Self Organizing Networks

WLAN IEEE 802.11 aka Wi-Fi

SS 2023 Lecture – Part 2

Max Riegel

SS2023 Lectures overview

- **June 8th** ***- electronic***
  - Wi-Fi Applications and markets
  - Wi-Fi Standardization environment
  - Wi-Fi Spectrum

- **June 15th - TU Campus C25.012**
  - Wireless channel characteristics
  - Direct Sequence Spread Spectrum (initial Wi-Fi radio)
  - Orthogonal Frequency Division Multiplex
  - Wi-Fi 2 .. Wi-Fi 7 radios

- **June 22nd -** ***electronic***
  - IEEE 802.11 Architecture
  - Medium access functions
  - System management

- **June 29th** ***- ????***
  - MAC layer management
  - MAC layer frame formats
  - Quality of Service

- **July 6th - TU Campus C25.012**
  - Wi-Fi security
  - Mobility enhancements

WLAN IEEE 802.11 aka Wi-Fi

STANDARD REFERENCE

IEEE Std 802.11™-2020 + amendment 802.11ax™-2021

- *Can be downloaded at no charge through the IEEE Get Program*
  - https://ieeexplore.ieee.org/browse/standards/get-program/page/series?id=68
- *No all the features specified in the standard are available in real Wi-Fi products*
- *This lecture presents behavior of real Wi-Fi products as specified by Wi-Fi Alliance in its certification programs*
  - https://www.wi-fi.org/discover-wi-fi/specifications

IEEE Standard for Information technology

Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

- Revision of IEEE Std 802.11-2016
  - Revision of IEEE Std 802.11-2012
    - Revision of IEEE Std 802.11-2007
      - Revision of IEEE Std 802.11-1999
        - First IEEE 802.11 standard release in 1997
- Comprises initial IEEE Std 802.11-1999 and all amendments IEEE 802.11a-1999 … IEEE 802.11aq-2018
  - *i.e.:* a, b, d, e, g, h, I, j, k, n, p, r, s, u, v, w, y, z, aa, ac, ad, ae, af, ah, ai, aj, ak, aq

Amendment standard IEEE Std 802.11ax-2021

- Amendment 1: Enhancements for High-Efficiency WLAN

Amendment draft standard IEEE P802.11be/D3.0

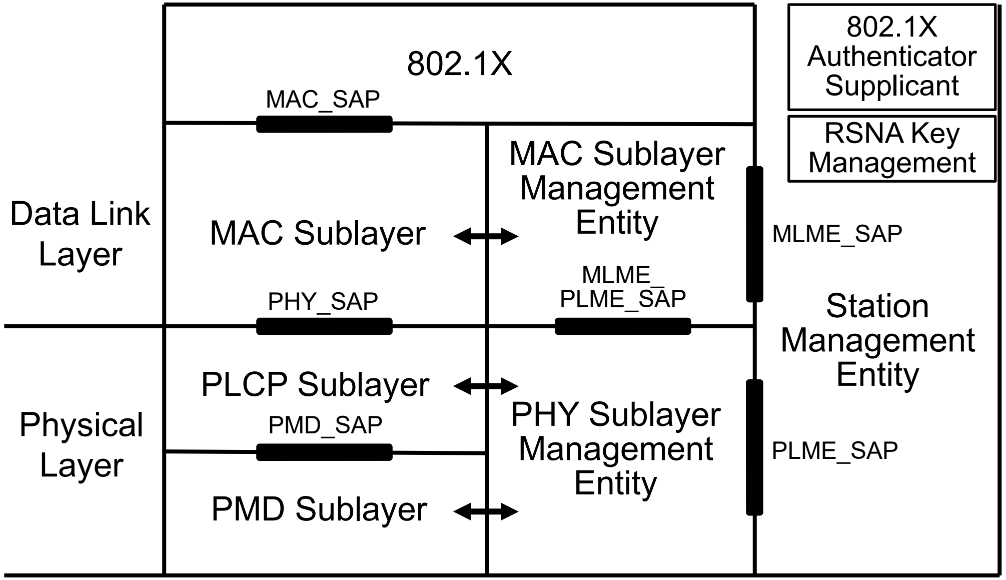
- *Amendment 8: Enhancements for extremely high throughput (EHT)*

WLAN IEEE 802.11 aka Wi-Fi

IEEE 802.11 ARCHITECTURE

IEEE 802.11 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

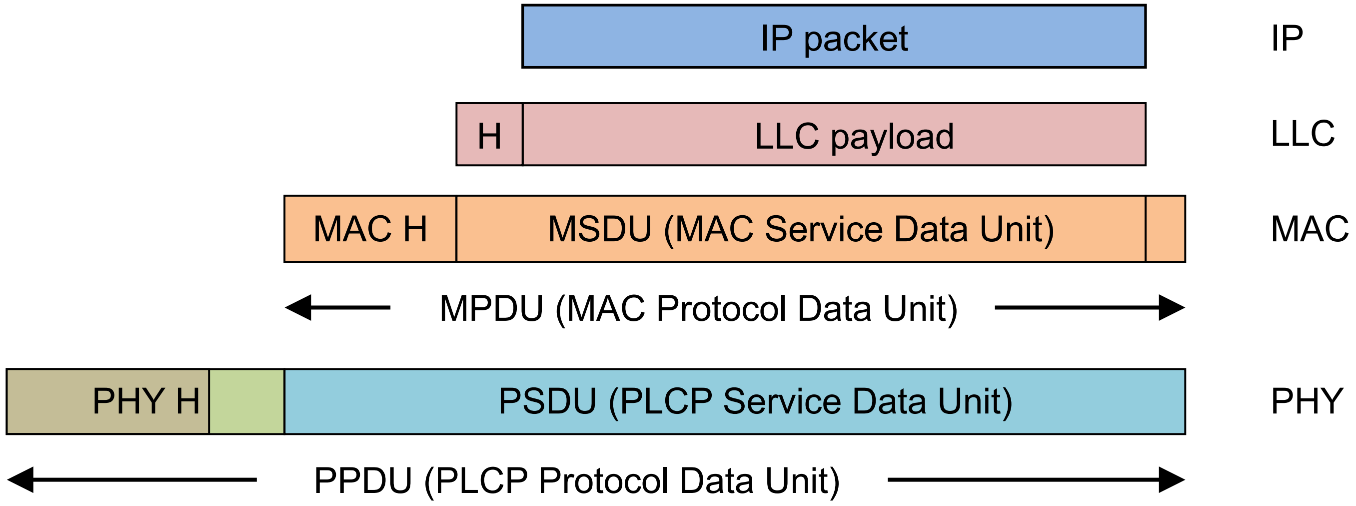


IEEE802.11 MAC Overview

- One common MAC supporting multiple PHYs
- CSMA/CA (collision avoidance) with optional “point coordination”
- Connectionless service
  - Transfer 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 problem (RTS/CTS)
- Power savings (Sleep intervals)
- Association, deassociation, and reassociation (handover capability)
- Security (WPA3)
- “Infrastructure” configuration with multiple APs interconnected through DS (distribution system) to extend coverage area of service set

IEEE 802.11 Frame structure

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



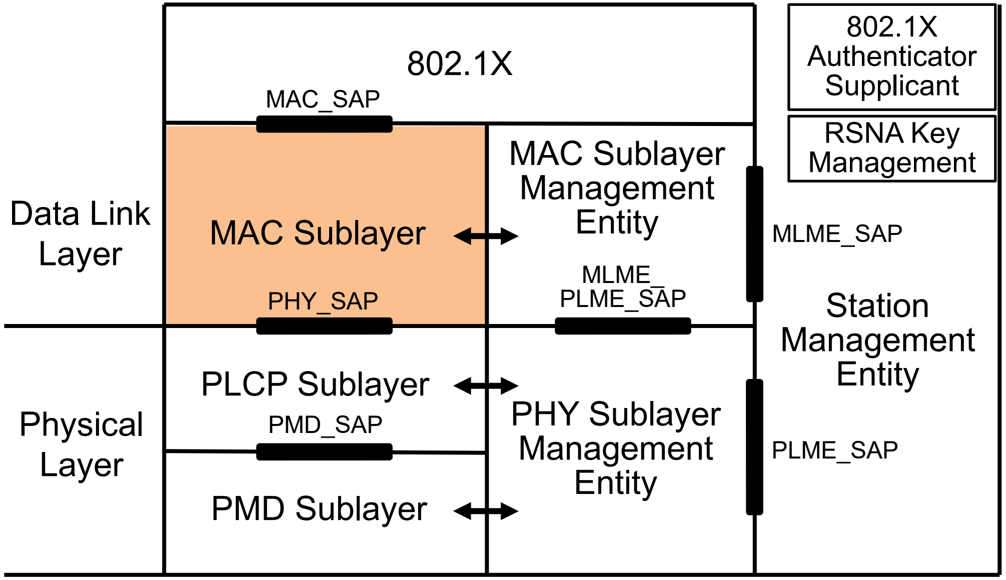
- IEEE 802.11 PHY header carries the information for setting up the reception of radio frames
- Physical Layer Convergence Protocol (PLCP) provides a PHY independent Service Access Point (SAP) for higher layers

WLAN IEEE 802.11 aka Wi-Fi

MEDIUM ACCESS FUNCTIONS

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

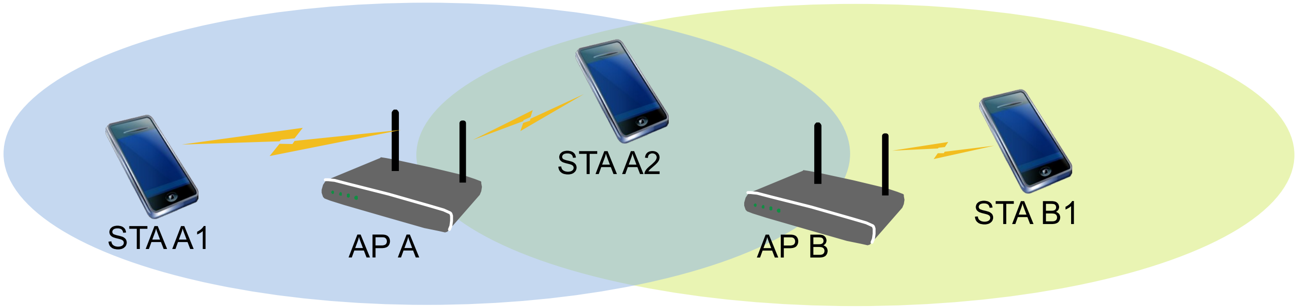


Topics covered in this section

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

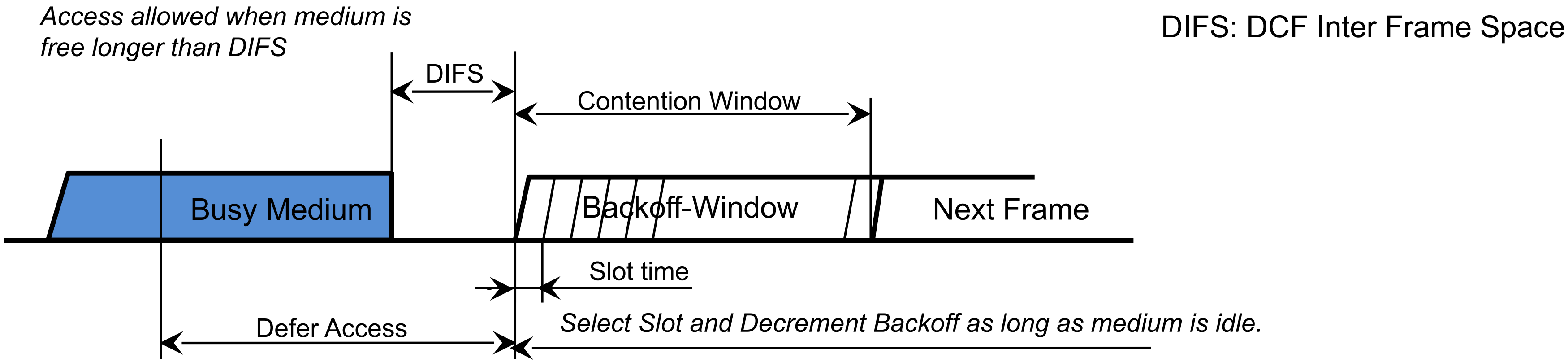
Shared Spectrum Medium Access Challenges

