

WLAN IEEE 802.11 aka Wi-Fi

Max Riegel

Lectures overview

June 14th

- Wi-Fi deployments
- Standardization environment
- Wi-Fi system architecture
- Wi-Fi security

June 21st

- Medium access functions
- MAC layer management frame formats
- Quality of Service
- Wi-Fi roaming and Hotspot 2.0
- Wi-Fi Direct

June 28th

- Wireless channel characteristics
- Wi-Fi radio for 2.4 GHz and 5 GHz bands
- WiGig extension for 60 GHz bands
- Wi-Fi extension for below 1GHz bands
- WLAN management

Self Organizing Networks SS2018 (WLAN) ©Max Riegel, 2018 2018-06-21 2

Standards environments

STANDARD REFERENCE

Self Organizing Networks SS2018 (WLAN) ©Max Riegel, 2018 2018-06-21 3

IEEE Std 802.11™-2016



- Can be downloaded at no charge by IEEE Get Program
 - <http://standards.ieee.org/getieee802/download/802.11-2016.pdf>
- No all the features specified in the standard are available in real Wi-Fi products
- Where appropriate presentation adopts 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>

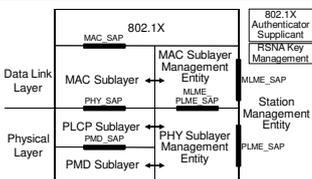
IEEE Standard for Information technology
Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

- Revision of IEEE Std 802.11-2012
 - Revision of IEEE Std 802.11-2007
 - First IEEE 802.11 standard release in 1997
 - First IEEE 802.11 standard release in 1997
- Comprises initial IEEE Std 802.11-1999 together with all amendments IEEE 802.11a-1999 ... IEEE 802.11af-2013
 - 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

Self Organizing Networks SS2018 (WLAN) ©Max Riegel, 2018 2018-06-21 4

IEEE802.11 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



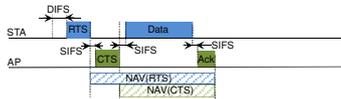
Self Organizing Networks SS2018 (WLAN) ©Max Riegel, 2018 2018-06-21 5

WLAN IEEE 802.11 MEDIUM ACCESS FUNCTIONS

Self Organizing Networks SS2018 (WLAN) ©Max Riegel, 2018 2018-06-21 6

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

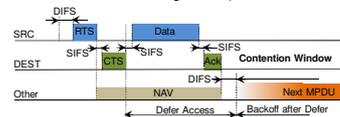
- Used to handle congested/heavily loaded radio environment through control of AP



- 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 to adjust their channel access procedure

CSMA/CA protocol

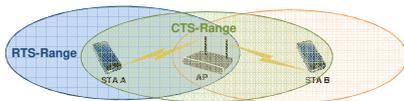
- Defer access based on Carrier Sense.
 - Either physical through CCA (Clear Channel Assessment) from PHY
 - Or virtual carrier sense state through NAV (Network Allocation Vector)



- Direct access when medium is sensed free longer than DIFS, otherwise defer and backoff.
- Receiver of directed frames return ACK immediately when CRC is correct.
 - When transmitter does not receive ACK then retransmission of frame is initiated after a random backoff

Hidden Node Problem

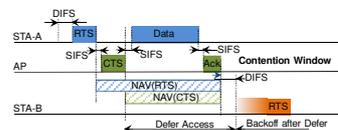
- Problem occurs when contending stations for the medium do not hear each other



- 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)

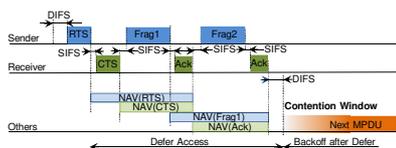
Hidden Station Solution

- 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



Summary: Basic Access Protocol Features

- Distributed Coordination Function (DCF) for efficient medium sharing.
 - Use CSMA with Collision Avoidance derivative.
 - Based on Carrier Sense function in PHY called Clear Channel Assessment.
- Robust for interference.
 - CSMA/CA + ACK for unicast frames, with MAC level recovery.
 - 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.
- Includes fragmentation to cope with various PHY conditions and longer frame sizes.

