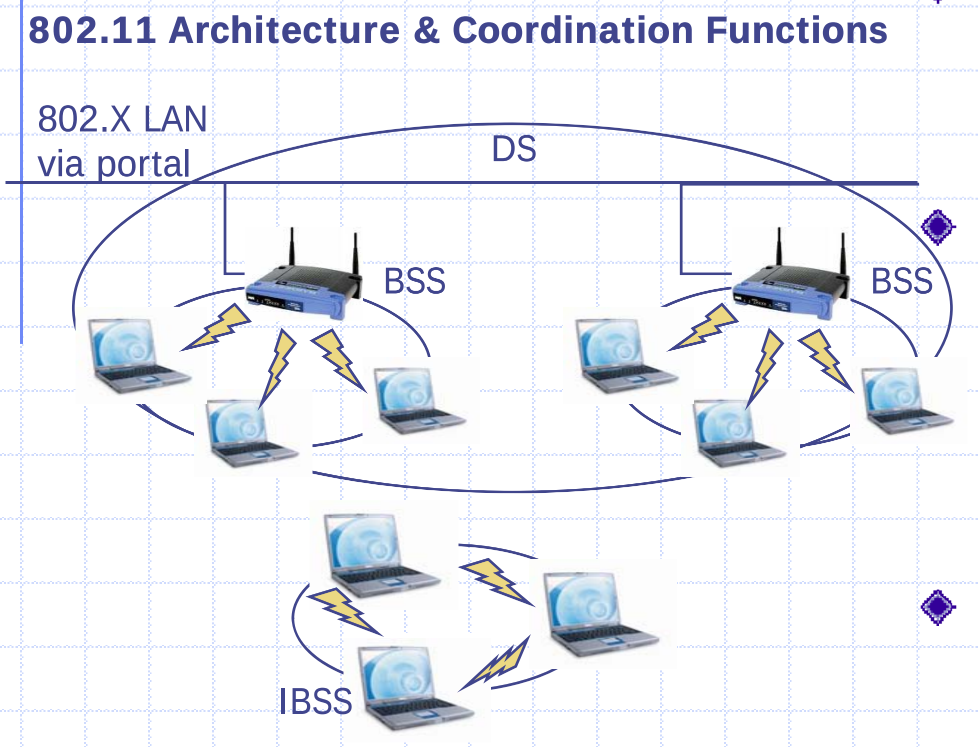
IEEE 802.11 Wireless Local Area Networks

Architecture



- The 802.11 architecture with typical scenarios of the different service sets (Basic Service Set-BSS, Independent BSS-IBSS, Distribution System-DS)
- BSS is a group of stations controlled by the so-called Coordination Function (CF). The Distributed CF (DCF) is used by all stations in the BSS, whereas the Point CF (PCF) is an optional extension for the support of QoS.
- DCF and PCF are concepts for spectrum management and medium access.

Architecture

- An IBSS is the simplest 802.11 network type, consisting of a minimum of 2 stations. No station has priority over another, the responsibility of coordinating the medium access is distributed among all stations.
- An infrastructure-based BSS includes 1 stations that has access to the wired network (Access Point-AP).
- An ESS (Extended Service Set) consists of 1 or more BSSs connected over the Distribution System (DS).

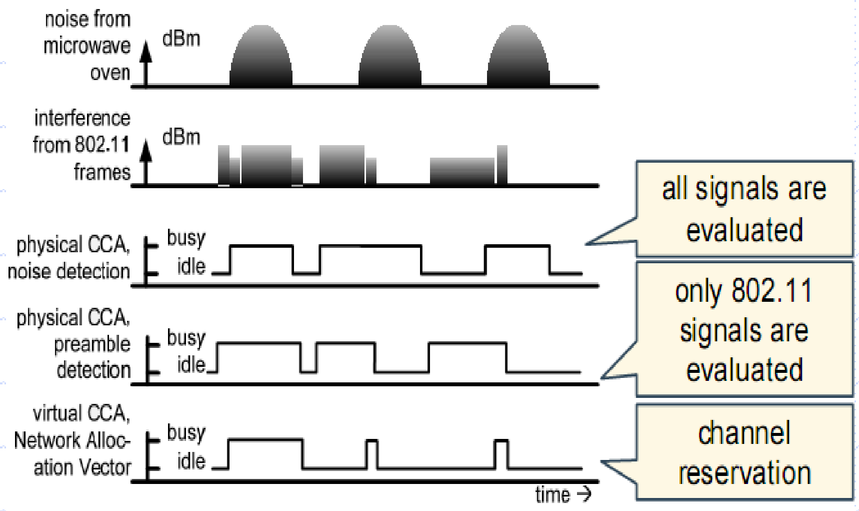
Services

- There are 2 categories of services in 802.11: the Station Service (SS) and the Distribution System Service (DSS).
- The main SS of a BSS is the MAC Service Data Unit (MSDU) delivery. Other SSs include (de)-authentication and privacy.
- An AP provides the Distribution System Service (DSS). The DSSs enable the MAC to transport MSDUs between stations that are not in direct communication. So DSSs are not available in an IBSS.
- DSSs include (re-)association, (dis)-association, and integration. The integration enables the delivery of MSDUs between non-802.11 LANs and the DS.

Medium Access Control Protocol

- 802.11 MAC protocol is built with the help of 2 coordination functions: DCF for traffic without QoS (asynchronous services) and PCF for traffic with QoS requirements (synchronous services).
- In the following, an infrastructure-based BSS is considered.
- The basic 802.11 MAC protocol is the DCF that works as a listen-before-talk scheme, based on the Carier Sense Multiple Access (CSMA)

Listen Before Talk



noise from microwave oven
dBm
interference from 802.11 frames
dBm
physical CCA, noise detection
busy
idle
physical CCA, preamble detection
busy
idle
virtual CCA, Network Allocation Vector
busy
idle
time →

all signals are evaluated

only 802.11 signals are evaluated

channel reservation

- The channel sensing function is called Clear Channel Assessment (CCA). It uses a power threshold. If a station detects a signal with power larger than this threshold, the radio channel is assumed to be busy, otherwise the channel is idle.
- There are different variants of CCA

Listen Before Talk

- The Network Allocation Vector (NAV) is an addition to the physical sensing of the radio channel. It is referred to as virtual carrier sensing and in fact has the function of reserving the channel for some time. It is a timer.