- Multiple concurrent transmissions in the same channel might create collisions, which disallow to correctly receive the transmitted frames



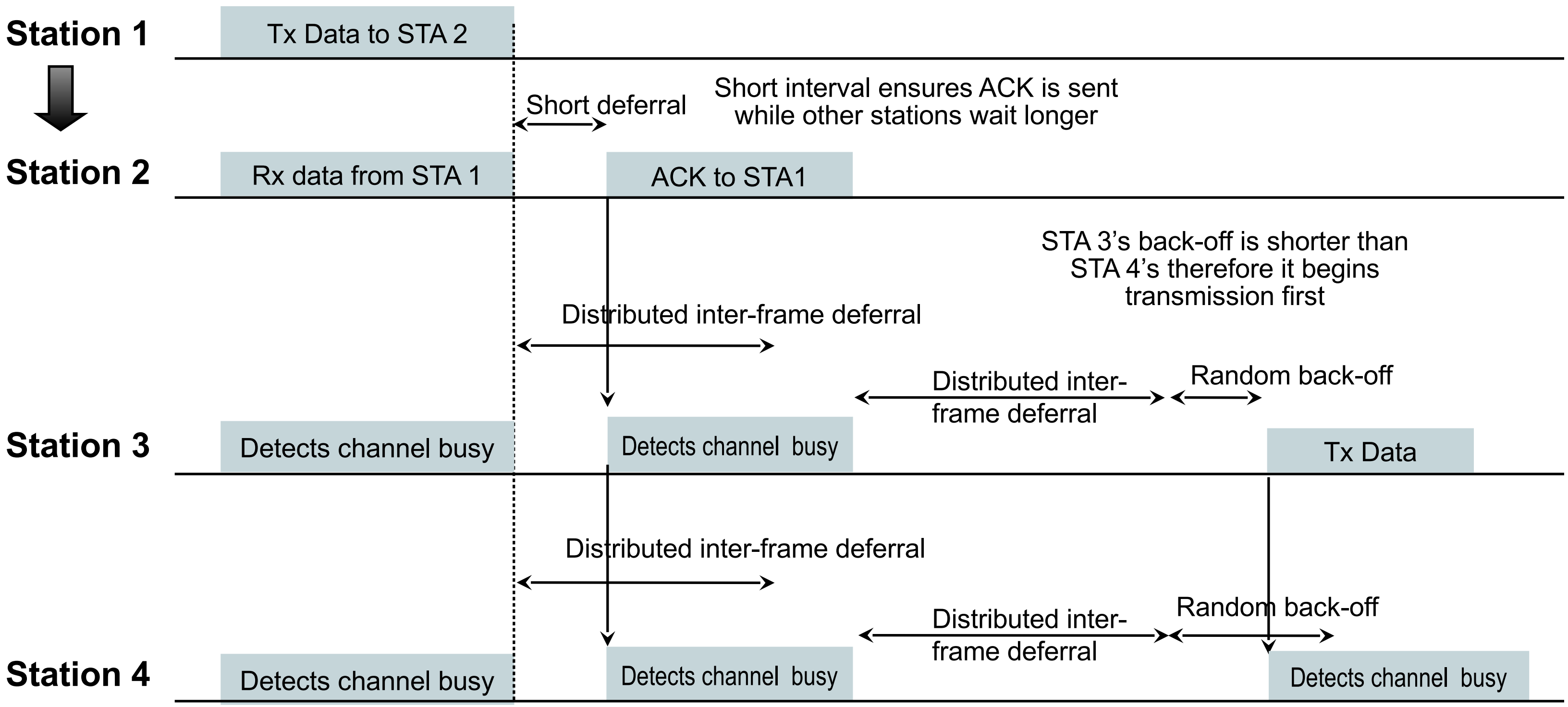
- No wireless issue only; same issue exists in <u>shared</u> wired medium as well
  - Ethernet introduced CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to minimize impairments through collisions
  - CSMA denotes method that potential transmitters first listen to the medium to ensure that no other transmission is ongoing before starting own transmission
    - Same behaviour that humans are usually applying when taking with each other
  - Nevertheless, collisions occur through multiple transmitters waiting for the end of an ongoing transmission and starting their transmission right after.
    - Legacy Thin/Thick-wire Ethernet introduced Collision Detection with instantaneous stop and retrial after some wait time – like humans;-).
- Wireless medium is somewhat more difficult
  - CSMA can be deployed the same way as on the shared wired medium
  - However, when transmission is ongoing, a station can’t detect collisions occuring somewhere else in the shared domain
    - Transmitter learns about collisions only through missing acknowledgements from receiver
  - Randomized backoff when medium is becoming free is used to minimize collision probability (Collision Avoidance)

Carrier Sense Multiple Access with Collision Avoidance

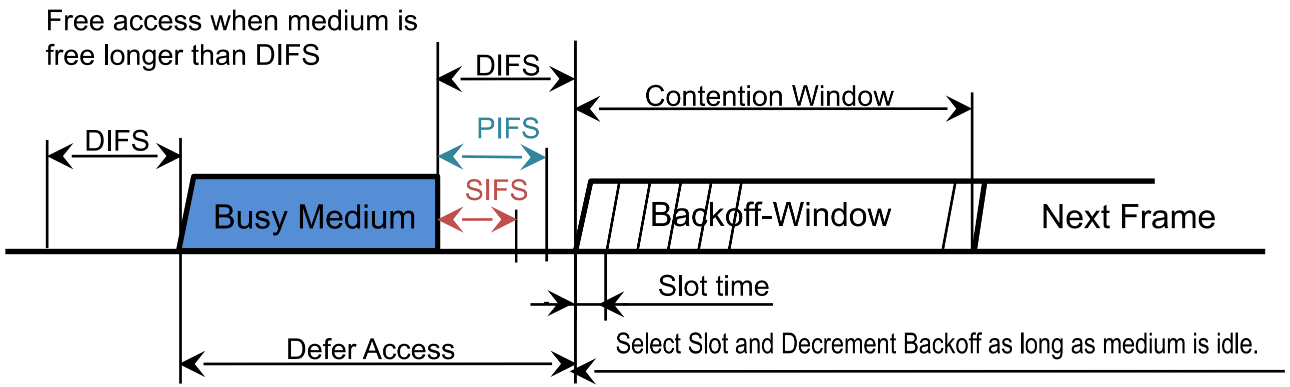


- CSMA/CA reduces collision probability where mostly needed.
  - Stations (also APs) are waiting for medium to become free.
  - Random backoff is used after a defer, resolving contention to avoid collisions.
    - Random backoff is an equally distributed value in the range 0..CWmin; CWmin = 15
  - Exponential 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.

Distributed Coordination Function (DCF)



Clear Channel Access (CCA): Determining empty channel



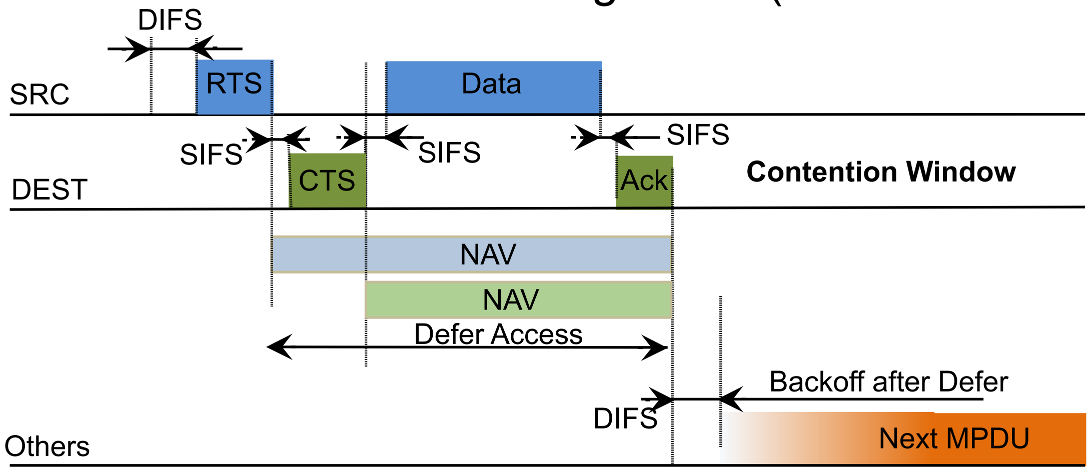
Standard	Slot time (µs)	DIFS (µs)
IEEE 802.11b	20	50
IEEE 802.11a/n/ac	9	34
IEEE 802.11g/n	9	28

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

- Medium is sensed for becoming idle.
  - Random backoff is applied after DIFS to avoid collisions.
  - In the case of retransmissions exponential backoff is used to avoid collapse of the system.
- 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 addition to physical sensing there is also predictive signaling of medium occupancy through timer values.

Physical and virtual carrier sensing operation

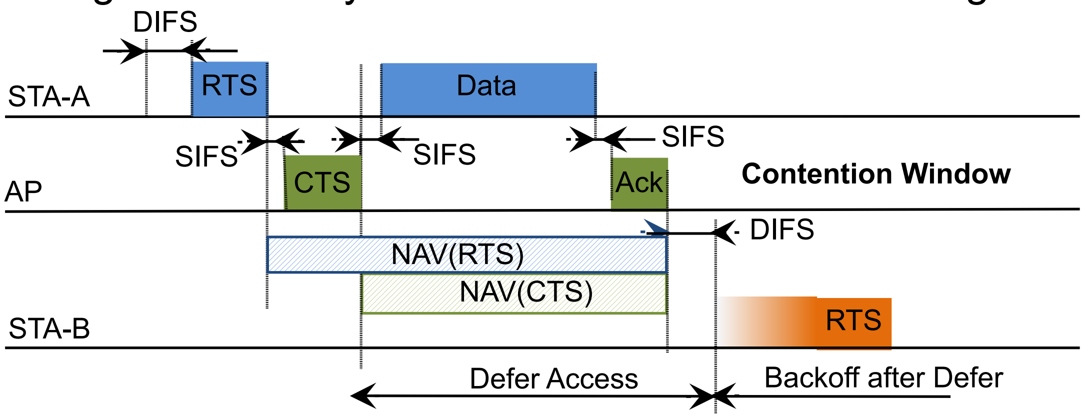
- Defer access based on Carrier Sense.
  - Either physical through CCA (Clear Channel Assessment) from PHY
  - Or virtual carrier sense state through NAV (Network Allocation Vector)



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

Request-To-Send/Clear-To-Send (RTS/CTS)

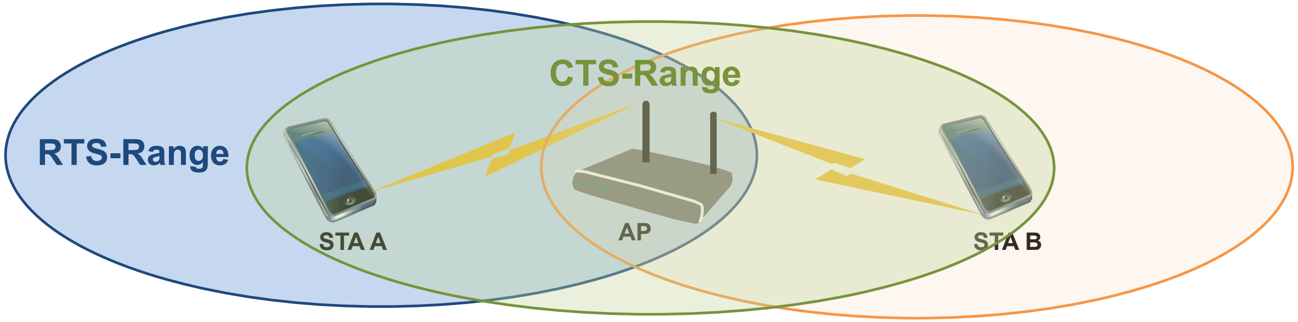
- Used to handle congested/heavily loaded radio environment through central control of AP



- STA 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
  - NAV represents the overall transmission duration, i.e. the time needed for transmitting the data frame including the following ACK
- The AP acknowledges the medium reservation with a CTS frame, which contains the updated reservation time in the NAV
- STA might start transmitting its data when the CTS message arrives
- All stations monitor RTS/CTS frames and use the gathered information from the NAV(CTS) to adjust their channel access procedure.