WLAN IEEE 802.11

MAC LAYER MANAGEMENT

Self Organizing Networks SS2018 (WLAN) ©Max. Regal, 2018 2018-06-21 19

MAC layer management in IEEE802.11 architecture

- 802.1X
 - Port Access Entity
 - Authenticator/Supplicant
- RSNA Key Management
 - Generation of Pairwise 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

The diagram shows the IEEE 802.11 architecture. It is divided into a Data Link Layer and a Physical Layer. The Data Link Layer contains the MAC Sublayer and the MAC Sublayer Management Entity (MLME). The Physical Layer contains the PLCP Sublayer, the Physical Medium Dependent (PMD) Sublayer, and the PHY Sublayer Management Entity (PLME). The MAC Sublayer and PLCP Sublayer are connected to the PMD Sublayer. The MLME and PLME are connected to the MAC Sublayer and PLCP Sublayer respectively. The diagram also shows the 802.1X Authenticator/Supplicant and RSNA Key Management entities connected to the MAC Sublayer. The Station Management Entity is connected to the MLME and PLME. The diagram also shows the MAC SAP, PHY SAP, and PLME SAP interfaces.

Self Organizing Networks SS2018 (WLAN) ©Max. Regal, 2018 2018-06-21 22

Topics covered in this section

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

Self Organizing Networks SS2018 (WLAN) ©Max. Regal, 2018 2018-06-21 21

MAC Layer Management - Overview

- System Management
 - Synchronization (Timer Synchronization Function)
 - Synchronization of timers of STAs and APs
 - 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
- Session Management
 - Scanning for available networks and node of attachments
 - Beaconing
 - Active/passive scanning
 - Generic Advertisement Service
 - Pre-association information query
 - Authentication
 - Association/Disassociation/Re-association
 - Joining a WLAN network
 - Detaching from an AP
 - Transfer of connectivity from one AP to another AP

Self Organizing Networks SS2018 (WLAN) ©Max. Regal, 2018 2018-06-21 22

WLAN IEEE 802.11 MAC Layer Management

SYSTEM MANAGEMENT

Self Organizing Networks SS2018 (WLAN) ©Max. Regal, 2018 2018-06-21 23

Infrastructure Beacon generation

The diagram shows the generation of infrastructure beacons. It features a Time Axis with a Beacon Interval. A Beacon is shown as a red bar, and a Busy Medium is shown as a blue bar. The Actual time stamp in Beacon is indicated by a vertical line. The diagram shows that the Beacon is transmitted at the end of the Beacon Interval, even if the medium is busy.

- 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.

Self Organizing Networks SS2018 (WLAN) ©Max. Regal, 2018 2018-06-21 Page 24

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
 - For IBSS realized by distributed procedure
- 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

Power Management Procedure

The diagram shows a timeline for a Power-Save STA (PS STA). It illustrates the relationship between TIM-Intervals and DTIM intervals. During a TIM-Interval, the STA is in a Power-Save state. At the start of a DTIM interval, the STA wakes up to receive a Broadcast frame. The diagram also shows PS-Poll and Tx operation occurring during the DTIM interval.

- STAs wake up shortly prior to an expected DTIM
 - DTIM = Delivery Traffic Indication Map
 - DTIM interval: interval at which buffered broadcast/multicast frames are transmitted
 - In the figure above: 3 beacon intervals
- If DTIM indicates frame buffered for particular STA,
 - STA sends PS-Poll and stays awake to receive data
 - Else STA goes back to Power Save state
- Broadcast frames are also buffered in AP.
 - All broadcasts/multicasts are buffered
 - Broadcasts/multicasts are only sent after DTIM.
 - DTIM interval is a multiple of TIM interval

WLAN IEEE 802.11 MAC Layer Management SESSION MANAGEMENT

IEEE 802.11 session establishment

The sequence diagram shows the following steps between a STA and an AP:

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

- 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

- 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

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 Page 31

Active scanning

- STA tunes to all channels and 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.

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 Page 32

Session Management

NETWORK SELECTION

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 33

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

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 34

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 (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)

GAS Initial Response Frame (Advertisement Protocol = ANQP)

- STA evaluates the response based on its subscription information and associated policy and choose to associate to the AP.

Associate and WPA2 EAP Authentication

ANQP Attributes

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

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 35

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.

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 36

Session Management

AUTHENTICATION

Self Organizing Networks SS2018 (WLAN) ©Max Reggel, 2018 2018-06-21 37

Authentication

STA → IEEE 802.11 Authentication (Open System) → AP
 ← IEEE 802.11 Authentication (Open System, Status) ←

- 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 deprecated 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)).

Self Organizing Networks SS2018 (WLAN) ©Max Reggel, 2018 2018-06-21 38

Session Management

ASSOCIATION

Self Organizing Networks SS2018 (WLAN) ©Max Reggel, 2018 2018-06-21 39

Association

STA → IEEE 802.11 Association Request → AP
 ← IEEE 802.11 Association Response ←

- 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

Self Organizing Networks SS2018 (WLAN) ©Max Reggel, 2018 2018-06-21 40

Message sequence for successful association

Association with active scanning but without network selection by ANQP

Details:

- ← 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)

Self Organizing Networks SS2018 (WLAN) ©Max Reggel, 2018 2018-06-21 41

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).

