Wireless LAN with focus on IEEE 802.11 and 802.11e

Slides contributed by

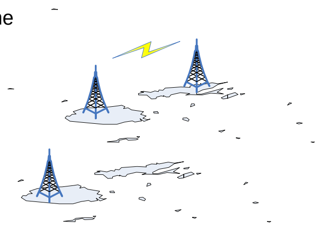
Thomas Nilsson
Dept. of computing Science
Umeå University
27 April 2006
nilsson@cs.umu.se

Lecture outline

- A short history of the WLAN development
- IEEE 802.11 with focus on the MAC layer
- Some performance issues related to 802.11
- IEEE 802.11e
- A brief overview of HiperLAN Type 1
- Some facts about HiperLAN Type 2

A Short History…

- **Classical Aloha**
  - University of Hawaii (ALOHANET) in 1970, interconnect the islands
  - Packet radio com. cf. DARPANET
  - No central control, packets arrived randomly in time
  - Max channel utilization of *0.18* was achieved
  - Simultaneous transmission resulted in collisions
- **Slotted Aloha**
  - Senders synchronized and transmissions started at slot boundaries, random backoff Increased capacity to *0.37*
- **Carrier Sense Multiple Access (CSMA)**
  - "Listen before sending scheme", send if channel idle
  - ***non-persistent***: sends immediately and if busy waits a random time until retry
  - ***p-persistent***: transmits with prob p if medium idle and defers next slot with 1-p
  - ***CSMA/CA***: backoff, carrier sensing to achieve fairness



3

A Short History…

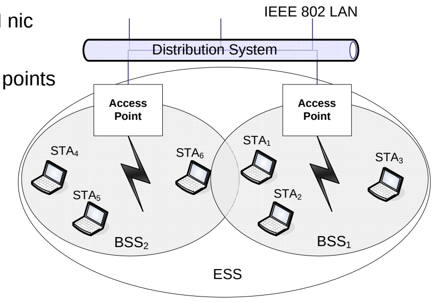
- **HiperLAN Type 1**
  - Published in 1996 by ETSI, No commercial success.
  - ***EY-NPMA*** (Elimination Yield Non-Preemptive Multiple Access)
  - Nodes transmits bursts of different lengths (Geometric distribution)
  - Efficient protocol, small prob. of collisions, supports some QoS
- **IEEE 802.11**
  - Uses CSMA/CA, standard first published in 1997 by IEEE, no QoS
  - Commercial success, most widely deployed WLAN standard
  - Little competition from other technologies
- **HiperLAN Type 2**
  - Published in 2000 by ETSI, quite unlike HiperLAN Type 1
  - Complex standard, TDMA/TDD scheme, central control, supports QoS
  - No products available only prototypes, uncertain future

4

Components and Architecture of 802.11

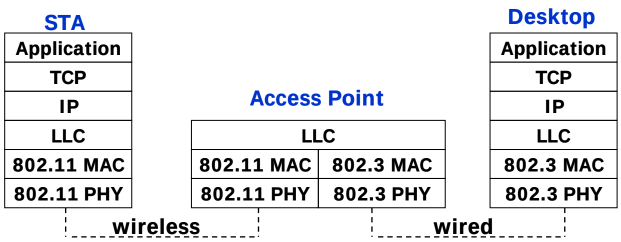
The 802.11 standard defines the following components

- **Station (STA)**
  - A mobile node, e.g. Laptop with WLAN nic
- **Access Point (AP)**
  - STAs connected/associated to access points
- **Basic Service Set (BSS)**
  - Access Point and mobile STAs
- **Basic Service Area (BSA)**
  - Geographical area covered by a BSS
- **Extended Service Set (ESS)**
  - A set of BSSs joined together
- **Distribution System (DS)**
  - Interconnects multiple BSS, backbone network, e.g. Ethernet IEEE 802.3



802.11 Protocol Architecture

- **802.11 Layers defined**
  - PHY Layer (Physical Layer) - Many different technologies
  - MAC Layer (Medium Access) - Only one MAC technology so far…
  - LLC (Logical Link Control) - a logical interface to higher layers