Timing and Interframe Spaces

- The time between 2 MAC frames is called the Interframe Space (IFS). 802.11 defines 4 different IFSs.
- All interframe spaces are independent of the channel data rate. The shorter the IFS, the higher priority in medium access.
- aSlotTime: is used to calculate the IFSs. SIFS and aSlotTime are the basis of all other duration. In 802.11a, aSlotTime=9µs.

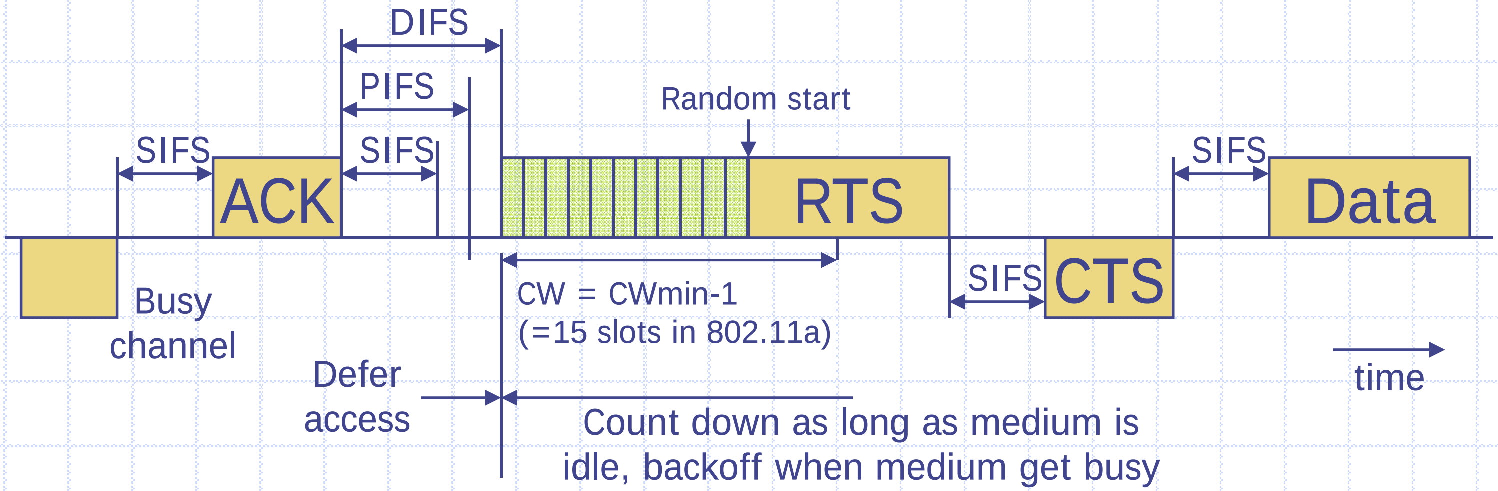
Timing and Interframe Spaces

- SIFS (Short IFS): is used to prioritize the immediate ACK of a data frame, the response (CTS) to a RTS, a subsequent MPDU of a fragmented MSDU, response to any polling using the PCF, and any frames of the AP during the CFP. SIFS = 16µs for 802.11a
- PIFS (Point Coordination Function IFS): used by stations operating under the PCF to obtain channel access with highest priority. PIFS = SIFS + aSlotTime. PIFS = 25µs for 802.11a
- DIFS (Distributed Coordination Function IFS): used by stations operating under the DCF to obtain channel access. DIFS = SIFS + 2.aSlotTime = 34µs
-

Collision Avoidance

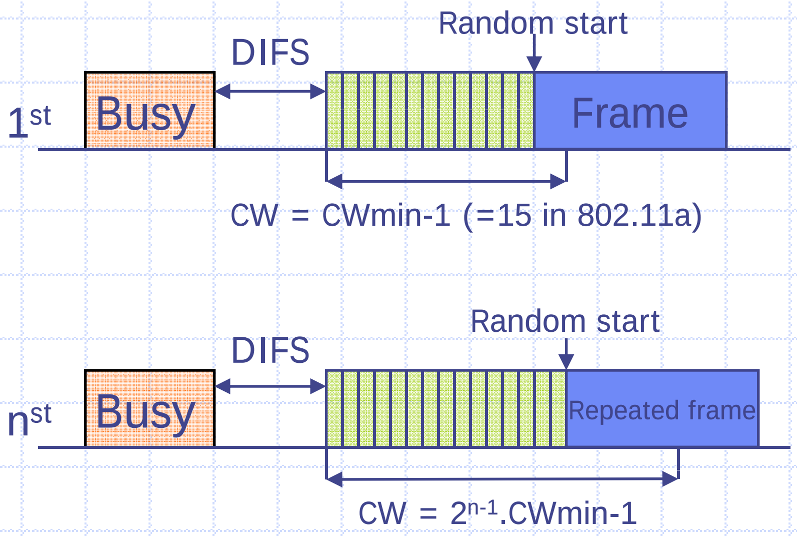
- A collision happens when there are more than 1 station attempts to transmit at the same time.
- In wireless communication, transmitter cannot detect a collision at receiver while transmitting. To account for this, 802.11 is based on CSMA/CA.
- If 2 or more stations detect the channel as being idle at the same time, inevitably a collision occurs when these stations initiate transmission at the same time. 802.11 defines a CA mechanism to reduce the probability of such collisions.

Collision Avoidance



- As part of CA, a station performs the backoff procedure before starting a transmission.
- Ex: After a successful frame exchange, a station wants to send another data frame. It starts transmitting RTS after sensing the channel is idle for a duration equal to DIFS and its following backoff slots.

Collision Avoidance



- After an unsuccessful transmission, the next backoff is performed with a doubled size of the contention window. This reduces the collision probability if there are multiple stations attempting to access the channel.