Self Organizing Networks SS2018 (WLAN) ©Max Reggel, 2018 2018-06-21 42

Session Management

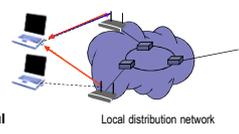
MOBILITY SUPPORT

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 43

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



Local distribution network

Process shown without reestablishing the security context!

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 Page 44

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

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 45

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

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 46

Session Management

MAC MANAGEMENT MESSAGES

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 47

MAC Management messages attributes

- Beacon (9.3.3.3)
 - Timestamp, Beacon Interval, Capabilities, ESSID, Supported Rates, Parameters, ...
 - Traffic Indication Map
- Probe Request (9.3.3.10)
 - SSID, Supported Rates, Parameters, ...
- Probe Response (9.3.3.11)
 - Timestamp, Beacon Interval, Capabilities, SSID, Supported Rates, Parameters, ...
 - Same as for Beacon except for TIM
- Authentication (9.3.3.12)
 - Authentication algorithm, Transaction number, Status code, Parameters, ...
 - Same format used for various actions
- Deauthentication (9.3.3.13)
 - Reason code
- Association Request (9.3.3.6)
 - Capability, Listen Interval, SSID, Supported Rates, ...
- Association Response (9.3.3.7)
 - Capability, Status Code, AID, Supported Rates, ...
- Reassociation Request (9.3.3.8)
 - Capability, Listen Interval, SSID, Current AP Address, Supported Rates, ...
- Reassociation Response (9.3.3.9)
 - Capability, Status Code, AID, Supported Rates, ...
- Disassociation (9.3.3.5)
 - Reason code

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 Page 48

WLAN IEEE 802.11
MAC FRAME FORMATS

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 49

Topics covered in this section

- MAC frame formats
 - Overview and comparison
 - Frame structure
 - Addressing
 - Header information

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 50

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

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 51

IEEE 802.11 MAC Layer Frame Formats

• 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.

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 Page 52

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).

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 Page 53

Header field descriptions

| | | | | | | | | | | |
|------------------|------|---------|-------|---------|-----------|-------|----------|-----------|-----|------|
| 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

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 Page 54

WLAN IEEE 802.11

QUALITY OF SERVICE

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 55

Topics covered in this section

- Quality of Service
 - DCF and legacy PCF
 - IEEE 802.11e - 2005
 - Wi-Fi Multimedia (WMM)
 - Wi-Fi QoS in action

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 55

QoS in IEEE 802.11 is mainly part of MAC Sublayer

- 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

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 57

WLAN IEEE 802.11

DCF AND LEGACY PCF

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 58

DCF is based on Clear Channel Access (CCA)

| 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

- Stations are waiting 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 $0..CW_{min}$; $CW_{min} = 15$
 - Exponential backoff is used in the case of retransmissions
 - $CW = (2^k - 1)$ with $k = n+4$ with $n =$ number of retransmission; $CW_{max} = 1023$
 - Efficient Backoff algorithm stable at high loads.
 - Backoff timer elapses only when medium is idle.

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 Page 59

CSMA/CA protocol

- 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)
- Direct access when medium is sensed free longer than DIFS, otherwise defer and backoff.
- Receiver of directed frames return ACK immediately when CRC is correct.
 - When transmitter does not receive ACK then retransmission of frame is initiated after a random backoff

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 Page 60

QoS Limitations of legacy IEEE 802.11 MAC

- DCF (Distributed Coordination Function)
 - Relies on CSMA/CA and optional 802.11 RTS/CTS for sharing the radio resource between STAs
 - Only support best-effort services
 - No guarantee in bandwidth, packet delay and jitter
 - No Quality of Service (QoS) guarantees.
 - In particular, there is no notion of high or low priority traffic.
 - Throughput degradation in heavy loaded environments due to collisions
- PCF (Point Coordination Function)
 - Defined in legacy IEEE 802.11, now obsolete
 - AP assuming the full control over the medium during CFP
 - Not taking into account real scenarios with overlapping WLANs
 - Transmission duration of the polled stations is not known to the AP
 - Inefficient and complex central polling scheme

