Communication Systems
Wi-Fi (IEEE 802.11 WLAN) Part 3

WS 2025/2026@THI

Max Riegel
<max.riegel@ieee.org>

WS 2025/2026 Wi-Fi Lecture Topics

Part 1 (2025-11-25):

- Introduction
- Wi-Fi Architecture
- Wi-Fi Specifications
- Wi-Fi Spectrum
- Wireless Channel
- Wi-Fi PHY Evolution

Part 2 (2025-11-28):

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

Part 3 (2025-12-02):

- Wi-Fi Medium Access
- Wi-Fi MAC Management
- Wi-Fi QoS
- Wi-Fi MAC Layer Q&A

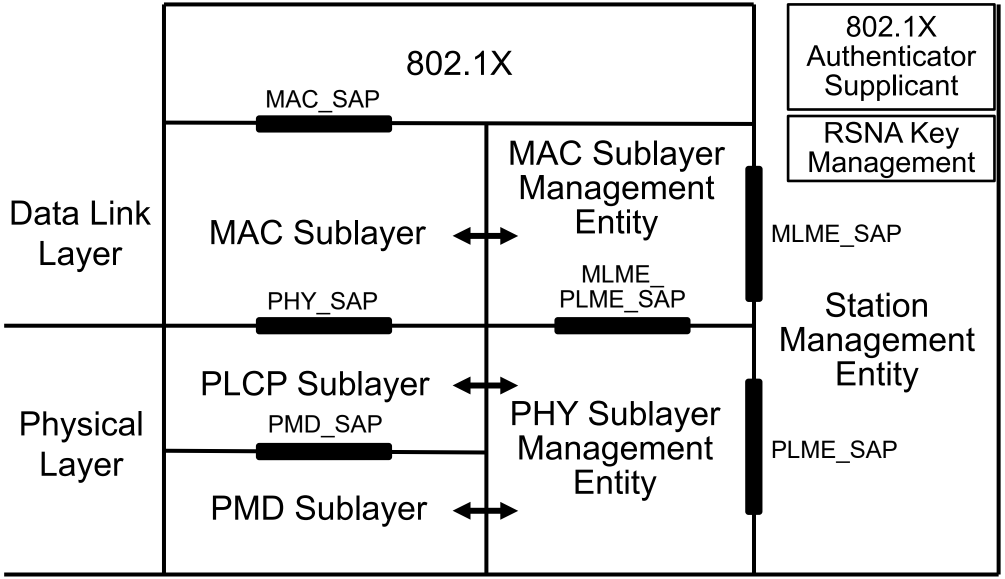
Part 4 (2025-12-05):

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

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
  - data 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

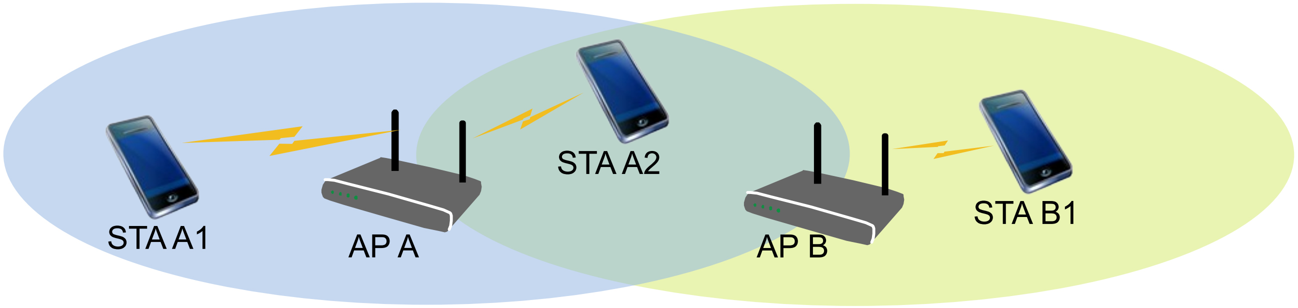


Wi-Fi MAC Layer

MEDIUM ACCESS CONTROL (MAC) SUBLAYER

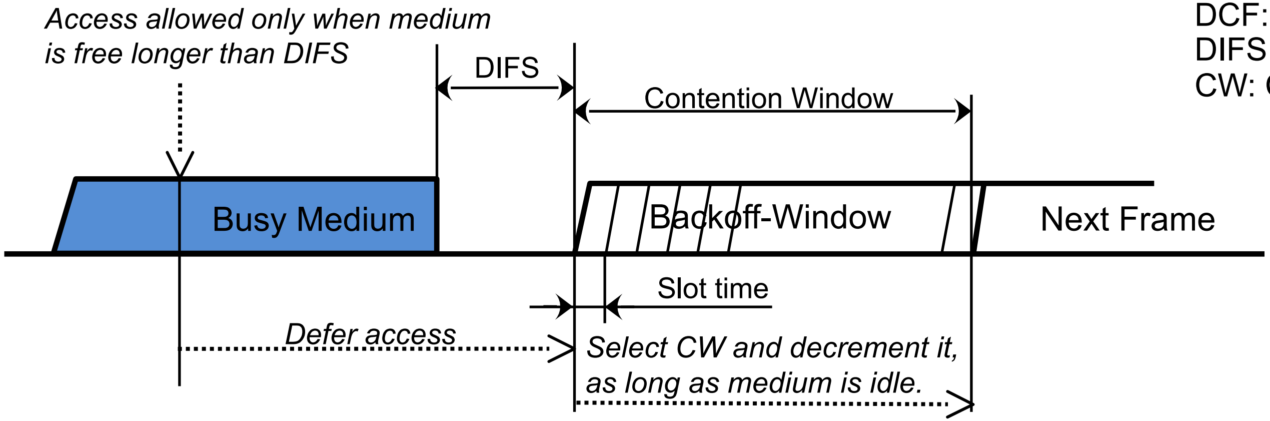
Shared Spectrum Medium Access Challenges

- 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.
  - With CSMA/**CD** (Carrier Sense Multiple Access/**Collision Detection**) a potential transmitters first listens to the medium to ensure that no other transmission is ongoing before starting its own transmission. When a collision is detected, the 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.

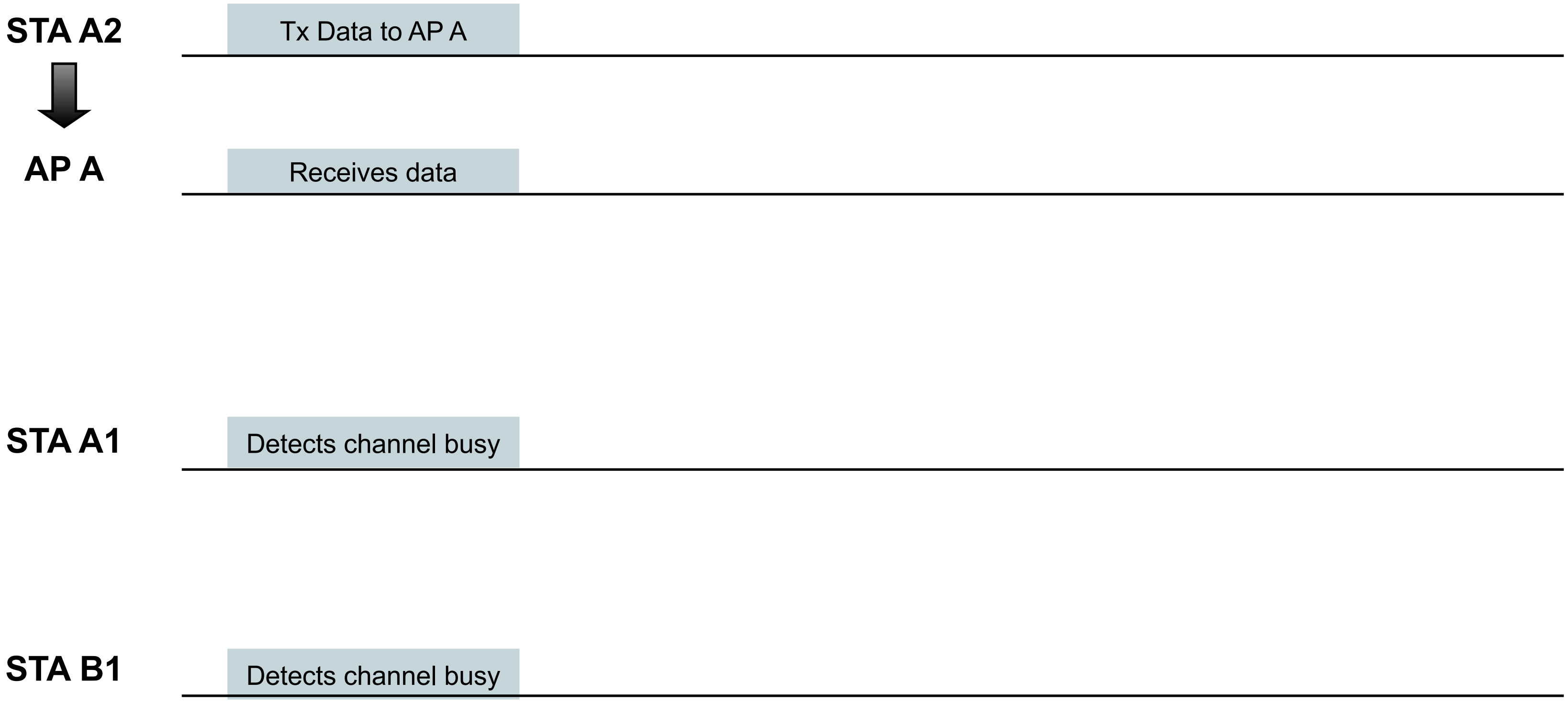
Carrier Sense Multiple Access with **Collision Avoidance**


Access allowed only when medium is free longer than DIFS
DIFS
Contention Window
Busy Medium
Backoff-Window
Next Frame
Slot time
Defer access
Select CW and decrement it, as long as medium is idle.