Collision Avoidance

- The station that deferred from channel access during the channel busy period do not select a new random backoff time, but continue to count down the time of previous backoff after sensing the channel as idle again. In this way, stations, which deferred from medium access because their random backoff was larger than other's, are given a higher priority when they resume the transmission attempt.

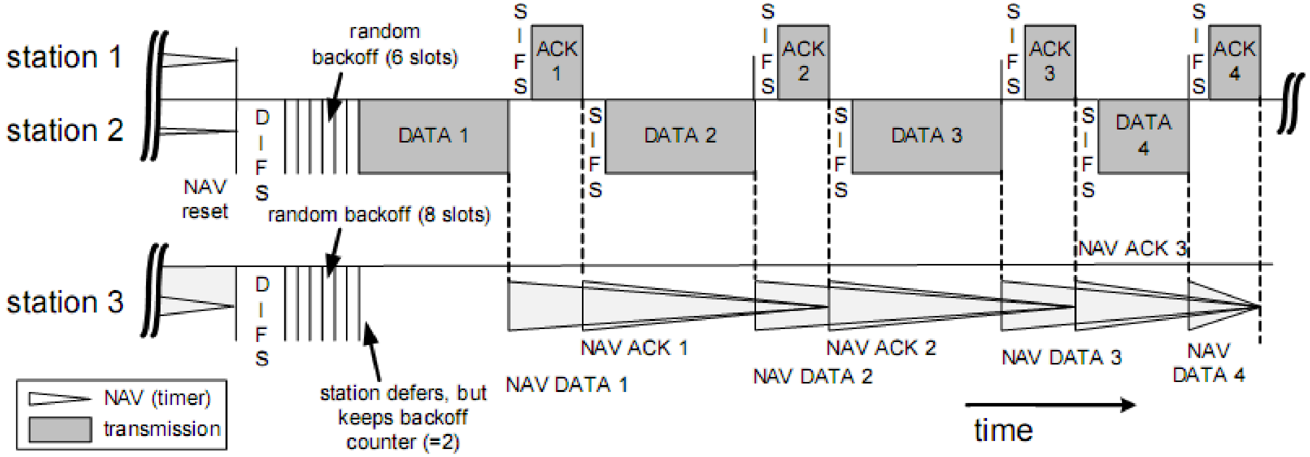
Recovery Procedure and Retransmissions

- When a frame exchange is not successful, the size of the frame is compared against a threshold which is implementation dependent before retransmission.
- Size < threshold, or the frame was RTS => increment SRC (Short Retry Counter); Else increment LRC (Long Retry Counter).
- The frame is discarded when SRC or LRC reaches a limit (default: SRC limit = 7, LRC limit = 4)
- Whenever an MSDU is successfully transmitted, SRC and LRC are reset.

Fragmentation

- The process of partitioning an MSDU into smaller MPDUs when its length exceeds a certain threshold is called fragmentation.
- The benefit of fragmentation is that in the case of failed transmission, the error is detected earlier and there is less data to retransmit.
- It also increases the probability of successful transmission of the MSDU in scenarios where the radio channel characteristics cause higher error probabilities for longer frames than for shorter ones.
- The obvious drawback is the increased overhead.

Fragmentation



- The process of recombining MPDUs into a single MSDU is called defragmentation.
- Only MPDUs with a unicast receiver address may be fragmented. Note: The maximum length of an MSDU is limited to 2346 byte.

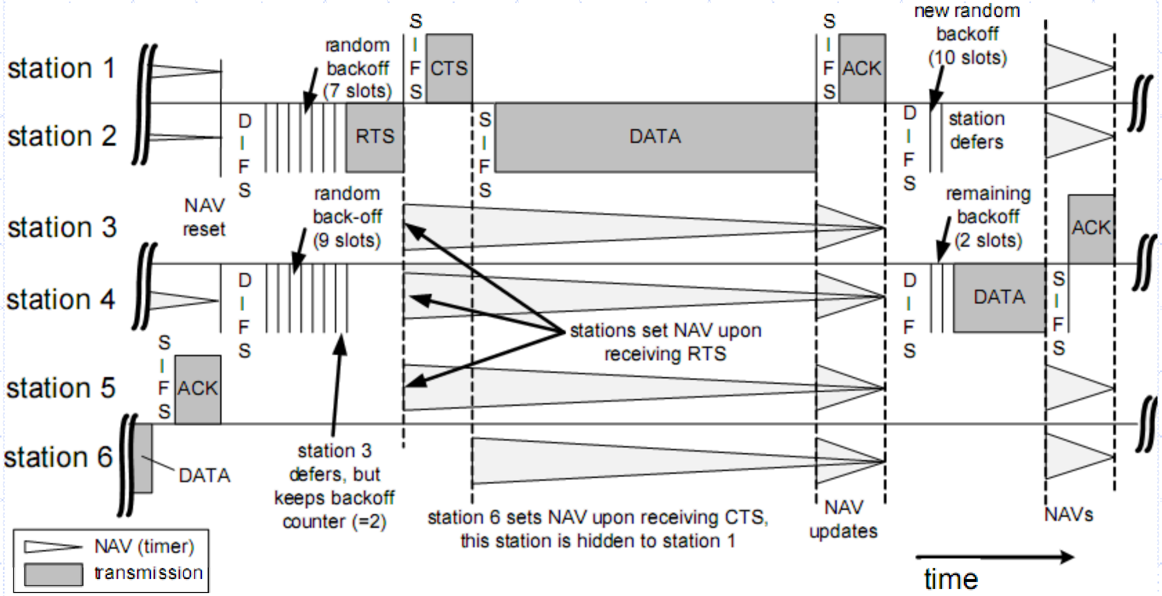
Hidden Stations and RTS/CTS

- Hidden Stations problem arises when a station is able to successfully receive frames from 2 different stations but the 2 stations cannot detect each other.
- To reduce throughput reduction owing to this problem, 802.11 specifies exchange of RTS/CTS frames as an option made by transmitting station.
- Consecutive frames in the sequence of RTS, CTS, data and ACK are spaced by an SIFS duration for transceiver turn-around.