WLAN IEEE 802.11 Quality of Service IEEE 802.11E-2005

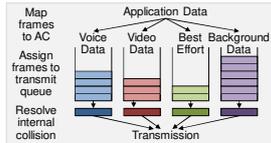
WLAN QoS in IEEE 802.11e – the theory

- IEEE 802.11e introduced MAC enhancements to IEEE 802.11 to facilitate QoS
 - Supports both IntServ and DiffServ models
 - Backward compatible with the DCF and PCF
- HCF (Hybrid Coordination Function)
 - Replaces both DCF and PCF
 - Consists of HCF Controlled Channel Access (HCCA) for contention free period and Enhanced Distributed Channel Access (EDCA) for contention period
 - Based on Traffic Categories (TC) for different services
 - Can meet predefined service rate, delay and/or jitter requirements of particular traffic flows.
 - Enhanced DCF (EDCF)
 - differentiated DCF access to the wireless medium for prioritized traffic categories (8 different traffic categories)
- Transmission Opportunities (TXOP)
 - An interval of time when a STA has the right to initiate transmissions
 - Multiple frames (i.e., MSDUs) can be transmitted during a TXOP with certain rules
- Block ACK
 - Group of frames received consecutively acknowledged by a BlockAck
- Direct Link Protocol (DLP)
 - STA-to-STA transmission in the infrastructure mode
- 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.



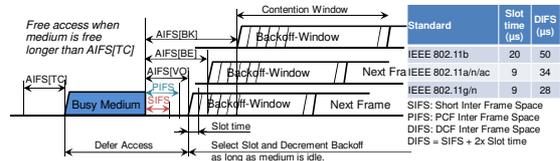
Quality of Service by Traffic Prioritization

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



| 802.1p contained in IEEE 802.1Q | | | | 802.11e | |
|---------------------------------|-----|---------|-----------------------|-----------------|-------------|
| Priority | PCP | Acronym | IEEE 802.1p | Access Category | Description |
| Lowest | 1 | BK | Background | AC_BK | Background |
| | 2 | BE | Best Effort | AC_BE | Best Effort |
| | 3 | EE | Excellent Effort | AC_BE | Best Effort |
| | 4 | CA | Critical Applications | AC_VI | Video |
| | 5 | VI | Video | AC_VI | Video |
| | 6 | VO | Voice | AC_VO | Voice |
| | 7 | IC | Internetwork Control | AC_VO | Voice |
| Highest | 7 | NC | Network Control | AC_VO | Voice |

EDCF



- 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 Quality of Service WI-FI MULTIMEDIA (WMM) QOS IN REAL EQUIPMENT

QoS support by Wi-Fi Multimedia

- Wi-Fi Multimedia (WMM) defines the features of IEEE 802.11e that are implemented in real products.
 - WMM supports only EDCA but not HCCA.
 - Prioritized QoS identifies 4 traffic classes (Access Categories)
 - Aligned to the 8 priorities defined within IEEE 802.1Q.

| Access Category | Description | 802.1p |
|--------------------------|--|--------|
| 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 (due to missing HCCA)

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.
- CWmin and CWmax derived from aCWmin and aCWmax values
 - Separately for each physical layer.

| AC | CWmin | CWmax |
|---------------------|----------------|----------------|
| Background (AC_BK) | aCWmin | aCWmax |
| Best Effort (AC_BE) | aCWmin | aCWmax |
| Video (AC_VI) | (aCWmin+1)/2-1 | aCWmin |
| Voice (AC_VO) | (aCWmin+1)/4-1 | (aCWmin+1)/2-1 |

- 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 | 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 | | |
| 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.

Improving 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 Quality of Service

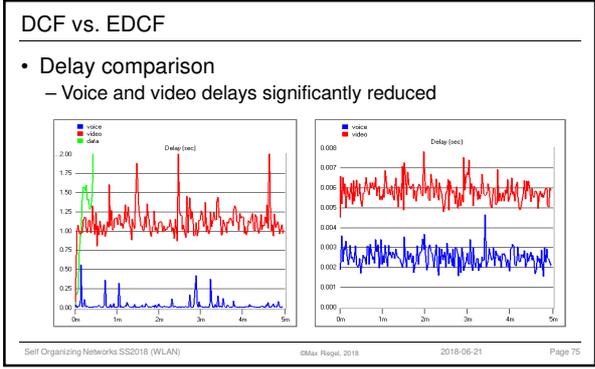
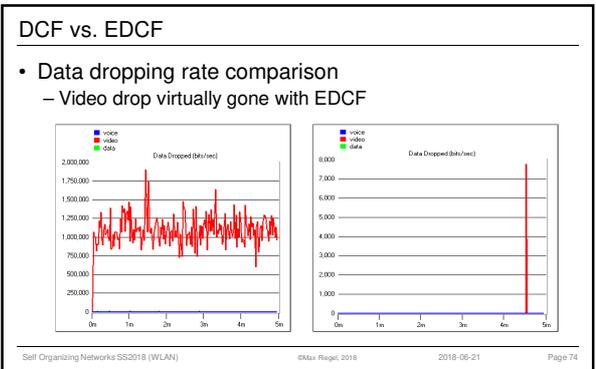
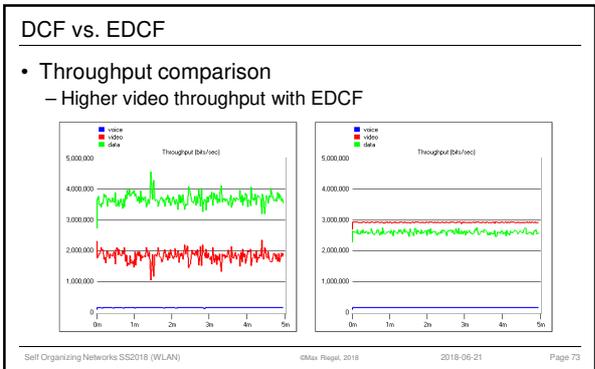
WI-FI QOS IN ACTION