- **The AP only works as a bridge**

802.11 Physical Layer

- **3 PHY layers defined in original 802.11 (1997)**
  - **Frequency Hoping Spread Spectrum** (FHSS)
    - Operating in 2,4 GHz, ISM band, no license required
    - Frequency hopping, similar to Bluetooth, rates up to 2 Mbps
  - **Direct Sequence Spread Spectrum** (DSSS)
    - Operating in 2,4 GHz band, ISM band
    - The signal is spread over a wider spectrum, rates up to 2 Mbps
  - **Infrared**
    - limited use…Short range, typically 10 meters, rates up to 2 Mbps
- **Several new PHY layers have been standardized**
    - But the MAC layer remains the same as in the first standard

7

802.11: Physical layer extensions

- **IEEE 802.11b**
  - Standardized in 1999, High Rate DSSS, CCK modulation
    - Spread Spectrum tech., chip rate 11 MHz, barker sequence, ISM band
  - Two different PHY header formats
    - Backward compatibility to previous DSSS
    - Less overhead (short preamble)
  - Supports rate: 5.5, 11 Mbps
    - Also supports the lower rates 1 and 2 Mbps (DBPSK, DQPSK)
    - Almost all products supports 802.11b
  - Subdivides the ISM band into
    - 13 overlapping channels or 3 non-overlapping channel

http://standards.ieee.org/getieee802/download/802.11b-1999.pdf

8

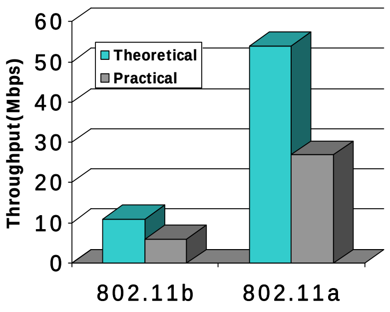
802.11: Physical layer extensions

- **IEEE 802.11a**
  - Standardized in 1999, Multi carrier modulation
  - OFDM (Orthogonal Frequency Division Multiplexing)
    - Bit stream is split into several low bit streams
    - Each bit stream uses a different carrier, 52 sub-carriers
  - Supports rates: 6,9,12,18,24,36,48,54 Mbps
    - BPSK,QPSK,QAM: Different number of bits/symbol
  - Uses the 5GHz band
    - Regulatory issues (not license free band in many European countries)
    - DFS and TPS may be required
    - Only Indoor use in Sweden, max power 200mW EIRP (5150-5250 MHz)
    - Hard to find the exact regulations in the band, PTS only gives little info

http://standards.ieee.org/getieee802/download/802.11a-1999.pdf

9

802.11a and b Throughput performance



- **Large protocol overhead**
  - Inefficient design of the MAC
  - and PHY layers limits the throughput
- **Work is ongoing (11n)**
  - To overcome these limitations
  - Achieve at least 100 Mbps at MAC
- **If considering more STAs**
  - Contention for the medium will arise resulting in an additional overhead

Note: This result is for a single user

10

802.11 Medium Access Control

- **MAC responsibilities**
  I. Controlling Access to Medium
  II. Reliable data delivery
  III. Fragmentation of frames
  IV. Roaming & authentication
  V. Power Save functionality

802.11 MAC Mechanisms

- **Access Mechanisms used by MAC**
  - **CSMA/CA**
    - The MAC algorithm used to access the medium
  - **Binary exponential backoff (BEB)**
    - Used to decrease the contention for the medium
  - **Carrier Sensing**
    - Used to determine if medium is idle or busy

802.11 Carrier Sensing

- **Physical carrier sense**
  - Senses the medium to determine if channel is idle
  - Based on CCA (Clear Channel Assessment)
  - Works be detecting a energy level of the channel
  - A interference strength above *the carrier sense threshold* -> busy
  - The implementation of CCA is PHY layer dependent
- **Virtual carrier sense**
  - Every STA keeps a Network Allocation Vector (NAV)
  - NAV tells the STA when medium is busy
  - NAV is updated by a field in the MAC frame of every packet heard
  - **NAV has precedence over physical carrier sense**