Hidden Stations and RTS/CTS

- The RTS/CTS carry in its duration fields the information, how long the sequence RTS, CTS, Data, ACK will take. Hence, other stations close to the transmitting station and hidden stations close to the receiving station will not start any transmissions; their NAV timer is set. (A hidden station close to receiving station might not receive the RTS due to the large distance, but will in most cases receive the CTS frame)

Hidden Stations and RTS/CTS



station 1
station 2
station 3
station 4
station 5
station 6
random backoff (7 slots)
SIFS
CTS
DIFS
RTS
DATA
SIFS
ACK
new random backoff (10 slots)
DIFS
station defers
NAV reset
random back-off (9 slots)
remaining backoff (2 slots)
ACK
DIFS
DATA
SIFS
stations set NAV upon receiving RTS
SIFS
ACK
DATA
station 3 defers, but keeps backoff counter (=2)
station 6 sets NAV upon receiving CTS, this station is hidden to station 1
NAV updates
NAVs
NAV (timer)
transmission
time

- Station 6 cannot detect the RTS from station 2, but can hear the CTS of station 1. Although station 6 is hidden to station 2, it refrains from channel access because of NAV.
- Note that SIFS is shorter than DIFS, which always gives CTS and ACK the highest priority for access to the channel

Scanning Procedures in WLAN 802.11

- IEEE 802.11 defines 2 scanning modes: passive and active.
- The decision on which scanning mode is to be applied is taken by the Station Management Entity (SME). The SME is a layer-independent entity that may be viewed as residing in a separate management plane. The exact functions of the SME are not specified by the standard. The SME executes actions related to general system management. It directs the MLME to perform either passive or active scanning.

Passive Scanning

- A station monitors each specified channel for a time span of at most MaxChannelTime. During the scanning, the station adds any received 802.11 beacon or probe response to its cached BSSID scan list.
- The scanning duration may vary, depending on the # of channels to be scanned, the BI, and the load of the system.

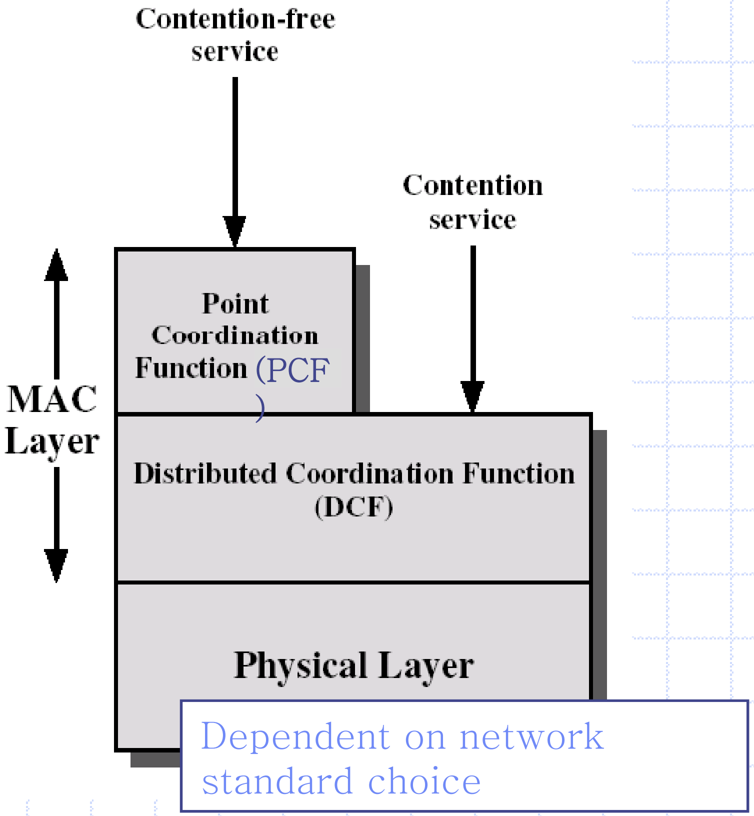
Active Scanning

- A station needs to generate specific request messages, so-called probe frames, then waiting for probe response. The probe response need to be acknowledged to ensure integrity of data delivery.
- The probe mechanism forces an AP to convey basically the same system information as done with the beacon without unnecessary waiting times.