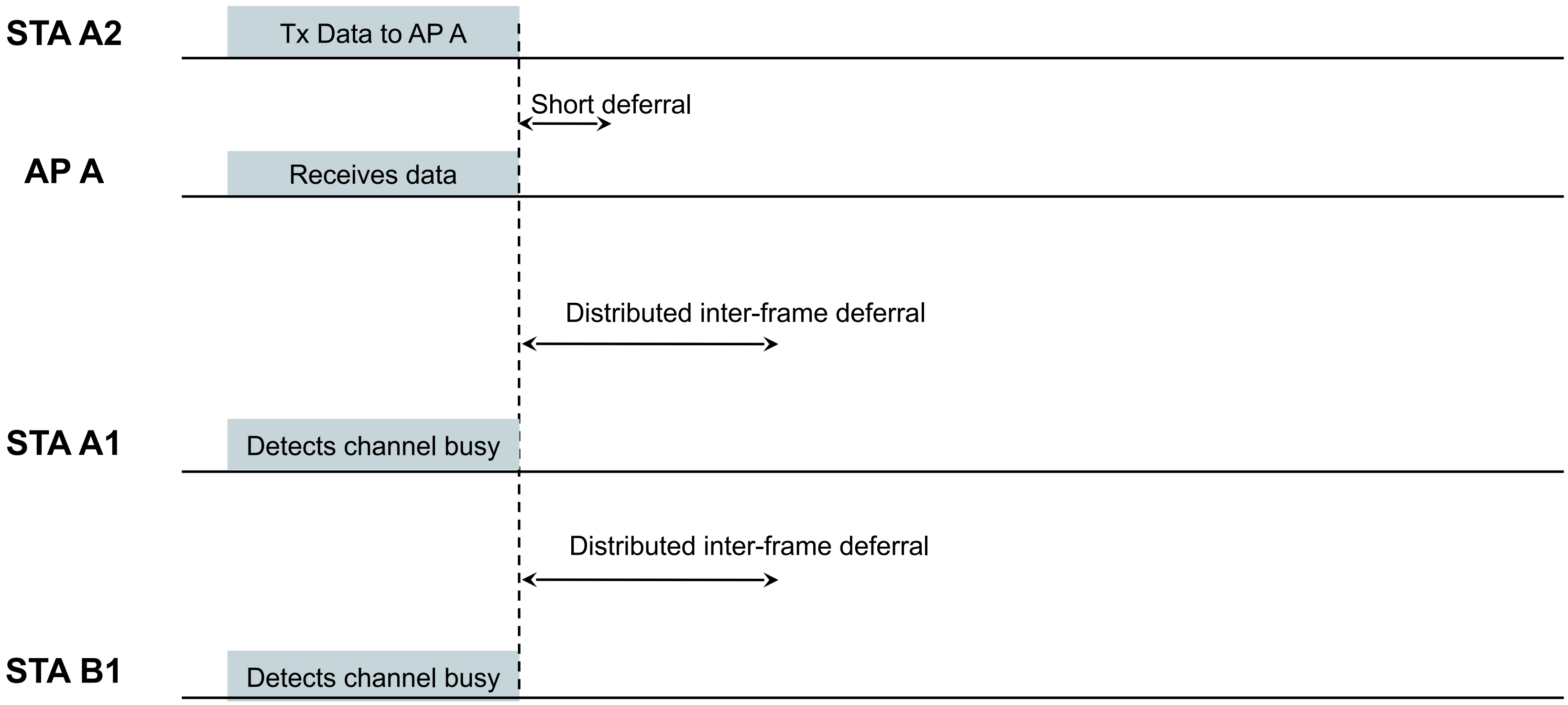
DCF: Distributed Coordination Function
DIFS: DCF Inter Frame Space
CW: Contention Window (multiple of slot time)

- 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

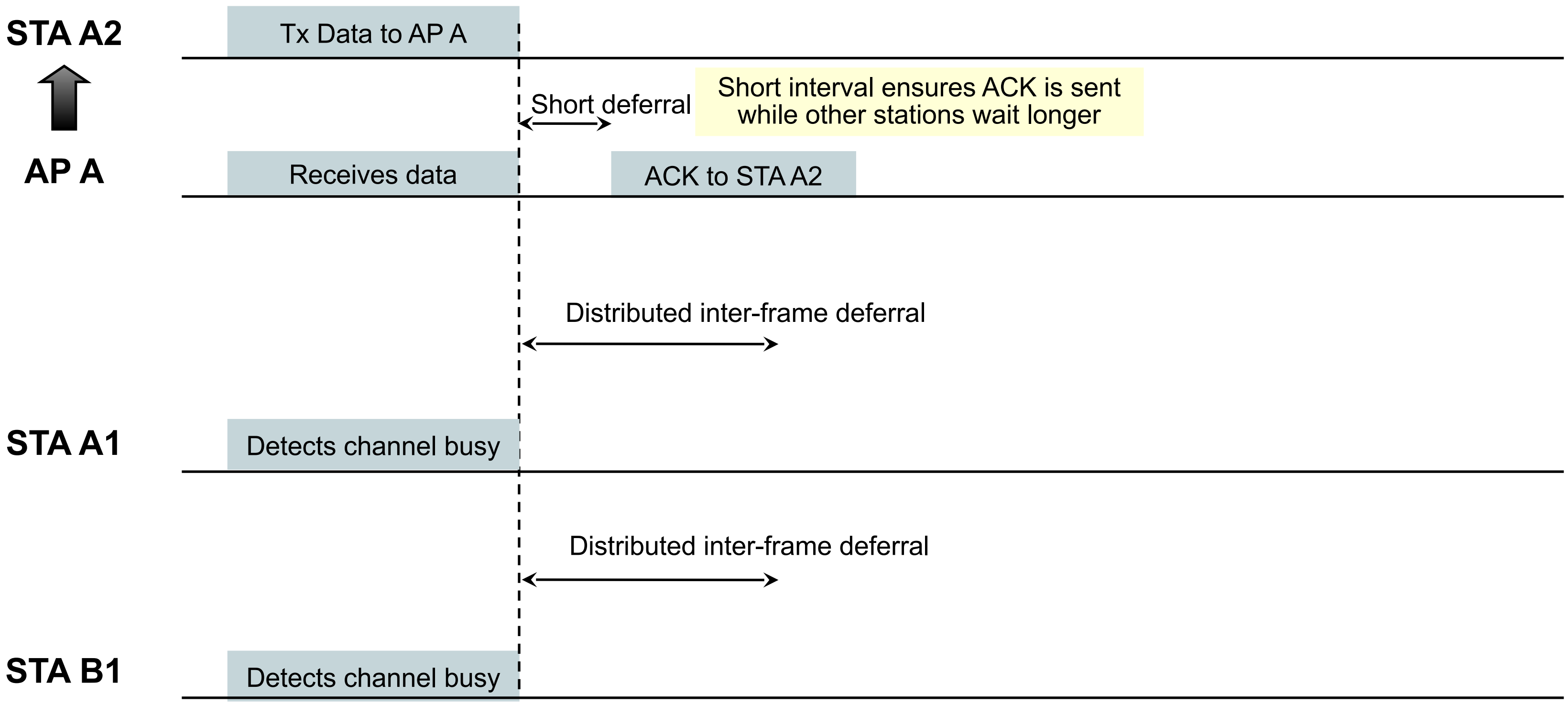
Distributed Coordination Function (DCF)



Distributed Coordination Function (DCF)

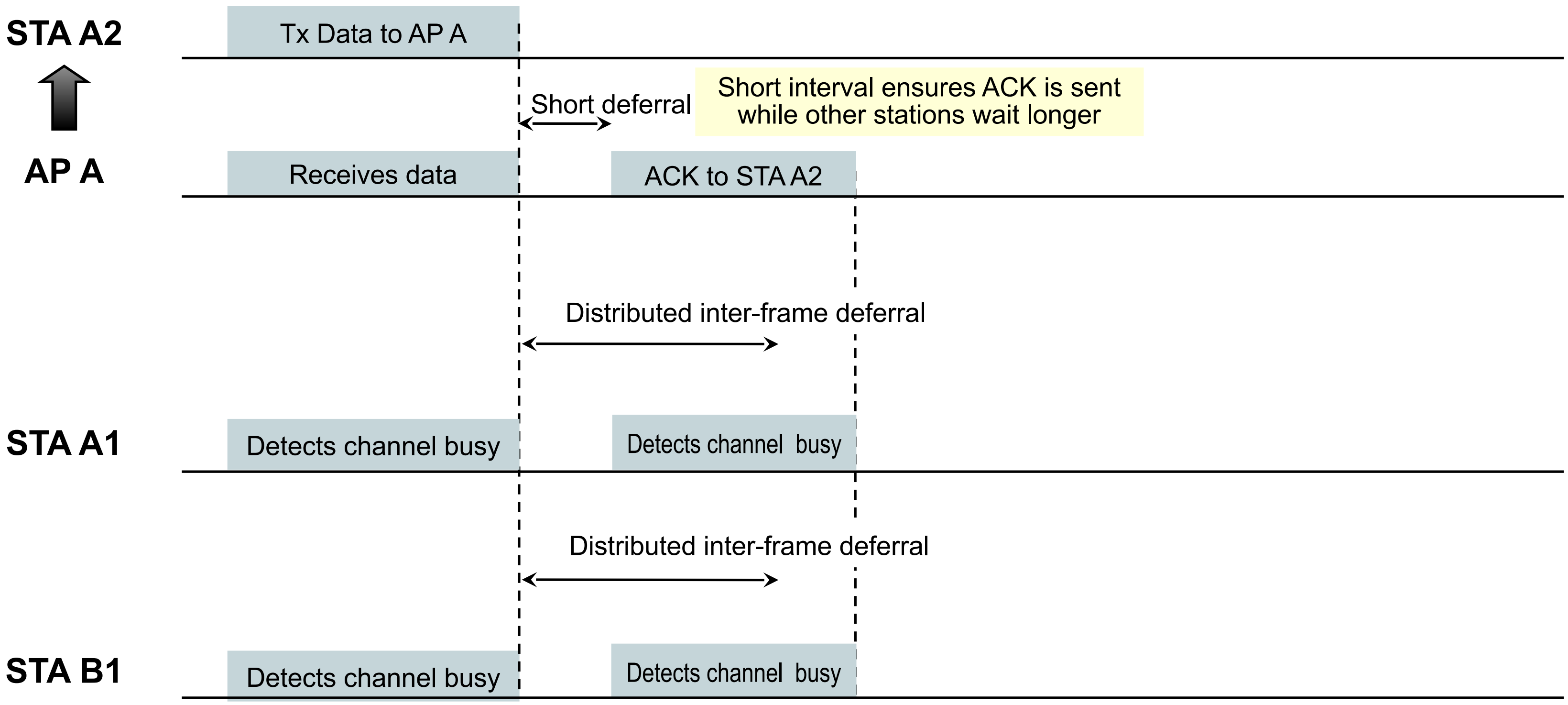


Distributed Coordination Function (DCF)



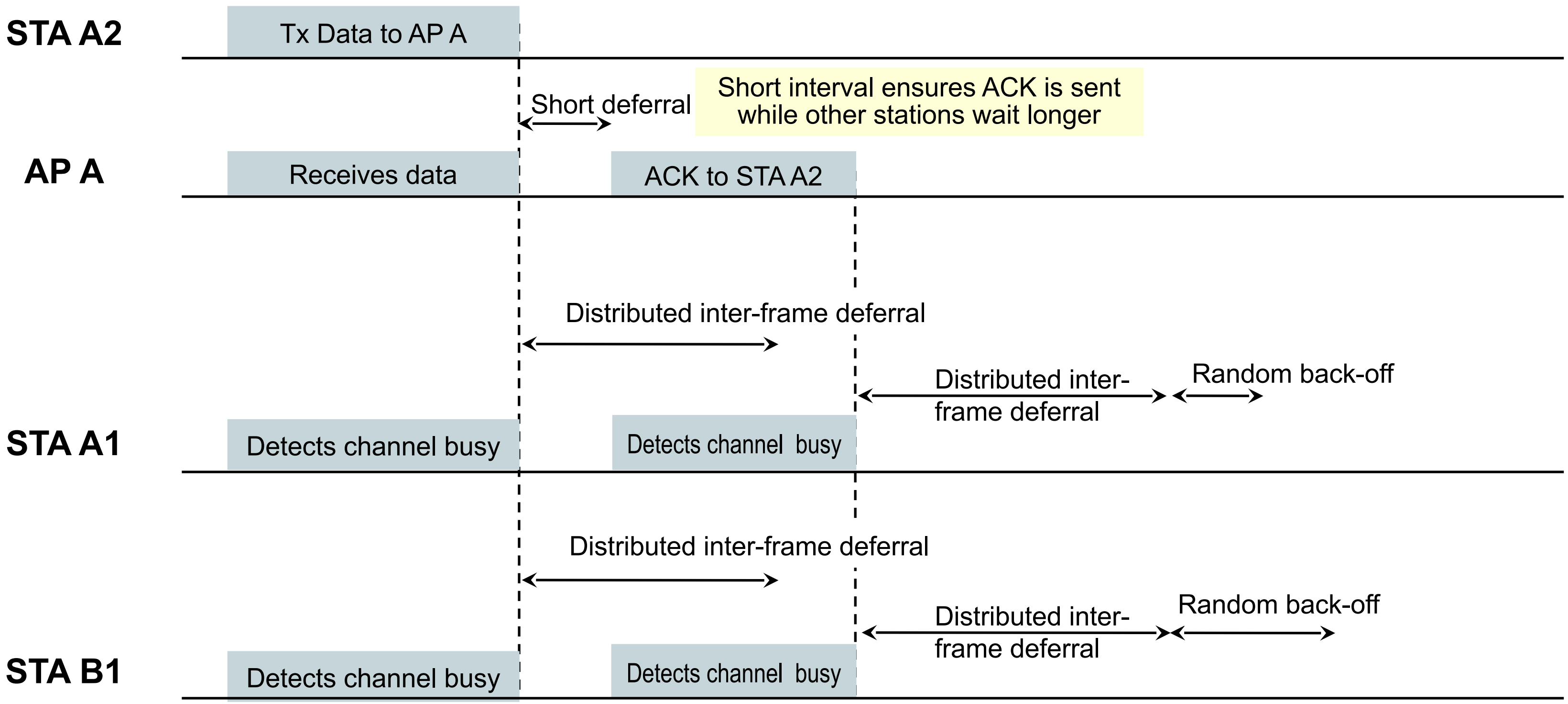
Short interval ensures ACK is sent while other stations wait longer

