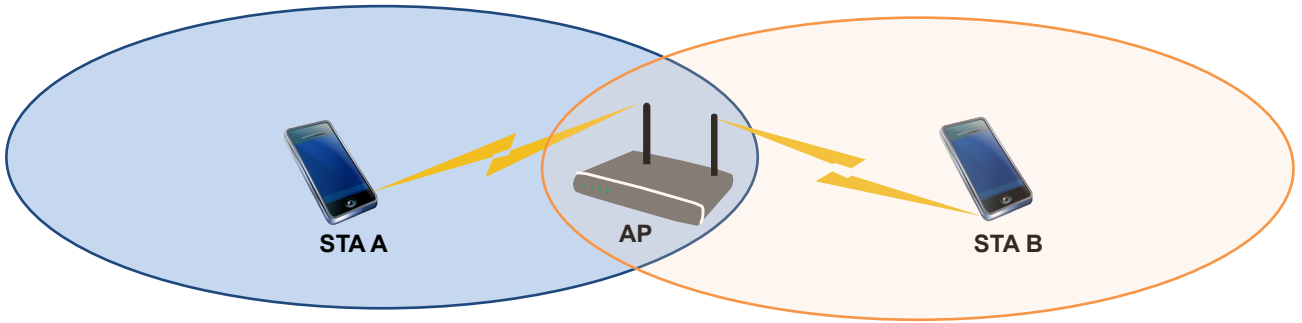
- A problem occurs when contending stations do not hear each other



  - STA-B cannot detect when STA-A occupies the medium.

Hidden Node Problem

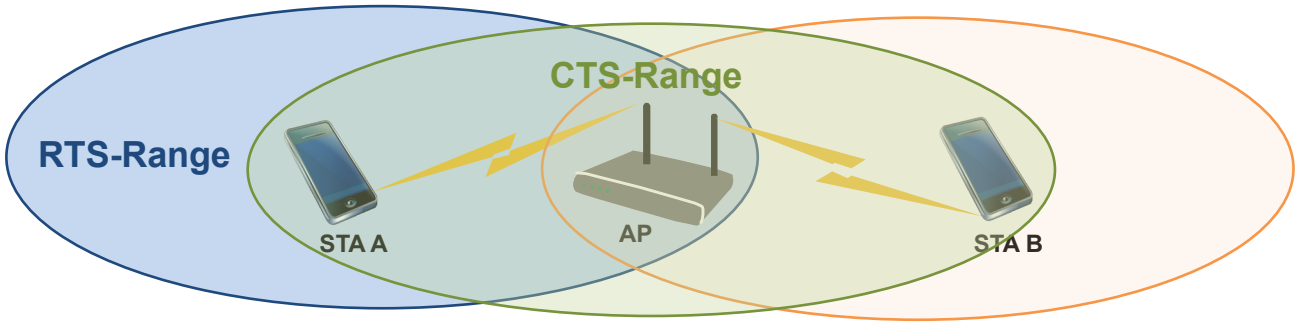
- A problem occurs when contending stations do not hear each other



  - STA-B cannot detect when STA-A occupies the medium.
  - STA-B may interfere with transmissions of STA-A to the AP.

Hidden Node Problem

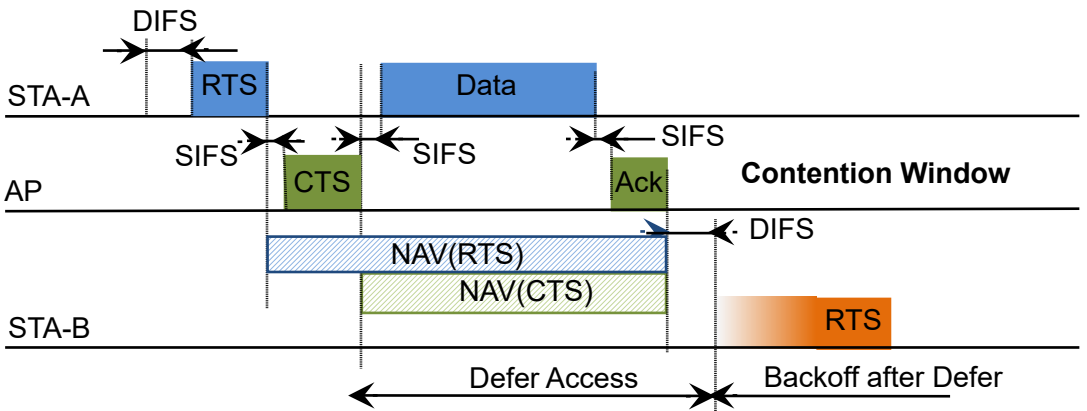
- A problem occurs when contending stations do not hear each other



  - STA-B cannot detect when STA-A occupies the medium.
  - STA-B may interfere with transmissions of STA-A to the AP.
- The issue is called 'hidden node problem' and may seriously impact the performance.
- IEEE 802.11 provides an mechanism to solve the problem:
  - RTS (Request To Send) and CTS (Clear To Send) to coordinate the access.

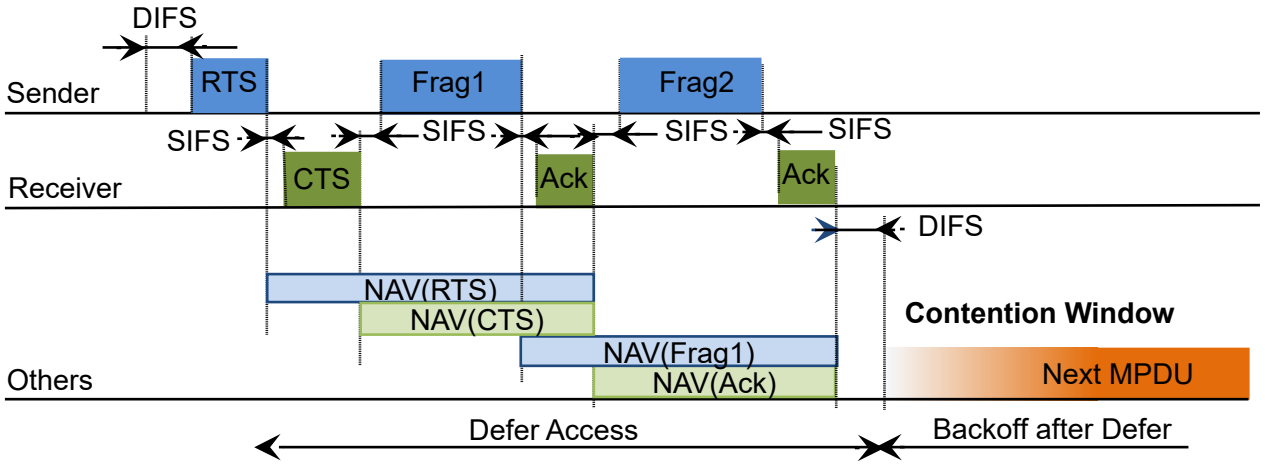
Hidden Node Solution

- STA-A sends a RTS frame to the AP with the amount of time stated in the NAV (Network Allocation Vector) to transmit its data frame including the ACK
  - The AP acknowledges the medium reservation with a CTS frame, which contains the updated reservation time in the NAV
  - STA-A might start transmitting its data when the CTS message arrives
- All stations monitor RTS/CTS frames and use the gathered information from the NAV to adjust their channel access procedure
  - STA-B only starts its transmission after expiration of the NAV preferably with RTS to let AP inform hidden neighbors about ongoing transmission.



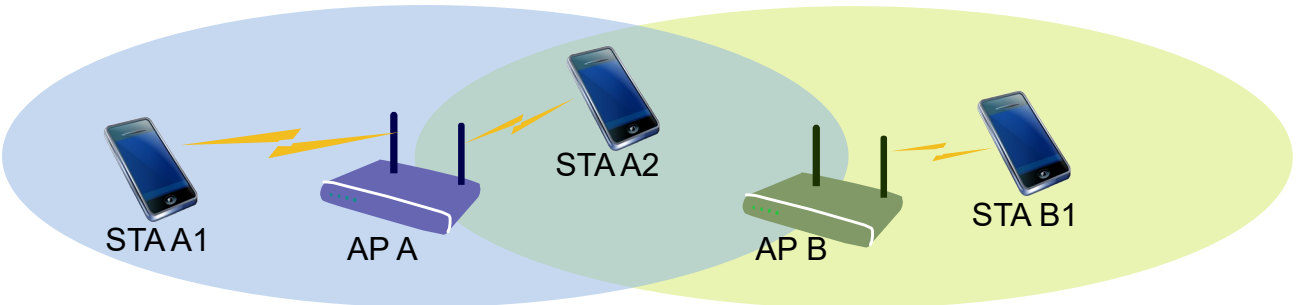
Fragmentation

- Packet loss probability increases when data packets are becoming big in a noisy environment
- Limiting the maximum packet size reduces the probability that a packet is hit by a bit failure.
- The MAC Layer provides the function to split packets into multiple smaller frames for transmission



Better spatial reuse through BSS Coloring

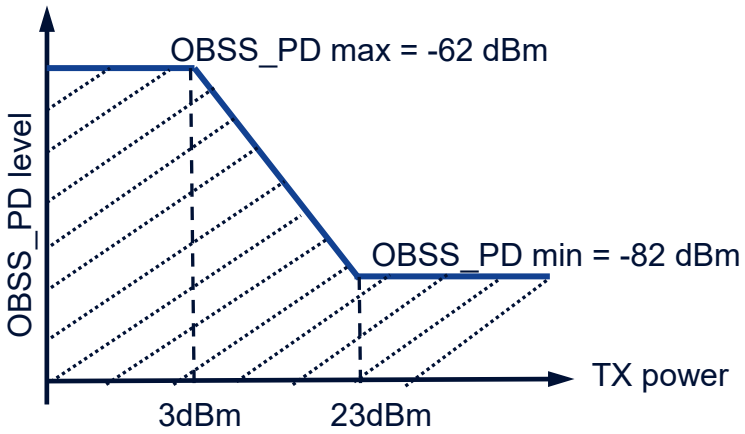
- In dense deployments, transmissions are stalled due to activities at distant BSS operating in the same channel.
- Still, successful transmission could be performed due to proximity of STA and AP despite parallel activies in the distant system.



- With Wi-Fi 6, CCA is enabled to determine intra-BSS frames from frames coming from other systems (OBSS).
  - BSS Coloring puts a 'color' value into the PHY header of each transmission frame.

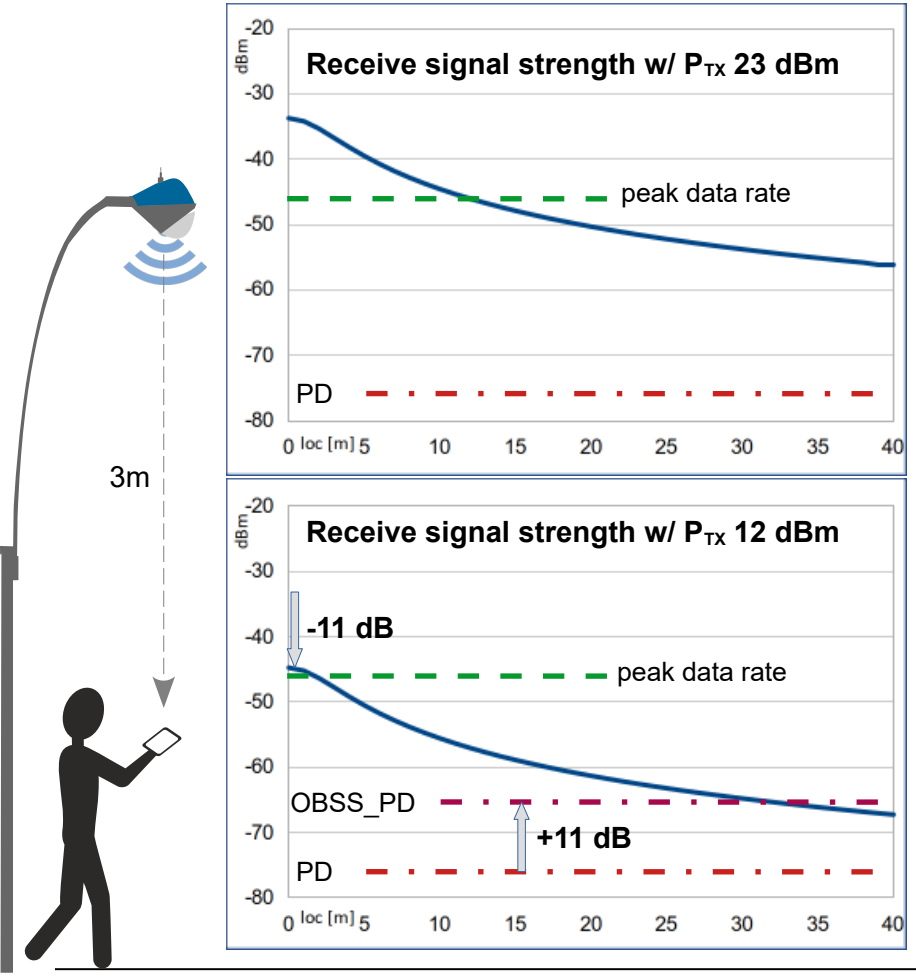
More aggressive transmissions through modified CCA

- A central network management can configure higher thresholds for preamble detection of frames originating from neighbor BSSs (different color) at all APs and STAs.
  - Preamble detection of OBSS frames can go up to the level of energy detection.
  - However, to mitigate negative side-effects, the transmission power for all frames has to be adjusted by the ratio amount to decrease overall interference levels.



- In addition, assignments and detection of Spatial Reuse Groups (SRG) are possible to determine between devices under common management, and devices not under common control.

How BSS coloring/spatial reuse of Wi-Fi 6 works…

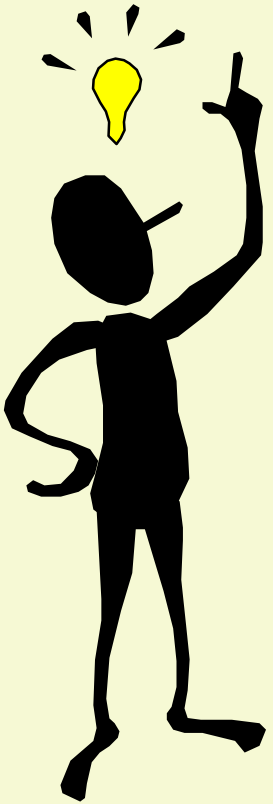


- Standard operation at 23 dBm TX power blocks any parallel transmission in the same channel at a large area.
- BSS coloring/spatial reuse allows an AP/STA to start a transmission at a higher sensing level (CCA)
  - when the interfering signal comes from a neighbor cell (visible through different BSS colors), and
  - the own transmission power is weak enough not to disturb the ongoing transmission in the neighbor cell.
- The example to the left shows that parallel transmissions at a distance of 30m would be feasible when lowering the transmission power by 11 dB.
  - Drawback of the approach is the lower RSSI leading to lower throughput per AP.

Summary: IEEE 802.11 basic access protocol features

- Efficient medium sharing through CSMA with enhancements for access control.
  - Access procedure denoted as ‘Distributed Coordination Function (DCF)’
  - Use of CSMA with Collision Avoidance through randomized delays.
  - Based on Carrier Sensing function in PHY called ‘Clear Channel Assessment (CCA)’.
  - Robust against high overload through exponential backoff in case of access collisions.
- Robust against interference and noisy channels.
  - CSMA/CA + ACK for unicast frames, with MAC level recovery to avoid negative impact to TCP/IP.
  - CSMA/CA without ACK for Broadcast frames.
- Parameterized use of RTS / CTS to provide a Virtual Carrier Sense function to protect against Hidden Nodes.
  - Duration information is distributed by both transmitter and receiver through separate RTS and CTS Control Frames.
- Fragmentation to cope with various PHY conditions and longer frame sizes.

Questions and answers

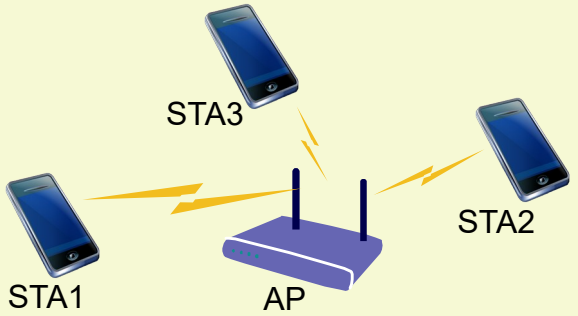


Medium Access Functions questions…

1) Why does CSMA/CD not work well in wireless medium?
2) Which means are used in IEEE 802.11 to avoid collisions?
3) What does SIFS mean, and when it is applied?
4) What is the difference between random backoff and exponential backoff?
5) How does virtual carrier sensing work?
6) When does a receiver respond with an ACK to a received frame?
7) What is the issue of the hidden node problem?
8) Which procedure is used to mitigate the hidden node problem?
9) By which mean better spatial reuse can be achieved?

CSMA/CA DCF timing and collision probabilities

- DCF (and EDCF) provide rules for starting transmissions after determination that medium is free. Randomization of access should avoid collisions.



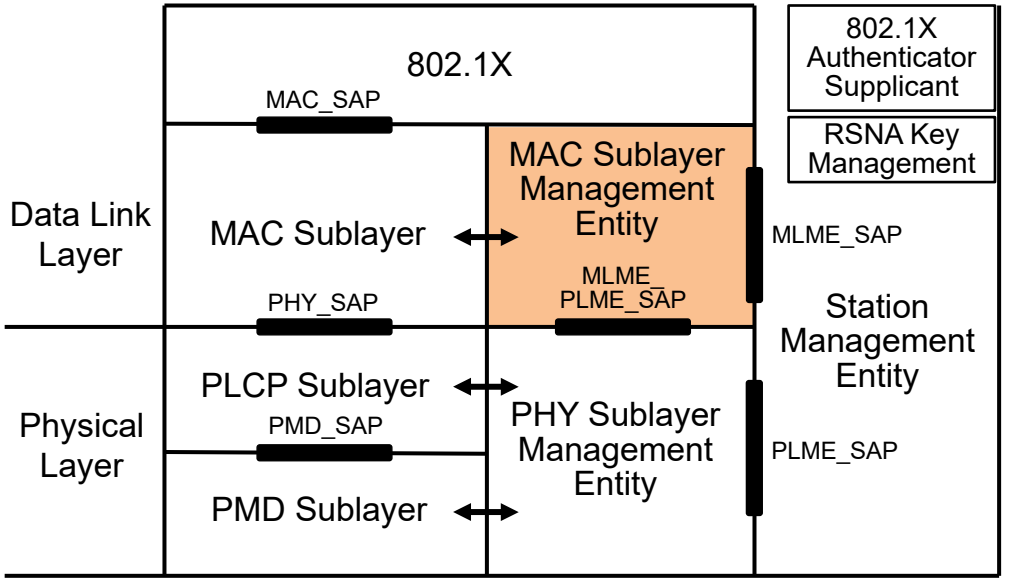
- Questions or the case of DCF @5GHz:
  - Q1: What is the minimum and maximum access delay after another transmission that a (single) station has to wait for access?
  - Q2: What is the likelihood that a collision occurs when 2 STAs compete?
  - Q3: What is the likelihood that a collision occurs when 4 STAs compete?
  - Q4: What is the minimum and maximum access delay after a collision?
  - Q5: What is the likelihood that a succeeding collision occurs w/ 2 STAs?
  - Q6: What is the minimum and maximum access delay after a 2nd collision?