Hidden Node Problem

- Problem occurs when contending stations for the medium do not hear each other

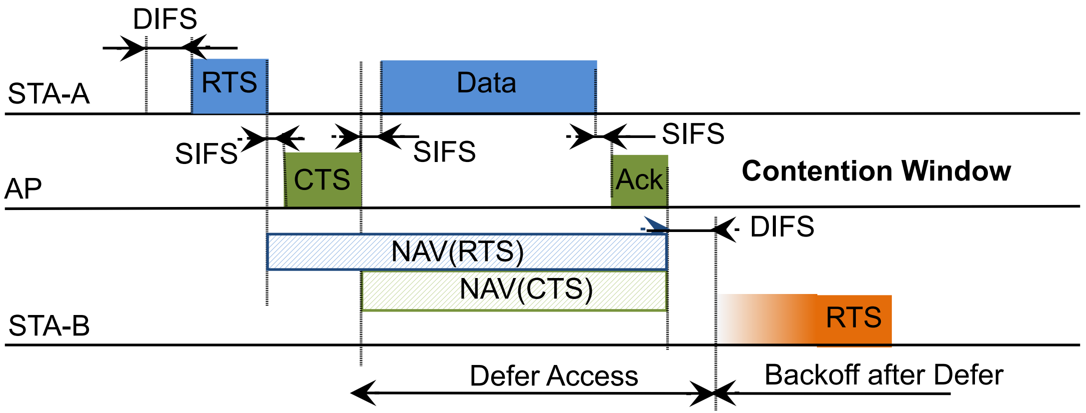


  - STA-B cannot detect when STA-A occupies the medium.
  - STA-B may interfere with transmissions of STA-A to the AP
- Without further measures the performance may be seriously impacted

- WLAN provides an mechanism to solve the hidden station problem:
  - Medium access control with RTS (Request To Send) and CTS (Clear To Send)

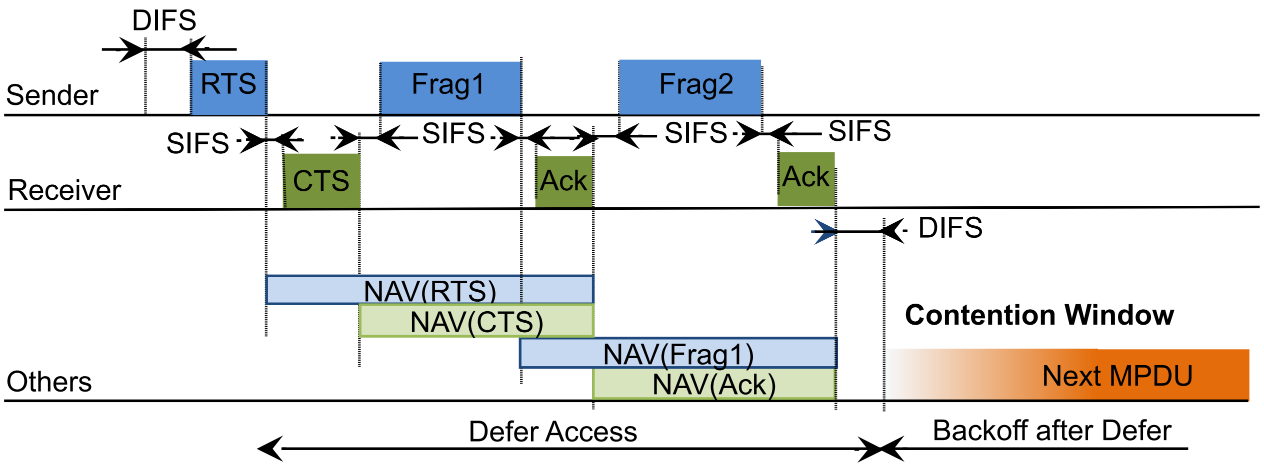
Hidden Station Solution

- 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.



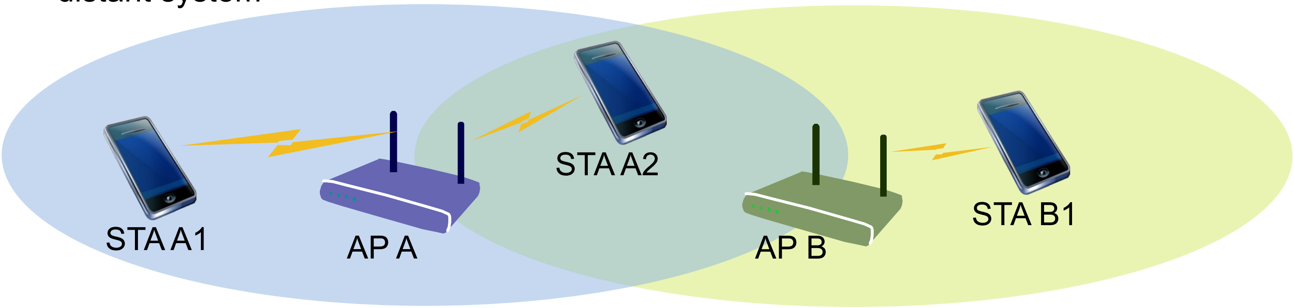
Fragmentation

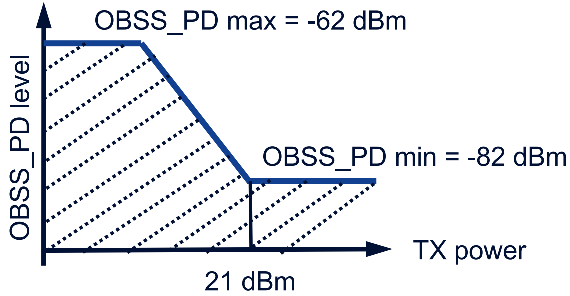
- Packet loss probability increases when data packets are becoming big in a noisy environment
- Limiting the maximum packet size reduces the probability that a packet is hit by a bit failure.
- The MAC Layer provides the function to split packets into multiple smaller frames for transmission



Spatial Reuse through BSS Coloring

- In dense deployments, CCA is often ‘over-protective’
  - Transmissions are stalled due to activities at a distant AP operating in the same channel
  - A successful transmission could be performed in the local system due to proximity of STA and AP despite parallel activies in the distant system



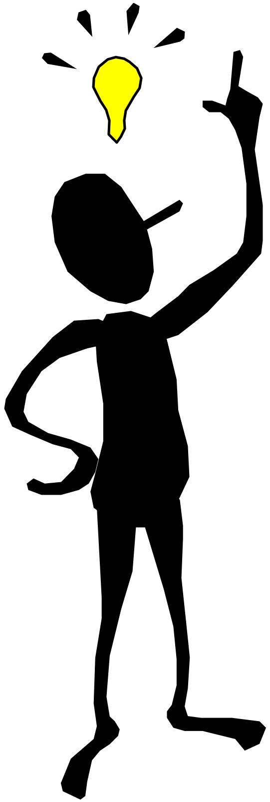


- Wi-Fi 6 introduces the possibility to determine intra-BSS frames from frames coming from other systems (OBSS)
  - Called ‘BSS Coloring’, which puts a color value into the PHY header of each transmission frame.
- In addition, assignments and detection of Spatial Reuse Groups (SRG) are possible to determine between devices under common management, and devices not under common control.
- According to detected interference levels, the preamble detection threshold of OBSS will be adjusted to allow for more aggressive spectrum reuse.
  - To mitigate negative side-effects also the transmission power of devices within a SRG is adjusted to lower overall interference level.

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 colisions.
- 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 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…

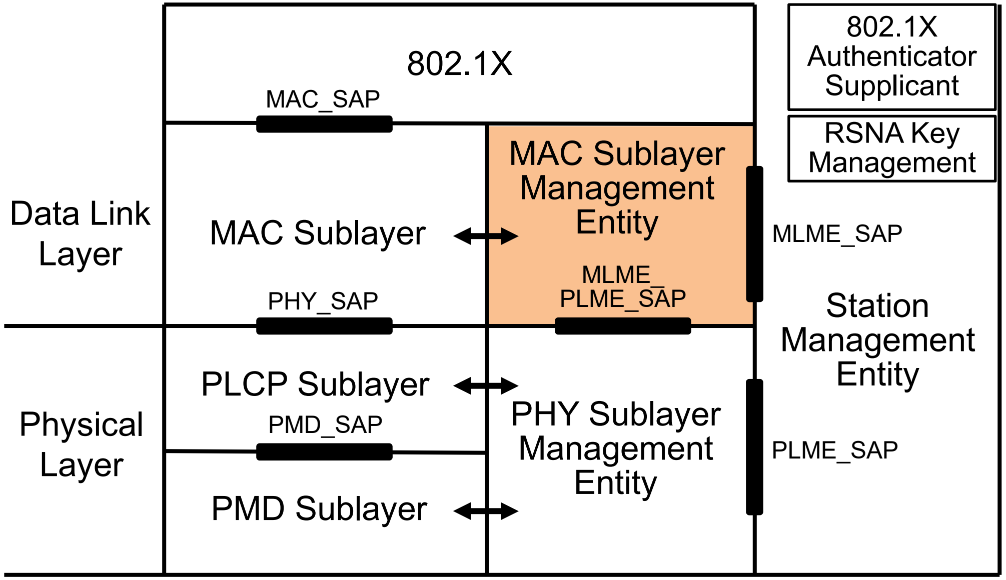
1) Why does collision detection with immediate termination of transmission usually not work in wireless medium?
2) What means are used by IEEE 802.11 to avoid collisions?
3) What does SIFS mean, and for which frame is it used?
4) What is the difference between random backoff and exponential backoff?
5) How is virtual carrier sensing done?
6) When does a receiver respond with an ACK to a received frame?
7) What is the issue of the hidden station problem?
8) Which procedure is used to mitigate the hidden station problem?
9) Which message is used by a receiver to respond to a ‘Request To Send’?
10) When is it beneficial to fragment the transmission of a long frame?