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:

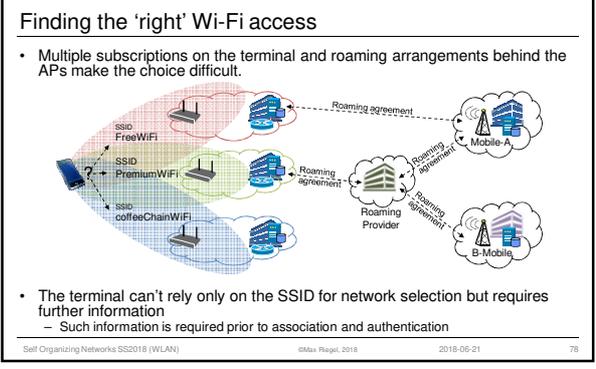
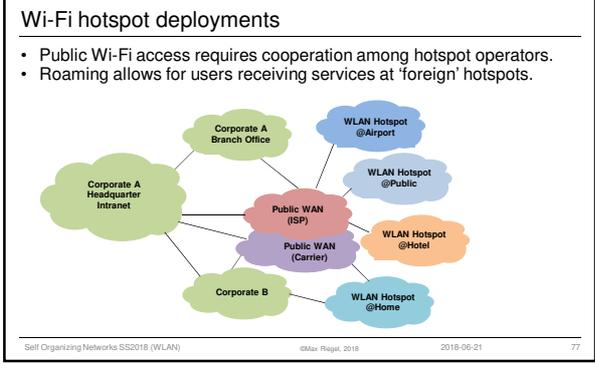
| Type | Inter-arrival Time (Avg. In sec) | Frame Size (bytes) | Data Rate (Mbps) |
|-------|----------------------------------|--------------------|------------------|
| Voice | Constant (0.02) | 92 | 0.0368 |
| Video | Constant (0.001) | 1464 | 1.4 |
| Data | Exponential (0.012) | 1500 | 1.0 |

| 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 |



WLAN IEEE 802.11
WLAN ROAMING AND HOTSPOT 2.0

Self Organizing Networks SS2018 (WLAN) ©Max Regal, 2018 2018-06-21 76

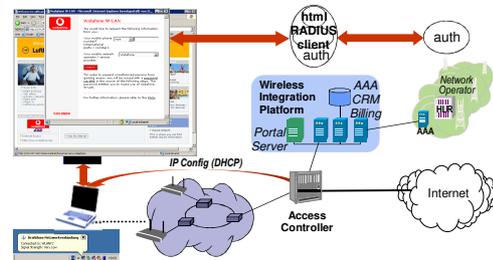


Public Wi-Fi access challenges

- Wi-Fi is used as a kind of nomadic Internet service.
- Secure automatic Wi-Fi connections exist for Residential Wi-Fi, Corporate Wi-Fi and Campus Wi-Fi.
 - Based on WPA2-PSK or WPA2-Enterprise
- Public Wi-Fi is still based on cumbersome captive portal pages for access network selection and authentication
 - Completely missing security requirements



Cumbersome captive portal based access control

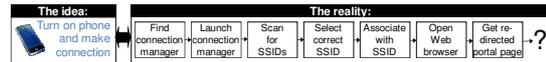


What's wrong with (current) public Wi-Fi access?