Medium Access Control with Support for Quality-of-Service

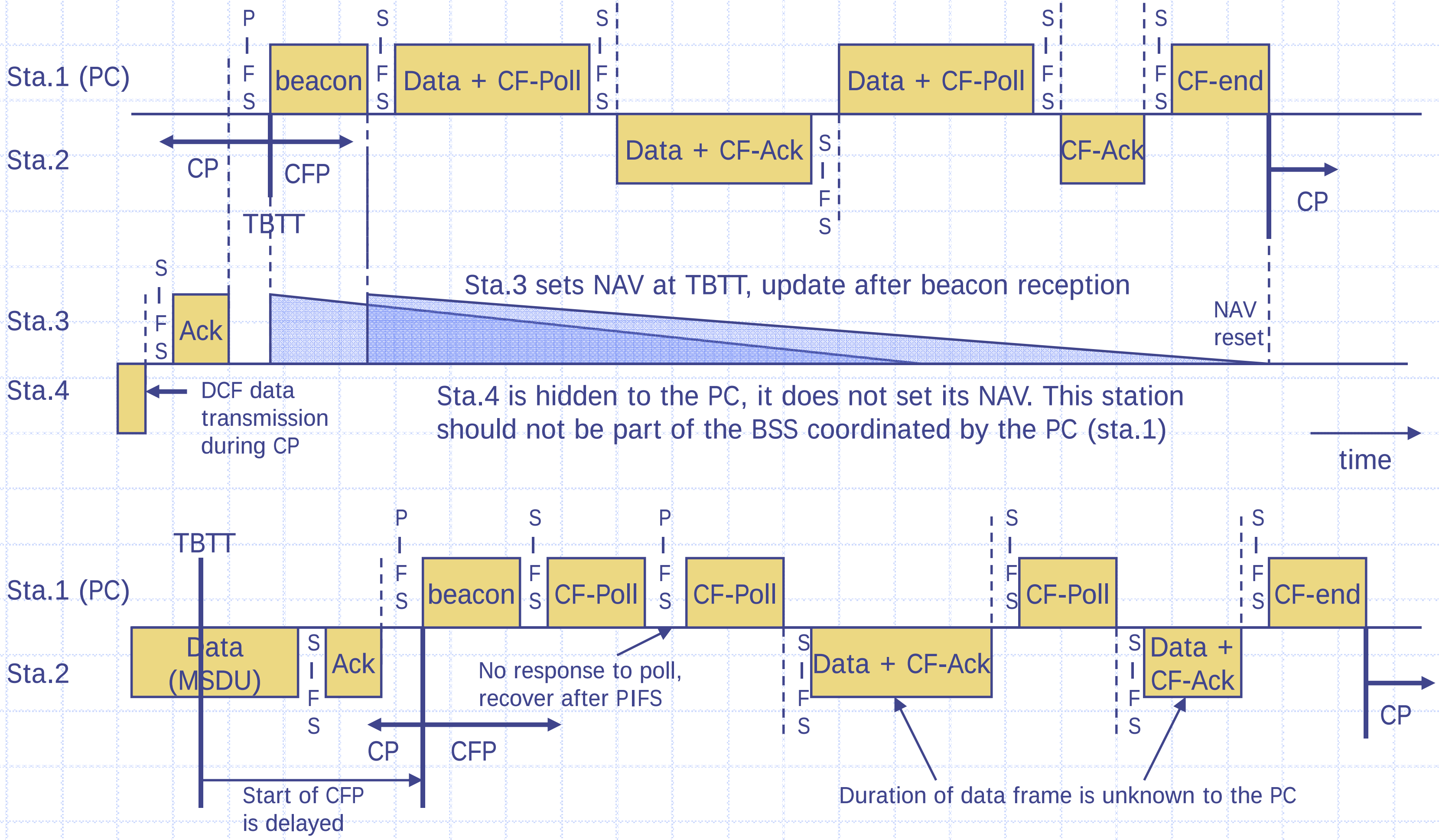
- IEEE 802.11 defines the Point Coordination Function (PCF) to let station have priority access to the radio channel, coordinated by a station called Point Coordinator (PC). PC typically resides in the AP.
- The PCF has higher priority than the DCF, because the period during which the PCF is used is protected from the DCF access by the NAV.

Medium Access Control with Support for Quality-of-Service


Contention-free service
Contention service
MAC Layer
Point Coordination Function (PCF)
Distributed Coordination Function (DCF)
Physical Layer
Dependent on network standard choice

- The time during which 802.11 stations operate is divided into repeated periods, called superframes. It starts with a beacon, includes CFP, CP.
- During the CFP, the PCF is used for accessing the channel, while the DCF is used during the CP.

Point Coordination Function



Point Coordination Function

- This previous figure is an example for the PCF operation. Station 1 is the PC and polls station 2. Station 3 detects the beacon frame and updates the NAV for the whole CFP. CFP may be delayed (lower part of the figure).
- PC has data pending for station 2 => combine data and poll frame into the data frame.
- The PC continues polling other stations until the CFP expires. No idle period longer than PIFS occurs during CFP.
- A CF-End control frame is transmitted to signal the end of the CFP.

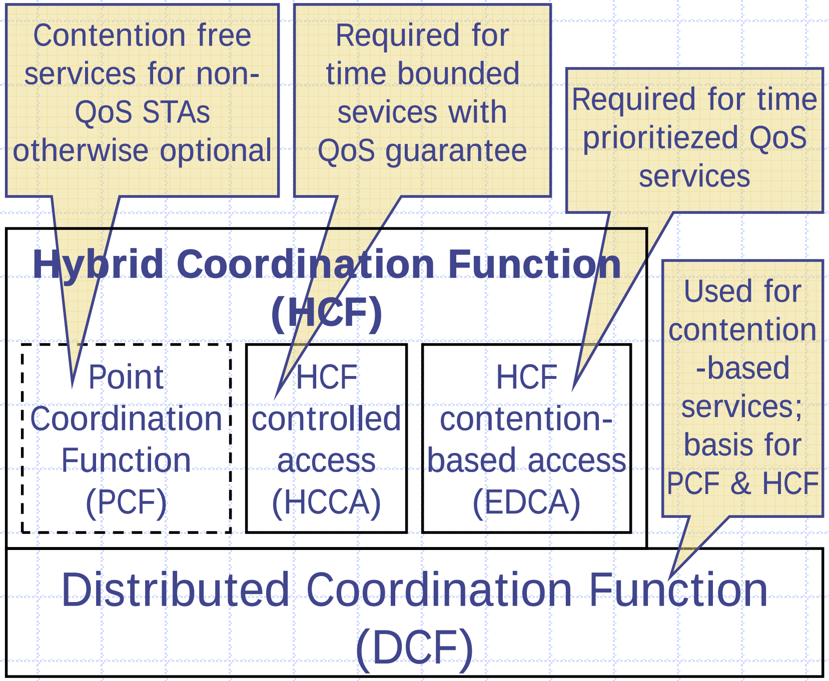
QoS Support with PCF

- The time the beacon is delayed from TBTT determines the delay of the transmission of time-bounded MSDUs that have to be delivered in the CFP.
- The duration of the MSDU delivery after polling is not under the control of the PC, which reduces the QoS provided to other stations that are polled during the rest of the CFP.

QoS Support Mechanisms of 802.11E

- The 802.11e extension introduces the Hybrid Coordination Function (HCF) for QoS support.
- The HCF defines 2 medium access mechanisms: (i) the contention-based channel access (referred to as Enhanced Distributed Channel Access-EDCA); (ii) the controlled channel access, which includes polling (HCF Controlled Channel Access-HCCA).
- With 802.11e, there may still be the 2 phases of operation within a superframe: CP, CFP. EDCA is used **only** in CP, while HCCA is used in **both** phases.