Wi-Fi MAC Layer

MAC SUBLAYER MANAGEMENT

MAC layer management in IEEE802.1 Architecture

- **802.1X**
  - Port Access Entity
  - Authenticator/Supplicant
- **RSNA Key Management**
  - Generation of Pair-wise and Group Keys
- **Station Management Entity (SME)**
  - interacts with both MAC and PHY Management
- **MAC Sublayer Management Entity (MLME)**
  - synchronization
  - power management
  - scanning
  - authentication
  - association
  - MAC configuration and monitoring
- **MAC Sublayer**
  - basic access mechanism
  - fragmentation
  - encryption
- **PHY Sublayer Management Entity (PLME)**
  - channel tuning
  - PHY configuration and monitoring
- **Physical Sublayer Convergence Protocol (PLCP)**
  - PHY-specific, supports common PHY SAP
  - provides Clear Channel Assessment signal (carrier sense)
- **Physical Medium Dependent Sublayer (PMD)**
  - modulation and encoding



Wi-Fi MAC Layer Management

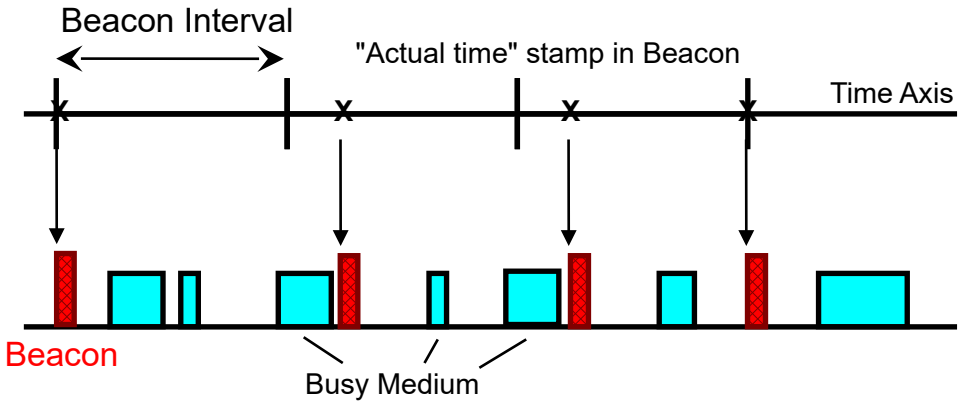
SYSTEM MANAGEMENT

System Management - Overview

- Synchronization
  - Synchronization (Timer Synchronization Function)
  - Beacon generation

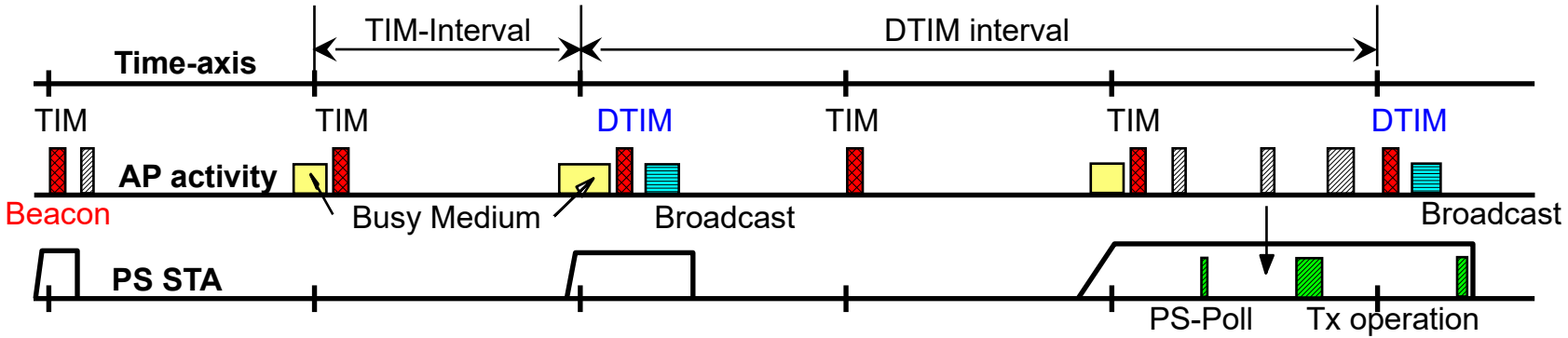
- Power management
  - Legacy power management
  - Unscheduled Automatic Power Save Delivery (U-APSD)
  - WMM Power Save Certification
  - Target Wake Time (TWT)

Synchronization through Beacon generation



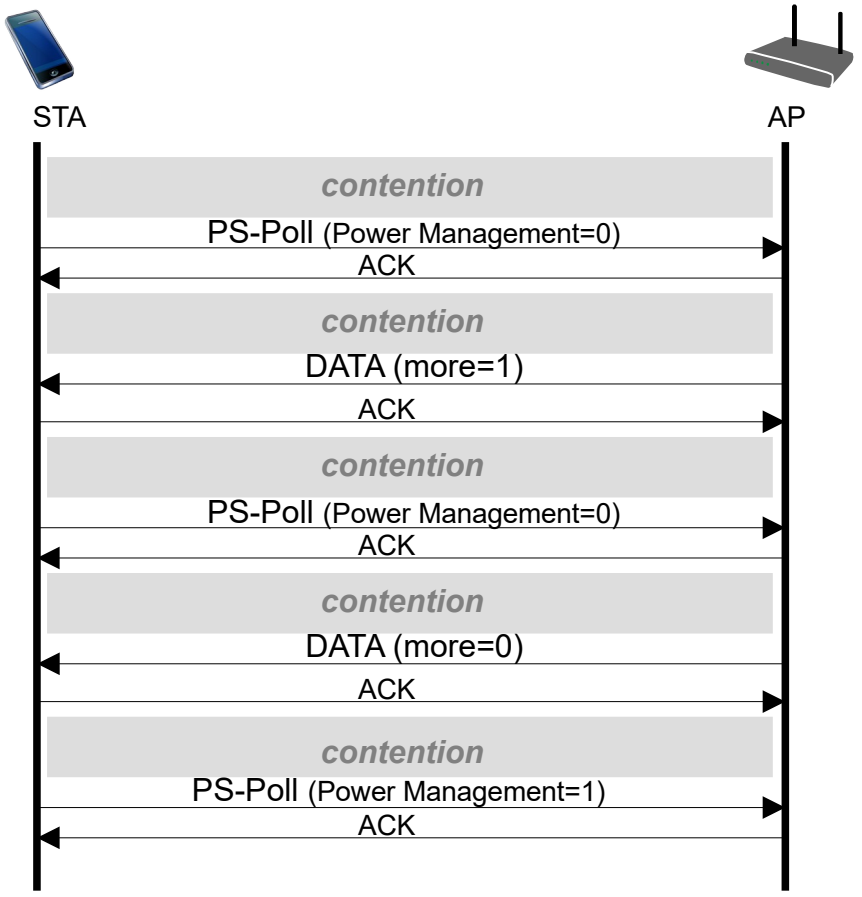
- APs in infrastructure networks send recurrently Beacons.
  - Beacon is a broadcast frame send out at Beacon intervals, usually about every 100ms.
  - Beacon contains a timestamp value, the SSID, and further information about offered services.
- Beacon transmissions may be delayed by CSMA deferral.
  - Subsequent transmissions recur at expected Beacon Interval
    - not relative to last Beacon transmission
- Timestamp contains timer value at transmit time.
  - Each station maintains a local clock that is synchronized through the timestamp

Legacy Power Management Procedure



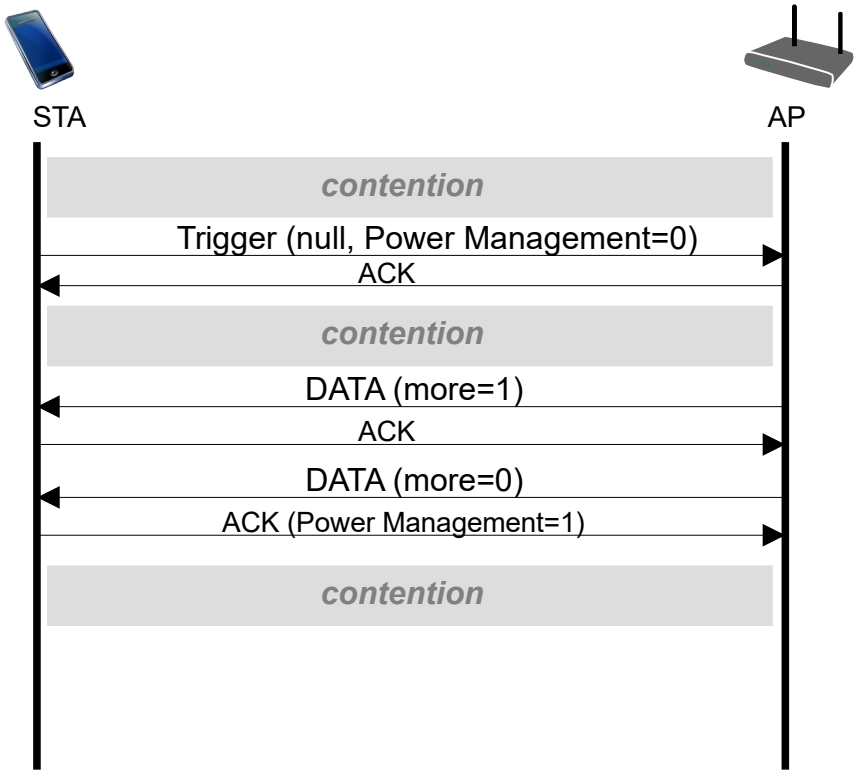
- AP operates as proxy for ‘sleeping’ Stations
  - AP buffers frames destined for sleeping stations and indicates availability of buffered frames in the Traffic Indication Map (TIM)
  - DTIM (Delivery Traffic Indication Map): TIM at which buffered broadcast/multicast frames are transmitted afterwards
  - Associated Stations can register at AP that they will go into a Power-Save mode disabling even their receivers for most of the time
- STAs have to wake up at least shortly prior to an expected DTIM
  - STAs have to act if TIM indicates that frames are buffered for particular STA
    - STA sends PS-Poll and stays awake to receive data
  - Else STA goes back to Power-Save state

Legacy Power Save messaging for retrieving buffered data



- After detecting buffered data in TIM, STA sends PS-Poll frame to AP to request delivery.
- AP sends buffered data potentially requiring multiple transmissions.
- Multiple channel assessment procedures (potentially with contention) needed.
- STA has to stay awake for lengthy periods through multiple contention periods.

Unscheduled Automatic Power Save Delivery (U-APSD)



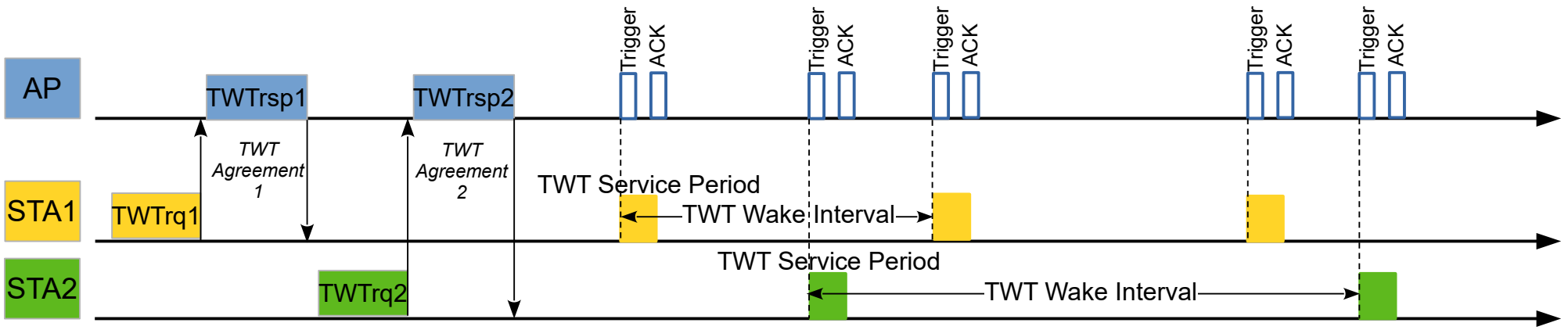
- Through U-APSD all buffered data is retrieved within one transmission cycle.
- STA sends trigger frame (e.g. null data frame) with Power Management=0
- When receiving data frame from STA, AP immediately responds with sending all buffered data to STA
  - Potentially within one burst
- STA goes back in sleep mode directly after transmission

WMM Power Save certification

- Optional amendment to Wi-Fi Alliance QoS (Wireless Multi-Media) certification
- Comprises legacy Power Save Procedure as well as U-APSD
- Additional functions to enhance power save efficiency:
  - Basic Service Set Max Idle Period
    - Basic Service Set Max Idle Period indicates the maximum time period of clients not being active (sending frames to AP).
    - Can be set to maximum 18 hours without being disconnected.
  - Directed Multicast Service
    - Directed Multicast Service (DMS) enables devices to request that APs transmit multicast and broadcast frames directly to the device using more efficient unicast frame transmissions.
    - Transmission rates for DMS can (might) be hundreds of megabits per second faster than regular multicast frames.
  - Proxy Address Resolution Protocol
    - AP knows about the hardware address and the internet address of all associated client devices.
    - Instead of sending ARP messages to the devices, APs directly respond to Proxy ARP requests on behalf of the device.
  - Proxy Neighbor Discovery
    - IPv6 uses the Neighbor Discovery protocol instead of ARP.
    - Proxy Neighbor Discovery service responds to Neighbor Solicitation Message with a Neighbor Advertisement Message on behalf of an associated client.

Target Wake Time (TWT) power save procedure

- Initially introduced by IEEE 802.11ah (HaLow) and taken over to Wi-Fi since Wi-Fi 6.
- STAs that expect to sleep for some period of time can negotiate a TWT contract with the AP.
- The AP stores any traffic destined for the STA until the TWT is reached.
- When the STA wakes at the prescribed time, it listens for its beacon and engages the AP to receive and transmit any data required before returning to its sleep state.
- The TWT wake intervals can be very short (microseconds) to very long (up to 4 years).



Target Wake Time (TWT) variations

- Individual TWT
  - Each STA negotiates its own sleep periods with the AP
- Broadcast TWT
  - AP provides sleep periods for a group of STAs and provides schedules through Beacons
- Opportunistic Power Save
  - AP divides beacon period into sub intervals and instructs STAs in which sub interval they will be served.
- Restricted TWT (introduced in Wi-Fi 7)
  - Possibility to instruct STAs to terminate their transmissions before a TWT service period begins (to avoid any collisions).

- Benefits of Target Wake Times:
  - Wake-up time and channel access spread out.
  - Allows AP to minimize contention through scheduling activity periods of STAs.
  - Reduces awake time for STAs to minimize power consumption.

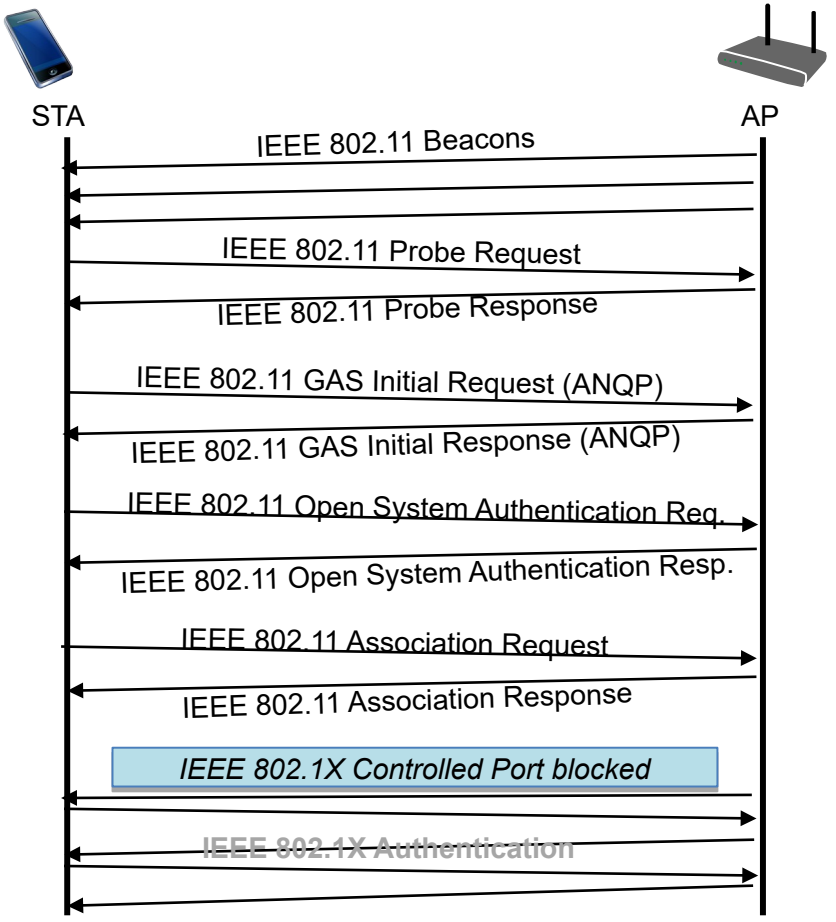
Wi-Fi MAC Layer Management

SESSION MANAGEMENT

Session Management - Overview

- Scanning for available networks and node of attachments
  - Beaconing
  - Active/passive scanning
- Network selection
  - Generic Advertisement Service
    - Pre-association information query
- Authentication
- Association/Disassociation/Re-association
  - Association: Joining a WLAN network
    - Session establishment
  - Disassociation: Detaching from an AP
    - Session termination
  - Re-association: Transfer of connectivity from one AP to another AP
    - Mobility management

IEEE 802.11session establishment



- Scanning
  - Beacon
  - Probe Request/Response
- Network Selection
  - GAS (ANQP Request/Response)
- Authentication
  - For legacy reasons OpenSystem Authentication Request/Response retained
    - Initially no use of IEEE 802.1X
- Association
  - Association Request/Response
- 802.1X Authentication/Authorization
  - IEEE 802.1X EAPoL follows association message exchange
    - Controlled port blocked
    - Uncontrolled port used for exchange of authentication messages
  - Authorization provided by AAA server to AP for configuration of data path