WLAN IEEE 802.11 aka Wi-Fi

MAC LAYER 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



Topics covered in this section

- MAC layer management
  - System management
    - Timer synchronization function
    - Power management
  - Session management
    - Session establishment
    - Scanning
    - Network selection
    - Authentication
    - Association
    - Mobility support
    - Message attributes

WLAN IEEE 802.11 aka Wi-Fi

SYSTEM MANAGEMENT

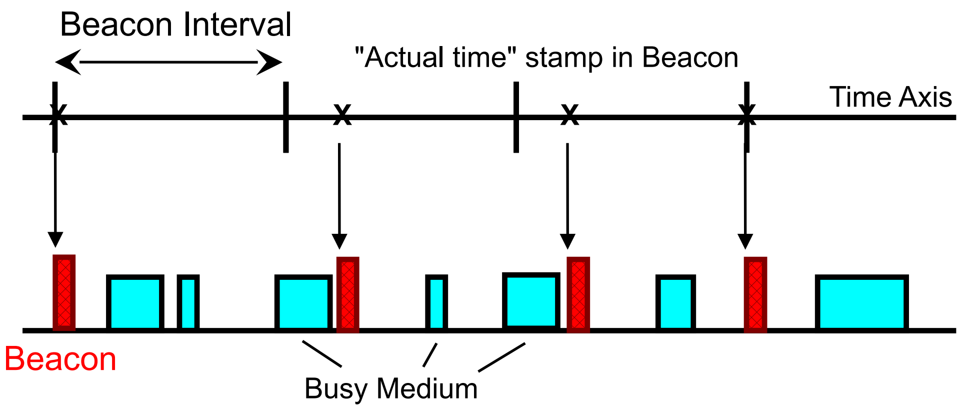
System Management - Overview

- Synchronization
  - Synchronization (Timer Synchronization Function)
    - Synchronization of timers of STAs and APs
  - Beacon generation
- Power management
  - Legacy power management
    - Support of periodic sleep of STAs with power save mode
      - Buffering of downstream MAC frames in the AP
      - Indication of pending traffic by Traffic Indication Map in Beacon
  - Target Wake Time (TWT)
    - Each STA negotiates its own TRX periodes
  - Enhanced power management procedures

Timing Synchronization Function (TSF)

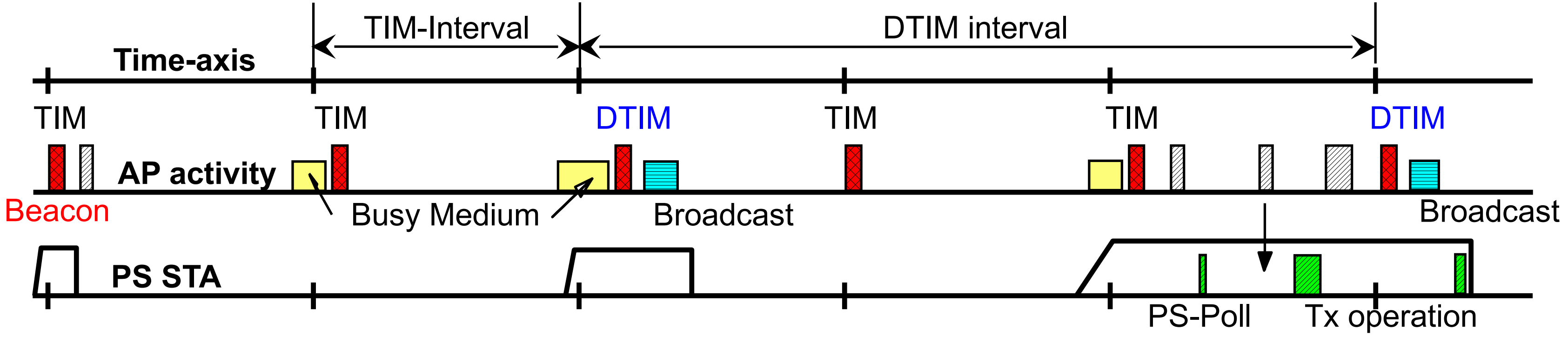
- All STAs maintain a local timer.
  - Used e.g. for NAV, Power Management and other purposes
  - All station timers in BSS are synchronized
- Timing Synchronization Function (TSF)
  - Keeps timers from all STAs in synch
  - AP controls timing in infrastructure networks
- Timing conveyed by periodic Beacon transmissions
  - Beacons contain Timestamp for the entire BSS
  - Timestamp from Beacons used to calibrate local clocks
  - Not required to hear every Beacon to stay in synch

Infrastructure Beacon generation



- APs send Beacons in infrastructure networks
  - Beacon is a broadcast frame recurrently send out at Beacon intervals
    - Beacon interval usually about every 100ms
  - Beacon contains SSID and further information about the functions offered by the AP
- Transmission may be delayed by CSMA deferral.
  - Subsequent transmissions at expected Beacon Interval
    - not relative to last Beacon transmission
    - next Beacon sent at Target Beacon Transmission Time
- Timestamp contains timer value at transmit time.

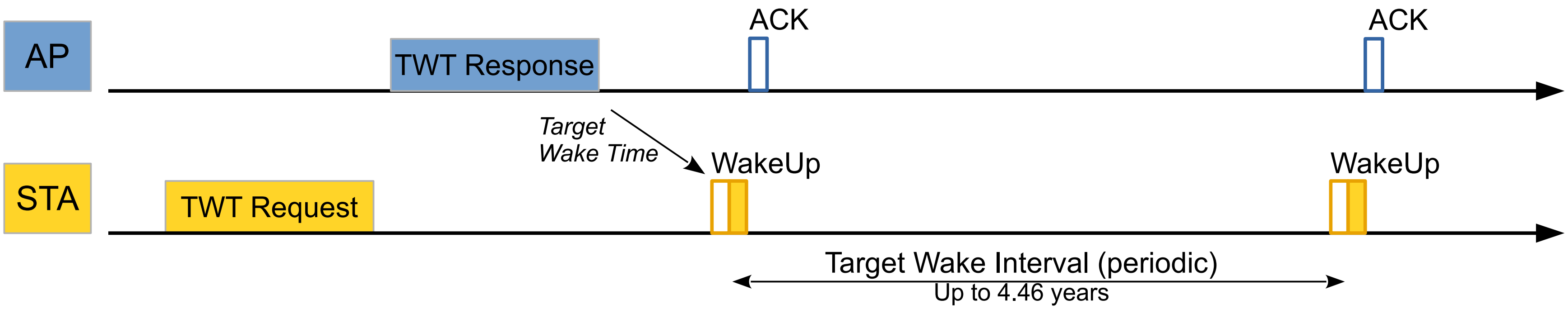
Legacy Power Management Procedure



- APs send periodic Beacons and operates as proxy for ‘sleeping’ Stations
  - Beacon is a broadcast frame recurrently send out at Beacon intervals, usually about every 100ms containing SSID and further information about the the AP
  - AP buffers frames destined for sleeping stations and indicates availability of buffered frames in the Traffic Indication Map (TIM)
  - 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 at least wake up shortly prior to an expected DTIM (Delivery Traffic Indication Map)
  - DTIM interval: interval at which buffered broadcast/multicast frames are transmitted
- If TIM indicates frame buffered for particular STA,
  - STA sends PS-Poll and stays awake to receive data
  - Else STA goes back to Power-Save state

Target Wake Time (TWT) power save procedure

- Initially introduced through IEEE 802.11ah (HaLow)
- STAs that expect to sleep for long periods 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 interval between TWT wake times can be very short (microseconds) to very long (years).

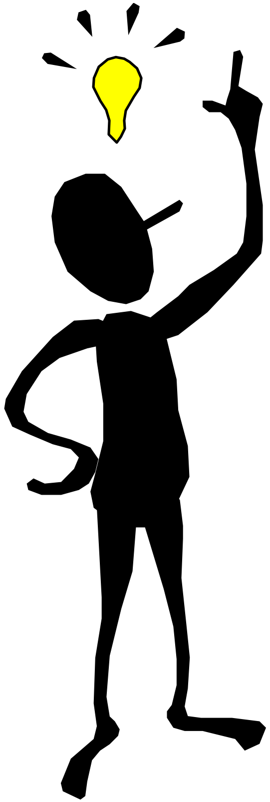


- Benefits of predefined TRX time
  - Wake-up time and channel access spread out
  - Allows AP to minimize contention
  - Reduces awake time for STAs, especially non-TIM STAs

Enhanced Power Management Procedures

Power Save Feature	How does it work?
Unscheduled Asynchronous Power Save Delivery (U-APSD)	Allows a STA to retrieve unicast QoS traffic buffered in the AP within one TXOP by sending trigger frames.
Target Wake Time (TWT)	Allows a STA to stay asleep for (long) periods of time and wake up at timeslots that are pre-scheduled (targeted) with the AP.
Restricted Access Window (RAW)	During a 'RAW' only a pre-defined subset of STAs are allowed to conduct uplink transmissions. This can reduce power consumption due to reduced contention for the medium.
Extended Max Idle Period	Extends the period during which a STA is allowed to be asleep before the AP disregards the STA. Theoretical maximum period is over 5 years, in practice this will be implementation dependent.
Hierarchical TIM	Method to more efficiently encode the Traffic Indication Map to reduce the 'on air time' for the TIM and to accommodate large number of STAs per AP.
Non-TIM Operation	Removes the need for a STA to periodically wake up to check beacon messages. In addition, the TIM part of the beacon can be ignored, when receiving a beacon.

Questions and answers



System management Questions…

1) What does MLME stand for?
2) Which sublayer provides the convergence protocol between the PMD Sublayer and the MAC sublayer in the protocol architecture?
3) What function provides the Distribution System of the Infrastructure configuration?
4) What are the two main functions of the MAC layer systems management?
5) What is the purpose of the Timer Synchronization Function?
6) Please shortly outline the role of the Delivery Traffic Indication Message for the power management in IEEE 802.11
7) What does TWT mean, and by which method does it provides better power management than legacy TIM?