QoS Support Mechanisms of 802.11E



Contention free services for non-QoS STAs otherwise optional
Required for time bounded sevices with QoS guarantee
Required for time prioritiezed QoS services
Used for contention-based services; basis for PCF & HCF
Hybrid Coordination Function (HCF)
Point Coordination Function (PCF)
HCF controlled access (HCCA)
HCF contention-based access (EDCA)
Distributed Coordination Function (DCF)

- Main elements of 802.11e MAC architecture in the context of 802.11.
- DCF is the basis for the contention-based access of the HCF and PCF.

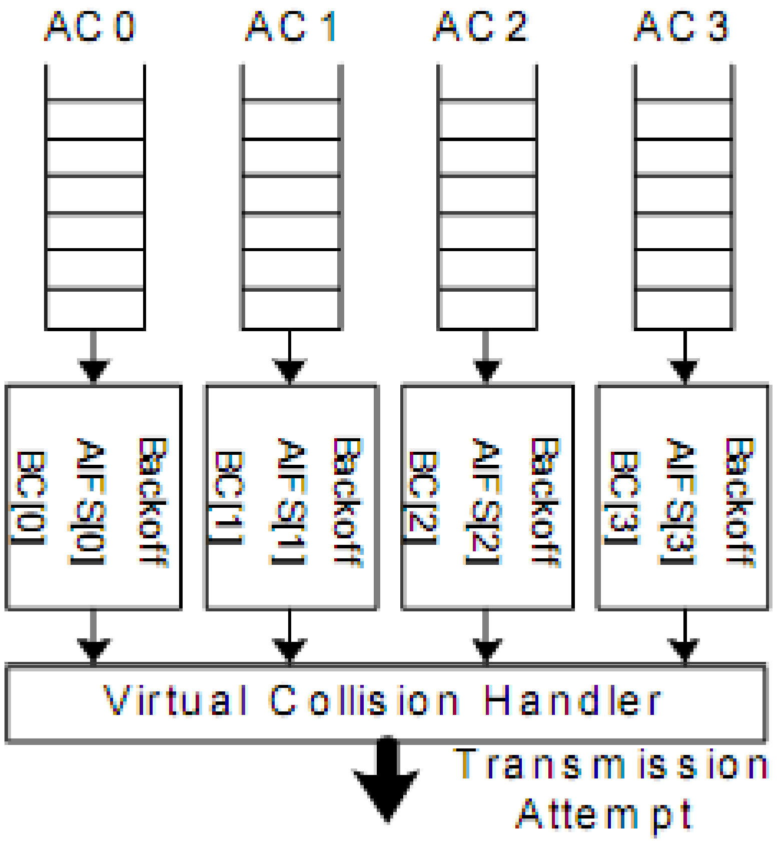
QoS Support Mechanisms of 802.11E

- Concepts:
  - QBSS: a QoS supporting BSS, including an 802.11e-compliant HC.
  - HC (Hybrid Coordinator): the station that operates as the central coordinator for other stations, similar to PC in BSS.
- There are multiple backoff processes operating in parallel within one 802.11e station, which will be explained later on. (Therefore, in the following we'll refer to backoff that attempt to deliver MSDUs, instead of stations)

Improvements of the Legacy 802.11 MAC

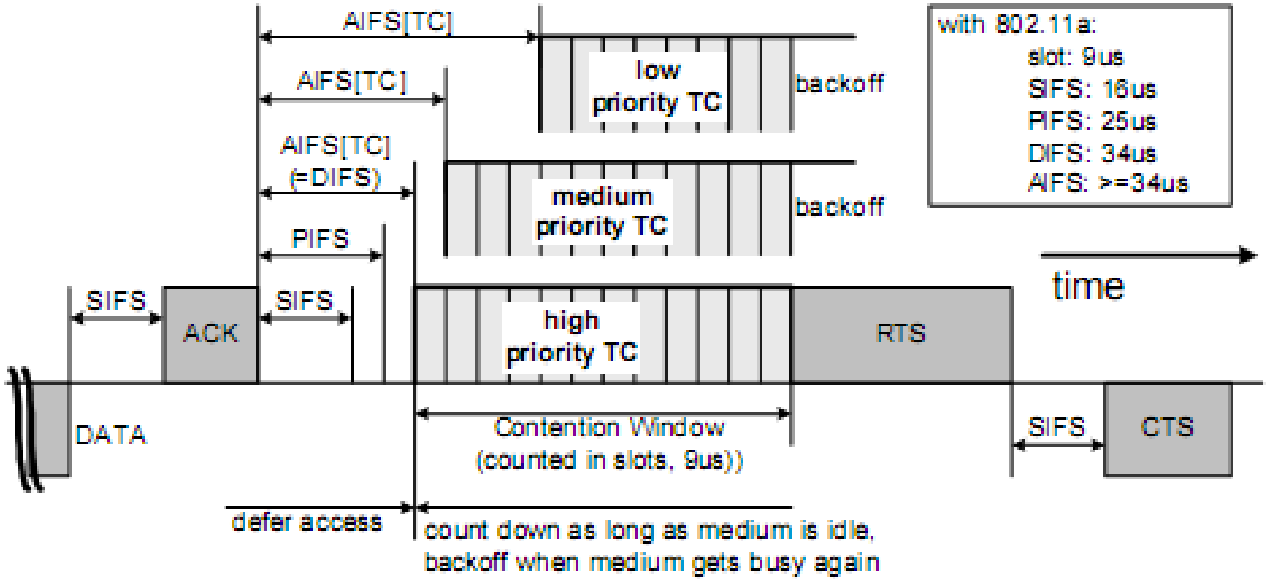
- A TXOP (transmission opportunity) is an interval of time, during which a backoff entity has the right to deliver MSDUs, is defined by its starting time and duration.
- TXOPs, which are obtained via the contention-based medium access, are referred to as EDCA-TXOPs, and limited by TXOPlimit
- HCCA-TXOPs (or polled TXOPs) are obtained by the HC via the controlled medium access, and protected by NAV.
- A time period in which the HC has control over the wireless medium is called Controlled Access Phase (CAP)

Contention-based Medium Access



- There are 4 ACs (Access Categories), thus, 4 backoff entities exist in every 802.11e stations.
- ACs are labeled according to their target application: AC_VO (voice), AC_VI (video), AC_BE (best effort), AC_BK (background).
- Each backoff entity within a station independently contends for a TXOP.