- Usability Problems
 - Web-page redirection (browser hijacking)
 - Error prone for many reasons
 - Login process
 - Browser-based authentication required before any other application can be used.
 - Credentials with hidden time-limits
 - No reliable indication whether the service has been stopped due to problems or expiration
 - Hotspot selection.
 - Manual interaction and selection required when multiple hotspots appear
 - Hotspots operated by roaming partners
 - Roaming relationship can't be detected before bringing up the portal pages
- Security Threats in portal-based hotspots
 - Evil twin attack
 - An attacker mimics a legitimate hotspot by a rogue access point using the same SSID
 - Session hi-jacking
 - An attacker takes over the Wi-Fi connectivity by causing the user's mobile device to disassociate from the Wi-Fi network.
 - Eavesdropping
 - An attacker intercepts the Wi-Fi communications and derives personal information such as passwords, credit card numbers, photographs, and emails.
- Security threats are caused by missing link layer security!

Wi-Fi Alliance Hotspot 2.0

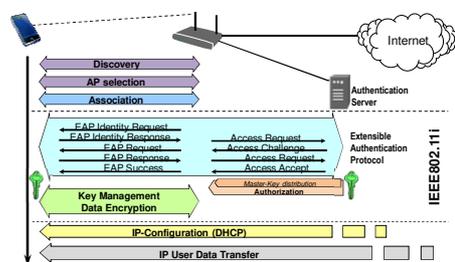
- Public Wi-Fi access as simple and easy as cellular communication



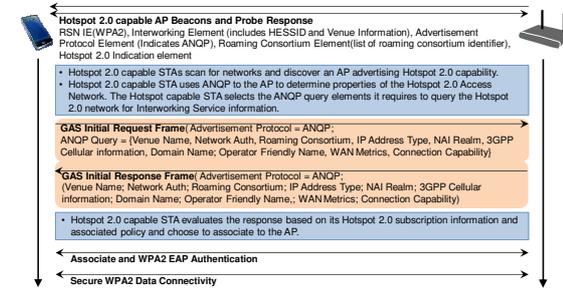
- Essential pieces already exist:
 - Appropriate Wi-Fi security framework already available (WPA2-Enterprise)
 - Widely deployed in Wi-Fi certified products for many years
 - Support of EAP-SIM/EAP-PEAP/EAP-TLS/EAP-TTLS in devices
 - Build-in Wi-Fi connection managers in mobile operating systems
 - Device configuration allowing prioritized selection of known Wi-Fi networks
 - Standard for Wi-Fi network discovery and selection support (IEEE 802.11u)
- Missing: network selection support for roaming, online registration, online provisioning
 - Wi-Fi Alliance Hotspot 2.0 program addressed the missing pieces => PASSPOINT™ Certified

Hotspot 2.0 security and automatic login

WPA2-Enterprise provides automatic login when there is a valid credential.



ANQP Usage by Hotspot 2.0

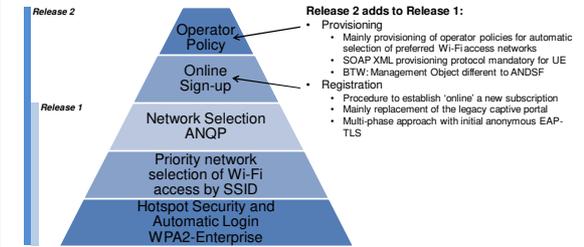


E.g. ANQP Information Elements

- | | |
|--|--|
| <p>IEEE 802.11 ANQP Information Elements</p> <ul style="list-style-type: none"> Venue Name <ul style="list-style-type: none"> Zero or more venue names associated with the BSS to support the user's selection. Network Authentication Type <ul style="list-style-type: none"> A list of authentication types carrying additional information like support for online enrollment or redirection URL. Roaming Consortium <ul style="list-style-type: none"> A list of information about the Roaming Consortium and/or SSPs whose networks are accessible via this AP. IP Address Type Availability <ul style="list-style-type: none"> Information about the availability of IP address version and type that could be allocated to the STA after successful association. NAI Realm <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> Cellular information such as network advertisement information e.g., network codes and country codes to assist a 3GPP STA in selecting access 3GPP networks. Domain Name <ul style="list-style-type: none"> A list of one or more domain names of the entity operating the IEEE 802.11 access network. | <p>Hotspot 2.0 ANQP Information Elements</p> <ul style="list-style-type: none"> HS Query list <ul style="list-style-type: none"> A list of identifiers of HS 2.0 ANQP elements for which the requesting mobile device is querying in a HS ANQP Query. HS Capability list <ul style="list-style-type: none"> A list of information/capabilities that has been configured on an AP. The HS Capability list element is returned in response to a GAS Query Request. Operator Friendly Name <ul style="list-style-type: none"> Zero or more operator names operating the IEEE 802.11 AN. WAN Metrics <ul style="list-style-type: none"> Information about the WAN link connecting a IEEE 802.11 AN and the Internet. Connection Capability <ul style="list-style-type: none"> Connection status of the most commonly used communications protocols and ports. NAI Home Realm Query <ul style="list-style-type: none"> Used by the STA to determine if the NAI realms for which it has security credentials are realms corresponding to SSPs or other entities whose networks or services are accessible via this BSS Operating Class Indication <ul style="list-style-type: none"> Information on the groups of channels in the frequency band(s) the Wi-Fi access network is using |
|--|--|