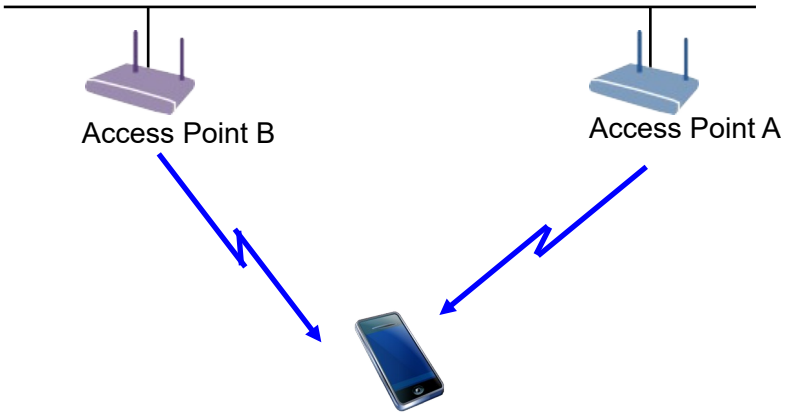
Wi-Fi MAC Layer – Session Management

SCANNING

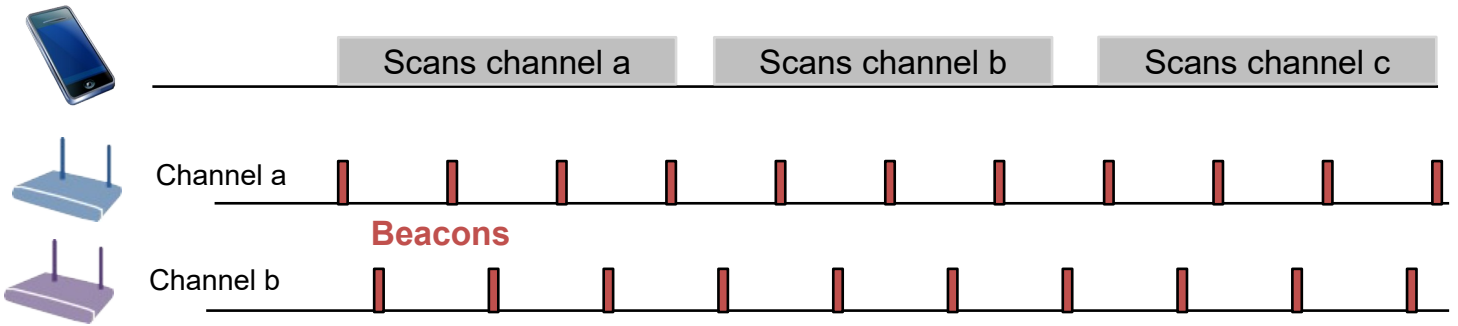
Scanning

- Scanning is process of finding available APs and WLANs
  - WLANs identified by Service Set Identifier (SSID)
    - SSID is an arbitrary human readable network name with up to 32 ASCII characters
    - All APs of a WLAN (= Extended Service Set) have the same SSID
      - SSIDs are not necessarily unique
    - To enable unique WLAN names, SSID can be amended by Homogeneous Extended Service Set Identifier (HESSID)
      - HESSID is a MAC address (BSSID) of one of the APs of the ESS
  - APs identified by Basic Service Set Identifier (BSSID)
    - BSSID is the MAC address used in the radio transmission frames as AP address
- WLAN identification information can be detected
  - Either by decoding information carried in the Beacons
    - Passive Scanning
  - Or by sending out broadcast frames querying responses with WLAN identification information from adjacent Aps
    - Active Scanning

Passive scanning

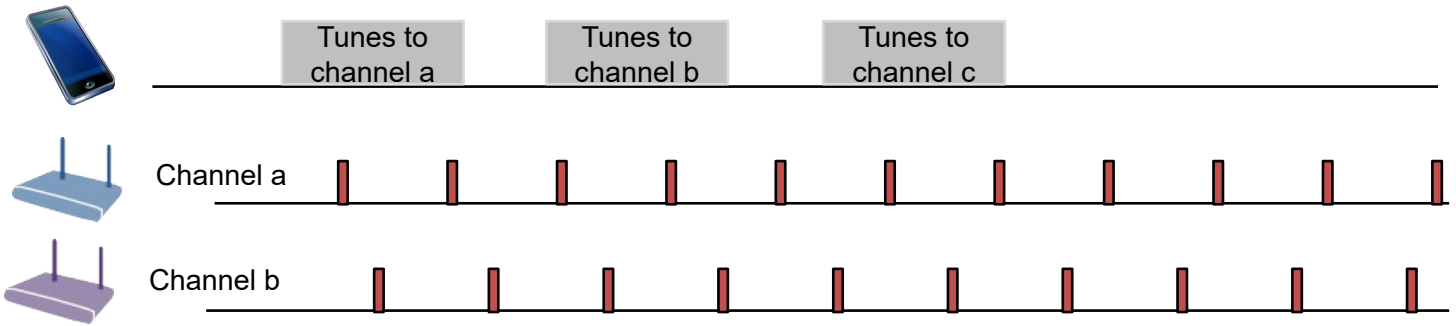


- APs send Beacons every 100..200ms
- STA subsequently tunes to all channels and listens for Beacons
- To successfully detect all Beacons, STA stays on a channel for about 200-300ms
- Scan of 2.4 GHz band takes about 2.5-4 s



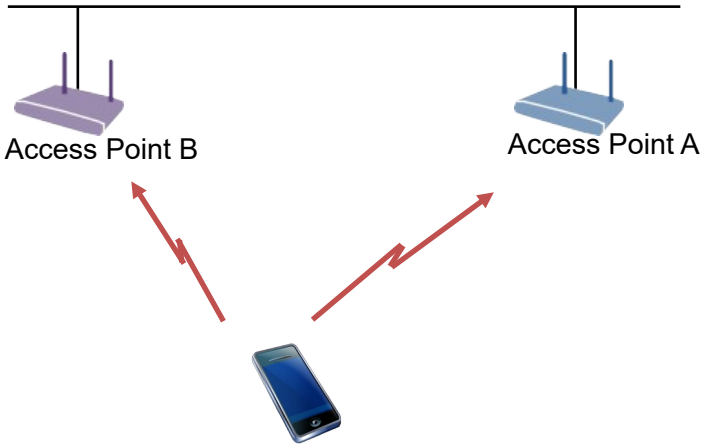
Active scanning

- STA tunes to all channels an sends Probe Requests.
- APs respond within a few ms.
- Query can either be directed to a particular WLAN or can send to all WLAN to respond.
- Even when transmitter is engaged in STA, active scanning is often more power effective.

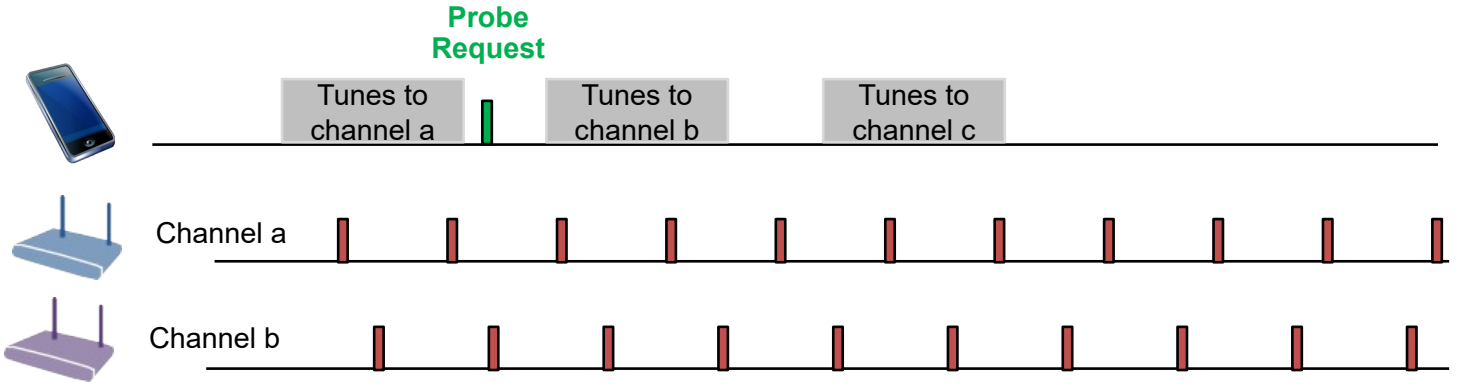


Active scanning

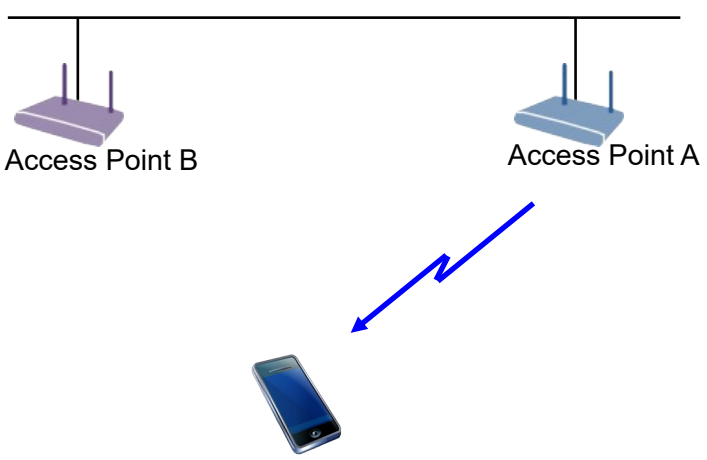
Station broadcasts Probe Request.



- STA tunes to all channels an sends Probe Requests.
- APs respond within a few ms.
- Query can either be directed to a particular WLAN or can send to all WLAN to respond.
- Even when transmitter is engaged in STA, active scanning is often more power effective.

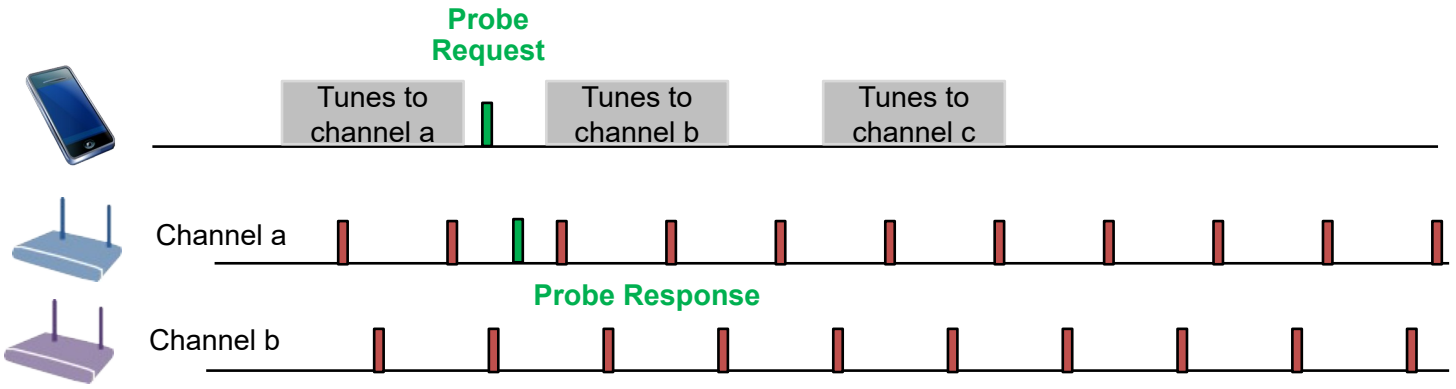


Active scanning



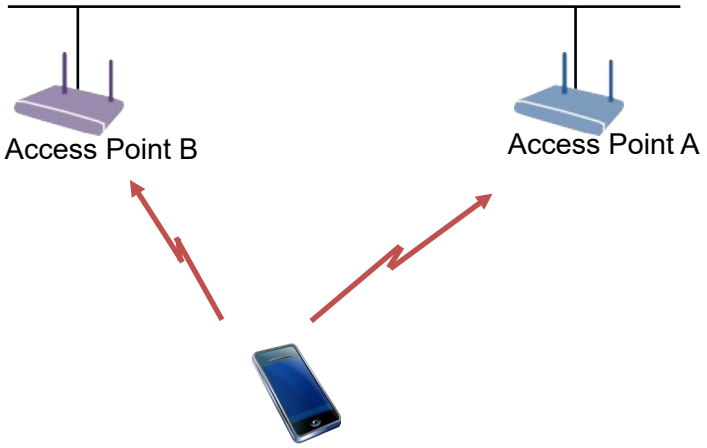
APs send Probe Response.

- STA tunes to all channels an sends Probe Requests.
- APs respond within a few ms.
- Query can either be directed to a particular WLAN or can send to all WLAN to respond.
- Even when transmitter is engaged in STA, active scanning is often more power effective.

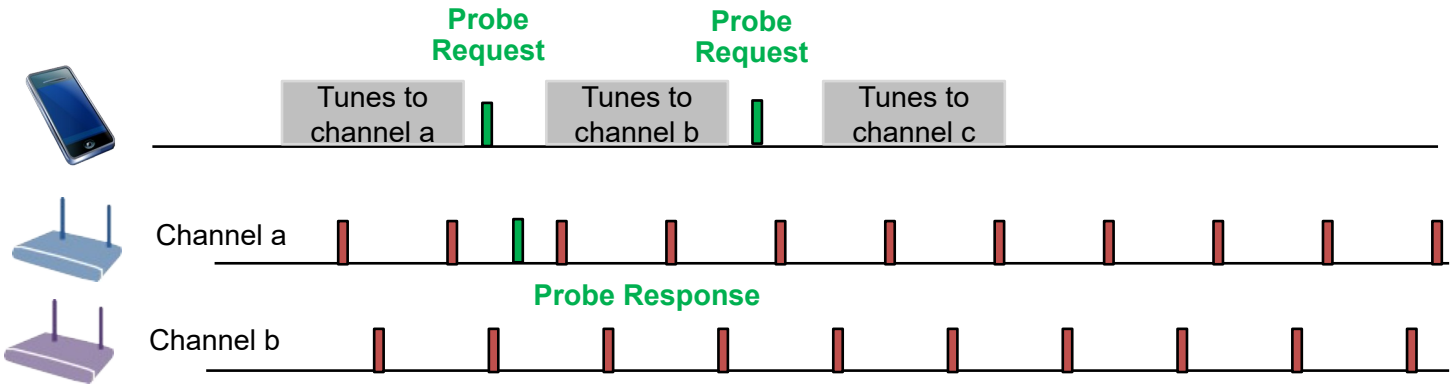


Active scanning

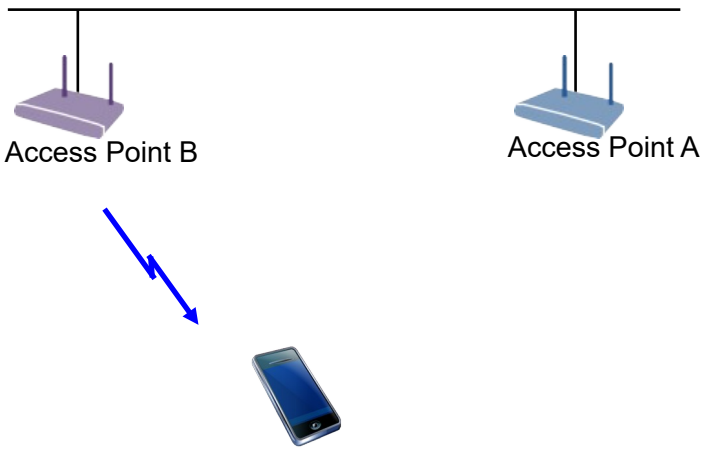
Station broadcasts Probe Request.



- STA tunes to all channels an sends Probe Requests.
- APs respond within a few ms.
- Query can either be directed to a particular WLAN or can send to all WLAN to respond.
- Even when transmitter is engaged in STA, active scanning is often more power effective.

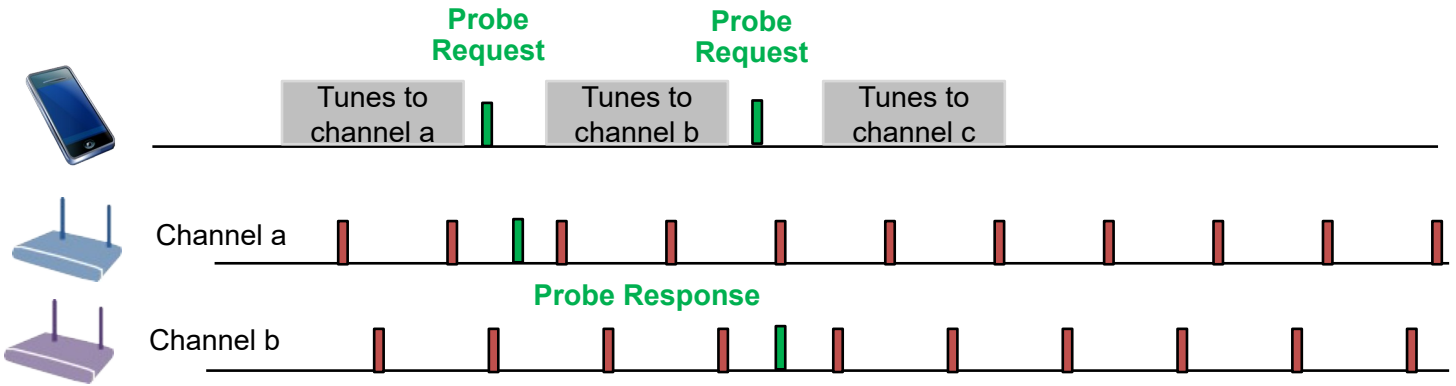


Active scanning

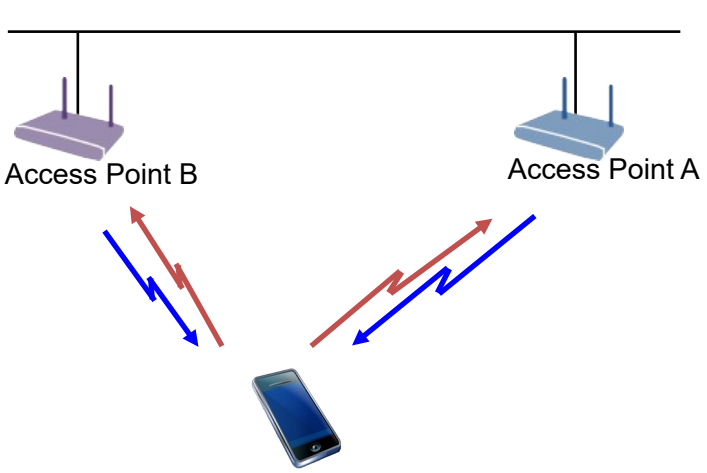


APs send Probe Response.

- STA tunes to all channels an sends Probe Requests.
- APs respond within a few ms.
- Query can either be directed to a particular WLAN or can send to all WLAN to respond.
- Even when transmitter is engaged in STA, active scanning is often more power effective.