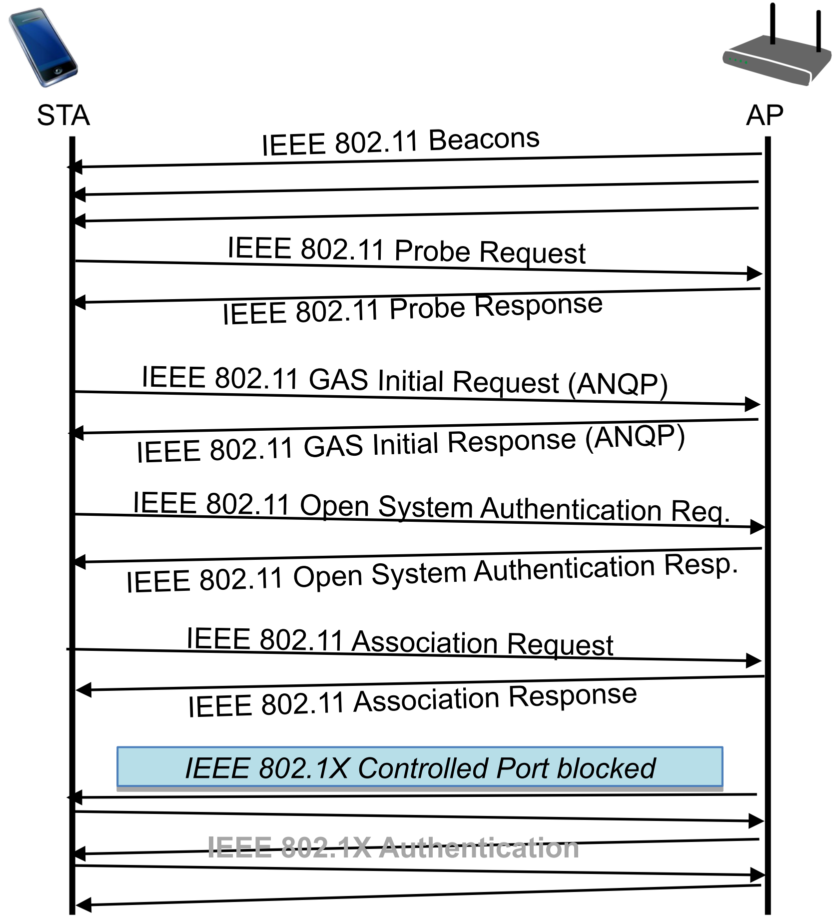
WLAN IEEE 802.11 aka Wi-Fi

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

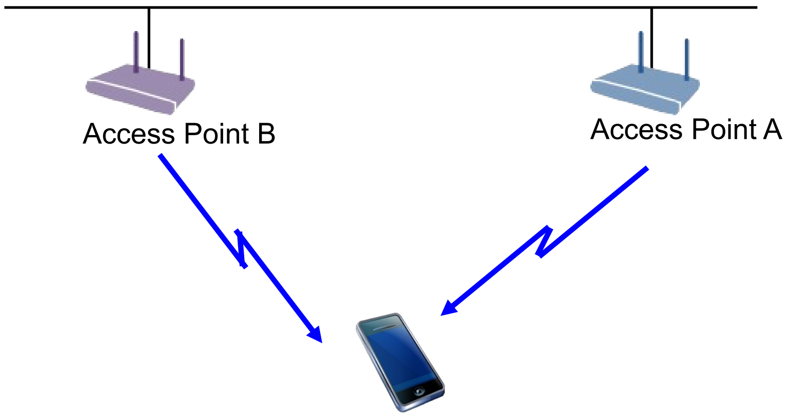
Session Management

SCANNING

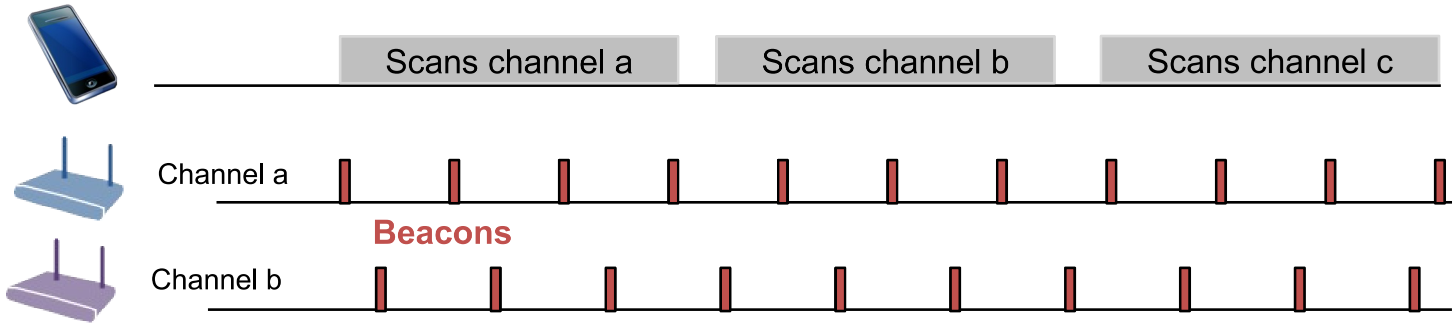
Scanning

- 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

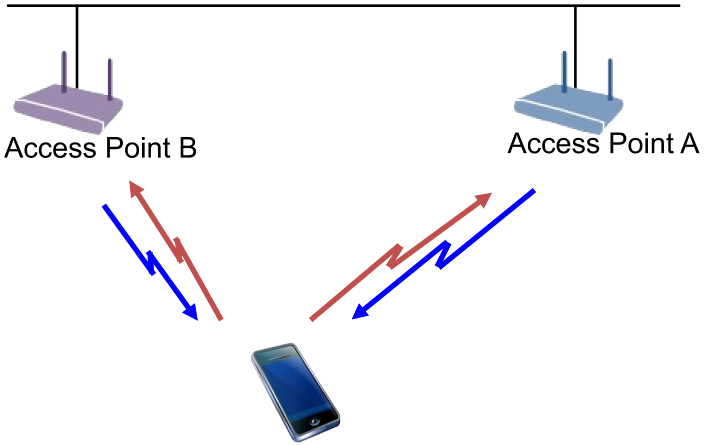


- APs send Beacons every 100..200ms
- STA subsequently tunes to all channels and listens for Beacons
- To successfully detect all Beacons, STA stays on a channel for about 200-300ms
- Scan of 2.4 GHz band takes about 2.5-4 s

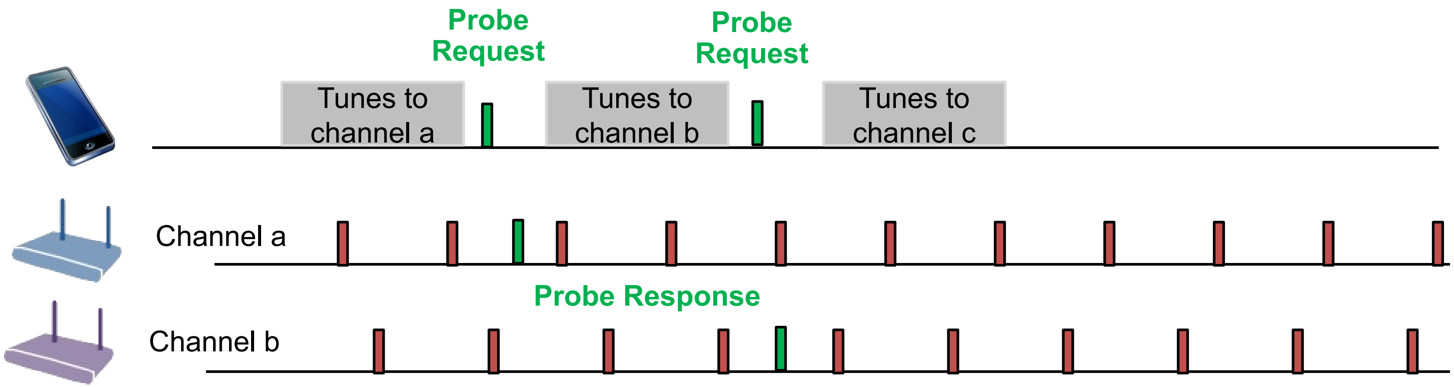


Active scanning

Station sends Probe.
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.



Session Management

NETWORK SELECTION

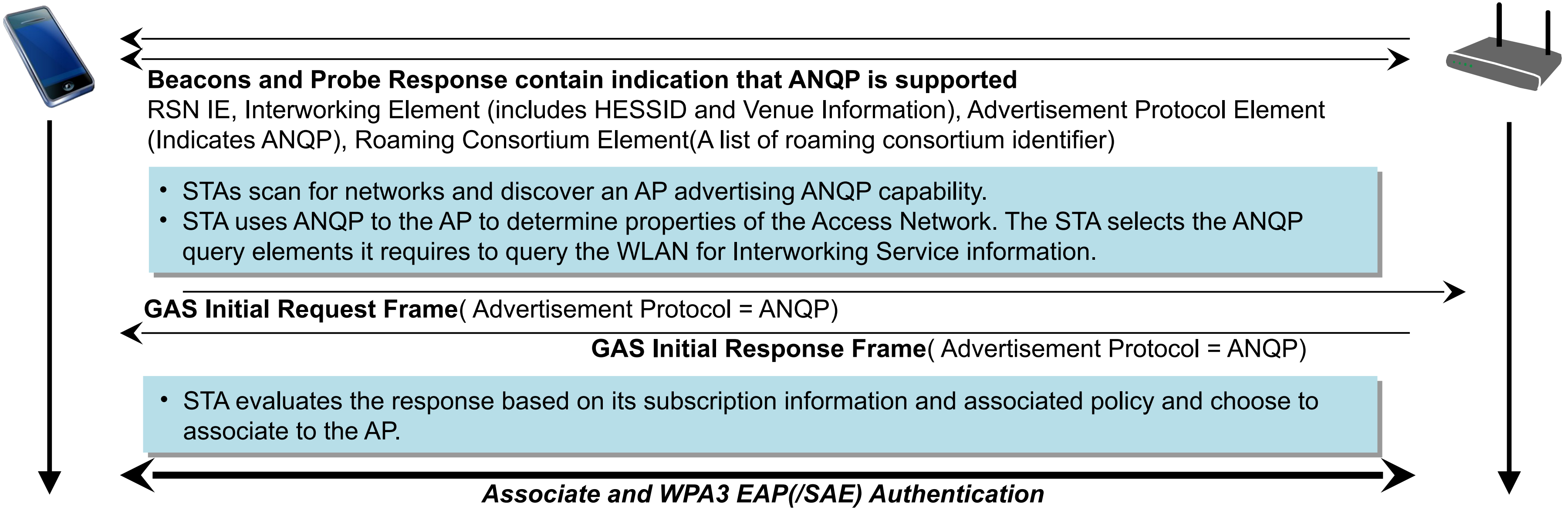
Generic Advertisement Service

- 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



ANQP Attributes

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

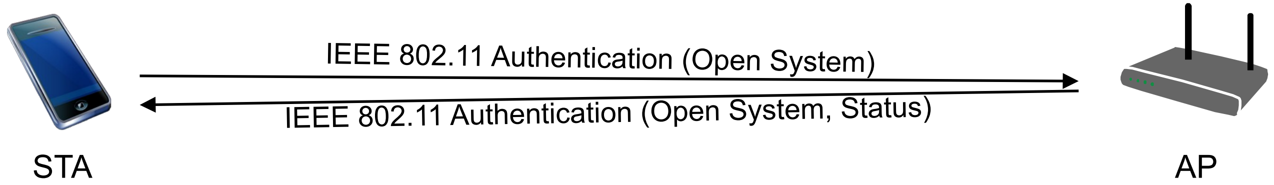
ANQP Attributes

- 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.

Session Management

AUTHENTICATION

Authentication

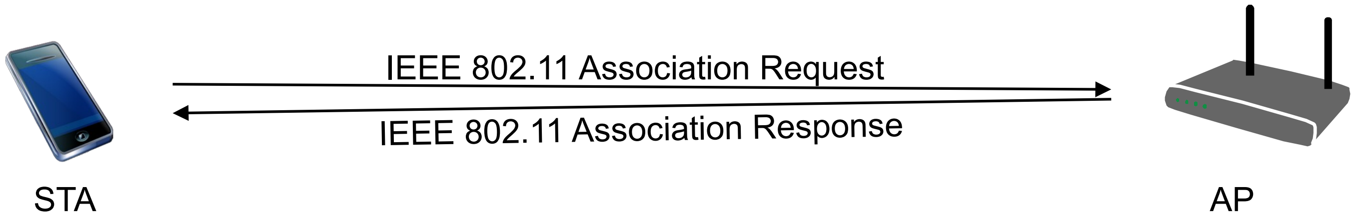


- Authentication before association is ‘leftover’ of legacy IEEE Stds 802.11 without WPA2 support (prior to IEEE 802.11i aka WPA2).
- For conformance and compatibility reasons Open System Authentication is performed, which only checks for the MAC addresses of the STA.
  - In legacy IEEE 802.11, AP could 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)).

Session Management

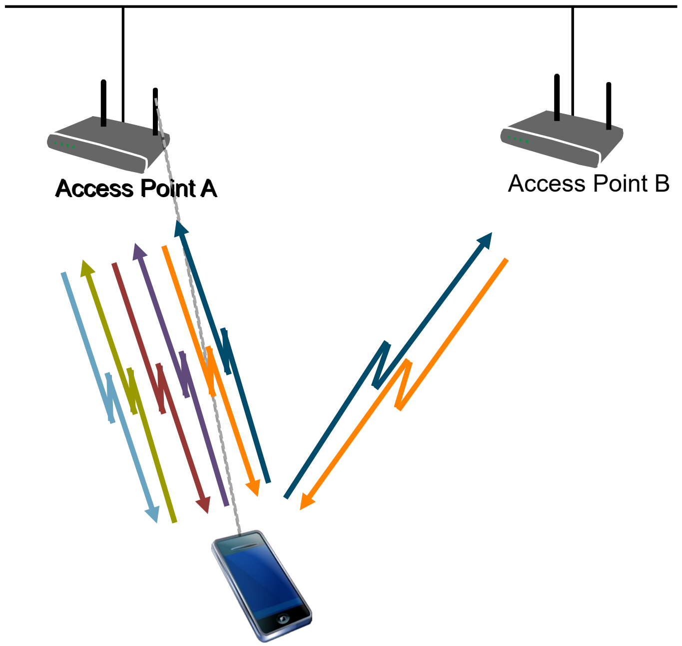
ASSOCIATION

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

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

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).