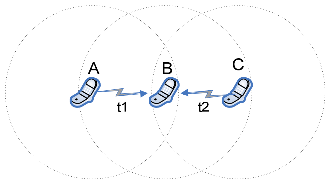
802.11 CSMA/CA

- CSMA/CA /(Collision Avoidance)
  - Carrier Sense Multiple Access with Collision Avoidance
  - For wireless communication
  - Collision avoidance before transmission
  - CS is used to determine if medium is idle before sending data
- CSMA/CD /(Collision Detection)
  - Carrier Sense Multiple Access with Collision Detection
  - Used in wired Ethernet, IEEE 802.3
  - A collision is detected while transmitting
  - Sender aborts the transmission if collision is detected

Why is collision avoidance used in wireless and not collision detection?

802.11 CSMA/CA

- **Collision detection not feasible in Wireless LANs**
  - The collision happens at the receiver side
    - Strong attenuation cf. wired networks



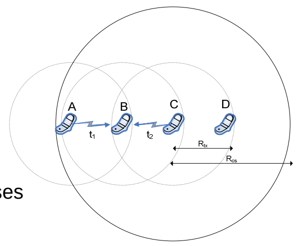
1. A and C out of range
2. A starts transmitting at t1
3. C senses medium idle and starts transmitting at t2
4. Collision happens at B
A and C do not know about the collision

A is called a "hidden terminal" with respect to C and vice versa

  - Radio architecture
    - Switching between receive and transmit (Half Duplex) , Only one antenna
  - Difference in energy/power for transmit and receive
    - Transmit power >> receive power (million times), difficult to detect difference

802.11: Physical Carrier Sense threshold

- **The Physical Carrier Sense Threshold**
  - Translates to a detection range (R_{cs})
  - Usually larger than the transmission range (R_{tx})
- **Size of the CS threshold**
  - **Increased Threshold**
    - The detection range increases.
    - HT problem decreases and ET problem increases
    - Spatial reuse of the channel decreases
  - **Decreased Threshold**
    - The detection range shrinks
    - ET problem decreases and HT problem increases
    - Spatial reuse of the channel increases



- **The CS threshold has a large effect**
  - The HT and ET problems and the spatial reuse of the channel
  - -> Capacity of the whole system

Binary Exponential Backoff (BEB)

- **802.11 Backoff has mainly two purposes**
  - Adjust the contention level under various traffic loads
  - Provide some degree of fairness among STAs
- **Backoff Counter**
  - Determines time to wait before a transmission attempt
  - Uniformly chosen within CW
  - Only decremented when medium is idle
  - Packet sent when counter reaches zero
- **Contention Window (CW)**
  - Upper and lower bound on the backoff counter
  - CW is doubled for every collision or lost frame

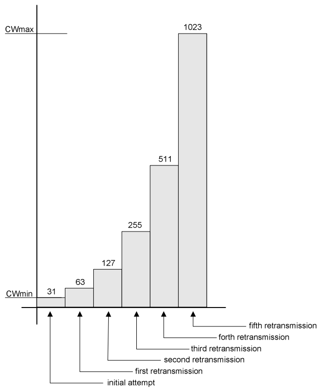
802.11 Binary Exponential Backoff

- **Binary Exponential Backoff definition**

$$BO \in U\{0, CW\}$$
$$CW \in [CW_{min}, CW_{max}]$$

- **Uniform distribution**
- **Backoff performed per packet basis**
- ***Pre* and *post* backoff**
- **CW parameters are PHY dependent**

802.11b: $Cw_{min} = 31$ $Cw_{max} = 1023$
802.11a: $Cw_{min} = 15$ $Cw_{max} = 1023$