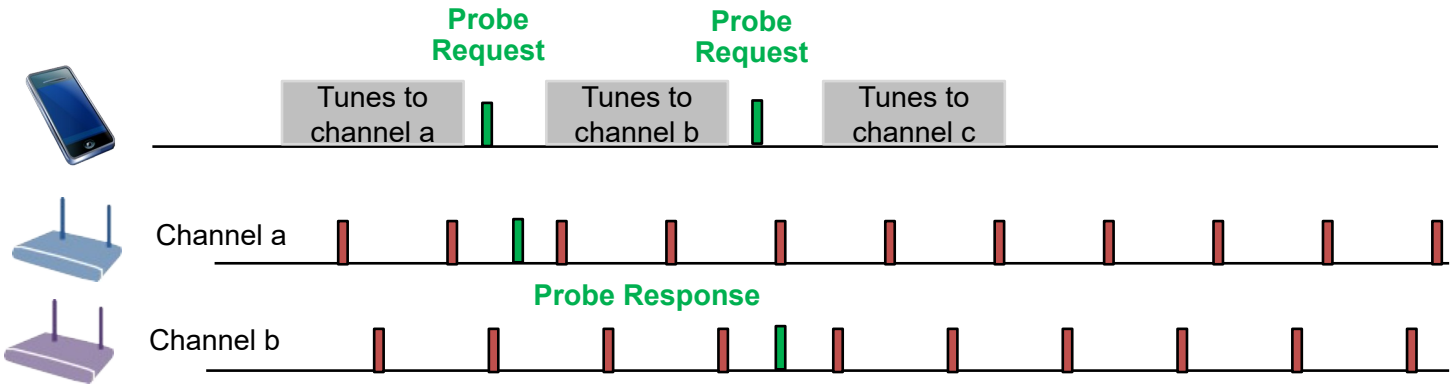
Active scanning



Station broadcasts Probe Request.

APs send Probe Response.

- STA tunes to all channels an sends Probe Requests.
- APs respond within a few ms.
- Query can either be directed to a particular WLAN or can send to all WLAN to respond.
- Even when transmitter is engaged in STA, active scanning is often more power effective.



Wi-Fi MAC Layer – Session Management

NETWORK SELECTION

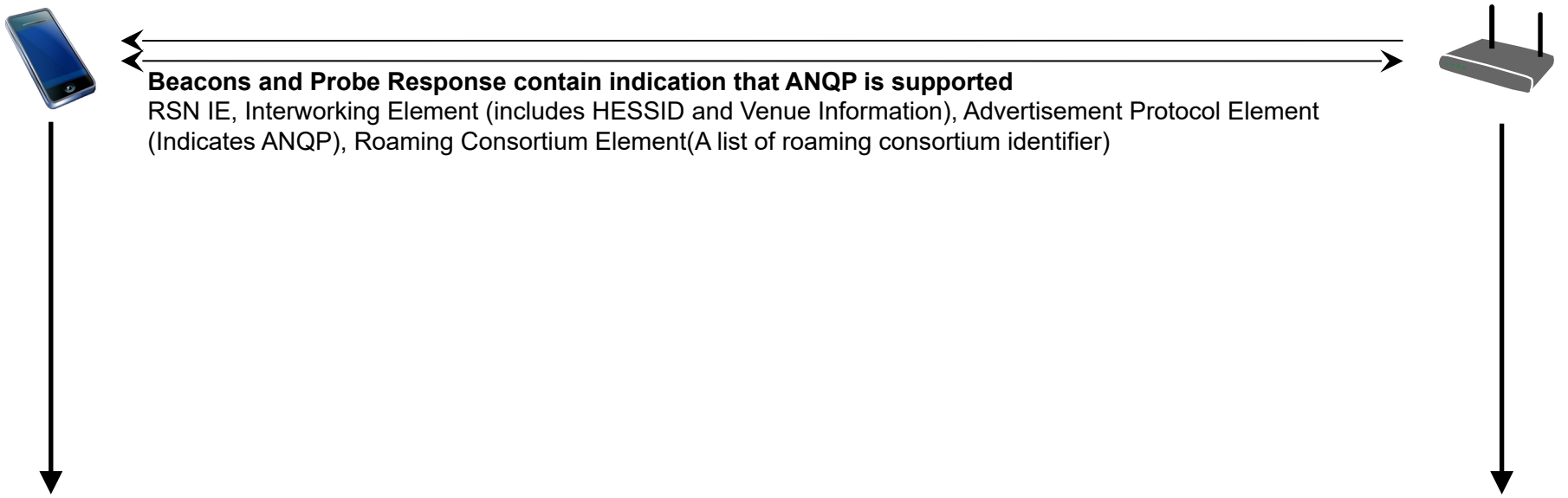
Generic Advertisement Service

- A Wi-Fi terminal scans the air for finding the near-by access points
  - Either by passive scanning (Beacon)
  - or by active scanning (Probe Request & Probe Response)
- Questions arising when discovering an access point:

  - ***Is this my Home Service Provider?***
  - ***Is this a Visited Service Provider?***
  - ***Will this Service Provider offer the services I need?***
  - ***Do I need any provisioning for this Service Provider?***

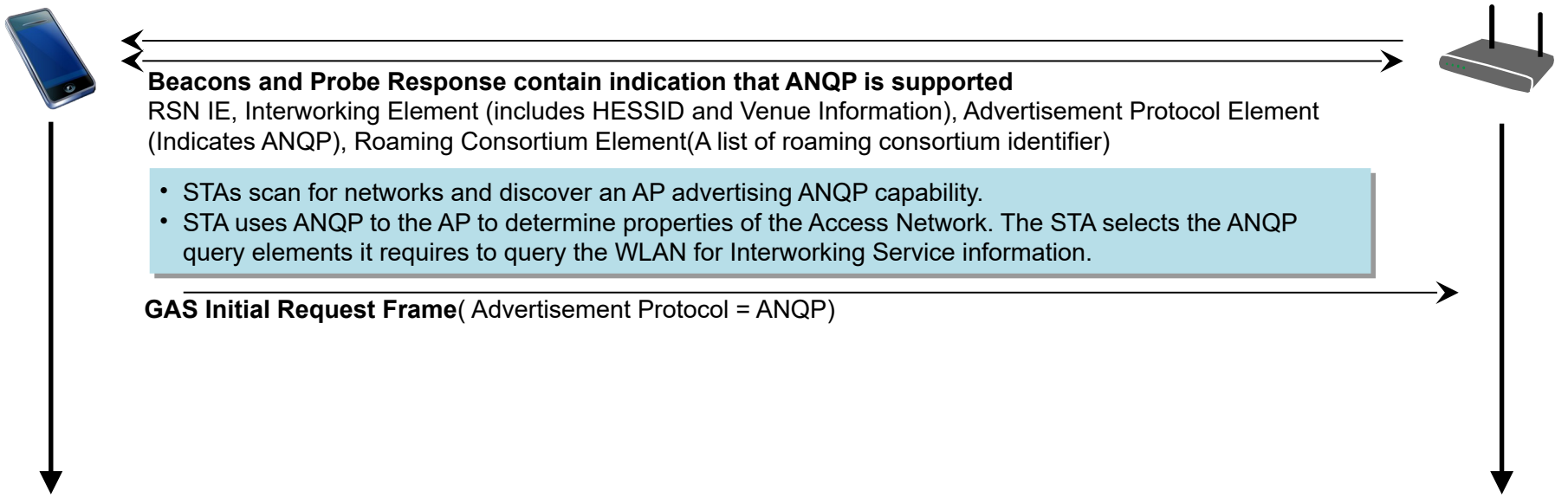
- The information in the beacon or probe response is often not sufficient to make the appropriate decision
- Introduced by 802.11u, IEEE 802.11 defines a protocol allowing to query additional information about the Wi-Fi access before initiating the association and authentication
- GAS (Generic Advertisement Service) provides a container for the ANQP (Access Network Query Protocol), which provides more information about the Wi-Fi access

Network discovery by ANQP



Beacons and Probe Response contain indication that ANQP is supported
RSN IE, Interworking Element (includes HESSID and Venue Information), Advertisement Protocol Element (Indicates ANQP), Roaming Consortium Element(A list of roaming consortium identifier)

Network discovery by ANQP

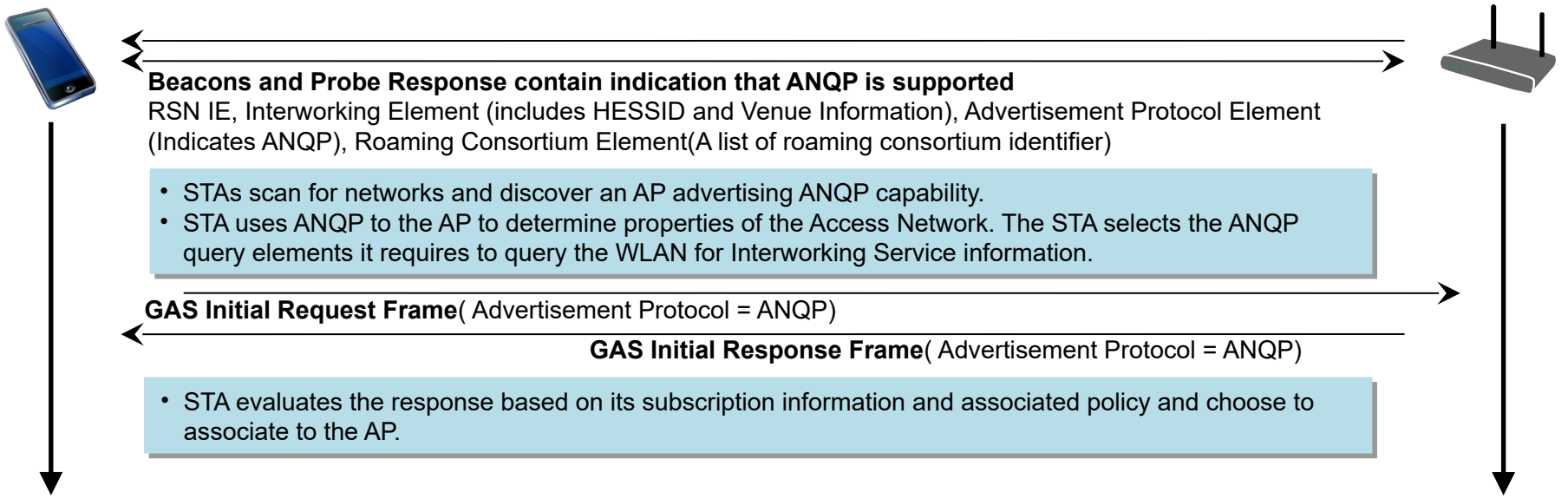


Beacons and Probe Response contain indication that ANQP is supported
RSN IE, Interworking Element (includes HESSID and Venue Information), Advertisement Protocol Element (Indicates ANQP), Roaming Consortium Element(A list of roaming consortium identifier)

- STAs scan for networks and discover an AP advertising ANQP capability.
- STA uses ANQP to the AP to determine properties of the Access Network. The STA selects the ANQP query elements it requires to query the WLAN for Interworking Service information.

GAS Initial Request Frame(Advertisement Protocol = ANQP)

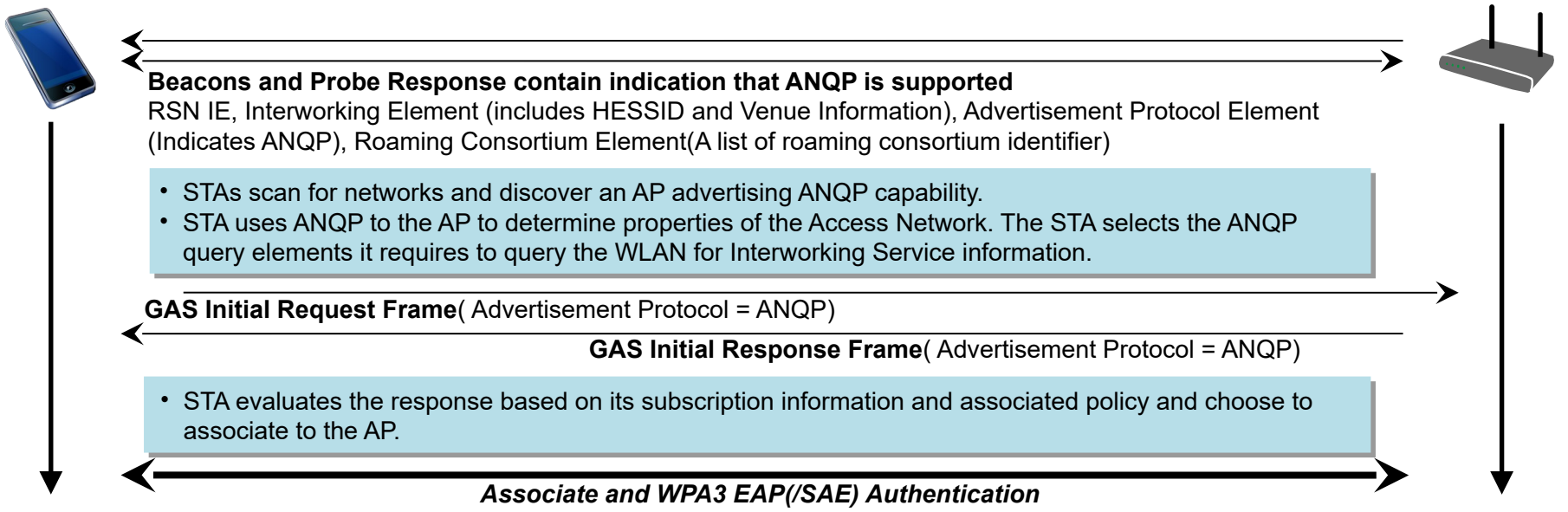
Network discovery by ANQP



ANQP Attributes

- Venue Name
- Network Authentication Type
- Roaming Consortium
- IP Address Type Availability
- NAI Realm
- 3GPP Cellular Network
- Domain Name

Network discovery by ANQP



ANQP Attributes

- Venue Name
- Network Authentication Type
- Roaming Consortium
- IP Address Type Availability
- NAI Realm
- 3GPP Cellular Network
- Domain Name

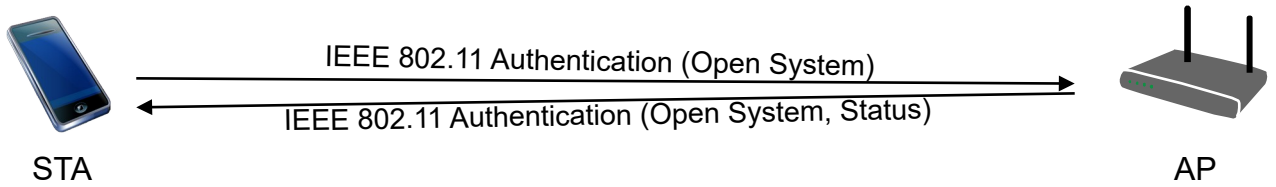
ANQP Attributes

- Venue Name
  - Provides zero or more venue names associated with the BSS to support the user's selection.
- Network Authentication Type
  - Provides a list of authentication types carrying additional information like support for online enrollment or redirection URL.
- Roaming Consortium
  - Provides a list of information about the Roaming Consortium or Subscription Service Providers (SSPs) whose networks are accessible via this AP.
- IP Address Type Availability
  - Provides STA with the information about the availability of IP address version and type that could be allocated to the STA after successful association.
- NAI Realm
  - Provides a list of Network Access Identifier (NAI) realms corresponding to SSPs or other entities whose networks or services are accessible via this AP; optionally amended by the list of EAP Method, which are supported by the SSPs.
- 3GPP Cellular Network
  - Contains cellular information such as network advertisement information e.g., network codes and country codes to assist a 3GPP non-AP STA in selecting an AP to access 3GPP networks.
- Domain Name
  - Provides a list of one or more domain names of the entity operating the IEEE 802.11 access network.

Wi-Fi MAC Layer – Session Management

AUTHENTICATION

Authentication

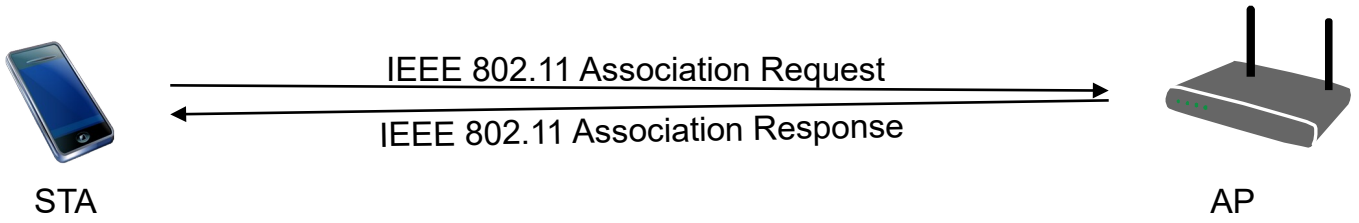


- Authentication before association is ‘leftover’ of legacy IEEE Stds 802.11 without WPA2/3 support (prior to IEEE 802.11i/RSN).
- For conformance and compatibility reasons Open System Authentication is performed, which only checks for the MAC addresses of the STA.
  - In legacy IEEE 802.11, AP could authenticate STA by its WEP (Wire Equivalent Privacy).
    - WEP is depreciated now.
- Open System Authentication is the only check performed in unencrypted WLAN
  - MAC address authentication is often used to bypass captive portal in public access for ‘known’ users.
- Other methods for pre-association authentication can be used for Fast Transition (FT Authentication) and Mesh Networking (simultaneous authentication under equals (SAE)).

Wi-Fi MAC Layer – Session Management

ASSOCIATION

Association



- Association establishes the data connection at the AP by assigning a virtual port for the STA
  - The STA sends an Association Request message containing its Listen Interval, various capabilities, the SSID to join and the supported transmission rates.
  - The AP checks for the acceptance of the parameters send in the Association Request frame and sends back an Association Response message, which contains an Association ID (AID), which allows unique identification of a station at the AP
    - AIDs are also needed for power management
- Once virtual port is available, Ethernet frames can be exchanged between STA and AP

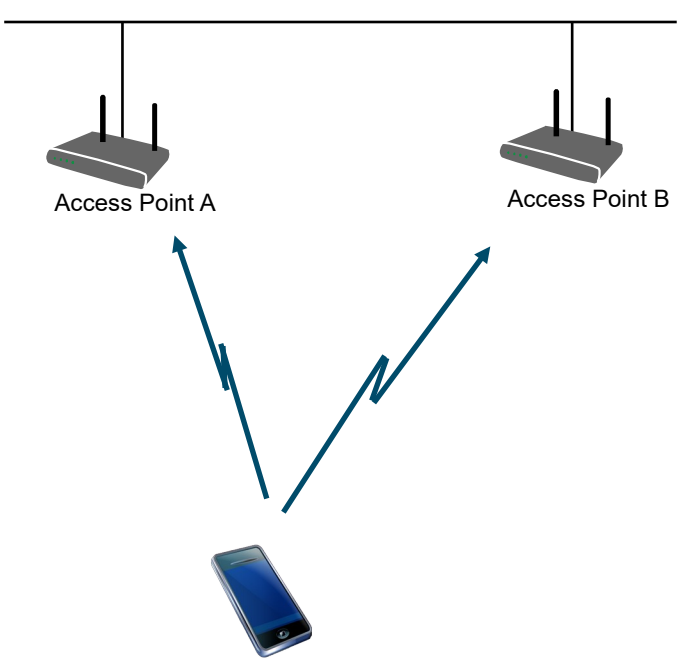
Disassociation, Re-association

- Disassociation
  - Frame containing a reason code for termination of an association
- Re-association
  - Special form of Association procedure to support reconnection to another AP of the same ESS
  - Request frame additionally contains BSSID of previous AP
    - Allows new AP to contact previous AP for transfer of previous session info and pending data frames
  - Re-association is used for realizing ‘mobility’ in IEEE 802.11 within the same ESS (SSID).