Contention-based Medium Access



- After detecting the medium being idle for a duration of AIFS[AC] (Arbitration Interframe Space), backoff entity start down-counting. AIFS is calculated as follow:
  - AIFS[AC] = SIFS + AIFSN[AC].aSlotTime >= 2
- Min and Max of the contention window are the other parameters dependent on AC.

Contention-based Medium Access

- The size of the CW in backoff stage i, after i-1 times unsuccessful transmission is:
  - CWi[AC] = min[2^i(CWmin[AC]+1)-1,CWmax[AC]]
- The collision probability increases with smaller CWmin[AC] if there are more than 1 backoff entity of the respective AC operating in the QBSS.
- The smaller CWmax[AC], the higher the medium access priority. However, a small CWmax[AC] may increase the collision probability.
- Besides retry counters similar to legacy 802.11, 802.11e also defines a maximum MSDU lifetime per AC to allow a frame remain in MAC.

Contention-based Medium Access

- Once a TXOP is obtained, a backoff entity may continue to deliver more than 1 MSDU consecutively during the same TXOP, which may take up to TXOPlimit[AC]. This concept is referred to as continuation of an EDCF-TXOP.
- Each AC has: QSRC[AC], QLRC[AC] (short and long retry counters). They are used for MAC frames of different lengths. Their default values are not given.
- When more than 1 entities in the same station reach 0 at the same time, a virtual collision occurs. The backoff entity with higher priority will transmit, whereas the others act as if a real collision occurred on the medium.

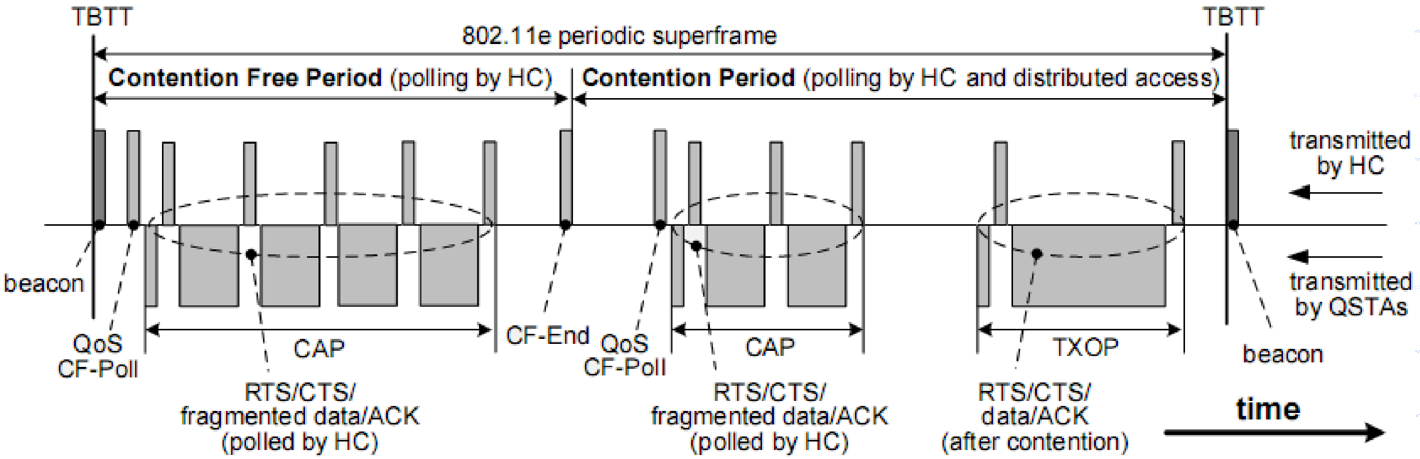
Controlled Medium Access

- The controlled medium access of the HCF, referred to as HCCA extends the EDCA access rules by allowing the highest medium access to the HC during both CFP and CP.
- HC may allocate TXOPs to itself to initiate MSDU deliveries whenever required, after detecting the medium idle for PIFS duration and without backoff.
- To give HC higher priority over legacy DCF and EDCA, AIFSN[AC] must be selected such that the earliest medium access for EDCA is DIFS for any AC.
- QoS CF-Poll from HC can be transmitted after a PIFS idle period, without backoff.

Controlled Medium Access

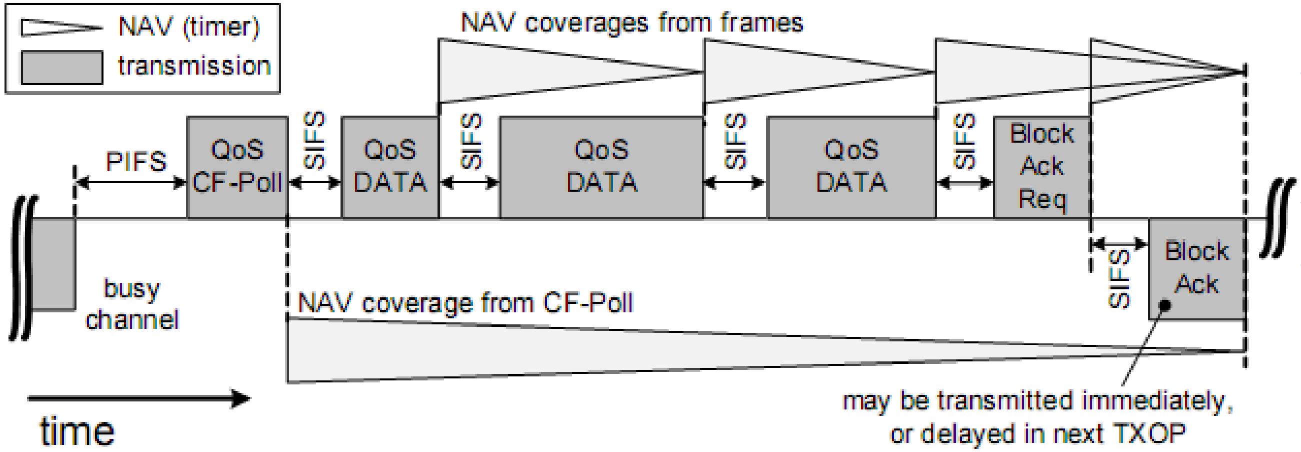
- During CFP, 802.11e backoff entities will not attempt to access the medium without being explicitly polled, hence, only HC can allocate TXOPs by transmitting QoS CF-Poll.
- During a polled TXOP, a polled station can transmit multiple frames, with SIFS between 2 consecutive frames as long as the entire exchange duration does not exceed TXOPlimit.