Distributed Coordination Function (DCF)

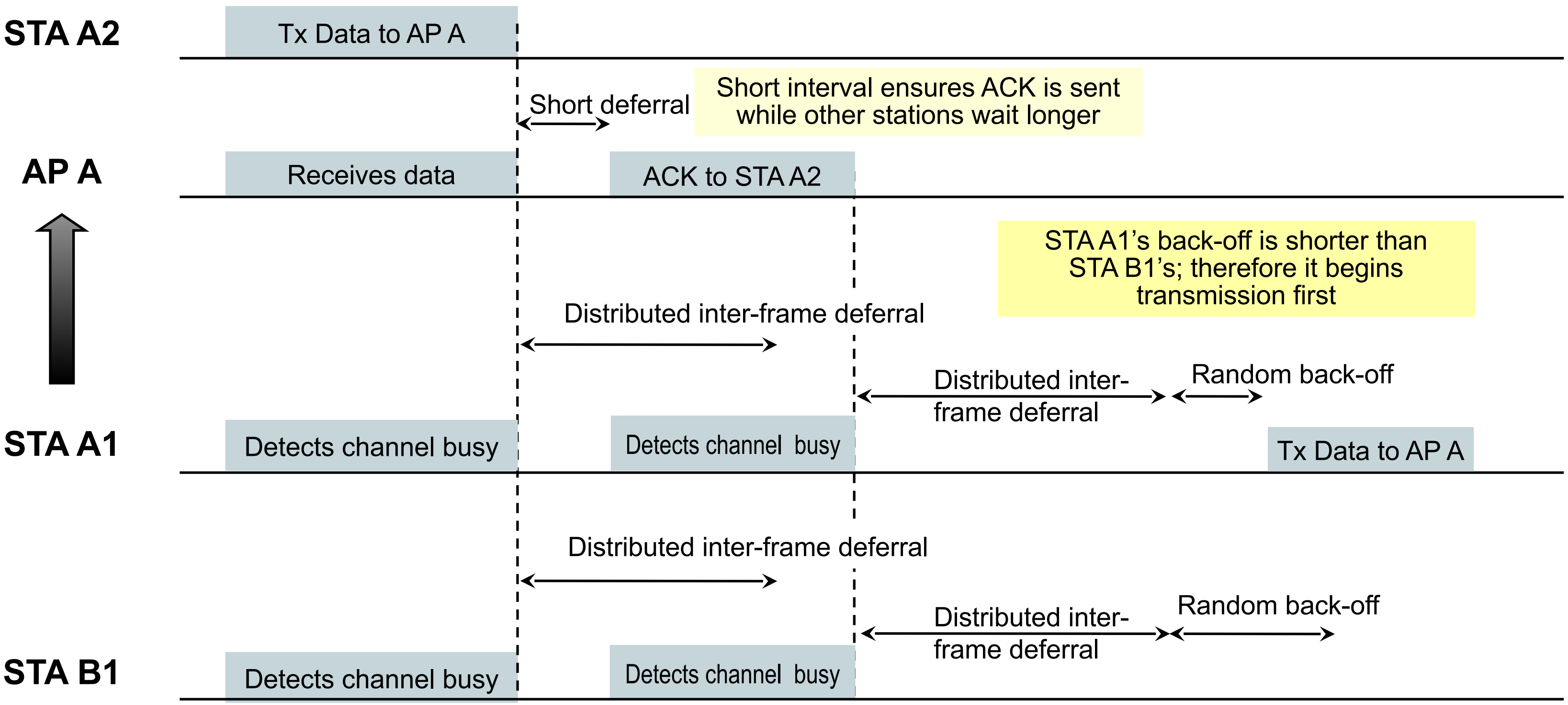


Short interval ensures ACK is sent while other stations wait longer

Distributed Coordination Function (DCF)


STA A2
Tx Data to AP A
Short deferral
Short interval ensures ACK is sent while other stations wait longer
AP A
Receives data
ACK to STA A2
Distributed inter-frame deferral
Distributed inter-frame deferral
Random back-off
STA A1
Detects channel busy
Detects channel busy
Distributed inter-frame deferral
Distributed inter-frame deferral
Random back-off
STA B1
Detects channel busy
Detects channel busy

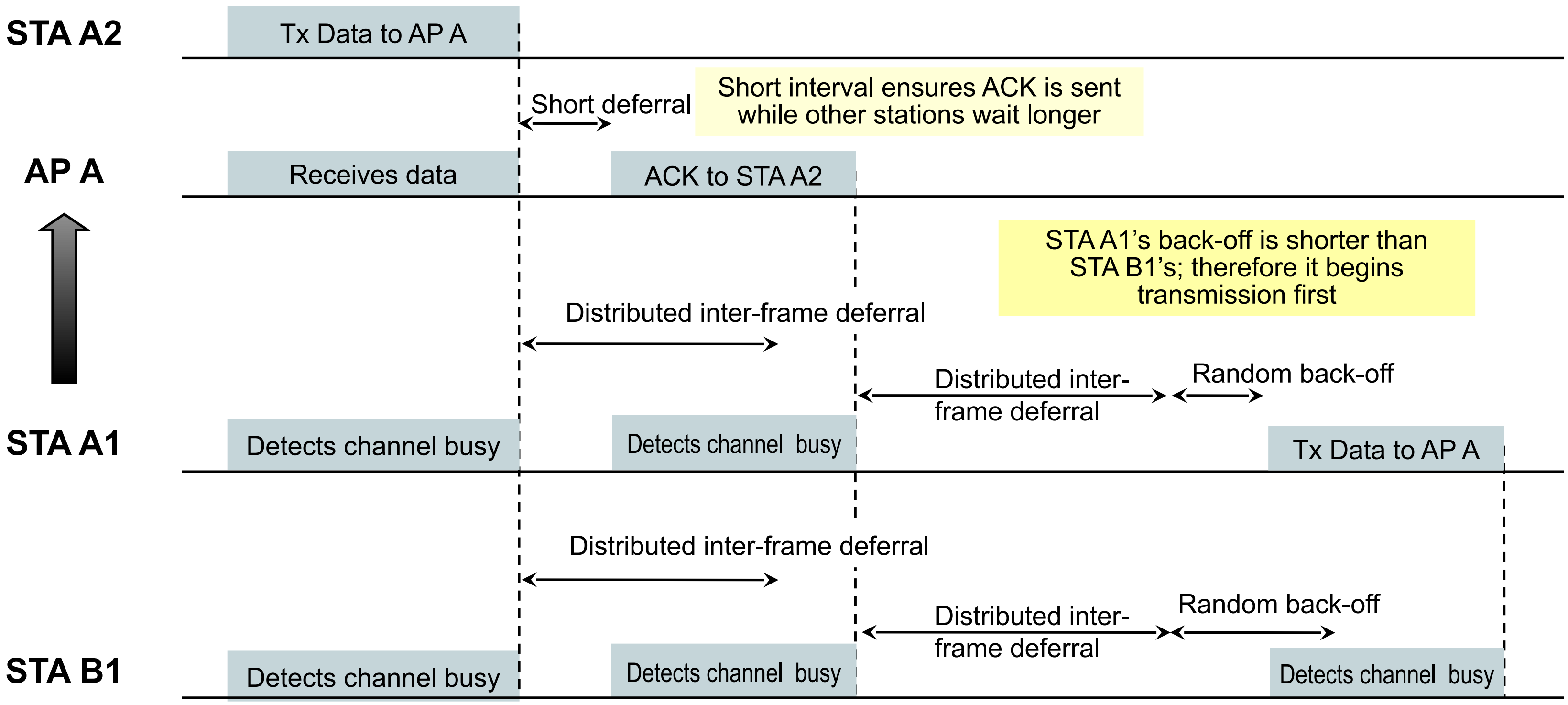
Distributed Coordination Function (DCF)



Short interval ensures ACK is sent while other stations wait longer

STA A1’s back-off is shorter than STA B1’s; therefore it begins transmission first

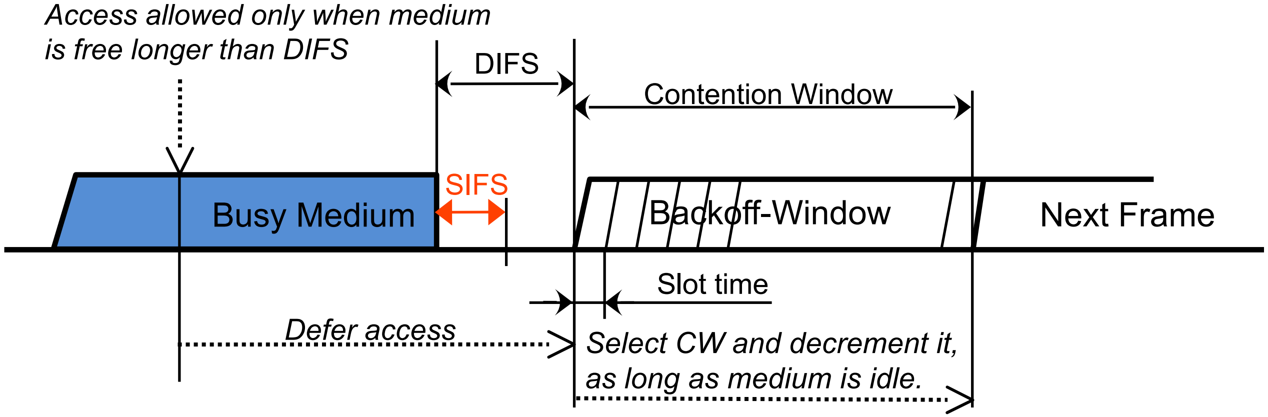
Distributed Coordination Function (DCF)



Short interval ensures ACK is sent while other stations wait longer

STA A1’s back-off is shorter than STA B1’s; therefore it begins transmission first

Physical carrier sensing: Clear Channel Assessment (CCA)


Access allowed only when medium is free longer than DIFS
DIFS
Contention Window
SIFS
Busy Medium
Backoff-Window
Next Frame
Slot time
Defer access
Select CW and decrement it, as long as medium is idle.