Wi-Fi MAC Layer – Session Management

INITIAL CONNECTION SETUP

Message sequence for successful connection setup

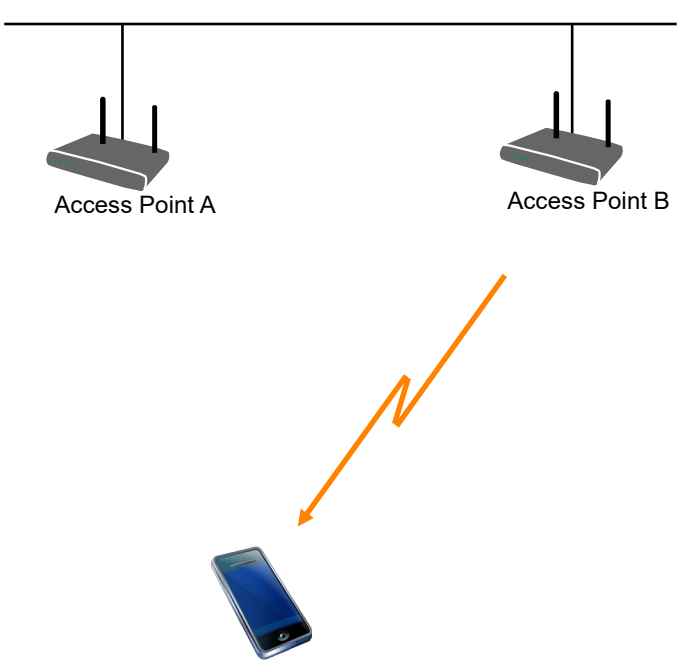


Connection establishment with active scanning but without network selection by ANQP

Details:

← Station sends Probe Request

Message sequence for successful connection setup



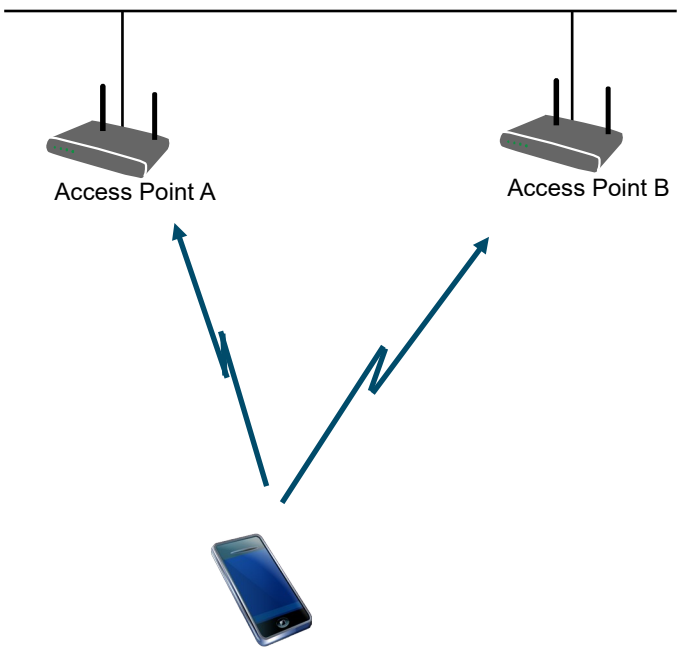
Connection establishment with active scanning but without network selection by ANQP

Details:

Station sends Probe Request

APs send Probe Response

Message sequence for successful connection setup

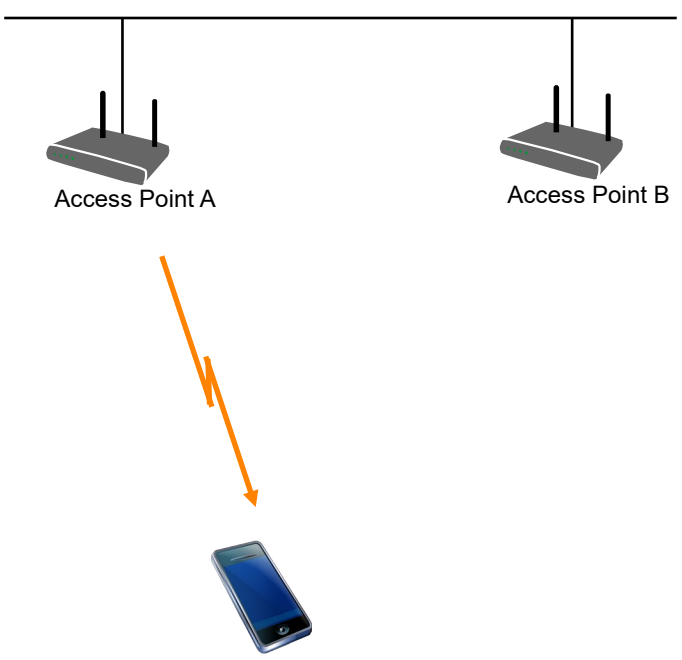


Connection establishment with active scanning but without network selection by ANQP

Details:

- Station sends Probe Request
- APs send Probe Response
- Station sends Probe Request

Message sequence for successful connection setup



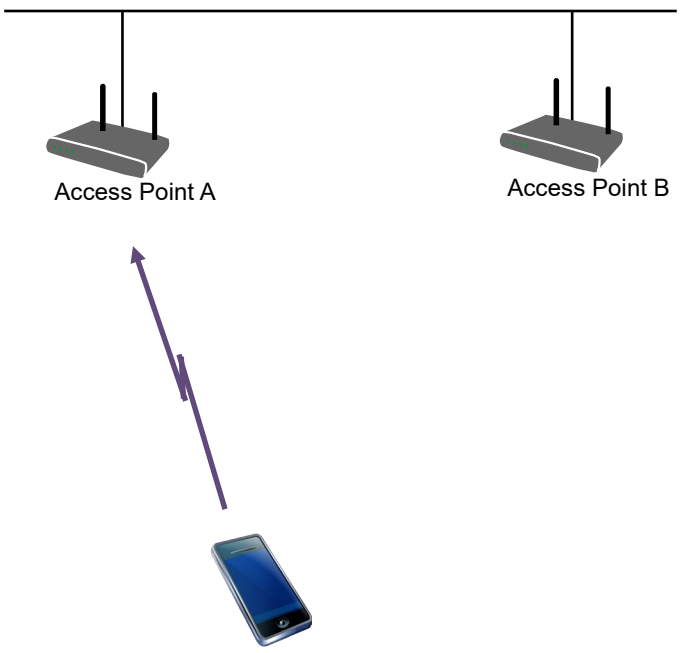
Connection establishment with active scanning but without network selection by ANQP

Details:

- ← Station sends Probe Request
- → APs send Probe Response
- ← Station sends Probe Request
- → APs send Probe Response

=> Station chooses best AP

Message sequence for successful connection setup

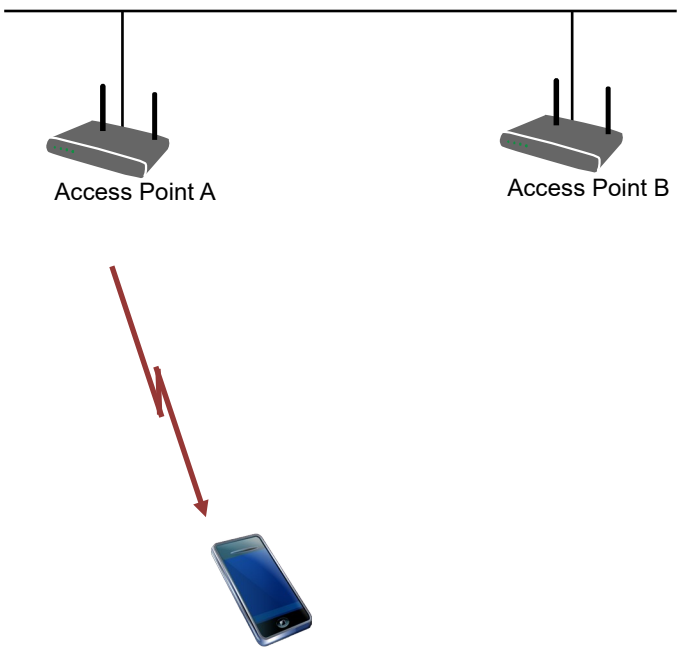


Connection establishment with active scanning but without network selection by ANQP

Details:

- Station sends Probe Request
- APs send Probe Response
- Station sends Probe Request
- APs send Probe Response
- => Station chooses best AP
- Station sends Authentication Request to the chosen AP

Message sequence for successful connection setup

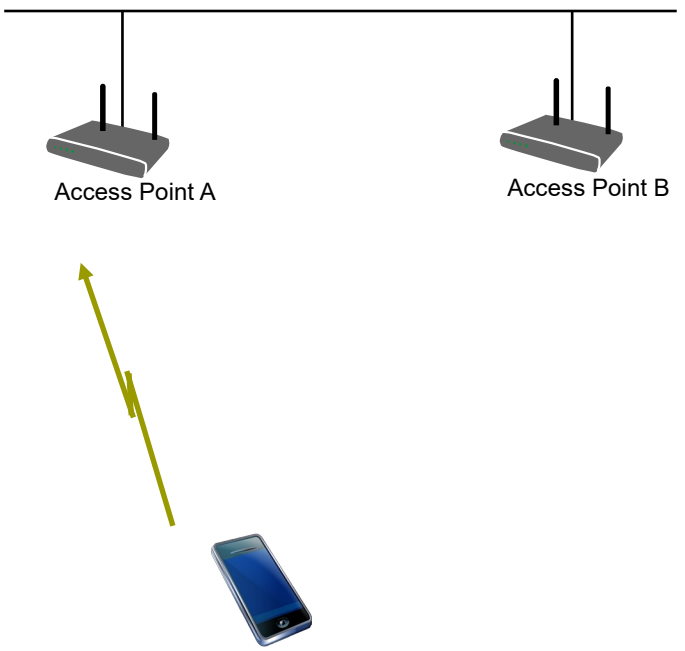


Connection establishment with active scanning but without network selection by ANQP

Details:

- Station sends Probe Request
- APs send Probe Response
- Station sends Probe Request
- APs send Probe Response
- => Station chooses best AP
- Station sends Authentication Request to the chosen AP
- AP sends Authentication Response (success)

Message sequence for successful connection setup

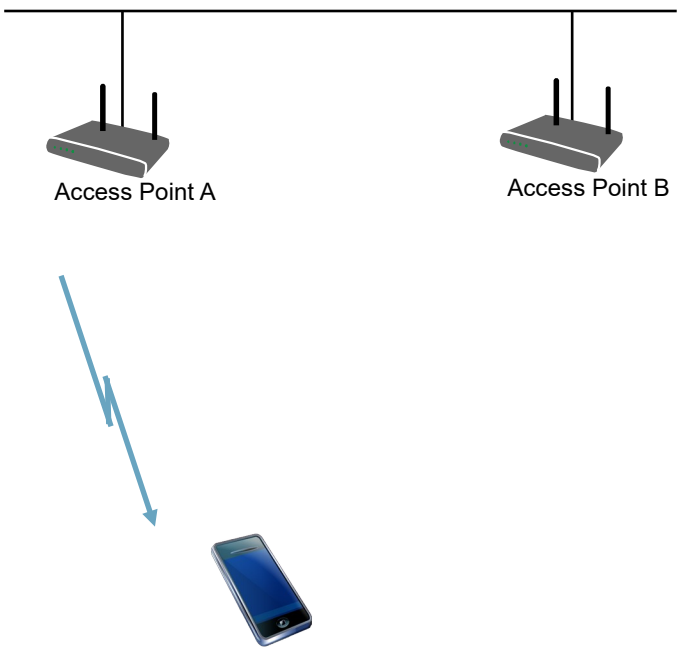


Connection establishment with active scanning but without network selection by ANQP

Details:

- Station sends Probe Request
- APs send Probe Response
- Station sends Probe Request
- APs send Probe Response
- => Station chooses best AP
- Station sends Authentication Request to the chosen AP
- AP sends Authentication Response (success)
- STA sends Association Request to the chosen AP

Message sequence for successful connection setup



Connection establishment with active scanning but without network selection by ANQP

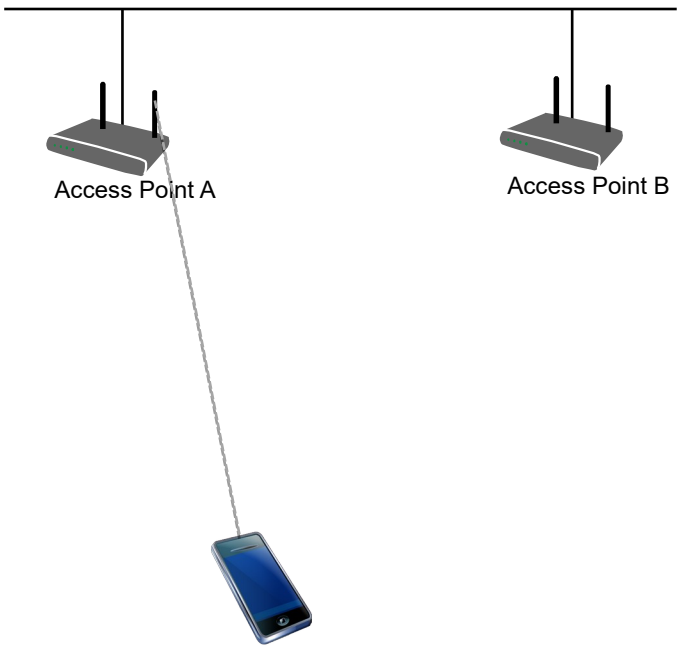
Details:

- Station sends Probe Request
- APs send Probe Response
- Station sends Probe Request
- APs send Probe Response

=> Station chooses best AP

- Station sends Authentication Request to the chosen AP
- AP sends Authentication Response (success)
- STA sends Association Request to the chosen AP
- AP sends Association Response (success)

Message sequence for successful connection setup

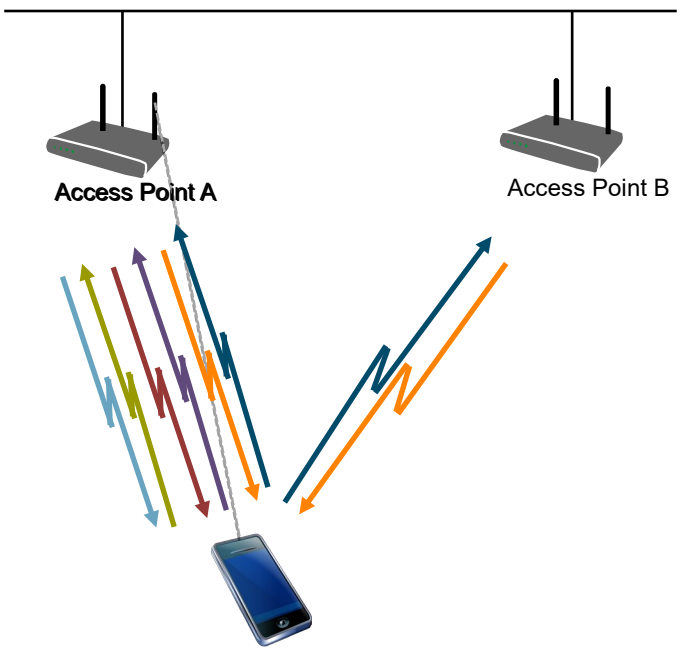


Connection establishment with active scanning but without network selection by ANQP

Details:

- Station sends Probe Request
- APs send Probe Response
- Station sends Probe Request
- APs send Probe Response
- => Station chooses best AP
- Station sends Authentication Request to the chosen AP
- AP sends Authentication Response (success)
- STA sends Association Request to the chosen AP
- AP sends Association Response (success)
- L2 connection established

Message sequence for successful connection setup



Connection establishment with active scanning but without network selection by ANQP

Details:

- Station sends Probe Request
- APs send Probe Response
- Station sends Probe Request
- APs send Probe Response

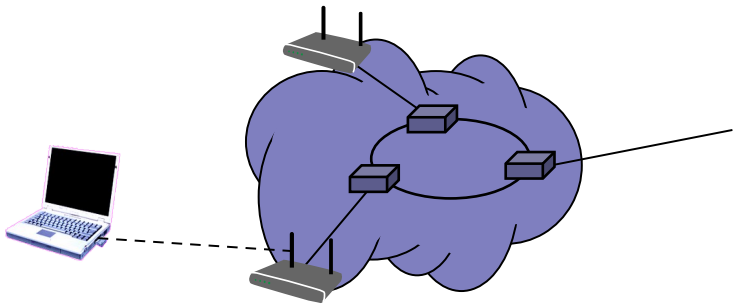
=> Station chooses best AP

- Station sends Authentication Request to the chosen AP
- AP sends Authentication Response (success)
- STA sends Association Request to the chosen AP
- AP sends Association Response (success)
- L2 connection established

Wi-Fi MAC Layer – Session Management

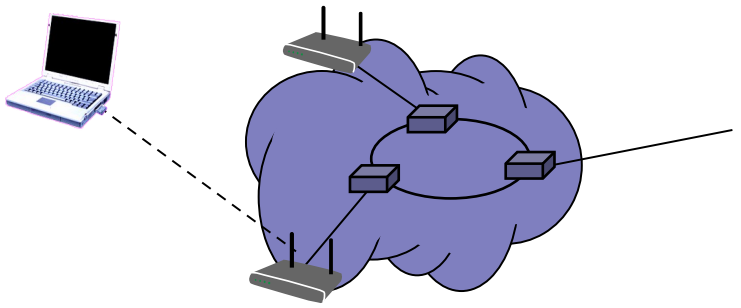
TRANSITION TO ANOTHER AP

Mobility inside an ESS by link layer functions



Mobility inside an ESS by link layer functions

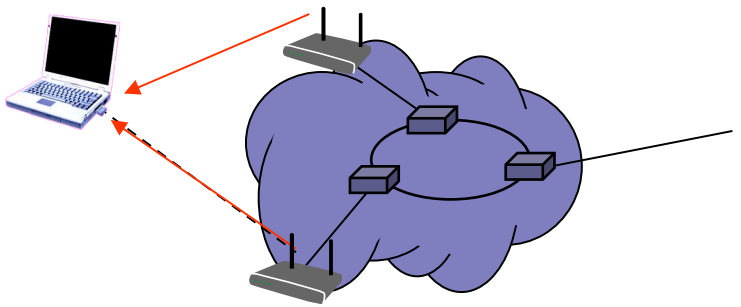
Station decides that link to its current AP is poor…



Mobility inside an ESS by link layer functions

Station decides that link to its current AP is poor…

- **Station uses scanning function to find another AP**
  - or uses information from previous scans

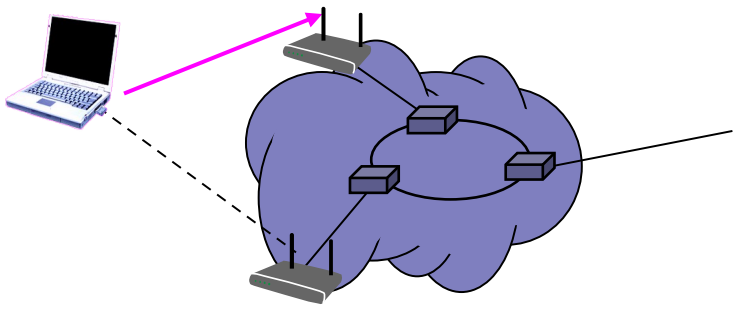


Local distribution network

Mobility inside an ESS by link layer functions

Station decides that link to its current AP is poor…

- **Station uses scanning function to find another AP**
  - or uses information from previous scans
- **Station sends Re-association Request to new AP**

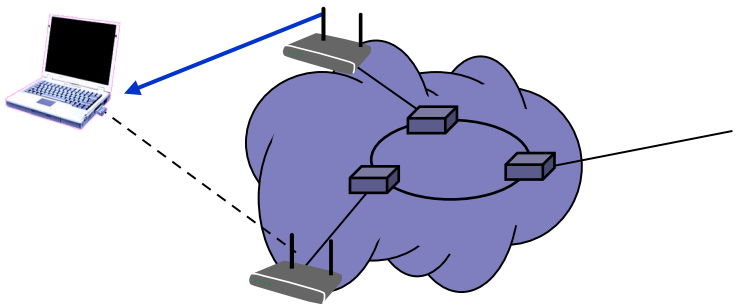


Process shown without reestablishing the security context!