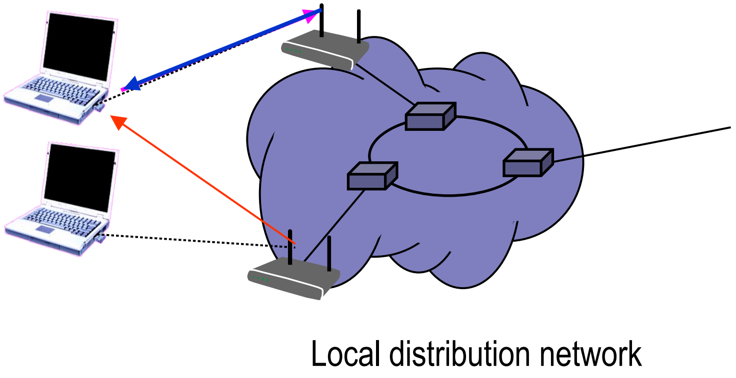
Session Management

MOBILITY SUPPORT

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

Session Management

MAC MANAGEMENT MESSAGES

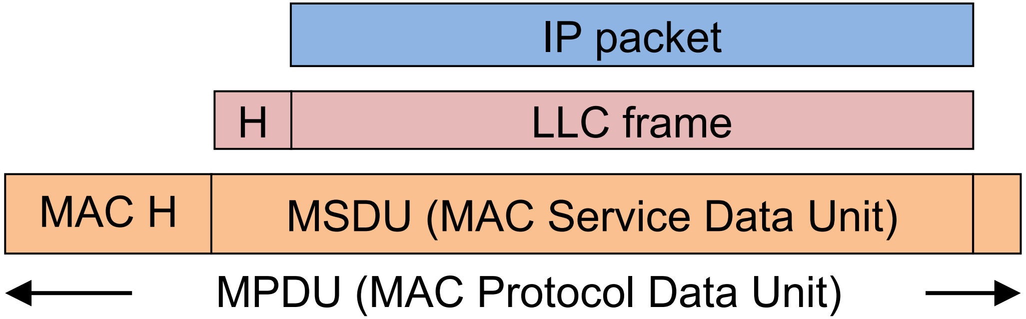
Basic MAC management messages attributes

- 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

WLAN IEEE 802.11 aka Wi-Fi

MAC FRAME FORMATS

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

802.11 MAC Header

Bytes:	2	2	6	6	6	2	6	0 - 2312	6
	Frame Control	Duration ID	Address1	Address2	Address3	Sequence Control	Address4	MSDU	CRC

Bits:	2	2	6	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

- 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

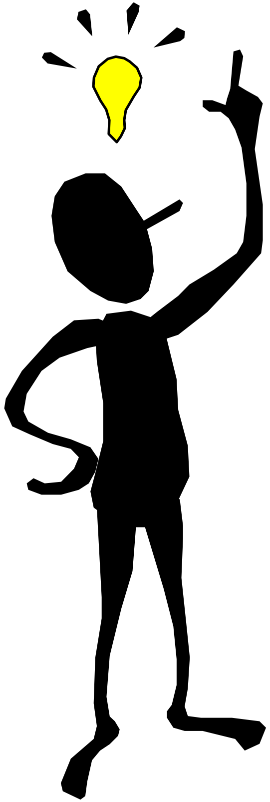
- Addr 1 = Destination of the radio frame
- Addr 2 = Transmitter Address (TA) identifies entity to receive the ACK frame
- Addr 3 = Entity on DS sending/receiving frame
- Addr 4 = Needed to identify the original source in case of WDS (bridging over the air).

Header field specification

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

- 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

Questions and answers



Mac Layer Management Questions…

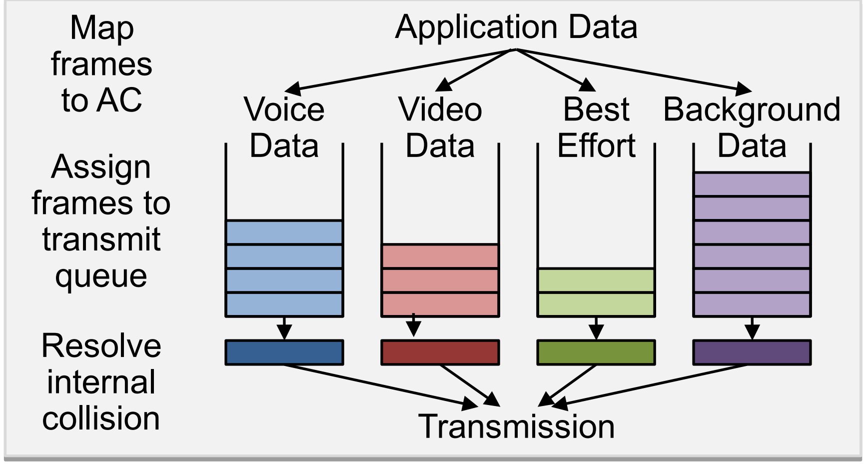
1) Which sequence of MAC management procedures is necessary for the establishment of a connection in IEEE 802.11
2) What is the purpose of scanning?
3) What are beacons in IEEE 802.11?
4) Explain the difference between active scanning and passive scanning.
5) What stands 'GAS' in IEEE 802.11 for?
6) What is the purpose of ANQP in IEEE 802.11?
7) How is ANQP related to GAS?
8) What is the purpose of IEEE 802.11 association procedure?
9) What is a Reassociation in IEEE 802.11?
10) Please shortly explain the MAC procedures for handover from on AP to another AP of the same ESS.
11) What are the limitations of Layer 2 mobility management?

WLAN IEEE 802.11 aka Wi-Fi

QUALITY OF SERVICE

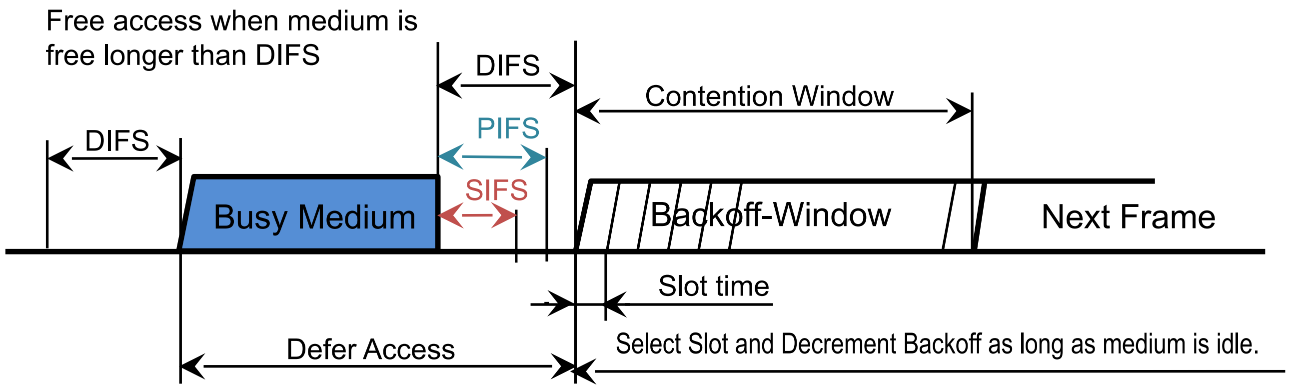
Quality of Service through Traffic Priorization

- Traffic is classified according to its importance and forwarding requirements
- Traffic Categories (TC) for prioritization
  - Differentiated channel access for frames with different user priorities
  - 8 different priorities, similar to IEEE 802.1Q specification



-	IEEE 802.1D/Q 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

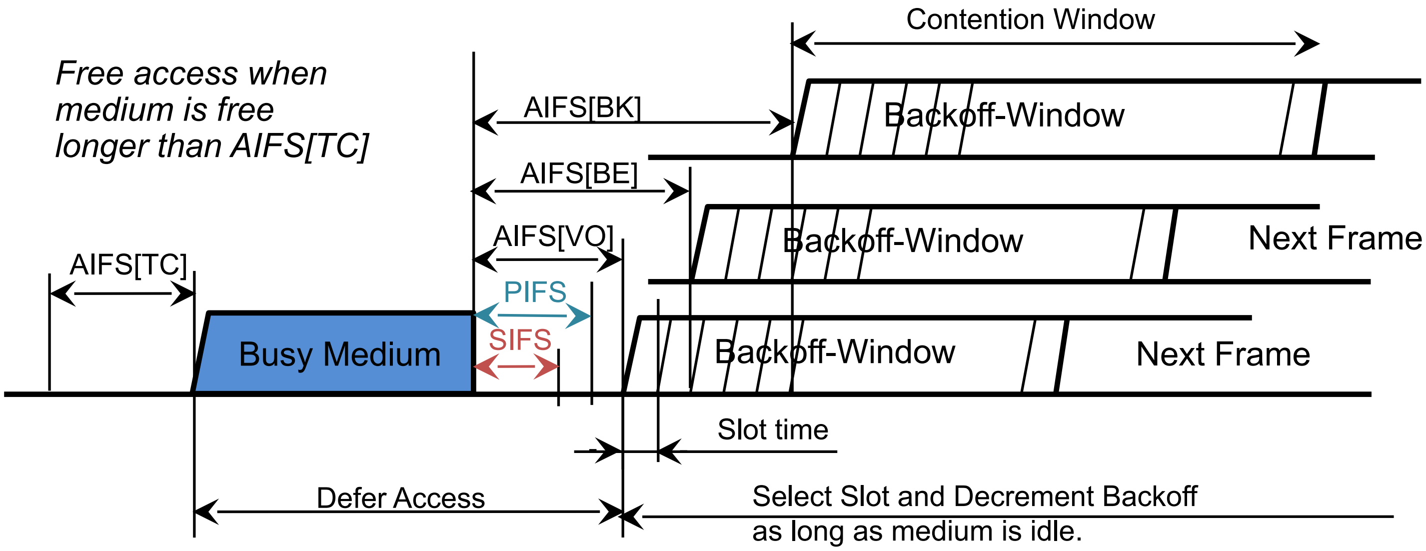


Standard	Slot time (µs)	DIFS (µs)
IEEE 802.11b	20	50
IEEE 802.11a/n/ac	9	34
IEEE 802.11g/n	9	28

SIFS: Short Inter Frame Space
PIFS: PCF 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)	DIFS (µs)
IEEE 802.11b	20	50
IEEE 802.11a/n/ac	9	34
IEEE 802.11g/n	9	28

SIFS: Short Inter Frame Space
PIFS: PCF 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

WLAN IEEE 802.11 aka Wi-Fi

WI-FI MULTIMEDIA (WMM)

QoS support provided by Wi-Fi Multimedia

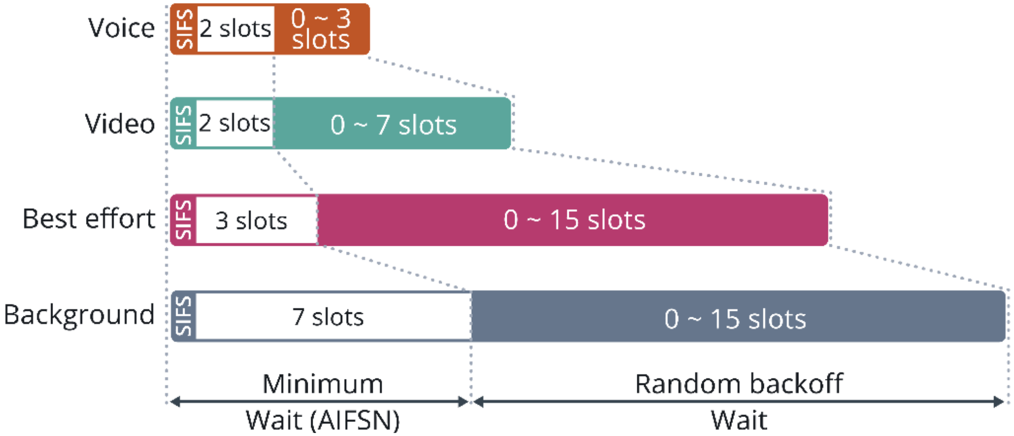
- Wi-Fi Multimedia (WMM) defines the QoS capabilities of Wi-Fi.
  - WMM makes use of EDCF for traffic prioritization.
  - Prioritized QoS identifies 4 traffic classes (Access Categories)
    - Aligned to the 8 priorities defined within IEEE 802.1Q.