802.11:Binary Exponential Backoff

- **Example of CW adjustment**

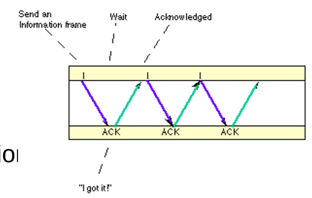
Attempt	Contention Window	Size	ACK
1	$CW = CW_{min}$	$2^5 - 1 = 31$	NO
2	$CW = (CW + 1)2 - 1$	$2^6 - 1 = 63$	NO
⋮	⋮	⋮	NO
n	$CW = min(CW_{max}, (CW + 1)2 - 1)$	$min(1023, 2^n - 1)$	YES
1	$CW = CW_{min}$	$2^5 - 1 = 31$	YES
1	$CW = CW_{min}$	$2^5 - 1 = 31$	YES

- **Two additional parameters affecting the CW**
  - Maximum number of transmission attempts for
    - Data packets is called ***Short Retry Limit***, default value is 4
    - Control packets is ***Long Retry Limit***, default value is 7
  - Interestingly, the SRL prevents CW from reaching CW_{max}

19

802.11: Stop and Wait ARQ

- **Automatic Repeat Request (ARQ)**
  - Error control
  - and flow control mechanism
- **Stop and Wait ARQ protocol**
  - Each packet reception confirmed with an ACK frame
  - Serves 2 purposes: detect lost packets and adjust the CW
- **Large overhead in ARQ**
  - Sliding window protocols
    - ***Go-back-N***
    - ***Selective Repeat***
  - More suitable for continues transmissio
  - 802.11e option for Selective Repeat

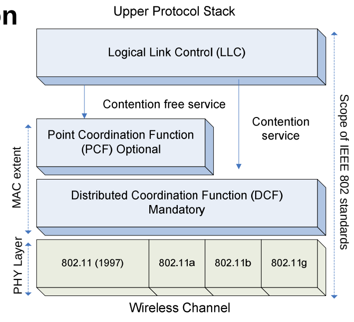


20

802.11 Medium Access Methods

Two methods to access the wireless medium exist

- **Distributed Coordination Function**
  - (DCF), Distributed algorithm
  - STAs contend for access
  - *Mandatory* in standard
- **Point Coordination Function**
  - (PCF), Centralized algorithm
  - AP is controlling access
  - Builds upon the mandatory DCF
  - *Optional* in standard

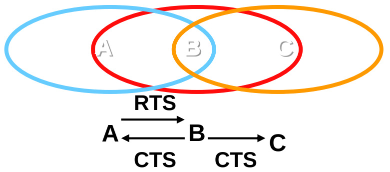


Medium Access Methods

- **Distributed Coordination Function (DCF)**
  - **Physical** and **Virtual** carrier sense (NAV) is used
  - **CSMA/CA**, STAs contend for access to the channel
  - **ARQ**: ACK required for each successful transmission
    - ACK Timeout -> lost packet
  - **Backoff** is used if medium is busy or frame is lost
  - Medium Reservation with **RTS/CTS**
    - Avoid collisions (hidden terminal problem)

RTS/CTS handshake

- **Request to Send/Clear to Send (RTS/CTS)**
  1. The source issues a Request to Send (RTS) packet
  2. The destination responds with a Clear to Send (RTS) packet
  3. Source starts transmitting the data
  4. Destination responds with an ACK
- **All STA hearing this "handshake" will know about the coming transmission and defer access**

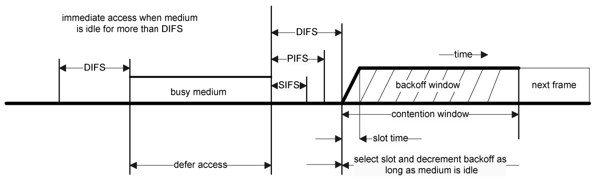


- **A and C want to send to B**
- **A sends RTS to B**
- **B sends CTS to A**
- **C "overhears" CTS from B**
- **C waits for duration of A's transmission**

23

Inter Frame Spaces (IFS)