Mobility inside an ESS by link layer functions

Station decides that link to its current AP is poor…

- **Station uses scanning function to find another AP**
  - or uses information from previous scans
- **Station sends Re-association Request to new AP**
- **If Re-association Response is successful**
  - then station has roamed to the new AP
  - else station scans for another AP

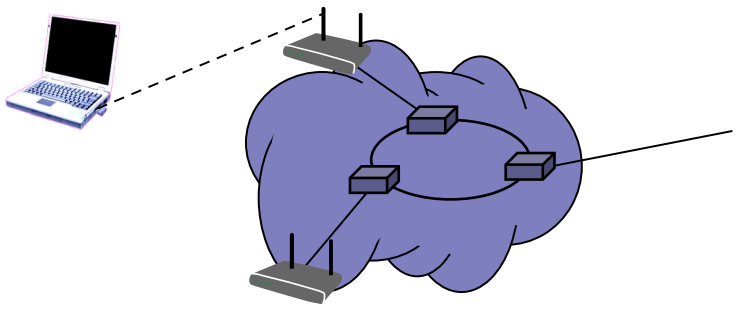


Process shown without reestablishing the security context!

Mobility inside an ESS by link layer functions

Station decides that link to its current AP is poor…

- **Station uses scanning function to find another AP**
  - or uses information from previous scans
- **Station sends Re-association Request to new AP**
- **If Re-association Response is successful**
  - then station has roamed to the new AP
  - else station scans for another AP
- **If AP accepts Re-association Request**
  - Normally old AP is notified through Distribution System
  - AP indicates Re-association to the Distribution System

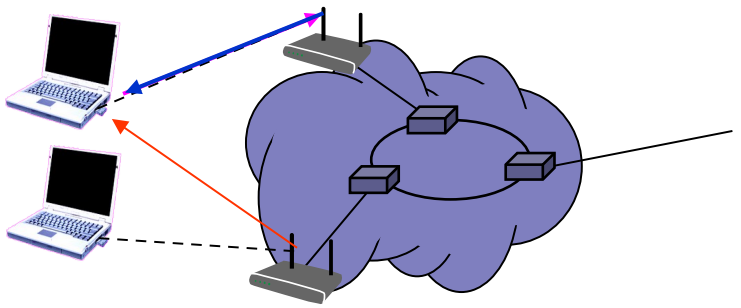


Process shown without reestablishing the security context!

Mobility inside an ESS by link layer functions

Station decides that link to its current AP is poor…

- **Station uses scanning function to find another AP**
  - or uses information from previous scans
- **Station sends Re-association Request to new AP**
- **If Re-association Response is successful**
  - then station has roamed to the new AP
  - else station scans for another AP
- **If AP accepts Re-association Request**
  - Normally old AP is notified through Distribution System
  - AP indicates Re-association to the Distribution System



Process shown without reestablishing the security context!

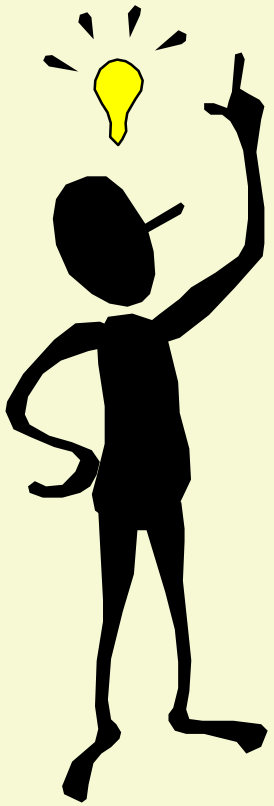
Handoff Time

- Total handoff time not deterministic but influenced by statistical variations of multiple protocol steps
  - Main variation by scanning procedure and period (~ 90%)
  - Most of the messaging may occur for scanning
  - Actual handoff extremely fast (Reassociation Request & Response)
  - WPA2 security adds another challenge
    - Keying material to be established at the new AP
- Possibilities to reduce the handoff time:
  - Reduce time needed to detect new AP with better radio link
    - periodic scanning, despite being connected to the old AP
    - selective scanning (using only a subset of all possible channels)
    - exploiting other information about neighbor Aps
  - Reduce time to establish security context at new AP
    - Fast roaming support, introduced by 802.11r, allows for pre-establishment of keys

Layer 2 Mobility Considerations

- Link loss detection
  - The STA detects a low signal quality or no signal from the access point
    - Threshold decision (with hysteresis) (fast detection, commonly used)
  - The STA detects an increasing error rate of transmitted MAC frames
    - Slower than previous approach, but may be more predictive
- Requirement for the support of Layer 2 Mobility in WLAN:
  - All access points are connected directly over a single Ethernet
  - Inter access point communication happens by new AP informs infrastructure and previous AP by Layer-2 update frame on the wire
- For larger coverage areas this is not reasonable anymore
  - Layer 2 broadcast domains are of limited size
  - Multiple Distribution Systems are interconnected (usually with routers); Thus, layer 2 handoffs are not possible between the Distribution Systems
  - Solution by handoffs between the Distribution Systems are performed with higher layer mechanisms e.g. Mobile IP

Questions and answers



Mac Sublayer Management Questions…

1) What are the two main functions of the MAC layer systems management?
2) What are beacons in IEEE 802.11?
3) What is the purpose of the timestamp in the Beacons?
4) What is the role of the Delivery Traffic Indication Map for the power management in IEEE 802.11?
5) What does TWT mean, and through which method does it provides better power management than legacy TIM?
6) Which sequence of MAC management procedures is necessary for Wi-Fi session establishment?
7) What is the purpose of scanning?
8) Explain the difference between active scanning and passive scanning.
9) What stands 'GAS' in IEEE 802.11 for?
10) What is the purpose of ANQP in IEEE 802.11?
11) What is the purpose of IEEE 802.11 association procedure?
12) What is a Reassociation in IEEE 802.11?
13) Please explain the MAC procedures for handover from on AP to another AP of the same ESS.
14) What are the limitations of Layer 2 mobility management?

Wi-Fi MAC Layer – Session Management

MAC MANAGEMENT ATTRIBUTES

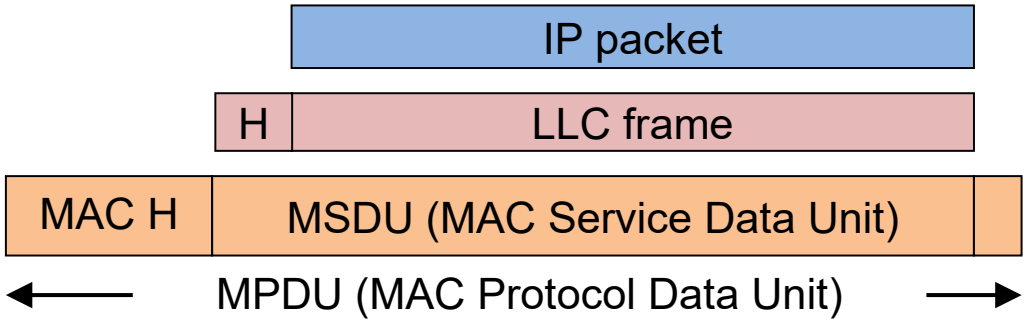
Basic MAC management messages attributes

- Beacon (9.3.3.2)
  - Timestamp, Beacon Interval, Capabilities, ESSID, Supported Rates, Traffic Indication Map, Parameters, … (see Table 9-32)
- Probe Request (9.3.3.9)
  - SSID, Supported Rates, Parameters, … (see Table 9-38)
- Probe Response (9.3.3.10)
  - Timestamp, Beacon Interval, Capabilities, SSID, Supported Rates, Parameters, …. (see Table 9-39)
    - Same as for Beacon except for TIM
- Authentication (9.3.3.11)
  - Authentication algorithm, Transaction number, Status code, Parameters, … (see Table 9-40)
    - Format used for various actions depending on authentication algorithm
- Deauthentication (9.3.3.12)
  - Reason code
- Association Request (9.3.3.5)
  - Capability, Listen Interval, SSID, Supported Rates, … (see Table 9-34)
- Association Response (9.3.3.6)
  - Capability, Status Code, AID, Supported Rates, … (see Table 9-35)
- Reassociation Request (9.3.3.7)
  - Capability, Listen Interval, SSID, Current AP Address, Supported Rates, … (see Table 9-36)
- Reassociation Response (9.3.3.8)
  - Capability, Status Code, AID, Supported Rates, … (see Table 9-37)
- Disassociation (9.3.3.4)
  - Reason code

Wi-Fi MAC Layer

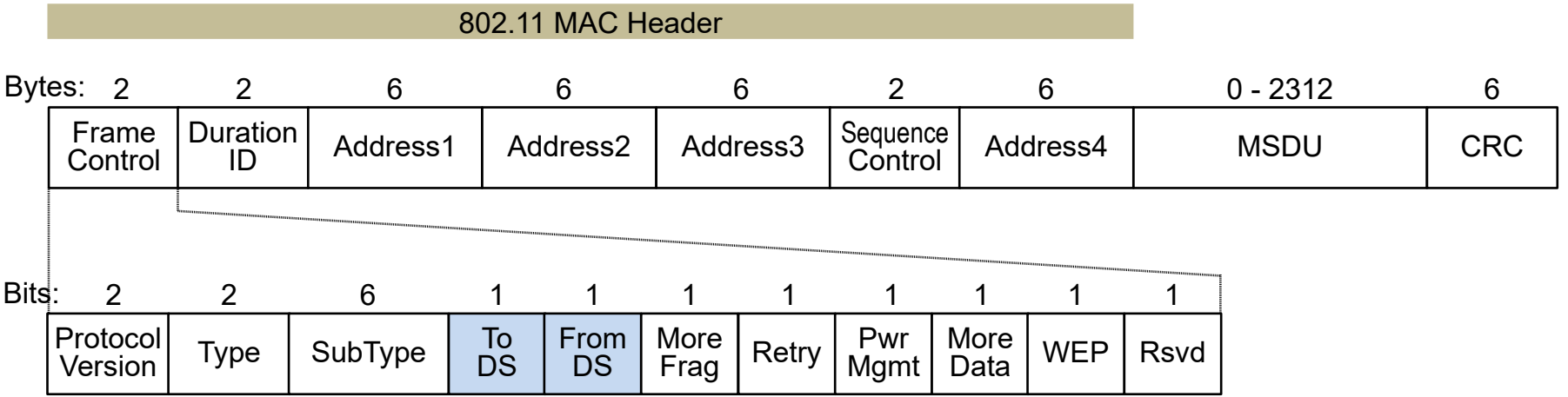
MAC FRAME FORMAT

MAC Frame format overview



- Differences to widely known MAC data units, e.g. Ethernet:
  - Up to 4 address values
    - Necessary to handle the message transfer over the air
  - Different types of MAC data units
    - Data frames for transporting the MAC Service Data Unit
    - Control data units for medium access control, e.g. RTS, CTS, ACK
    - Management data units for the MAC Layer management messages
  - Duration ID field
    - Duration value for the transmission of the frame to allow NAV/virtual sensing
  - Sequence Control fields
    - Fragment Number for marking fragments
    - Sequence Number for marking MAC service data units

IEEE 802.11 MAC Layer Frame Format

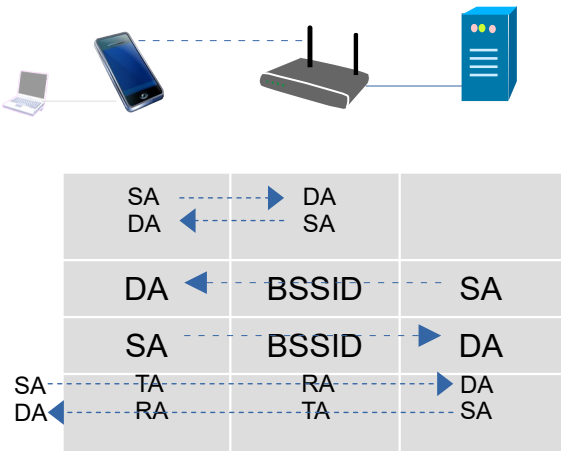


- MAC Header format differs per Type:
  - Control Frames (several fields are omitted)
  - Management Frames
  - MSDU Data Frames
- Includes Sequence Control Field for filtering of duplicate caused by ACK mechanism.

IEEE 802.11 Addressing

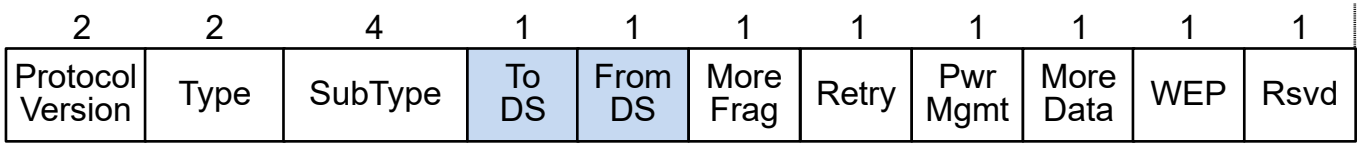
2	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	SubType	To DS	From DS	More Frag	Retry	Pwr Mgmt	More Data	WEP	Rsvd

To DS	From DS	Addr 1	Addr 2	Addr 3	Addr 4
0	0	DA	SA	BSSID	-
0	1	DA	BSSID	SA	-
1	0	BSSID	SA	DA	-
1	1	RA	TA	DA	SA



- Addr 1 = Destination of the radio frame
- Addr 2 = Transmitter Address (TA) identifies entity to receive the ACK frame
- Addr 3 = Entity on DS sending/receiving frame
- Addr 4 = Needed to identify the original source in case of WDS (bridging over the air).

Header field specification



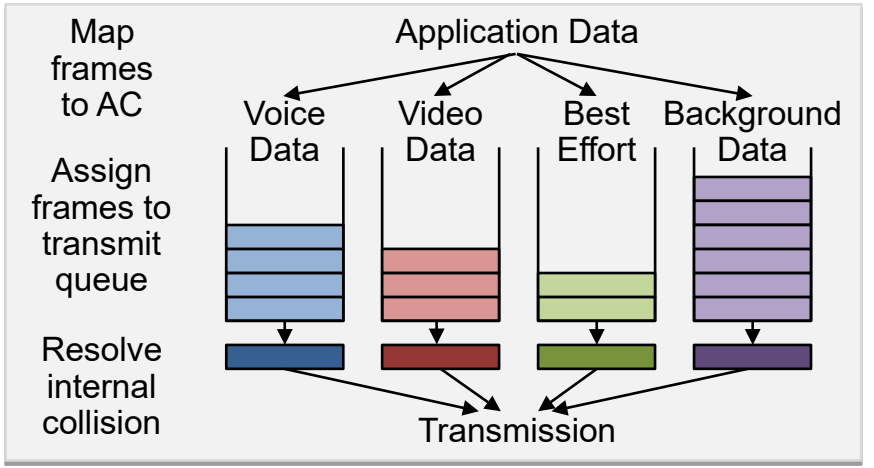
- Type / Subtype:
  - MAC frames function (management frame, control frame, data frame)
- More Frag:
  - Indicates whether the frame has been split
    and more fragments are about to follow
- Retry
  - Indicates that this frame has been retransmitted
- Pwr Mgmt (Power Management)
  - Indicates that the station is in power save mode
- More Data
  - Indicates that more frames follow
- WEP
  - Indicates that the payload is encrypted

Wi-Fi

QUALITY OF SERVICE

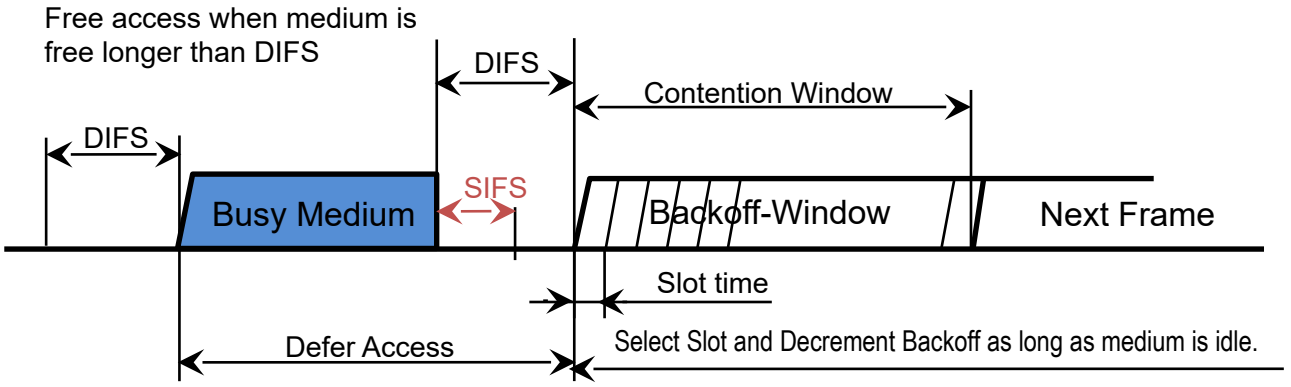
IEEE 802 Quality of Service through traffic prioritization

- Traffic is classified according to its importance and forwarding requirements.
- Traffic Categories (TC) for prioritization:
  - Differentiated channel access for frames with different user priorities
  - IEEE 802.1Q defines 8 different priorities.
  - IEEE 802.11 adopted the QoS principles of IEEE 802.1Q through IEEE 802.11e-2005.