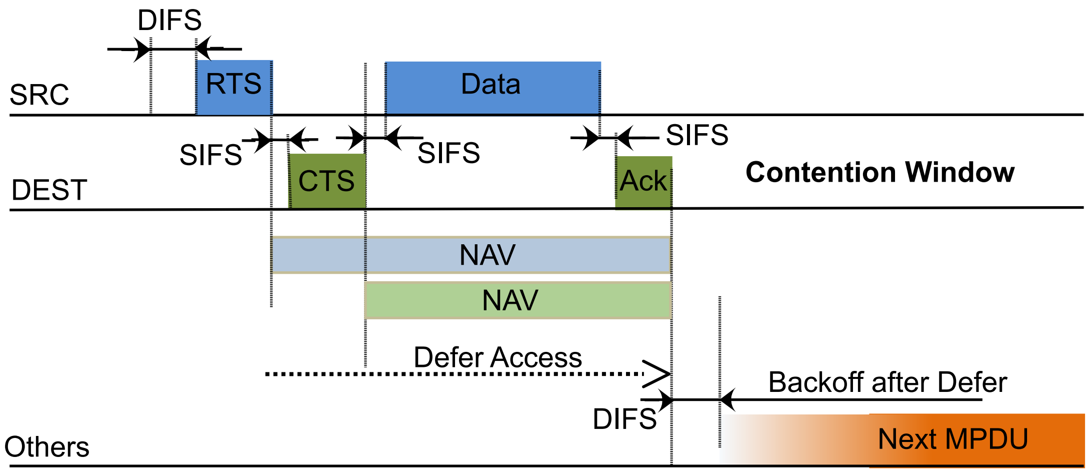
Band	SIFS[µs]	Slot time[µs]	DIFS[µs]
2.4 GHz	10	9	28
5 / 6 GHz	16	9	34

SIFS: Short 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 in the 2.4 GHz and 5 GHz band:
  - 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.

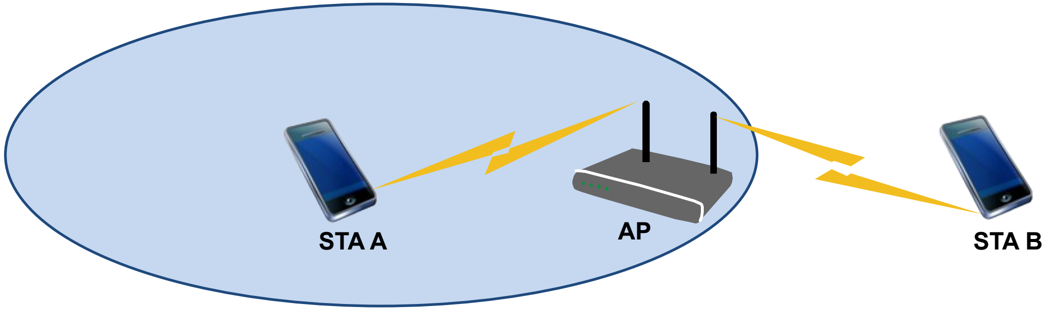
- Defering access in CSMA/CA also happens ‘virtually’ through NAV (Network Allocation Vector)
  - set by duration information in the MAC header



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

Hidden Node Problem

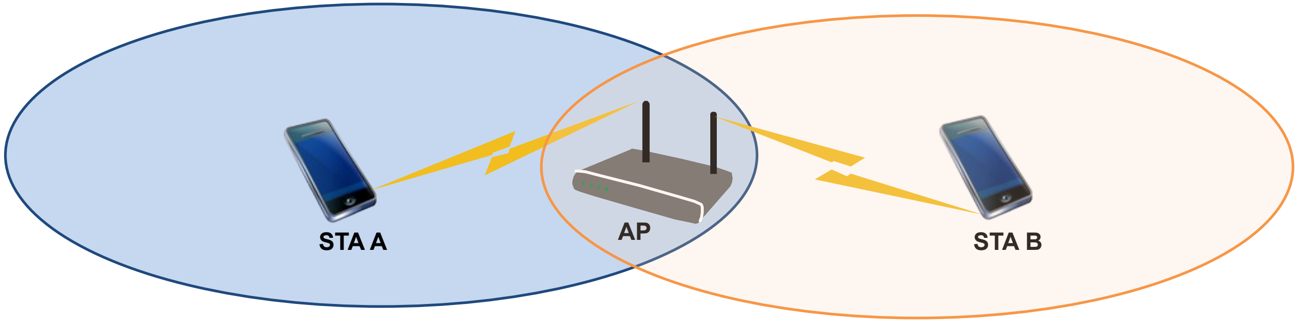
- A problem occurs when contending stations do not hear each other



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

Hidden Node Problem

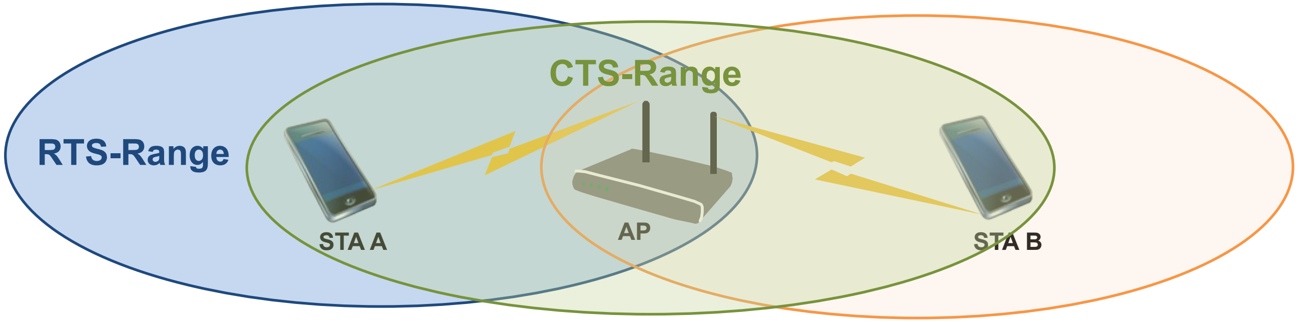
- A problem occurs when contending stations do not hear each other



  - 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

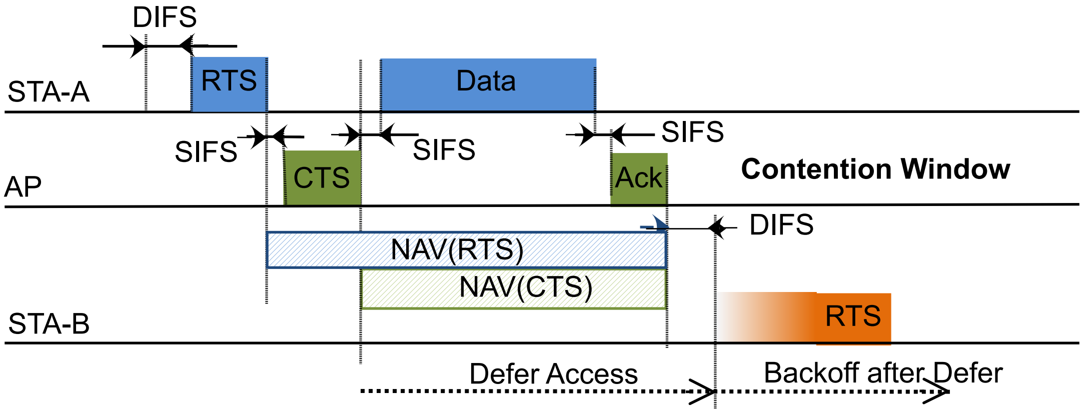
- A problem occurs when contending stations do not hear each other



  - 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.

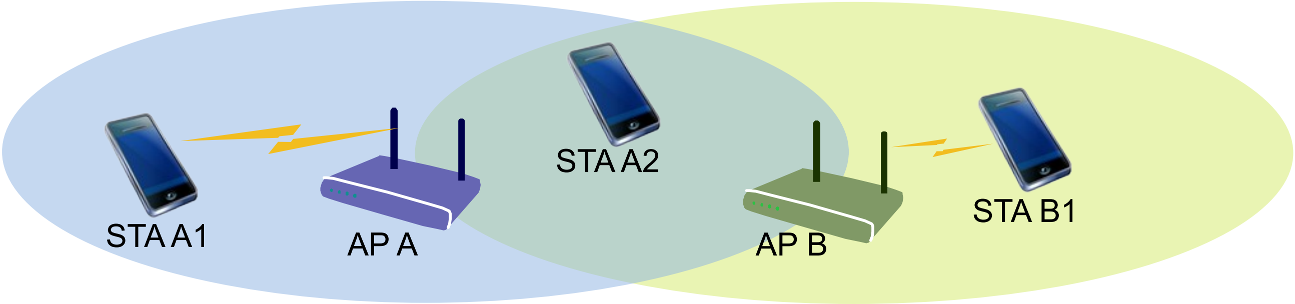
Hidden Node Solution

- 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.



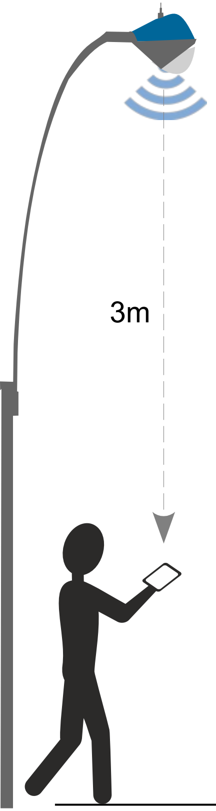
Better spatial reuse through BSS coloring

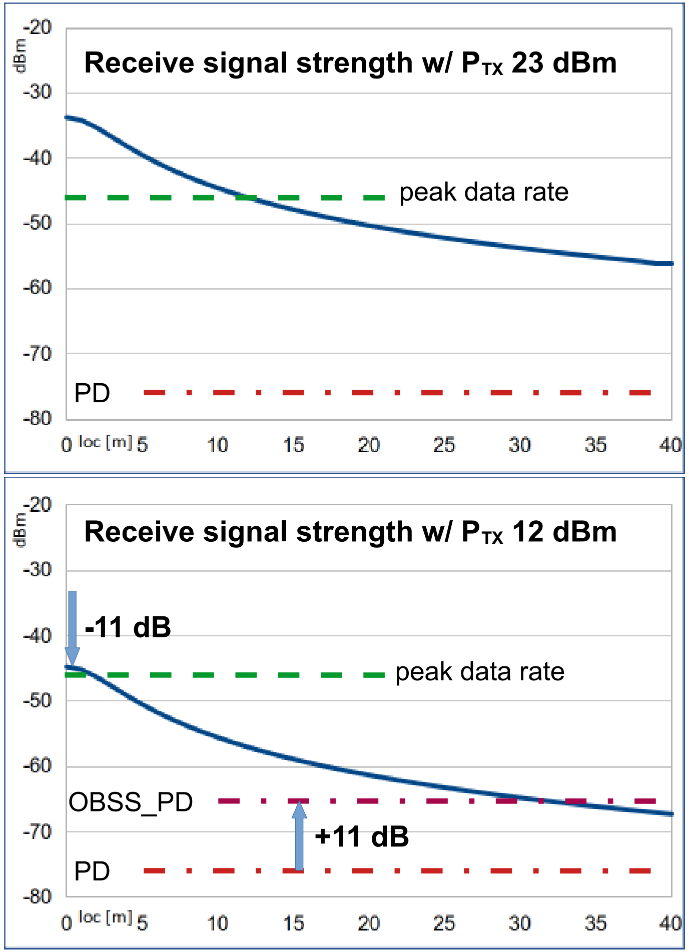
- In dense deployments, transmissions are stalled due to activities at distant BSS operating in the same channel.
- Still, successful transmission could be performed due to proximity of STA and AP despite parallel activies in the distant system.



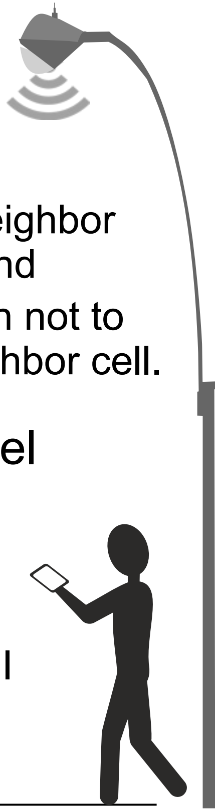
- With Wi-Fi 6/7, CCA is enabled to distinguish intra-BSS frames from frames coming from other systems (OBSS).
  - BSS Coloring puts a 'color' value into the PHY header of each transmission frame.