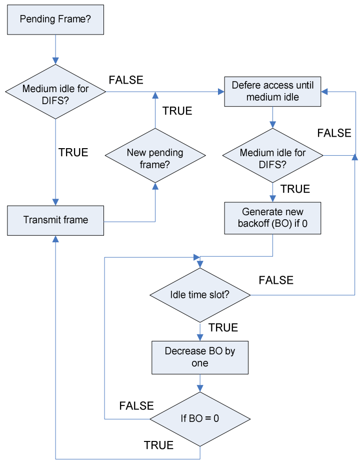
- **Transmissions are separated by short Inter Frame Spaces**
  - Used for priority access to the medium
  - Short IFS (***SIFS***) , Point Coordination Function IFS (***PIFS***) and
  - Distributed Coordination Function IFS (***DIFS***)



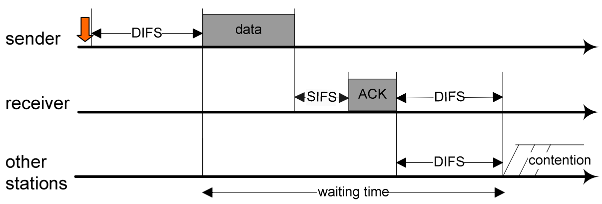
- **Extended Inter Frame Space (EIFS)**
  - STAs receiving a corrupted frame (and is not the receiver) should defer access when medium becomes idle again for a EIFS (approx the time to transmit an ACK)
  - Purpose is to provide enough time for the receiver (if correctly received the frame) to respond with an ACK frame

24

DCF Basic Access Method



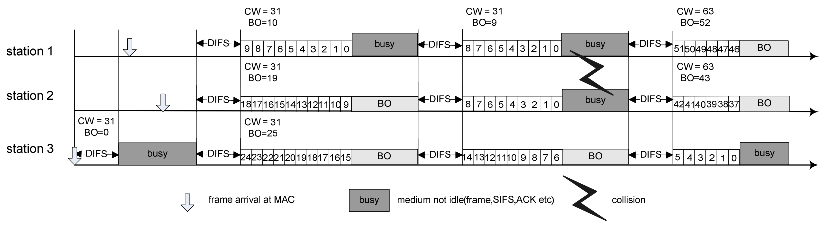
DCF Basic Access Method



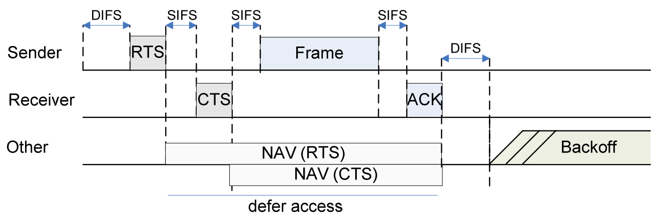
Backoff counter is decremented by one for every slot time medium is detected idle (after first waiting a DIFS)

Packet arrives at MAC layer

DCF Contention with collision



DCF Access using RTS/CTS



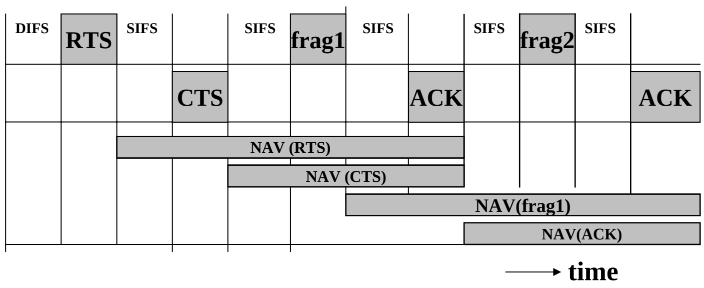
- **The RTS/CTS packet contains the duration of the transmission**
- **STAs hearing the RTS/CTS packet updates its NAV accordingly**
  - This is virtual carrier sensing
- **RTS/CTS imposes an additional overhead**
  - Overhead is larger for small packets, a RTS/CTS threshold is used