	IEEE 802.1Q traffic types			IEEE 802.11 traffic types		
Priority	PCP	Acronym	Traffic Type	Access Category	Alternate AC	Designation
Lowest	1	BK	Background	AC_BK	BK	Background
	0	BE	Best Effort	AC_BE	BE	Best Effort
	2	EE	Excellent Effort	AC_BK	BK	Background
	3	CA	Critical Applications	AC_BE	BE	Best Effort
	4	CL	Controlled Load	AC_VI	A_VI	Video
	5	VI	Video, < 100ms latency	AC_VI	VI	Video
	6	VO	Voice, < 10ms latency	AC_VO	VO	Voice
Highest	7	NC	Network Control	AC_VO	A_VO	Voice

Legacy DCF does not provide traffic priorization

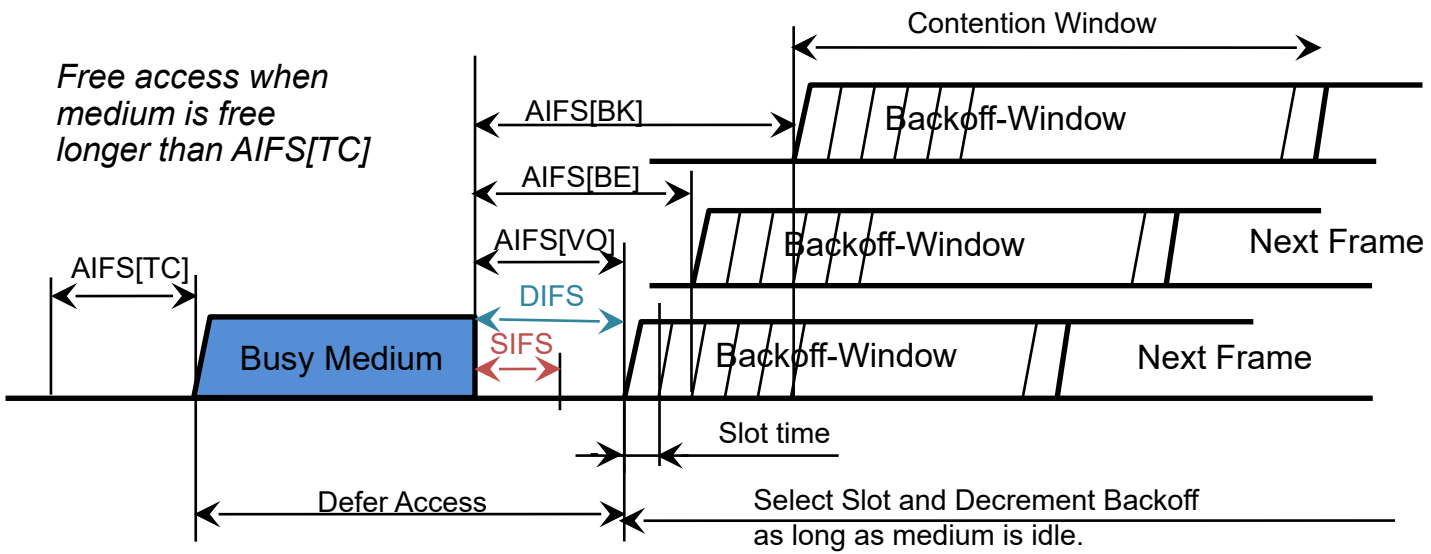


Standard	Slot time (µs)	SIFS (µs)
IEEE 802.11b	20	10
IEEE 802.11a/n/ac/ax/be	9	16
IEEE 802.11g/n/ax/be	9	10

SIFS: Short Inter Frame Space
DIFS: DCF Inter Frame Space
DIFS = SIFS + 2x Slot time

- All stations are waiting the same way for medium access by CCA
  - Medium has to be(come) idle.
  - Random backoff is used after a defer, resolving contention to avoid collisions.
    - Random backoff is an equally distributed value in the range 0..CWmin; CWmin = 15
  - Exponential backoff is used in the case of retransmissions
    - $CW = (2^k - 1)$ with k = n+4 with n= number of retransmission; CWmax = 1023
    - Efficient backoff algorithm stable at high loads.
- DCF access procedure can't differentiate traffic categories.

Enhanced DCF (EDCF) enables traffic prioritization



Standard	Slot time (µs)	SIFS (µs)
IEEE 802.11b	20	10
IEEE 802.11a/n/ac/ax/be	9	16
IEEE 802.11g/n/ax/be	9	10

SIFS: Short Inter Frame Space
AIFS: Arbitration Inter Frame Space
DIFS: DCF Inter Frame Space
DIFS = SIFS + 2x Slot time

- Based on modification of CSMA/CA access function with shorter arbitration inter-frame space (AIFS) for higher priority packets.
- High priority traffic waits a little less before packets are sent
  - High-priority traffic has a higher chance of being sent than low-priority traffic

Wi-Fi QoS

WI-FI MULTIMEDIA (WMM)

Wi-Fi Alliance Wi-Fi MultiMedia (WMM) specification

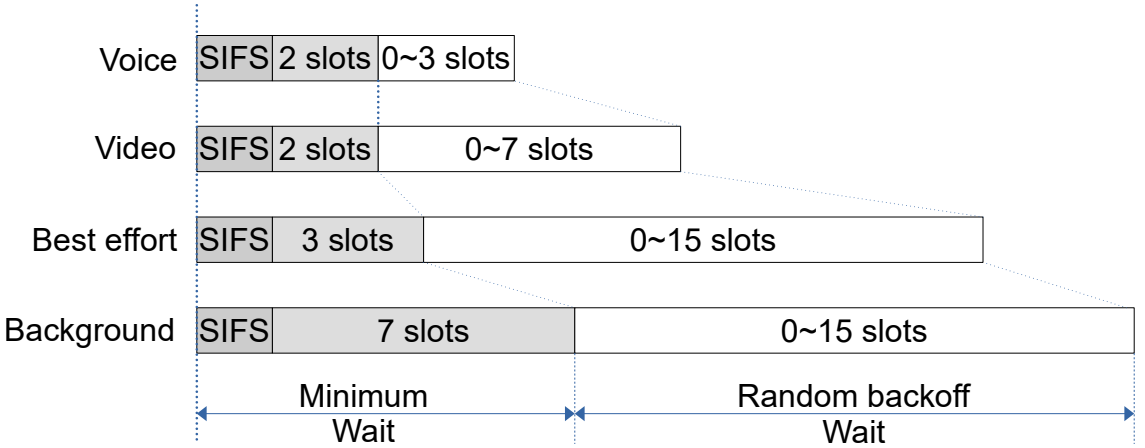
- Wi-Fi Multimedia (WMM) defines the actual QoS capabilities of Wi-Fi.
  - WMM makes use of EDCF for traffic prioritization.
  - Prioritized QoS identifies 4 traffic classes (Access Categories)
    - Aligned to the 8 priorities defined within IEEE 802.1Q.

Access Category	Description	802.1Q
WMM Voice Priority	Highest priority. Allows multiple concurrent VoIP sessions with low latency and jitter	7, 6
WMM Video Priority	Prioritize video traffic above other data traffic	5, 4
WMM Best Effort Priority	Traffic from legacy devices, or traffic from applications that do not require prioritization	3, 0
WMM Background Priority	Low priority traffic that does not require low latency or guaranteed throughput	1, 2

  - Parameterized QoS is only partially supported by an admission control scheme.

EDCF Parameters, as defined in Wi-Fi WMM

- WMM: Wi-Fi MultiMedia
- Levels of priority in EDCF are called Access Categories (ACs).
- Contention window (CW) set according to the traffic in AC
  - Wider window needed for categories with heavier traffic.
  - Window duration dependent of SIFS and slot time of PHY mode



- Default EDCA Parameters for wait times and TXOP for each AC:

Access Category	CWmin	CWmax	AIFSN	Max TXOP
Background (AC_BK)	15	1023	7	0
Best Effort (AC_BE)	15	1023	3	0
Video (AC_VI)	7	15	2	3.008ms
Voice (AC_VO)	3	7	2	1.504ms
Legacy DCF	15	1023	2	0

Optional: WMM Admission Control for parameterized QoS

- QoS is characterized by a set of parameters, called Traffic Specification (TSPEC)
- A Traffic Stream (TS) is set up between transmitter and receiver
- TSPEC specifies service rate, delay and jitter requirements of particular traffic flows.

Octets: 3	2	2	4	4	4	4	4	4
TS Info	Nominal MSDU Size	Maximum MSDU Size	Minimum Service Interval	Maximum Service Interval	Inactivity Interval	Suspension Interval	Service Start Time	Minimum Data Rate

4	4	4	4	4	2	2
Mean Data Rate	Peak Data Rate	Maximum Burst Size	Delay Bound	Minimum PHY Rate	Surplus Bandwidth Allowance	Medium Time

- Management commands for negotiation of TSPECs between STA and AP:
  - ADDTS Request
  - ADDTS Response
  - DELTS
- After successful negotiation of a TSPEC a STA can contend for a TXOP and then leverage the medium up to the TXOP time limit.
  - TXOP time limits of an AP are conveyed in the beacon.

WLAN IEEE 802.11 aka Wi-Fi

WI-FI QOS IN ACTION

WMM performance: Comparison DCF vs. EDCF

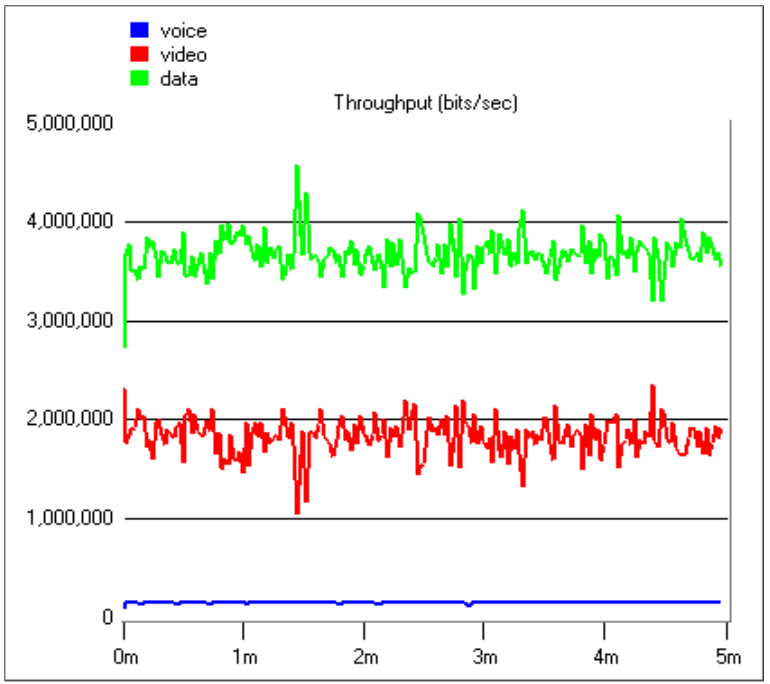
- E.g: Sunghyun Choi; J. del Prado; Sai Shankar N; S. Mangold,
  IEEE 802.11e contention-based channel access (EDCF) performance evaluation, IEEE International Conference on Communications, 2003.
  - http://www.cs.jhu.edu/~baruch/RESEARCH/Research_areas/Wireless/wireless-public_html/class-papers/802.11e-performance.pdf
  - Fixed data rate of 802.11b 11 Mbps; 2 video, 4 voice, and 4 data stations
  - Buffer size: 20 kbit for voice, 1Mbit for video, infinite for data
  - Traffic pattern and default EDCF parameters:

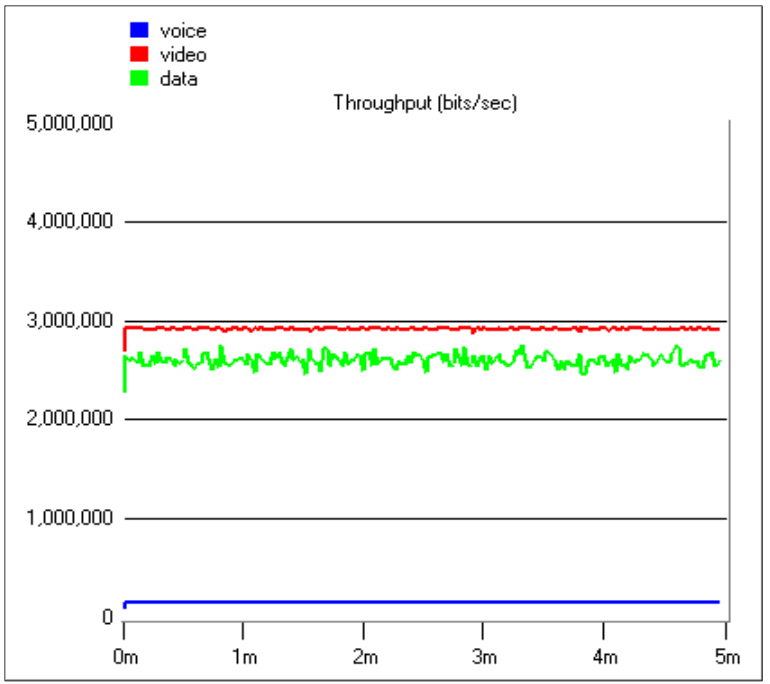
Type	Inter-arrival Time (Avg. in sec)	Frame Size (bytes)	Data Rate (Mbps)
Voice	Constant (0.02)	92	0.0368
Video	Constant (0.001)	1464	1.4
Data	Exponential (0.012)	1500	1.0

Type	Prior.	AC	AIFS	CWmin	CWmax	TXOP limit (msec)
Voice	7	3	PIFS	7	15	3
Video	5	2	PIFS	15	31	6
Data	0	0	DIFS	31	1023	0

DCF vs. EDCF

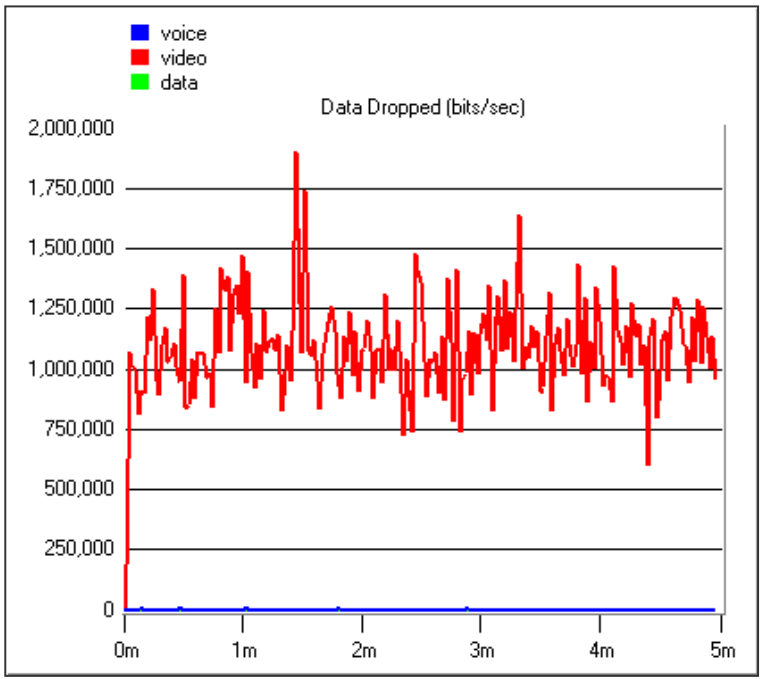
- Throughput comparison
  - Higher video throughput with EDCF

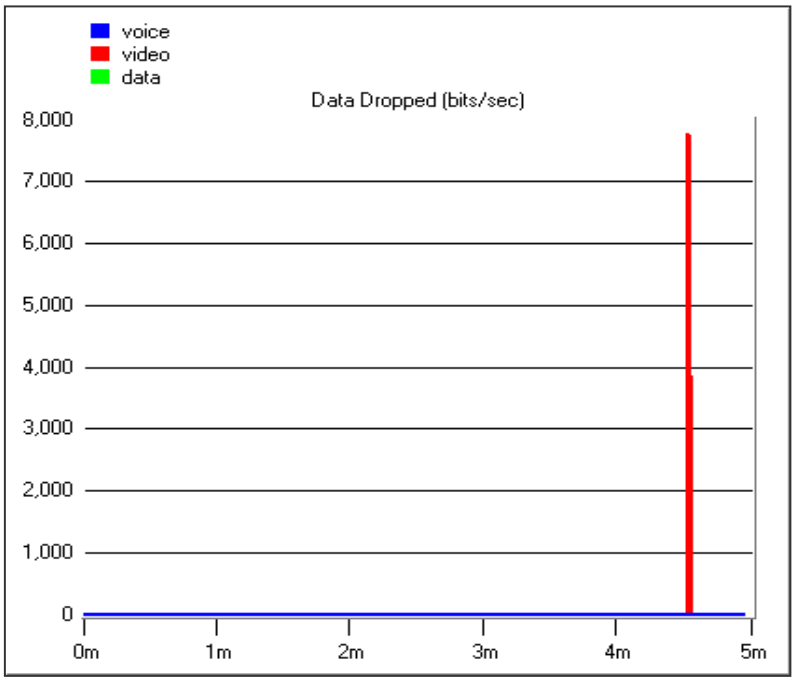




DCF vs. EDCF

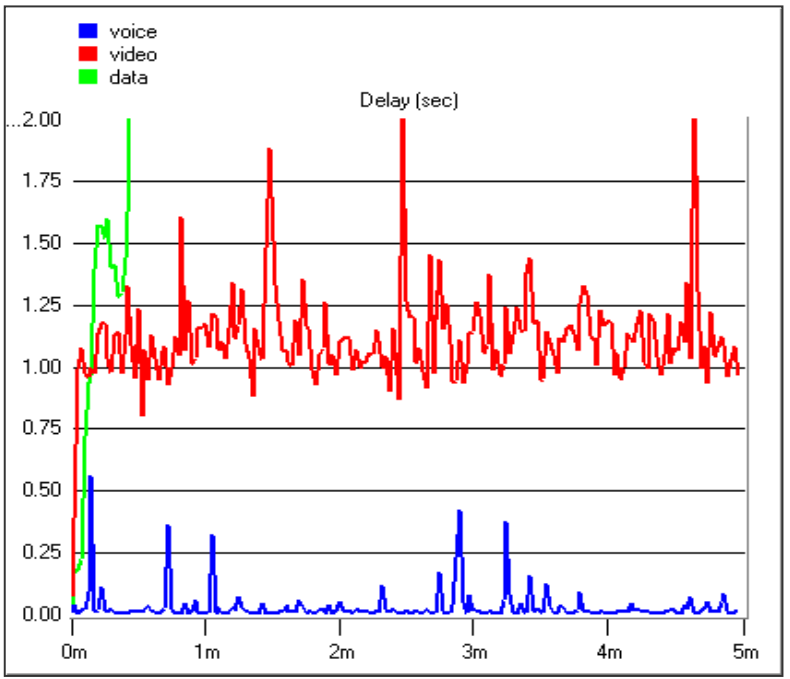
- Data dropping rate comparison
  - Video drop virtually gone with EDCF