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.



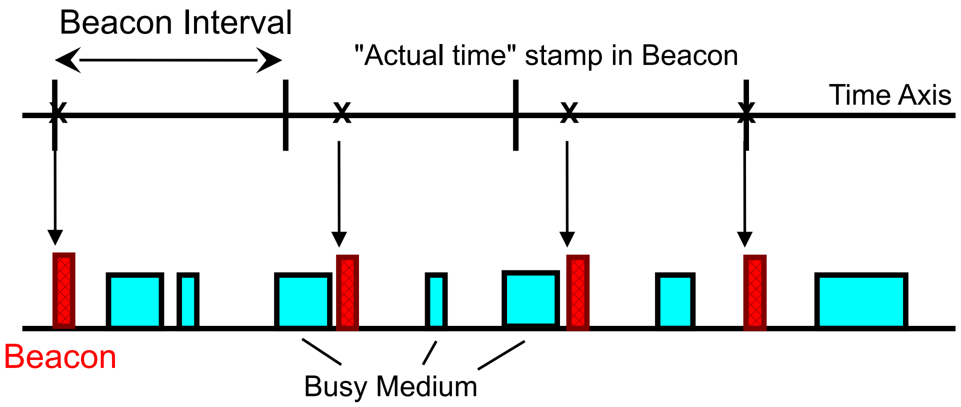
Wi-Fi MAC Layer

MAC SUBLAYER MANAGEMENT

Wi-Fi MAC Sublayer Management

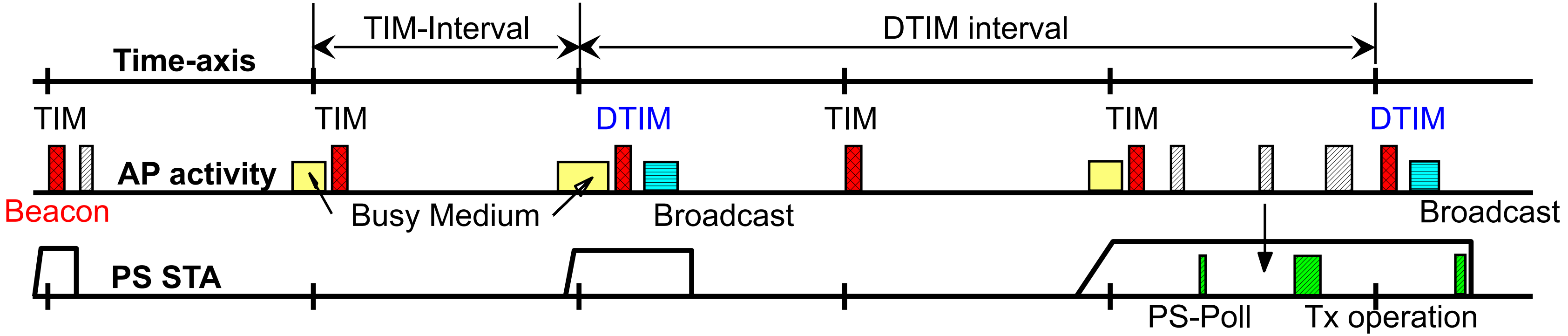
SYSTEM MANAGEMENT

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

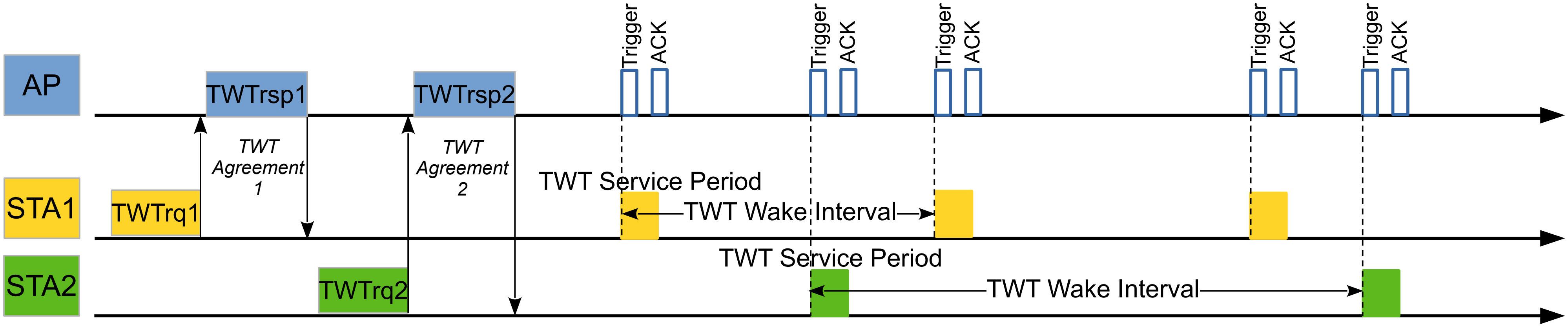
Legacy Power Management Procedure



- 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

Target Wake Time (TWT) power save procedure

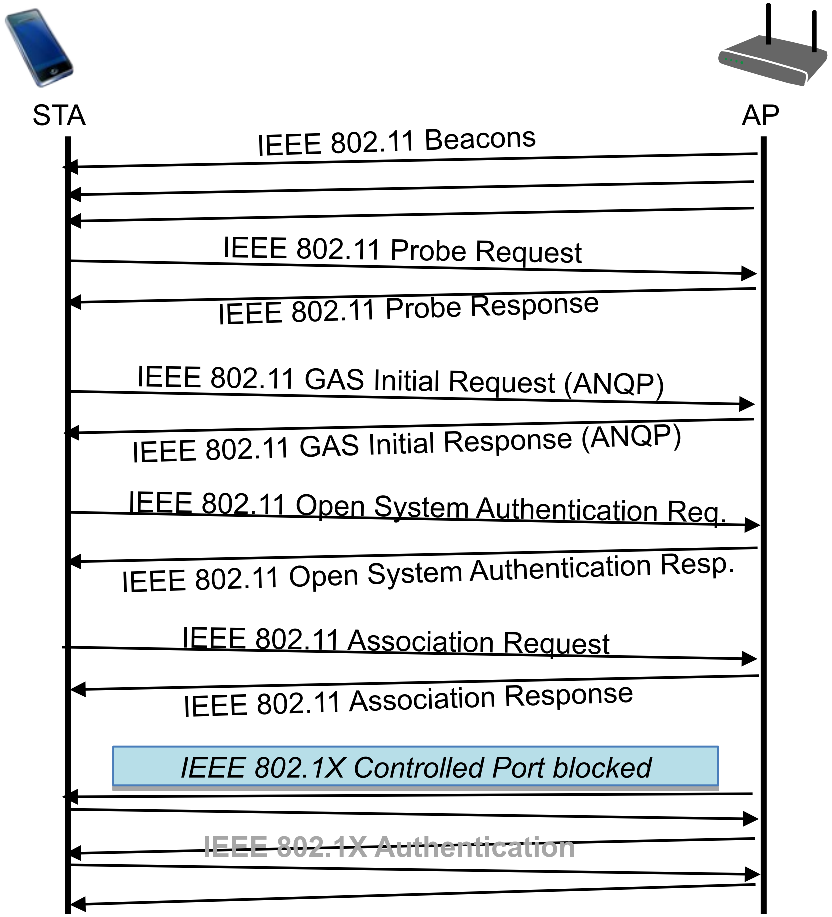
- Initially introduced by IEEE 802.11ah (HaLow) and taken over to Wi-Fi since Wi-Fi 6.
- STAs that expect to sleep for some period of time can negotiate a TWT contract with the AP.
- The AP stores any traffic destined for the STA until the TWT is reached.
- When the STA wakes at the prescribed time, 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).



Wi-Fi MAC Sublayer Management

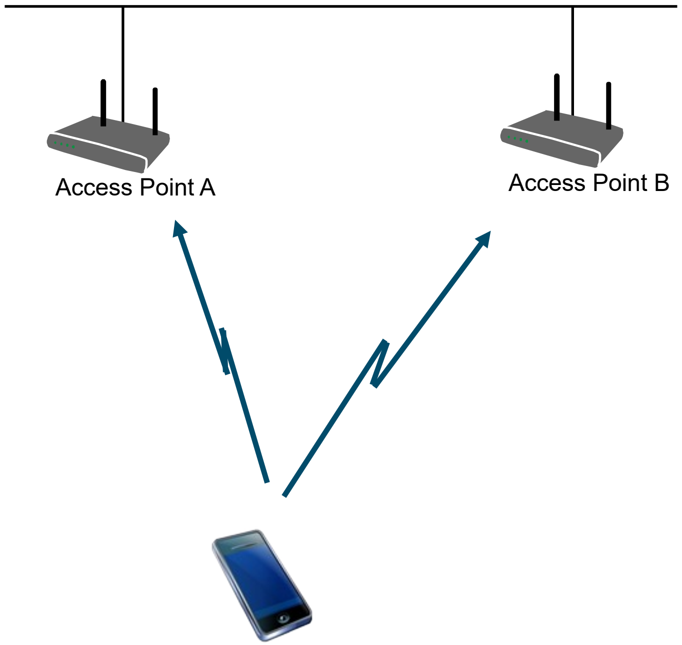
SESSION MANAGEMENT

Wi-Fi session establishment


STA
AP
IEEE 802.11 Beacons
IEEE 802.11 Probe Request
IEEE 802.11 Probe Response
IEEE 802.11 GAS Initial Request (ANQP)
IEEE 802.11 GAS Initial Response (ANQP)
IEEE 802.11 Open System Authentication Req.
IEEE 802.11 Open System Authentication Resp.
IEEE 802.11 Association Request
IEEE 802.11 Association Response
IEEE 802.1X Controlled Port blocked
IEEE 802.1X Authentication

- 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

Message sequence for successful connection setup

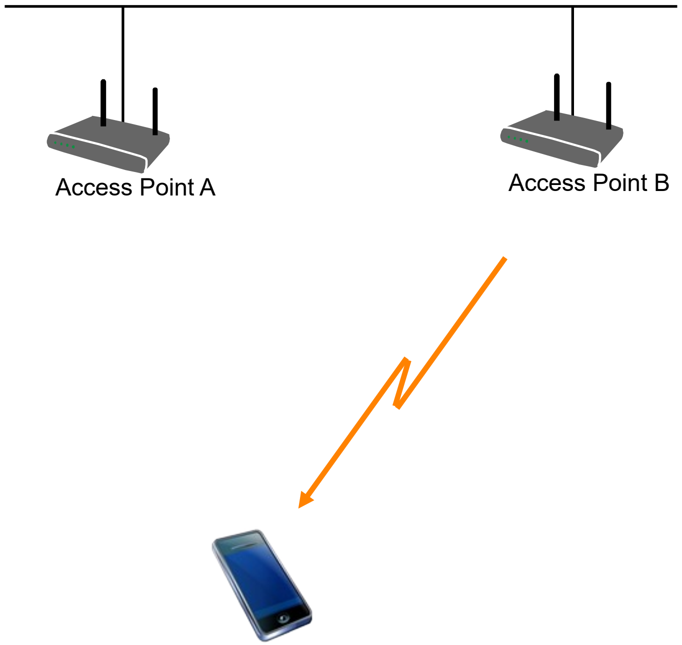


Connection establishment with active scanning but without network selection by ANQP

Details:

← Station sends Probe Request

Message sequence for successful connection setup



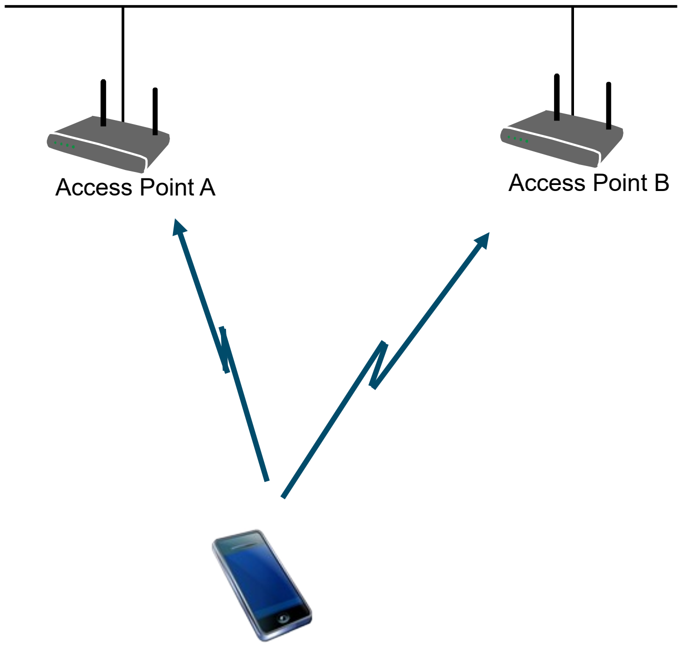
Connection establishment with active scanning but without network selection by ANQP

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

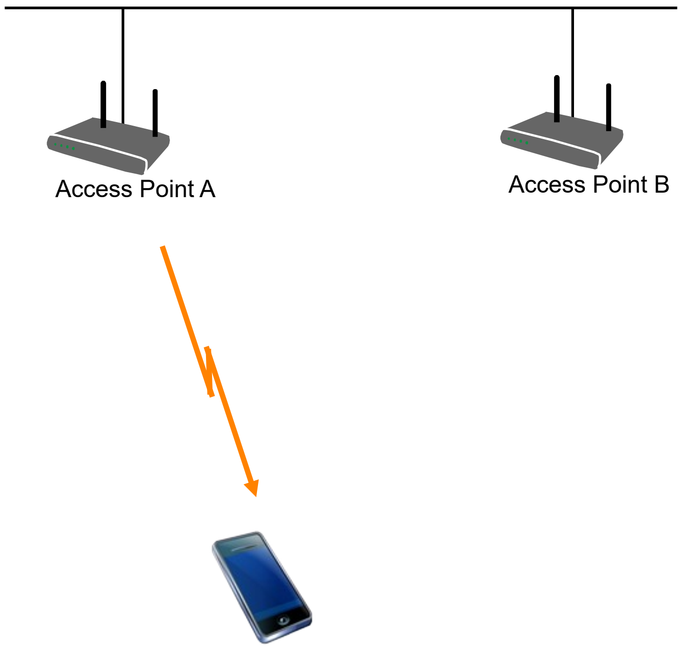
Details:

← 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

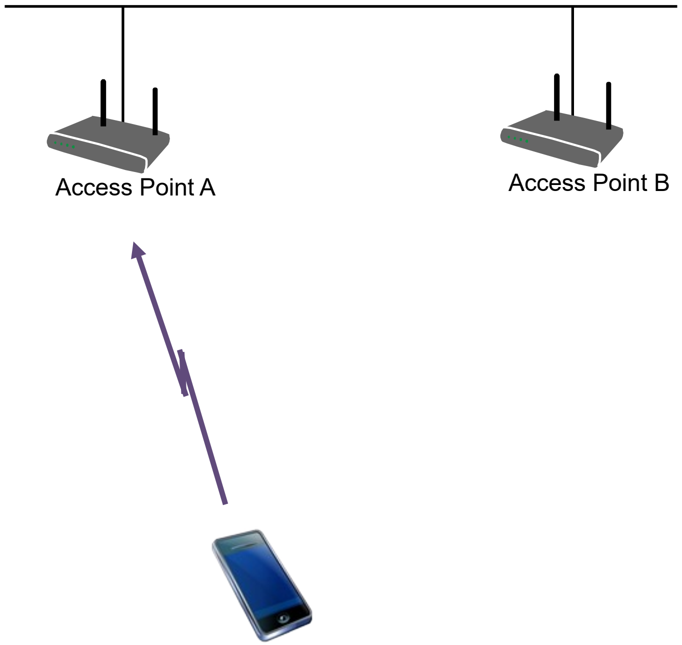
→ APs send Probe Response

← 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

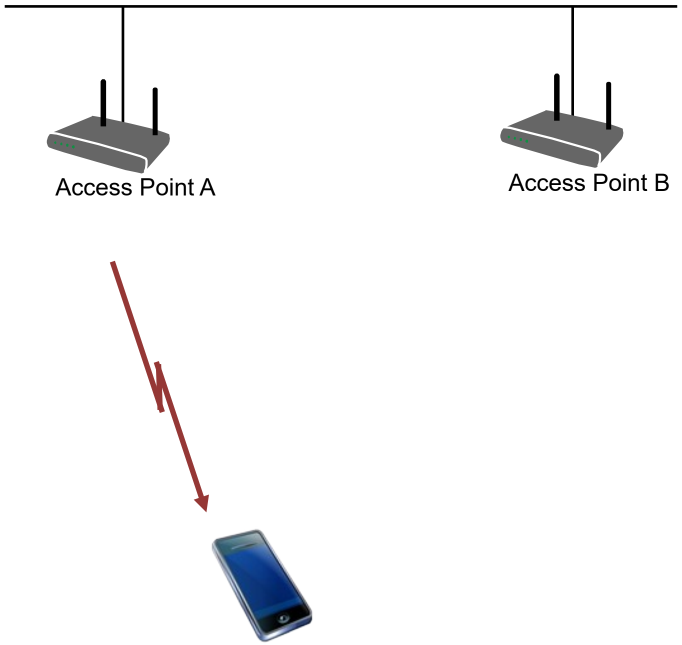
← Station sends Probe Request

→ 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

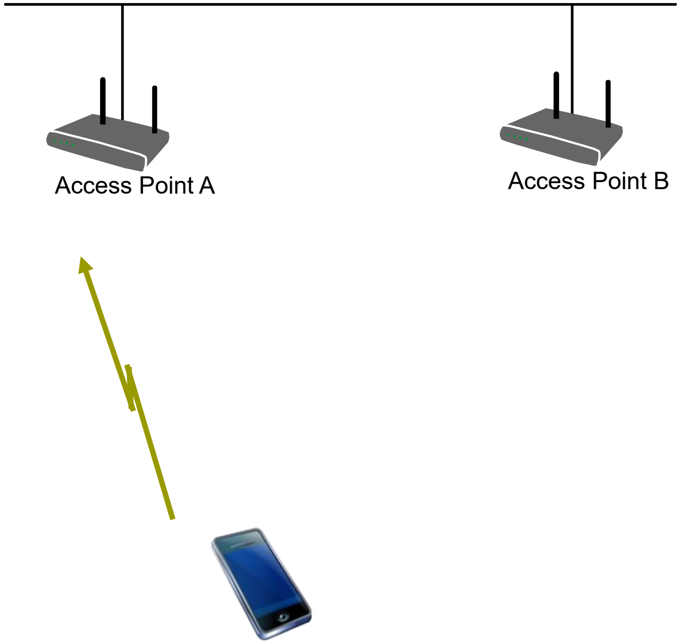
→ APs send Probe Response

=> 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

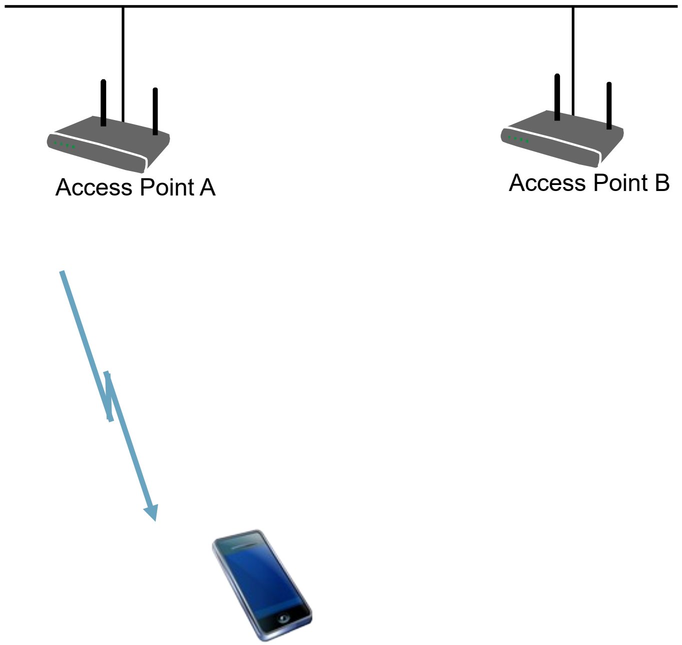
=> Station chooses best AP

← 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

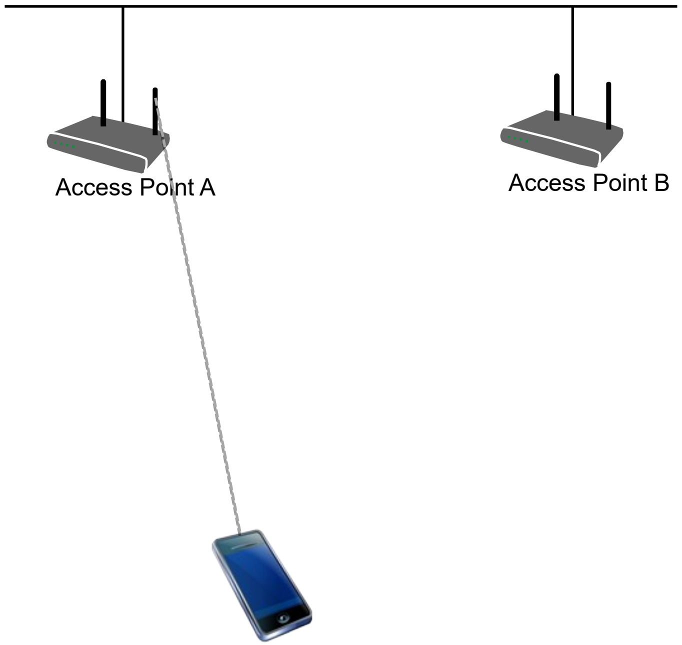
← Station sends Authentication Request to the chosen AP

→ 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

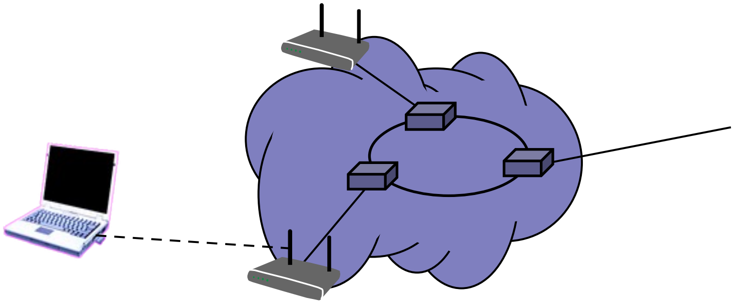
→ AP sends Association Response (success)