Fragmentation

- **Wireless LANs experience high bit error rates**
  - Error rates in WLANs >> LANs, Medium experience error bursts
- **Smaller probability of error with shorter frames**
  - Smaller frames have better chance of escaping error burst
  - Fragmentation may be a way to increase throughput
  - Increased overhead, more header information/per data unit
- **Fragmentation threshold**
  - Only packets above a threshold is fragmented, Manually configured

> The probability that a frame arrives without error P_1 assuming the bit errors P_b are indepedent and constant is
> $P_1 = (1 - P_b)^N$,
> where N is the number of bits per frame

Fragmentation burst



- If one fragment is lost backoff procedure is invoked
- Fragmentation may also be used without RTS/CTS

802.11 MAC Frame

Bytes:

2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration ID	Addr 1	Addr 2	Addr 3	Sequence Control	Addr 4	Frame Body	CRC

◁ **802.11 MAC Header** ▷ (Frame Control through Addr 4)

Bits:

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

Frame Control Field

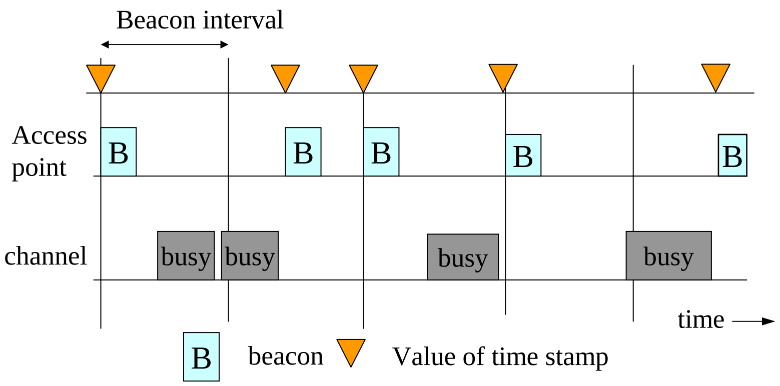
802.11 MAC Management

- **Synchronization**
  - STAs need to be synchronized with the WLAN (on the MAC layer)
  - In Infrastructured mode, STA synchronized with AP
  - Necessary for Power management and PCF operation
- **Power Management**
  - STAs may have limited battery capacity
  - Power Save features necessary, sleep mode
- **Roaming**
  - Terminals may enter a new BSS
  - Terminal must change AP
  - Like Handover in GSM (but not as smooth)
- **Authentication & encryption**
  - Authentication before access to the network
  - Encryption of data to prevent eavesdrop

Synchronization

- **All STA timers in a BSS are synchronized**
  - Needed for Power management and
  - PCF coordination
- **The access point maintains a clock**
  - The AP transmits periodic frames called *Beacons*
  - The Beacon contains the clock value
  - Time between two beacons are called the *beacon interval*
- **STAs hearing the beacon updates their clock**
  - This prevents clock drifting
- **The beacon is transmitted using normal CSMA/CA**
  - Beacon may be delayed significantly

Synchronization (cont.)



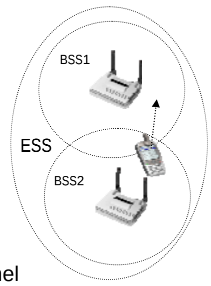
Power Management

- **Purpose is to save battery capacity**
  - Limited battery capacity and 802.11 drains batteries fast!
  - Cicso Aironet: Tx 530-560 mA, Rx 280-330 mA, Standby 200 mA
- **A STA may enter sleeping mode and turn of the radios**
  - This is notified to the AP (a bit in the MAC header is flipped)
  - The AP maintains a list of STAs in Power saving mode
  - Packets for a sleeping STAs are buffered in the AP
  - Buffered packets are sent to the STAs at designated times
- **STA must wake up periodically to receive beacons**
  - Beacon contains a *traffic indication map,* info on buffered frames
- **STAs are required to stay a wake to receive the buffered data**
  - STA sends a PS-poll frame to the AP and waits to receive the buffered data
  - In power save mode: the consumption can be reduced to 30 mA