IEEE 802.11e Superframe


TBTT
802.11e periodic superframe
TBTT
Contention Free Period (polling by HC)
Contention Period (polling by HC and distributed access)
transmitted by HC
transmitted by QSTAs
beacon
QoS CF-Poll
CAP
RTS/CTS/ fragmented data/ACK (polled by HC)
CF-End
QoS CF-Poll
CAP
RTS/CTS/ fragmented data/ACK (polled by HC)
TXOP
RTS/CTS/ data/ACK (after contention)
beacon
time

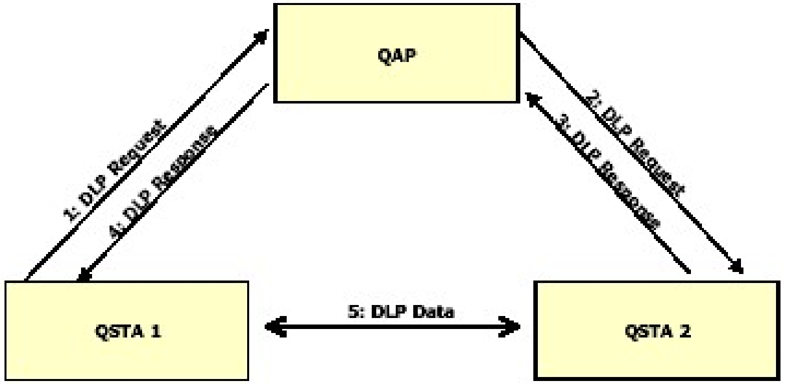
- The superframe starts with a beacon transmitted by HC.
- During CFP, the backoff entites only transmit upon being polled by HC.
- During the CP, HC may poll a station, which is different from PCF of the legacy 802.11

Block Acknowledgment



- Block acknowledgments allow a backoff entity to deliver a number of MSDUs being delivered consecutively during one TXOP and transmitted without individual ACK. => Throughput efficiency is improved.

Direct Link Protocol (DLP)



Over view of DLP for setting up a direct link

- The direct communication in 802.11e is referred to as Direct Link (DiL).
- A set up procedure, the Direct Link Protocol (DLP) is defined to establish a DiL between 802.11e backoff entities.

Radio Spectrum Management

- A standard amendment for spectrum and transmit power management extensions, known as 802.11h, has been specified and focuses on 2 services: Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC).
- While 802.11h targets on spectrum management, 802.11k specifies further measuring options, which are referred to as radio resource managements.

Information transferred

- Legacy 802.11 defines 3 different MAC frame types: management, control and data frames.
- Data frames are reserved for transporting layer. Data, control frames handle the access to the medium. Management frames serve for the administration of the BSS and terminals.
- All spectrum management actions (802.11h) and radio resource management actions (802.11k) therefore use the management format.

Specific Measurements in 802.11h

- 802.11h defines a couple of new Information Elements (transmitted in the frame body of Managemment frame).
- Measurement request/reports has 3 types: Basic request/report, Clear Channel Assessment (CCA) request/report, Receive Power Indication (RPI) histogram request/report. Basic Report generation is mandatory for STAs.
- Parameters included in the request field: Channel Number, Measurement Start Time, Measurement Duration.

Specific Measurements in 802.11h

- On reception of a measurement request of type Basic, an STA is obliged to perform required measurements and to reply with a Basic Report.
- On reception of a CCA Request, an STA optionally generates a corresponding CCA Report as reply. The CCA Busy Fraction field is the fractional duration over which the CCA indicated the channel was busy during the measurement duration.
- On reception of a RPI Histogram Request, an STA optionally reply.

Specific Measurements in 802.11K

- Radio resource measurement in 802.11k defines some further new Information Elements, such as AP Channel Report, Neighbor Report, RCPI.
- Channel Load Report: indicate Channel Load field, the proportion of time that the channel busy over measurement duration. Difference to CCA Report: including both physical and virtual carrier sense mechanisms.
- Noise Histogram Report: measurements are only taken when the NAV indicated idle channel. So it includes only non-802.11 energy in its result.

Specific Measurements in 802.11K

- Beacon Report: the aim is to gather information on other BSSs in the reception range of a stations.
- Frame Report: each entry is a summary of the traffic from one specific transmit address.
- Hidden Station Report: each entry comprises 1 doublet reporting the MAC address of a hidden station and the number of associated detected frames. Retransmission is not evaluated in the algorithm for finding hidden station.
- Medium Sensing Time Histogram Report: to estimate traffic load priorities or detect non-802.11 radio activities. Knowing the characteristic of another interference source may be exploited.

Specific Measurements in 802.11K

- STA Statistic Report: reports incrementally, listing the change in STA counters within measurement duration.
- LCI (Location Configuration Information) Report: used to convey information on specific positions of stations. 2 options: local position to ask for itself position or remote position to ask for the requested station’s.
- Measurement Pause Request: has no response. To delay processing of the next measurement request. This delay will be no less than the Pause delay specified in the Request.

Thank you for listening!