Hotspot 2.0 aka Passpoint

Also known as Next Generation Hotspot

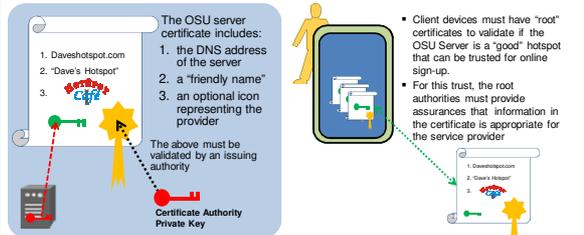


Online sign-up procedure

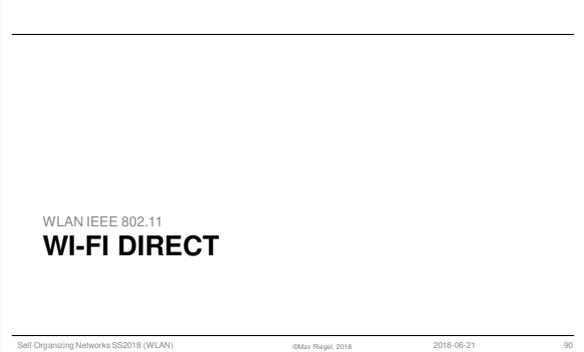
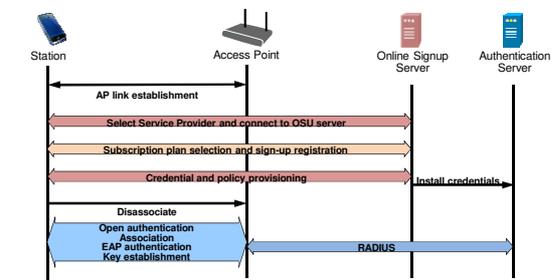
- Hotspots offering online sign have two ESSs:
 - An OSU ESS that supports online sign up
 - A production ESS that provides network access to the authenticated mobile device.
- In case of secure OSU ESS, same SSID as used for production ESS can be used, when un-authenticated STA is kept in 'isolated' mode with only access to OSU server.
- Registration procedures
 - The mobile device is setting up a new account with an SP or hotspot provider.
 - Begins with the mobile device authenticating the OSU server.
 - During the OSU procedure, the user will manually enter information, such as contact information and payment method, as required by the SP to obtain an account.
 - Credentials and related metadata provisioned are bound to this account.
- Provisioning procedures
 - Credentials and related metadata are downloaded to STA and installed for subsequent authenticated access to service

Client validation of authenticity of OSU information

- Online Sign Up Server Certificates are used for validation



Online-Signup Operational Phases



Wi-Fi Direct Overview

- Ability to create direct connections between Wi-Fi devices.
- No Wi-Fi router or AP required; devices can connect to each other anytime anywhere.
- Device discovery and service discovery support identification of potential peers before setting up connection.
- Connection set-up based on Wi-Fi Protected Setup for simple provisioning of secure context.
- Security based on WPA2-PSK.
- Optional support for Wi-Fi Direct Services, supporting transfer of files, printing documents, playing media, and displaying screens.
- Open service API for implementation of other services.
- Wi-Fi Direct is compatible with all Wi-Fi radio standards but does not support 802.11b (11 Mbps) mode.

Wi-Fi Direct P2P Groups and Clients

- Wi-Fi Direct is based on infrastructure mode
 - Group owner takes role of AP
 - Controls, which device can join
 - Provides BSS functions
 - Sending Beacons
 - Responding to probe requests
 - WPS internal registrar
 - Wi-Fi Direct devices can act either as group owner or P2P client
 - Legacy clients can connect as P2P client only
- Wi-Fi Direct devices can join standard infrastructure mode or can join/set-up Wi-Fi Direct peer-to-peer connection.
- Wi-Fi Direct devices can be concurrently connected to P2P group and infrastructure APs
 - Requires at least two independent MAC instances in the device
 - Can be used to provide infrastructure access to others in the group
 - Concurrency can be controlled through group owner
- Persistent groups allow to re-invoke previously established groups without re-provisioning