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

- 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 PHY mode.



- Default EDCA Parameters for each AC (e.g. 802.11a/n)

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

Parameterized QoS for Traffic Stream

- 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.

Improvements for channel utilization and efficiency

- Transmission Opportunities
  - TXOP is a time interval during in which a station can send as many frames as possible
    - But staying within the maximum duration of the TXOP
    - Frames too large for a single TXOP are fragmented into smaller frames.
    - TXOPs reduces the problem of low rate stations gaining too much channel time
- Block Acknowledgement
  - Group of frames received consecutively acknowledged by a BlockAck
- Direct Link Protocol (DLP)
  - STA-to-STA transmission in the infrastructure mode
    - DLP handles the problems related, e.g. power saving of the receiving STA
- Unscheduled Asynchronous Power Save Delivery (U-APSD)
  - Legacy power-save mode is based on DIFS without protection of medium access
  - Allows a STA to retrieve unicast QoS traffic within one TXOP buffered in the AP by sending trigger frames.
  - U-APSD exchange of frames occurs with SIFS separation
    - Medium remains locked during the exchange.

WLAN IEEE 802.11 aka Wi-Fi

WI-FI QOS IN ACTION

WMM performance: Comparison DCF vs. EDCF

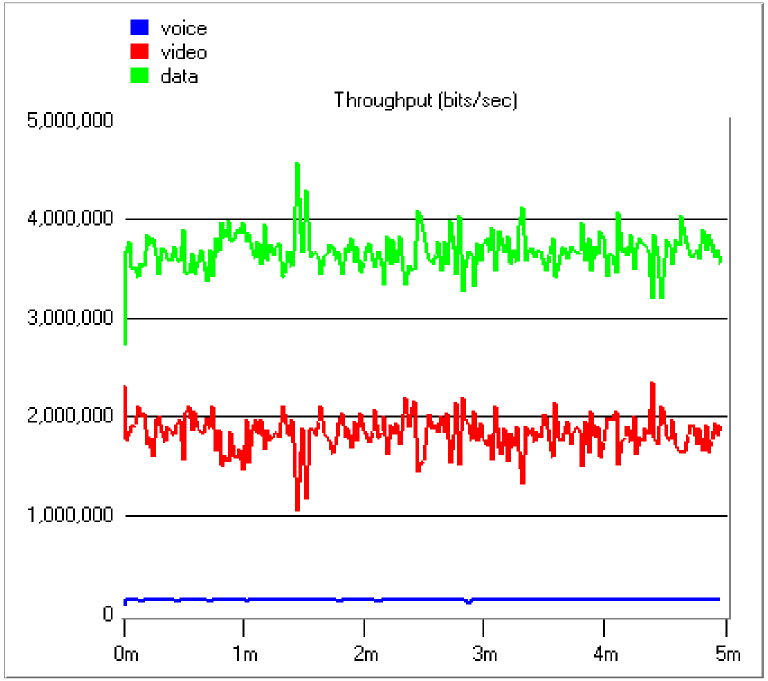
- E.g: Sunghyun Choi; J. del Prado; Sai Shankar N; S. Mangold, IEEE 802.11e contention-based channel access (EDCF) performance evaluation, IEEE International Conference on Communications, 2003.
  - http://www.cs.jhu.edu/~baruch/RESEARCH/Research_areas/Wireless/wireless-public_html/class-papers/802.11e-performance.pdf
  - 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:

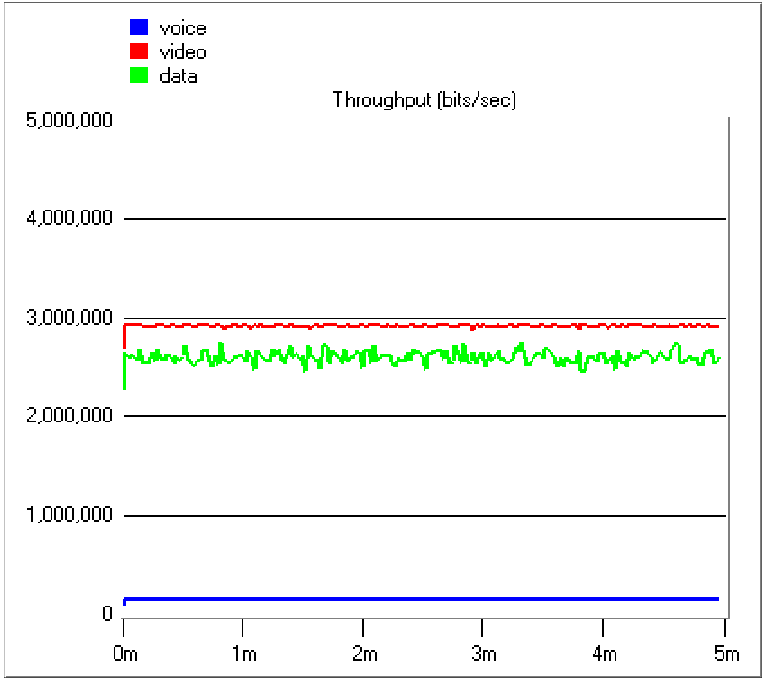
Type	Inter-arrival Time (Avg. in sec)	Frame Size (bytes)	Data Rate (Mbps)
Voice	Constant (0.02)	92	0.0368
Video	Constant (0.001)	1464	1.4
Data	Exponential (0.012)	1500	1.0

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

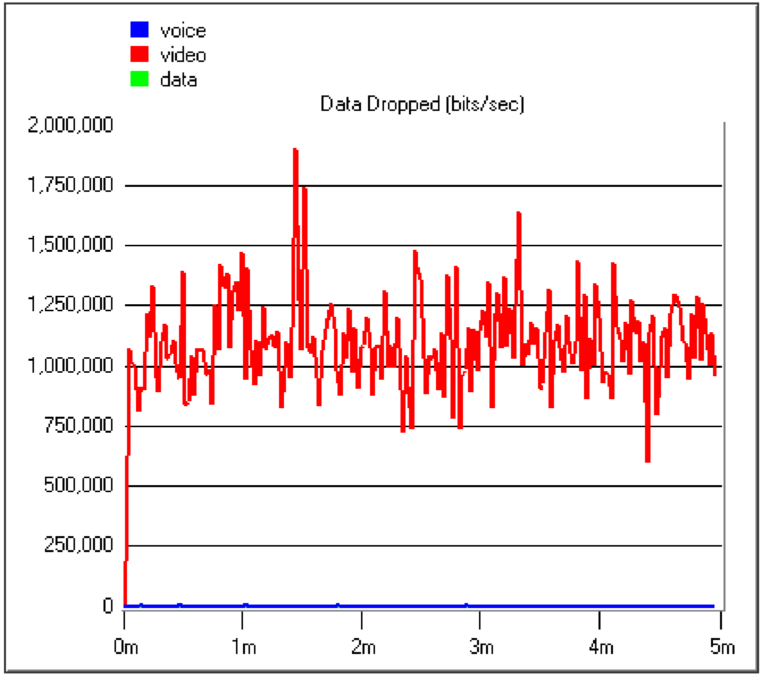
- Throughput comparison
  - Higher video throughput with EDCF

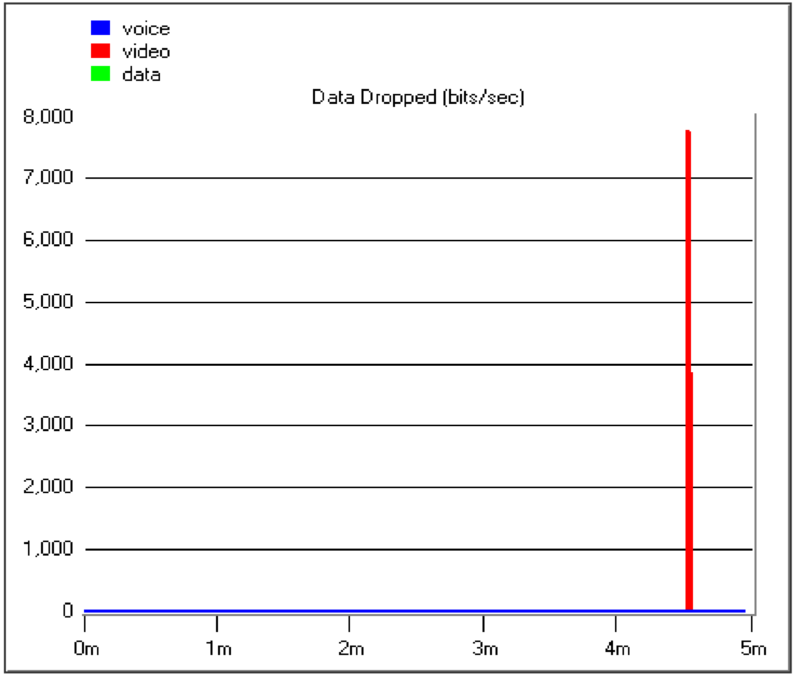




DCF vs. EDCF

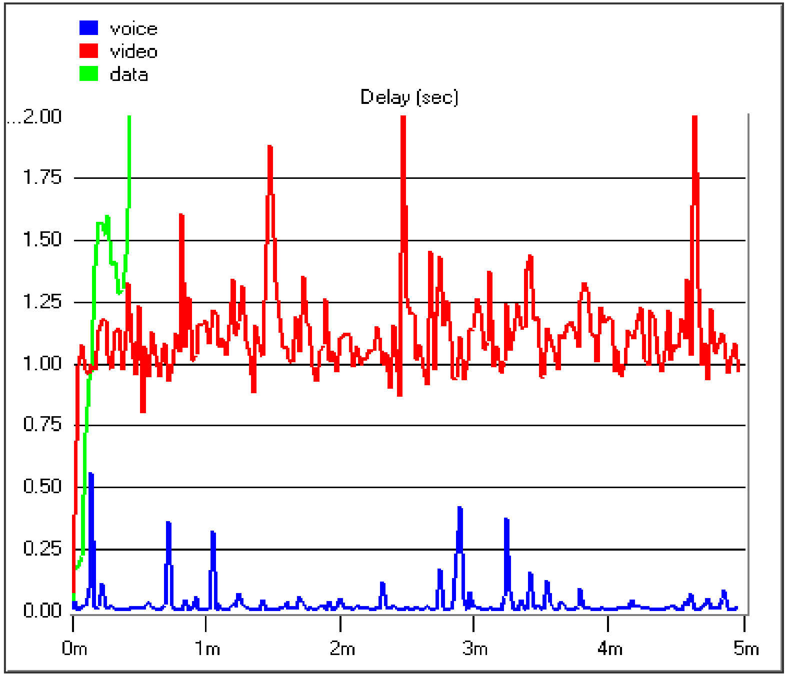
- Data dropping rate comparison
  - Video drop virtually gone with EDCF