35

Roaming between access points

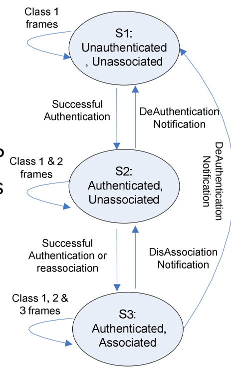
- If a Mobile STA moves beyond the coverage **of the AP**
  - but within range of another AP than (within the ESS only)
- Packet losses and incapability problems exists
  - IEEE 802.11f (Inter Access Point Protocol)
- STA decides that link to its current AP is poor
  - Radio link quality, e.g. SNR and BER, missed beacons etc
- STA uses scanning function to find another AP
  - ***Active* scanning**, STA sends a probe request on each channel
  - ***Passive* scanning**, STA listens for beacons on each channel
  - Station sends Re-association Request to new AP
- If Re-association Response is successful
  - STA has roamed to a new AP else STA scans for another AP



36

Association & Authentication

- **Authentication**
  - Shared key authentication, AP sends a challenge *k* STA encrypts *k* with the pre-shared key in the reply.
  - The WEP encryption is not secure…802.11i improves
- **Association**
  - STA needs to get synchronization information from AP
  - Exchange capability information, e.g. Supported rates
- **Disassociation**
  - May be performed by either STA or AP
  - Data cannot be sent to a disassociated STA

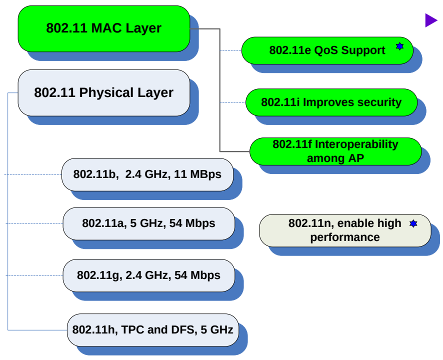


Class 1: Control frames, e.g. ACK, RTS, (de) Authentication
Class 2: Management frames, e.g. (re) (dis) Association
Class 3: Data frames

802.11 Link Adaptation (LA)

- **Adjust the modulation scheme based on the link quality**
  - Improve the performance by minimizing packet loss
  - Uses SNR/BER/ACK statistics to adjust the data rate
  - Not defined in IEEE 802.11 but manufacturer dependant
- **11b four rates (1-11Mbps) and 11a eight (6-54Mbps)**
  - Every rate has a limited operating range
  - Generally lower rates have larger operating ranges
- **When a STA moves beyond the optimal range of a rate**
  - the device will fall back to a lower rate
  - The result is better performance, less packet errors
- **However, LA may cause lower total system capacity!**
  - There is a performance anomaly using LA in a shared broadcast channel

The 802.11 Alphabet Soup



- **IEEE 802.11 task groups**
  - Updates and improves various parts of the standard
  - From a to z (20 in total)
  - Focus areas like
    - PHY layers, MAC layers
    - Spectrum regulations
    - Interoperability
  - Many groups have completed
  - Almost no letters left to be used
    - ?

Task group info and timeline: http://www.ieee802.org/11/802.11_Timelines.htm

802.11: Contention window performance

- When considering a ***fixed backoff scheme***. i.e. $CW_{min} = CW_{max}$
- The optimal CW under saturation is approximately

$$W^{opt} \approx n\sqrt{(2T)}^{*},$$

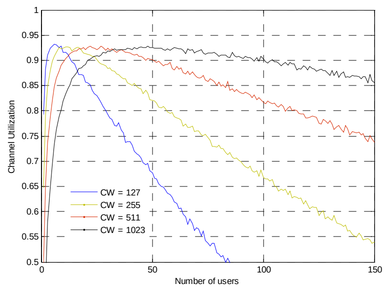
where T is the transmission time in $slotTimes$