=============== L2 connection established

Wi-Fi MAC Sublayer Management

WI-FI MOBILITY

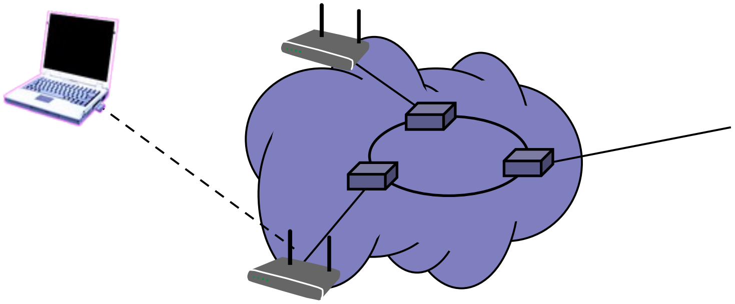
Wi-Fi mobility inside an ESS



Local distribution network

Wi-Fi mobility inside an ESS

Station decides that link to its current AP is poor…

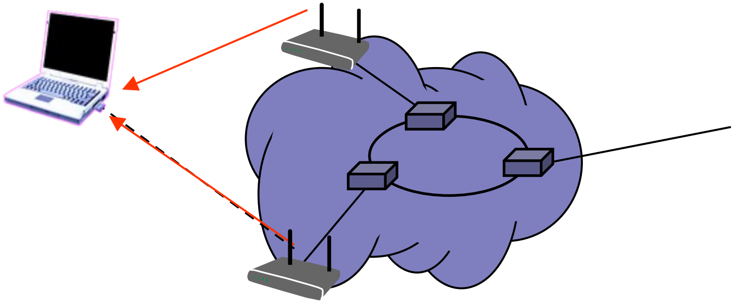


Local distribution network

Wi-Fi mobility inside an ESS

Station decides that link to its current AP is poor…

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

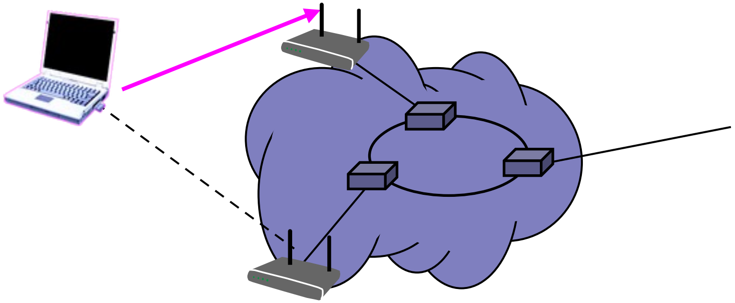


Local distribution network

Wi-Fi mobility inside an ESS

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**



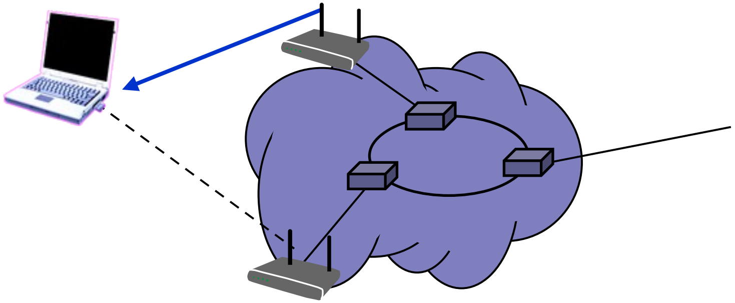
Local distribution network

Process shown without reestablishing the security context!

Wi-Fi mobility inside an ESS

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



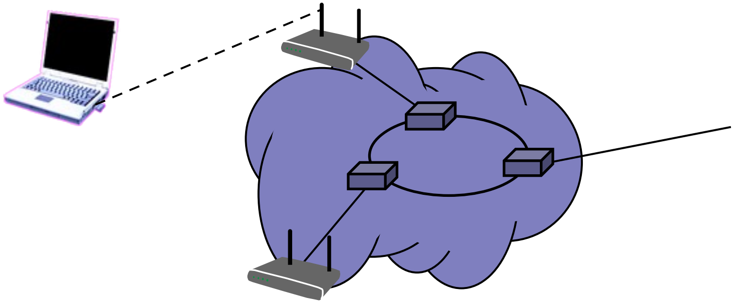
Local distribution network

Process shown without reestablishing the security context!

Wi-Fi mobility inside an ESS

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



Local distribution network

Process shown without reestablishing the security context!

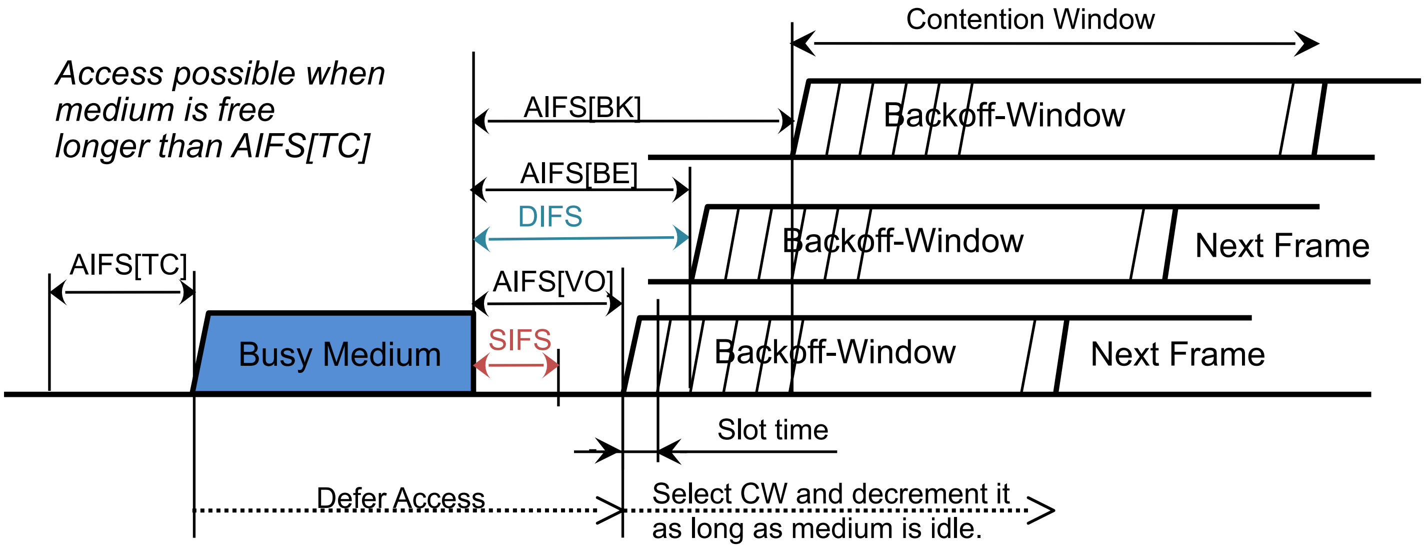
Handoff Time

- 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 messages)
  - However, WPA2/3 security adds another challenge
    - Security context and keying material has 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

Wi-Fi QoS

QUALITY OF SERVICE

Enhanced DCF (EDCF) enables traffic prioritization



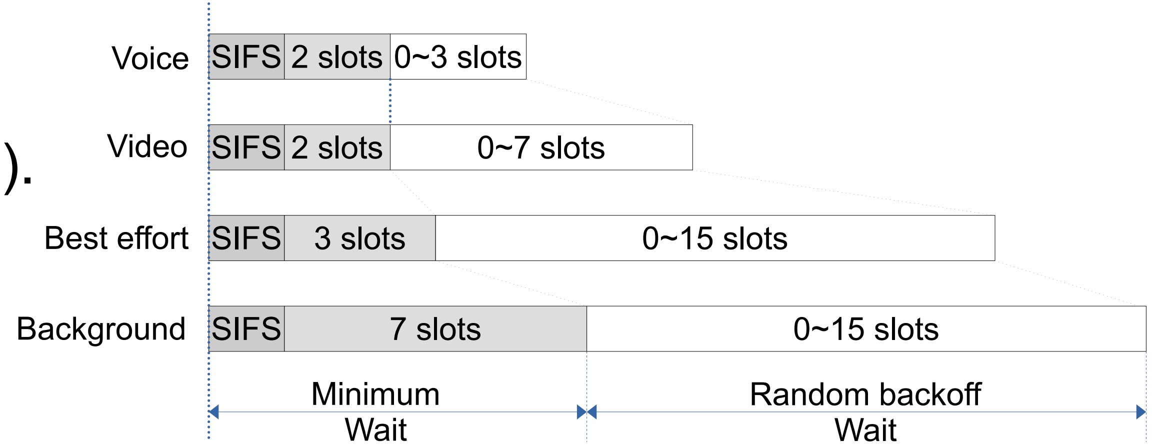
Band	SIFS[µs]	Slot time[µs]	DIFS[µs]
2.4 GHz	10	9	28
5 / 6 GHz	16	9	34

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

EDCF Parameters, as defined in 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.



Voice: SIFS | 2 slots | 0~3 slots

Video: SIFS | 2 slots | 0~7 slots

Best effort: SIFS | 3 slots | 0~15 slots

Background: SIFS | 7 slots | 0~15 slots

Minimum Wait

Random backoff Wait

- Default EDCA Parameters for contention window 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

Wi-Fi QoS 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:

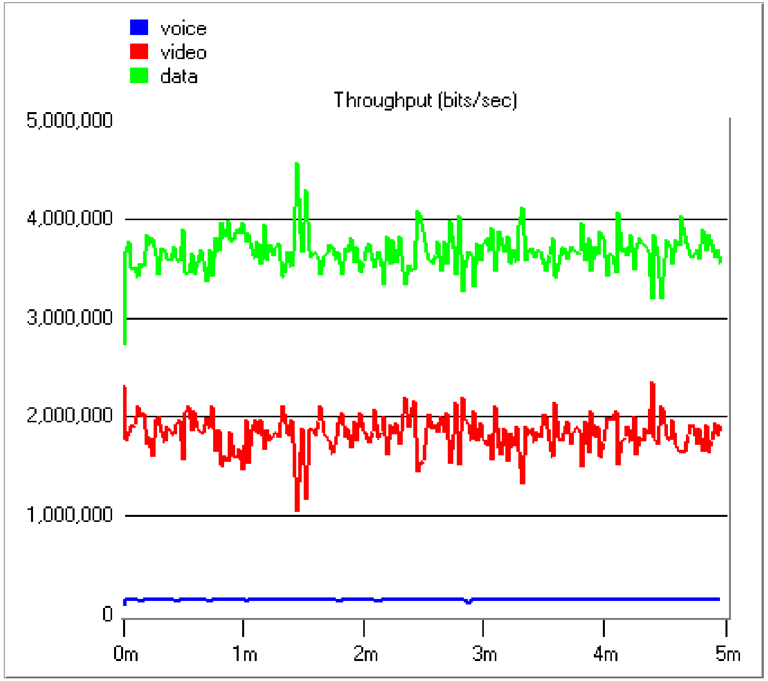
Type	Inter-arrival Time (Avg. in sec)	Frame Size (bytes)	Data Rate (Mbps)
Voice	Constant (0.02)	92	0.0368
Video	Constant (0.001)	1464	1.4
Data	Exponential (0.012)	1500	1.0