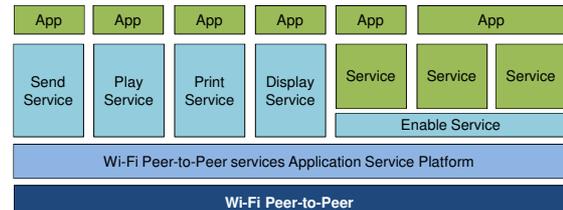


Wi-Fi Direct key mechanisms

| Feature | | Support |
|---------------------------------|---|-----------|
| Device Discovery | Mechanism to find Wi-Fi Direct devices and exchange device information. | Mandatory |
| Service Discovery | Mechanism to facilitate discovery of higher-layer services. Can be exercised prior to establishing a Wi-Fi Direct device connection. | Optional |
| P2P Group Management | | |
| Group Formation | Mechanism to determine which Wi-Fi Direct device is in charge of the Group. | Mandatory |
| Invitation | Mechanism that allows a Wi-Fi Direct device to invite another Wi-Fi Direct device to join an existing Group. | Optional |
| Client Discovery | Mechanism enabling a Wi-Fi Direct device to discover which Wi-Fi Direct devices are in an existing Group. | Mandatory |
| Power Management | | |
| P2P-PS and P2P-WMMB-PS | Adaptations of legacy Power Save and WMM-Power Save mechanisms that enable additional savings for Wi-Fi Direct devices. | Mandatory |
| Notice of Absence | Technique enabling a Wi-Fi Direct device that is in charge of a Group to reduce power consumption by communicating a planned absence. | Mandatory |
| Opportunistic Power Save | Technique enabling Wi-Fi Direct device that is in charge of a group to reduce power consumption by entering a doze state while connected Wi-Fi Direct devices are dozing. | Mandatory |

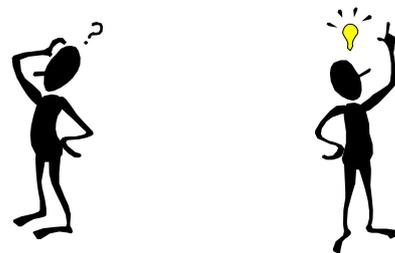
Wi-Fi Direct Services architecture

- Wi-Fi Direct supports P2P services framework, but does not mandate its use.
- P2P services framework facilitates interoperable implementations of common P2P services.



WLAN IEEE 802.11
END OF PART 2

Questions and answers



Questions...

Medium Access Functions

- 1) Why does collision detection with immediate termination of transmission usually not work in wireless?
- 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?

More questions...

Mac Layer Management

- 1) What does MLME stand for?
- 2) What are the two main functions of the MAC layer Systems Management?
- 3) What is the purpose of the Timer Synchronization Function?
- 4) Please shortly outline the role of the Delivery Traffic Indication Message for the power management in IEEE 802.11
- 5) Which sequence of MAC management procedures is necessary for the establishment of a connection in IEEE 802.11
- 6) What is the purpose of scanning?
- 7) What are beacons in IEEE 802.11?
- 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) How is ANQP related to GAS?
- 12) What is the purpose of IEEE 802.11 association procedure?
- 13) What is a Reassociation in IEEE 802.11?
- 14) Please shortly explain the MAC procedures for handover from on AP to another AP of the same ESS.
- 15) What are the limitations of Layer 2 mobility management?

More questions...

Quality of Service

- 1) How does the Distributed Coordination Function (DCF) work?
- 2) What means EDCF, and what enhancement does it add to DCF?
- 3) What HCF stands for, and what previous coordination function has been replaced by it?
- 4) By which standard amendment was QoS support added to IEEE 802.11?
- 5) What main functions were added to 802.11 by 802.11e?
- 6) How many priority classes does WMM support?
- 7) What is WMM?
- 8) What are the QoS classes supported by WMM?
- 9) Through which method are traffic classes realized in 802.11e?
- 10) What does TSPEC mean, and for what is it used?

More questions...

Hotspot 2.0

- 1) What is the benefit of 'Roaming'?
- 2) How is the access method for public Wi-Fi through opening a Web page called?
- 3) What is the main benefit of Hotspot 2.0?
- 4) What is ANQP used for Hotspot 2.0?
- 5) How can a station detect that an AP supports Hotspot 2.0?
- 6) What is the brand name of the Wi-Fi Alliance certification program for Hotspot 2.0?
- 7) In which release of Hotspot 2.0 was Online Sign-Up added?
- 8) What special server is needed for online signup support?
- 9) How many ESSs are required for online signup?
- 10) By which mean verifies the user the identity of the OSU provider?

Anything left for today?



See you again next week©