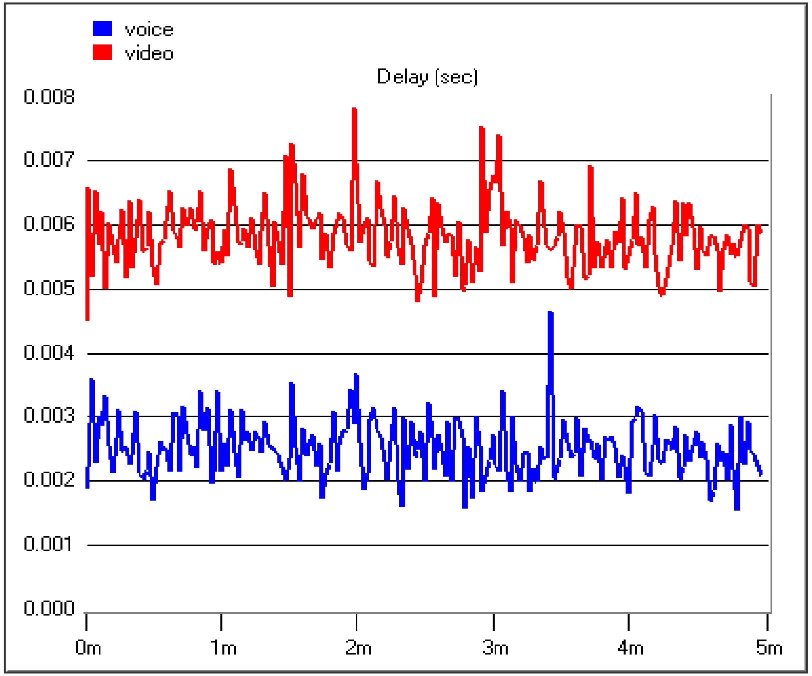




DCF vs. EDCF

- Delay comparison
  - Voice and video delays significantly reduced



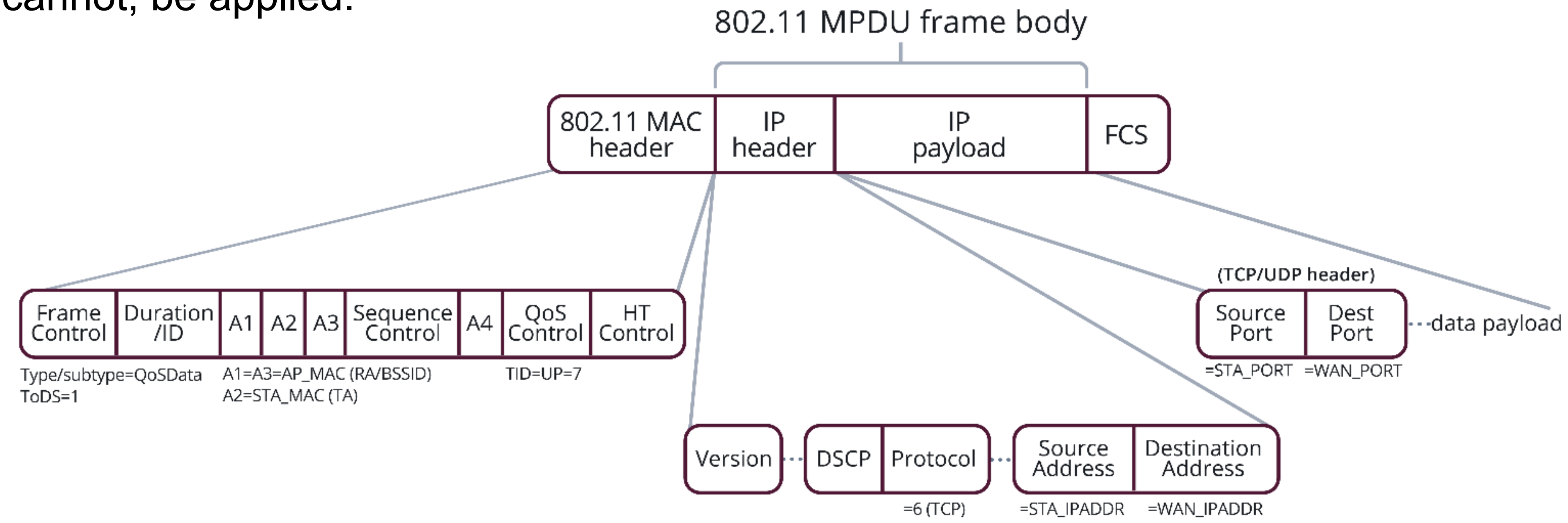


WLAN IEEE 802.11 aka Wi-Fi

WI-FI CERTIFIED QOS MANAGEMENT

How to assign User Priorities to packets?

- User Priority needs to be determined based on the higher layer QoS requirements of the application or service.
- Most commonly, applications signal this intent via DSCP marking within the IP packet header, which can then be mapped to a User Priority.
- However, there are many scenarios in which the appropriate DSCP marking is not, or cannot, be applied.

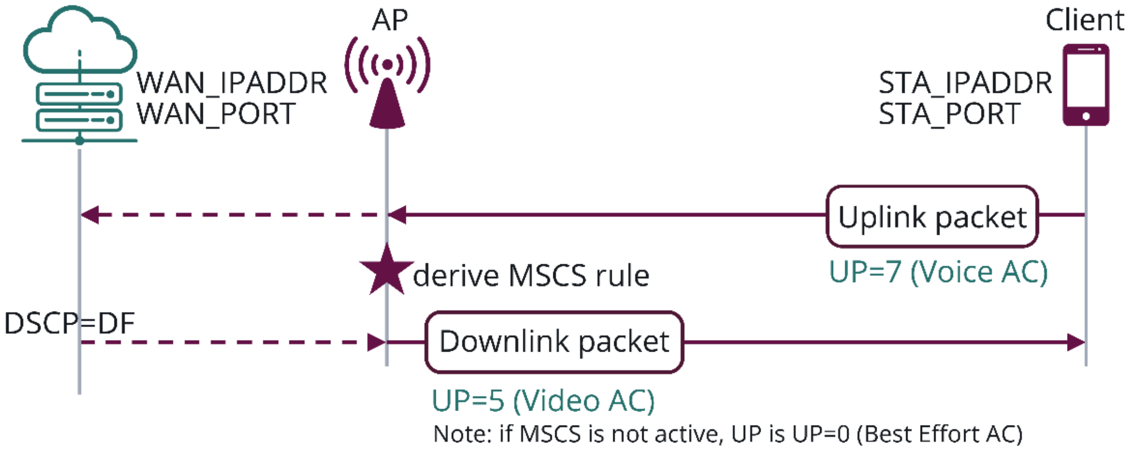


Wi-Fi CERTIFIED QoS Management

- Wi-Fi QoS Management enables negotiation and management of QoS treatment for traffic flows over-the-air between an AP and STA
- The WMM-based QoS treatment (UP/AC) of each flow might be determined from higher-layer marking such as DSCP, or implicitly from the uplink QoS of corresponding flows
  - The Wi-Fi QoS Management defines 4 different methods to map traffic streams to UP/AC: MSCS, SCS, DSCP mapping, and DSCP policy.
  - Leverages existing QoS protocols and primitives defined in IEEE 802.11 (e.g., MSCS, QoS Map) in order to classify flow(s) that require QoS treatment and allow management of QoS treatment, where either AP or STA might initiate the request
  - Aligns QoS treatment across Wi-Fi and wired networks
  - 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 flow classifiers.
- SCS could be described as more granular protocol compared to MSCS
  - MSCS only works when AP receives a corresponding uplink flow from STA
  - 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

WAN

IETF Diffserv Service Class	Per-Hop Behavior
Network Control	CS7
Internetwork Control	CS6
Telephony	EF
Voice Admit	VA
Signaling	CS5
Multimedia Conferencing	AF41, AF42, AF43
Real-Time Interactive	CS4
Multimedia Streaming	AF31, AF32, AF33
Broadcast Video	CS3
Low-Latency Data	AF21, AF22, AF23
Low-Priority Data	CS1
OAM	CS2
High Throughput Data	AF11, AF12, AF13
Standard	DF

Wi-Fi®

User Priority	Access Category
7	AC_VO (Voice)
6	AC_VO (Voice)
5	AC_VI (Video)
4	AC_VI (Video)
3	AC_BE (Best Effort)
1	AC_BK (Background)
0	AC_BE (Best Effort)

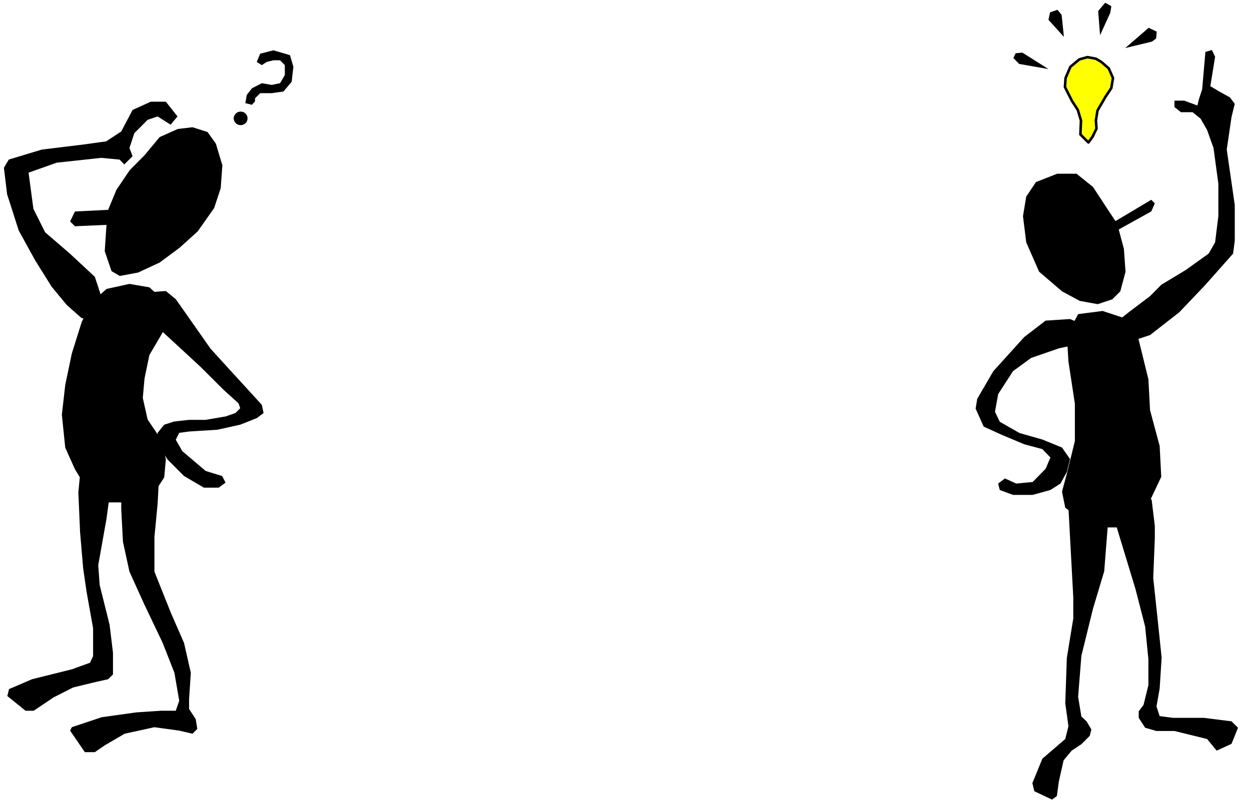
Default DSCP to User Priority Mapping based on RFC 8325

- 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 after STA roams between BSSs within the same ESS
- DSCP Policy can be negotiated post-association by either STA or by AP

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) By which standard amendment was QoS support added to IEEE 802.11?
4) What is AIFS?
5) How many traffic categories does exist in IEEE 802.1Q, and how many does WMM support?
6) How are the QoS classes denoted that are supported by WMM?
7) Through which method are traffic classes realized in IEEE 802.11?
8) What does TSPEC mean, and for what is it used?
9) What is the purpose of Wi-Fi QoS management?
10) Which methods to assign WMM traffic classes to traffic streams are provided through Wi-Fi QoS management?

WLAN IEEE 802.11 aka Wi-Fi

END OF PART 2

Anything left for today?

See you again in Chemnitz next week☺.