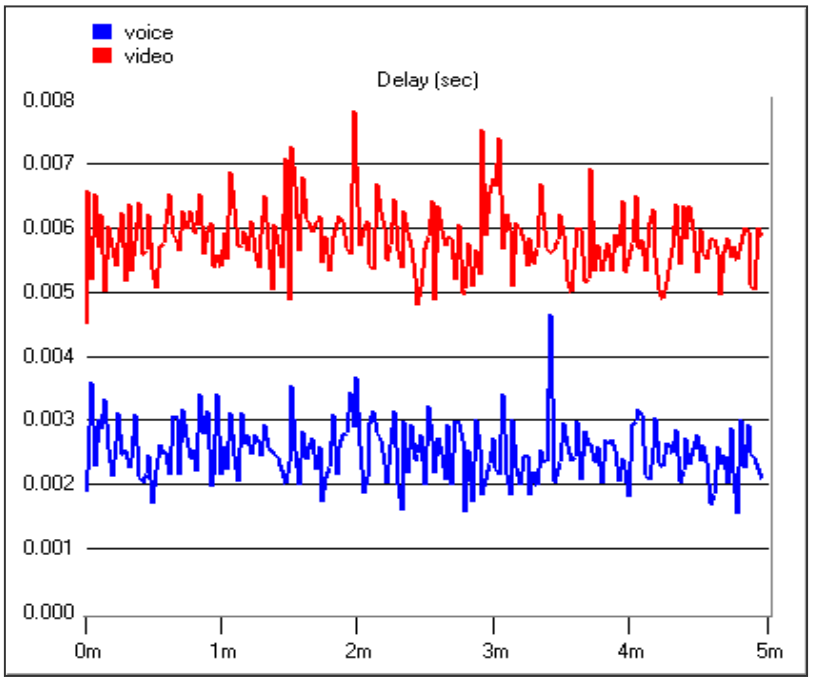




DCF vs. EDCF

- Delay comparison
  - Voice and video delays significantly reduced



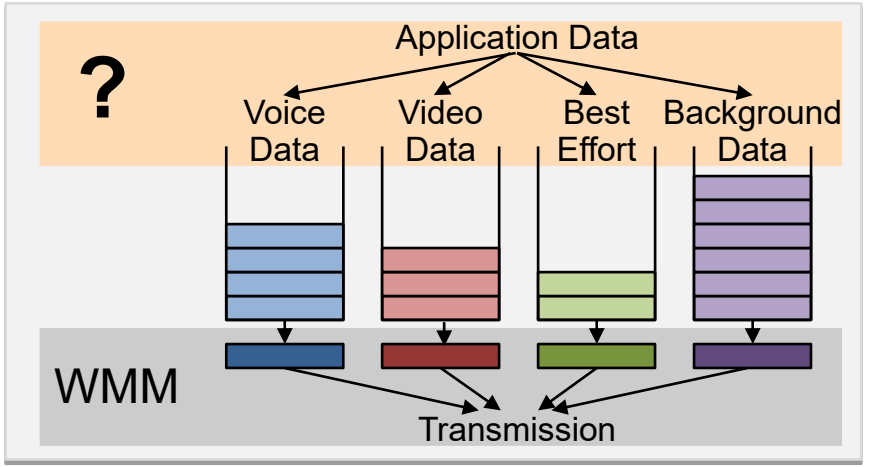


Wi-Fi QoS

WI-FI CERTIFIED QOS MANAGEMENT™

How to assign packets to priority queues?

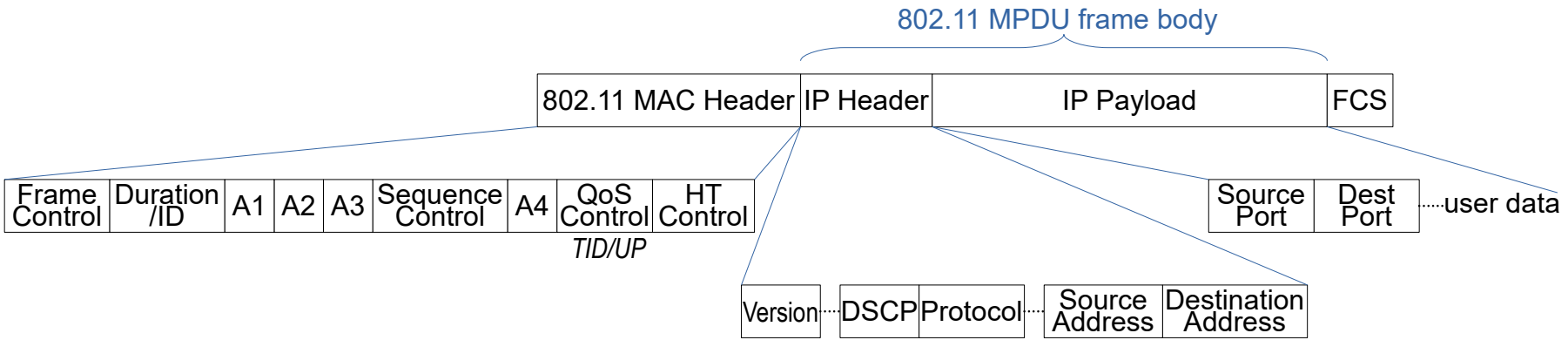
- WMM enables prioritized transmission of packets over the wireless medium.
- However, WMM does not provide means for assigning packets to priority queues/access classes (ACs).



- To enable end-to-end QoS, the priority of packets needs to be determined based on the higher layer QoS requirements of the application or service.
- Most commonly, applications can signal this intent via DSCP (Differentiated Services Code Point) marking within the IP packet header.
- Wi-Fi QoS Management™ enables negotiation and management of QoS treatment for traffic flows over-the-air between an AP and STA.

User Priorities through DSCP marking

- User Priorities can be signaled via DSCP marking within the IP packet header.
  - It can then be mapped to a User Priority for the transport in the underlying transmission technology.
- However, there are many scenarios in which the appropriate DSCP marking is not, or cannot, be applied.

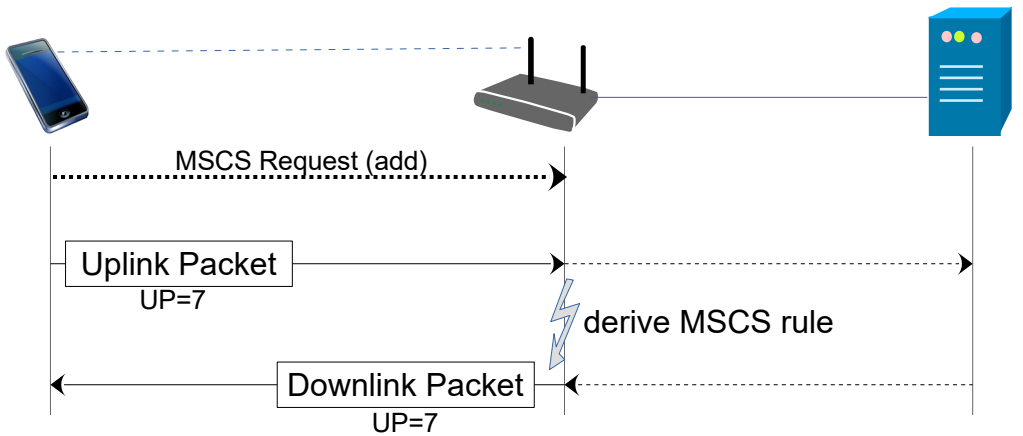


Wi-Fi CERTIFIED QoS Management™

- The Wi-Fi QoS Management™ defines 4 different methods to map traffic streams to UP/AC:
  - **MSCS (Mirrored Stream Classification Service),**
  - **SCS (Stream Classification Service),**
  - **DSCP Mapping, and**
  - **DSCP Policy.**
- It aligns QoS treatment across Wi-Fi and wired networks, and it even enables flow classification based on the SPI identifier of each IPsec child SA for Wi-Fi access to 3GPP 5G core networks.

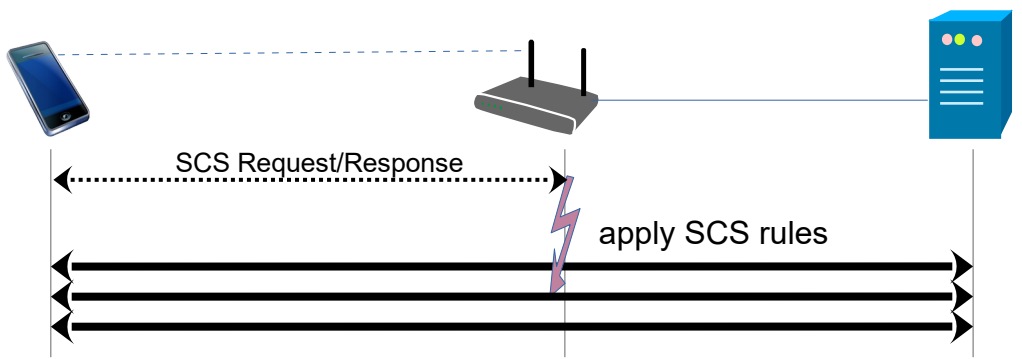
Mirrored Stream Classification Service (MSCS)

- Client device requests the AP to apply specific QoS treatment of downlink IP data flows using QoS mirroring of a given uplink IP data flow. Concept of “mirroring” or “reflecting”, wherein, AP derives QoS rules for downlink IP flows based on uplink flows it receives from STA
  - Advertised through the Extended Capabilities IE and setup either as part of Association or post-association MSCS exchange



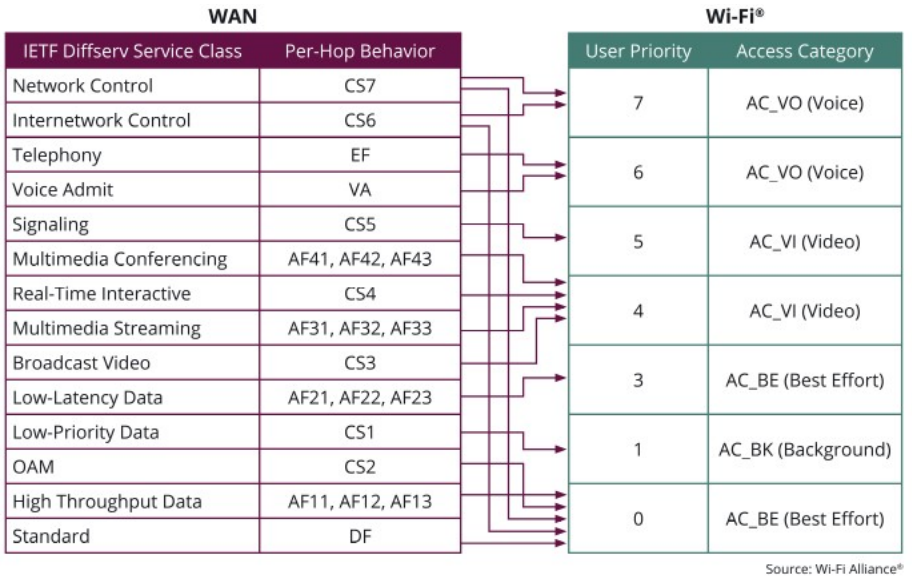
Stream Classification Service (SCS)

- Client device requests the AP to apply specific QoS treatment of downlink IP data flows using IP classifiers. It enables client OS/apps to request downlink QoS treatment by its AP based on explicit flow classifiers.
  - For the same downlink flow, SCS enables better control (i.e., different DSCP/UP, even if 5-tuple matches)
  - SCS can work independently or together with MSCS.
  - When a client device accesses a 3GPP 5G core network over Wi-Fi using IPsec, SCS enables differentiated QoS treatment for each downlink child SA, based on its unique index (SPI) classifier.



Differentiated Service Code Point (DSCP) Mapping

- Default DSCP to UP Mapping
  - Wi-Fi QoS Management-capable APs and STAs are required to support the default DSCP-to-UP mapping table mentioned in IETF RFC 8325
    - Applicable to both uplink and downlink traffic
    - Following the default table ensures a common set of values across all Wi-Fi QoS Management-capable APs and STAs

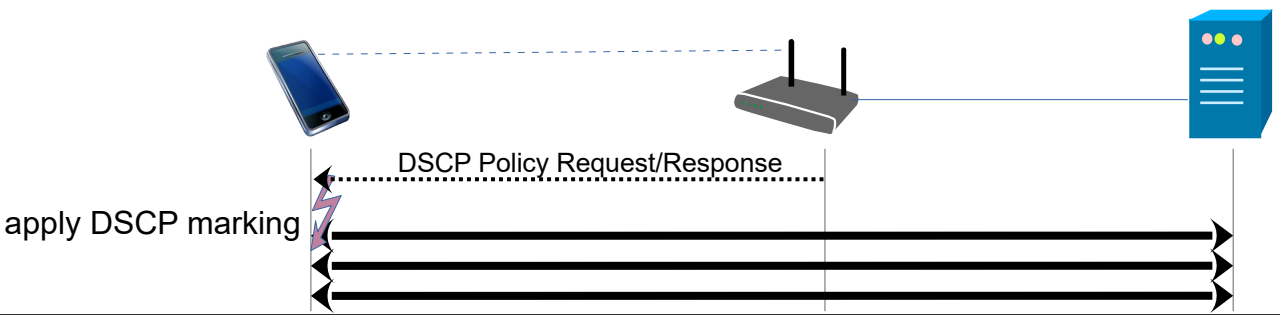


Default DSCP to User Priority Mapping based on RFC 8325

- DSCP-to-UP mapping through QoS Map
  - If a non-default DSCP-to-UP mapping table needs to be configured, then Wi-Fi QoS Management APs can include the QoS Map element in Association Response frame

DSCP Policy

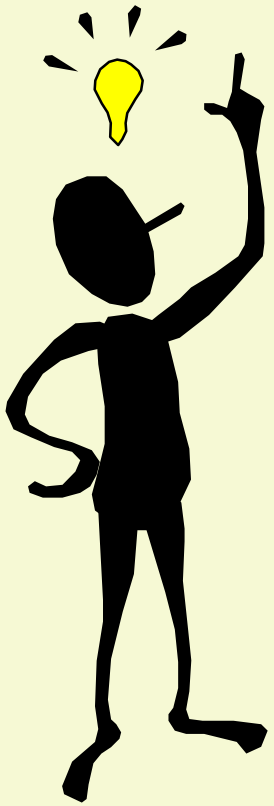
- Dynamic configuration of clients with uplink DSCP policies for specific traffic flows. This feature enables an AP to request a client to apply DSCP marking to specified uplink traffic flows identified by: IP tuple, Port range or Destination domain name
  - Can be used in conjunction with QoS Map element
  - When compared to DSCP-to-UP mapping, it allows a much granular level of control of uplink IP flows, thereby resulting in different DSCPs/UPs for the same uplink IP flows
  - Unlike MSCS, SCS, and QoS Map, DSCP policies continue to apply even after STA roams between BSSs within the same ESS
- DSCP Policy configurations can be initiated post-association by either STA or by AP



Wi-Fi QoS summary

- WMM provides four different user priorities
  - **Voice**, **Video**, **Best Effort**, **Background**, based on IEEE 802.11e QoS mechanisms
- Wi-Fi QoS Management provides four solutions for traffic classification
  - Mirrored Stream Classification Service (MSCS) (mandatory)
    - Station instructs AP to treat downlink IP flows using QoS mirroring
  - Stream Classification Service (SCS) (optional)
    - Station instructs AP to treat downlink IP flows using IP tuple and IPsec child security association (SA) classifiers,
  - Differentiated Service Code Point (DSCP) (manadatory)
    - Allows for setting tables between the DSCP marking in IP packet headers and the over-the-air QoS treatment on both APs and stations
  - DSCP Policy (optional)
    - AP defines treatment of uplink IP flows at station using DSCP marking policies.

Questions and answers



Quality of Service questions…

1) What does EDCF mean, and which enhancements were added to DCF?
2) How does Enhanced Distributed Coordination Function (EDCF) ensure backward compatibility to DCF?
3) What is AIFS?
4) How many traffic categories do exist in IEEE 802.1Q, and how many does WMM support?
5) How are the QoS classes denoted that are supported by WMM?
6) Through which method are traffic classes realized in IEEE 802.11?
7) What does TSPEC mean, and for what is it used?
8) What is the purpose of Wi-Fi QoS management?
9) Which methods to assign WMM traffic classes to traffic streams are provided through Wi-Fi QoS management?

CSMA/CA EDCF timing and collision probabilities

- Questions for the case of EDCF @5GHz:
  - Q1: What is the minimum and maximum access delay after another transmission that an AC_VO / AC_BE station has to wait for access?
  - Q2: What is the likelihood that a collision occurs when an AC_VO STA competes with an AC_BE STA?
  - Q3: What is the likelihood that a collision occurs when AC_VO STA competes with three AC_BE STAs?
  - Q4: What is the minimum and maximum access delay for an AC_VO /AC_BE STA after a collision?
  - Q5: What is the likelihood that a succeeding collision occurs when an AC_VO STA continues to compete with an AC_BE STA?
  - Q6: What is the minimum and maximum access delay for an AC_VO / AC_BE STA after a 2nd collision?

Wi-Fi MAC Layer & QoS

SUMMARY

IEEE802.11 MAC Summary

- One common MAC supporting multiple PHYs
- CSMA/CA (collision avoidance) with ‘virtual sensing’
- Connectionless service
  - Transfer of data on a shared medium without reservation
  - Data transmitted in bursts
  - Controlled through low-layer ACKs, so transmit at highest speed possible
  - Same service as used by Internet
- Robust against noise and interference (ACK)
- Hidden node mitigation (RTS/CTS)
- Power savings (Sleep intervals)
- Association, deassociation, and reassociation (handover capability)
- Wi-Fi QoS (WMM) and Wi-Fi QoS Management
- Security (WPA3), coming next...

End of part 3

Questions and remarks?