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

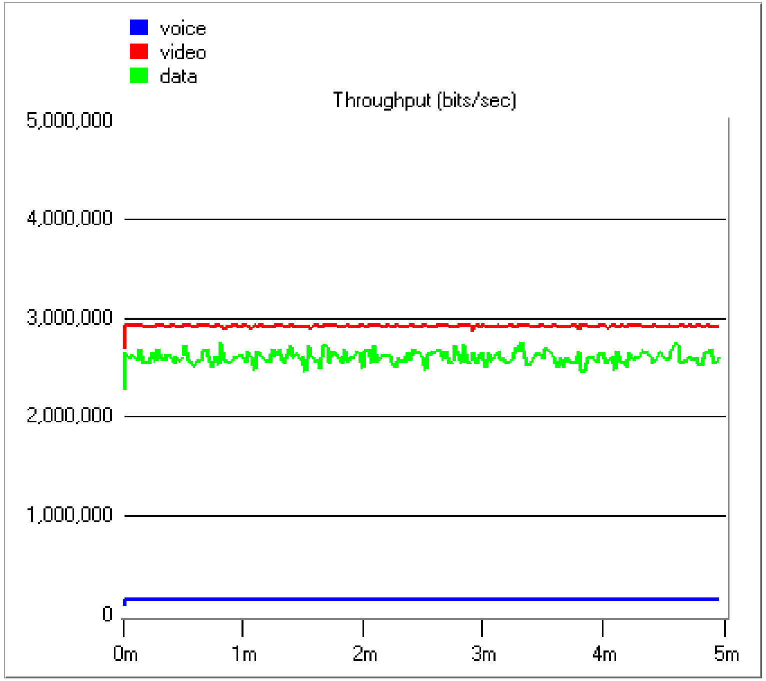
DCF vs. EDCF

- Throughput comparison
  - Higher video throughput with EDCF

DCF



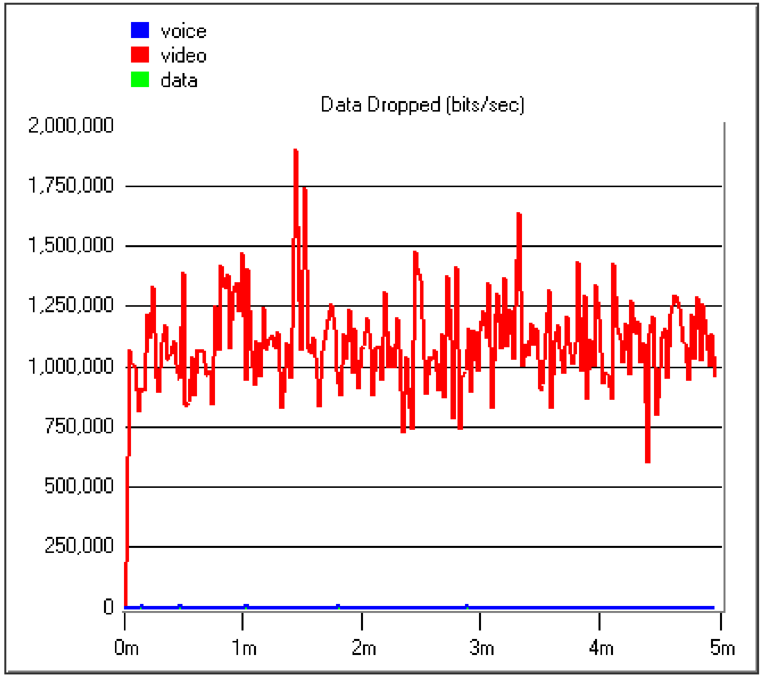
EDCF



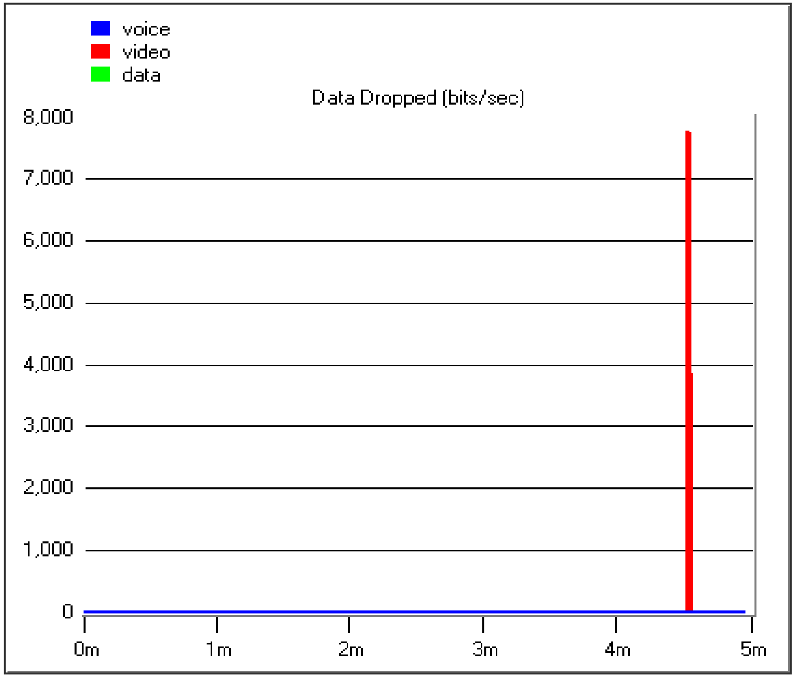
DCF vs. EDCF

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

DCF



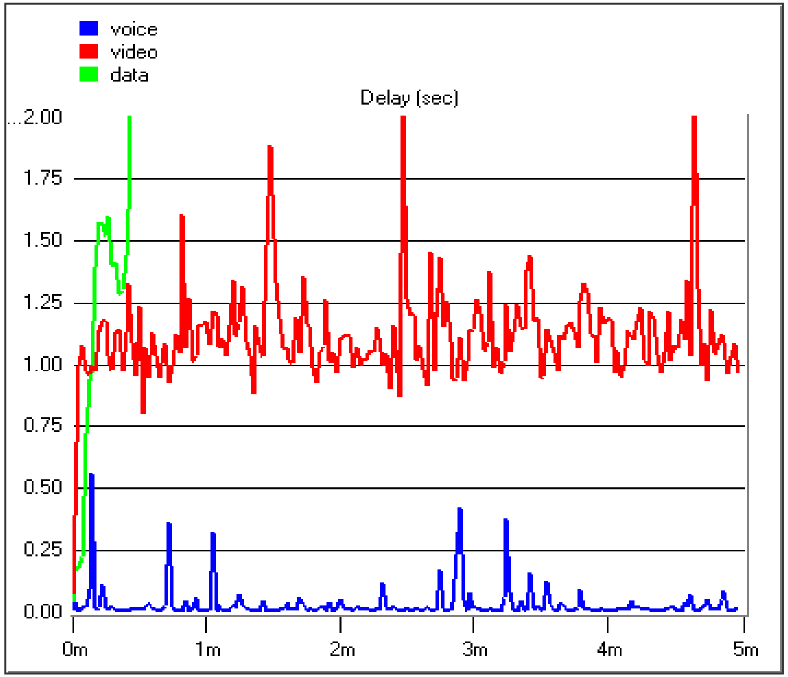
EDCF



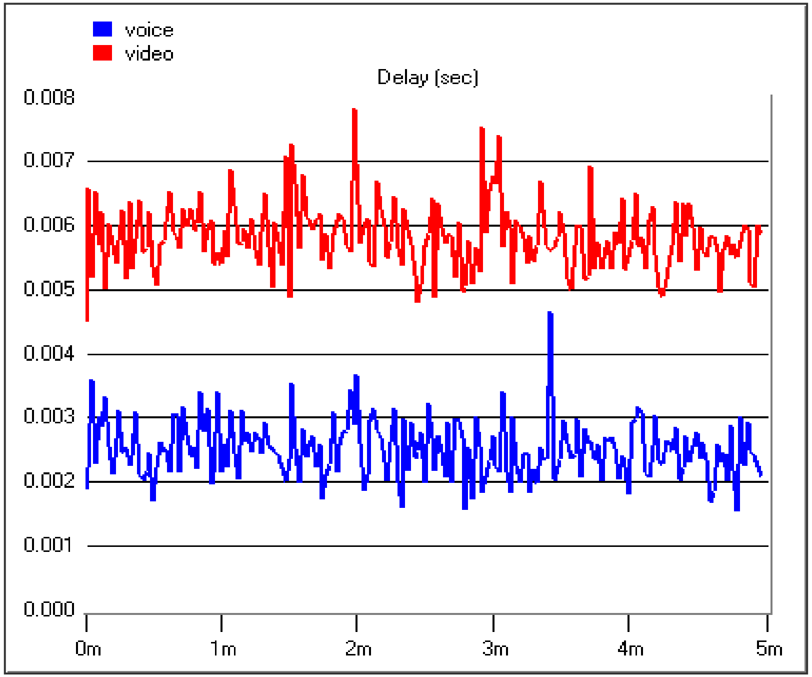
DCF vs. EDCF

- Delay comparison
  - Voice and video delays significantly reduced

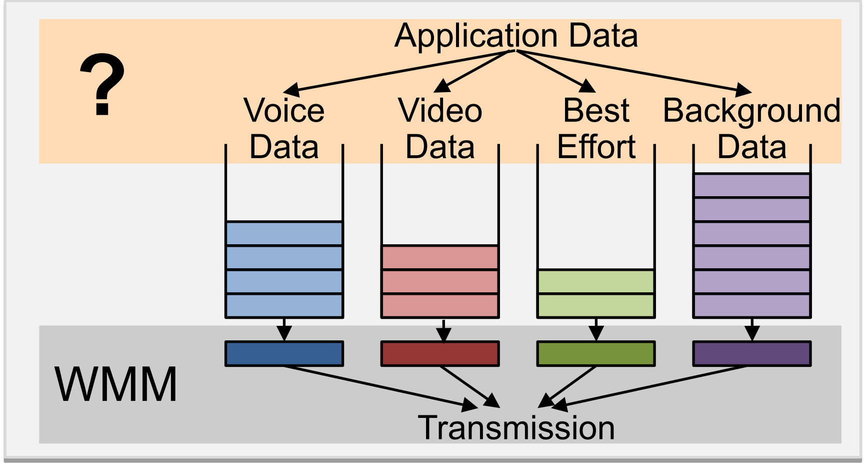
DCF



EDCF



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.

Wi-Fi QoS summary

- WMM provides four different user priorities
  - **Voice**, **Video**, **Best Effort**, **Background**, supported by EDCF 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.

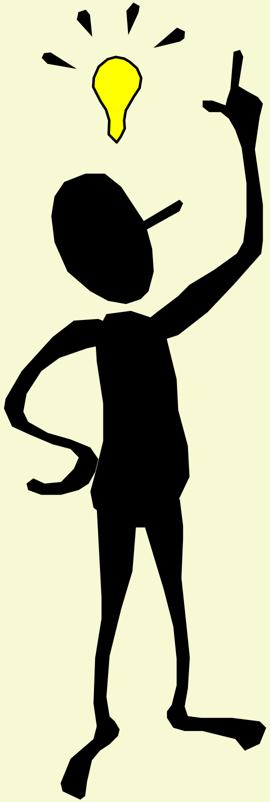
Wi-Fi MAC Layer

SUMMARY

Wi-Fi MAC Summary

- One common MAC supporting multiple PHYs
- CSMA/CA (collision avoidance) with physical and ‘virtual’ sensing
- Connectionless service through DCF
  - Transfer data on a shared medium without reservation
  - Controlled through low-layer ACKs, so transmit at highest speed possible
- Robust against noise and interference (ACK)
- Hidden node problem (RTS/CTS)
- Power savings (Sleep intervals)
- Session establischment through scanning, network selection, authentication, and association messaging
  - Orderly teardown through disassociation messaging
- Handover within an ESS through reassociation message
- Security established after link layer session establishment
- QoS (WMM) supported through EDCF and QoS Management

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?

Mac Sublayer Management questions…

1) What are the two main functions of the Wi-Fi MAC sublayer 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 why does it provide 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 IEEE 802.11 association procedure?
8) What is a Reassociation in IEEE 802.11?
9) Please explain the MAC procedures for handover from one AP to another AP of the same ESS without security re-establishment?

Wi-Fi 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) How are the Wi-Fi QoS classes denoted that are supported by WMM?
4) What is the purpose of Wi-Fi QoS management?

End of part 3

Questions and remarks