- More complex relationship when considering a CW doubling scheme
  - But the dependency still remains to the number of users
- The biggest problem is how to approximate the optimal CW
  - The binary exponential backoff (BEB) scheme in 802.11 does a bad job
  - The BEB is discrete with little precision
- The CW is reset to CW_{min} after each successful transmission
  - This may be non optimal under saturation

* G. Bianchi, Performance Analysis of the IEEE 802.11 DCF, IEEE Journal on Selected Areas in Communications, 18:3,2000

Contention window performance

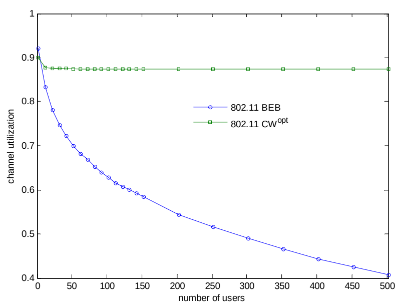
- **A simple simulation of DCF**
  - 802.11a and fixed CW for an increasing number of STAs,
  - Under saturation
  - For a given number of STAs,
    too small CW yields many collisions
    too large CW yields many idle slots
  - Cost for a collision is high since the whole packet is transmitted
  - ARQ is needed to detect the collisions
  - Capacity is wasted



Number of users	Optimal CW
10	$CW^{opt} \approx 213$
20	$CW^{opt} \approx 426$
50	$CW^{opt} \approx 1065$
100	$CW^{opt} \approx 2132$
150	$CW^{opt} \approx 3204$

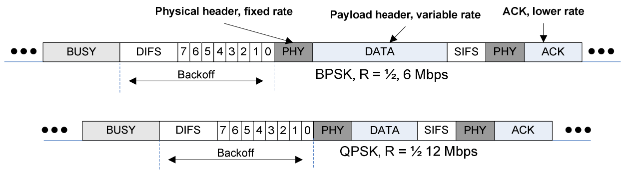
Contention window performance

- **A comparison between**
  - 802.11 BEB (normal)
  - 802.11 CW^{opt}, uses the optimal CW
  - BEB used in 802.11 is far from optimal,
  - especially for large number of users
  - for few stations the result is satisfactory



802.11: Theoretical throughput limit

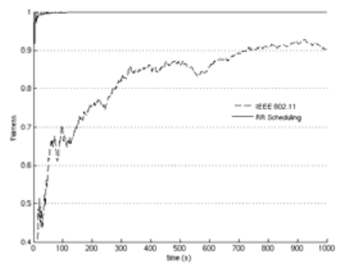
- **Physical layer and MAC layer overhead**
  - A Theoretical throughput limit exists even if the data rate goes to infinity[1]
  - Simply by increasing the rate without reducing the overhead is not an option
- **To achieve higher throughput, changes need to be done**
  - Task group **n** is working on both MAC and PHY enhancements to
  - achieve throughput figures above 100 Mbps
  - Frame aggregation: aggregate frames and thus reduce some overhead

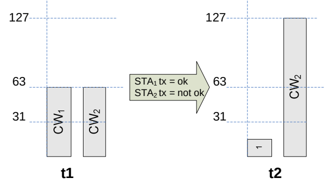


[1] Y. Xiao and R. Rosedahl, Throughput and Delay Limits of IEEE 802.11, IEEE Communications Letters, 6:8, 2002

802.11 Fairness among Stations

- **Fairness has many definitions**
  - Generally how the capacity is shared
  - Fairness on different time scales
    - *Short* and *long* term fairness
  - 802.11 is not considered to be fair in the shorter time context
  - Fairness between STAs, EBB favors STAs that exceeded last and vice versa.
  - EIFS may also be a factor influencing Fairness

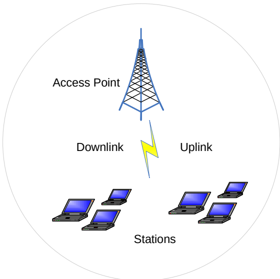


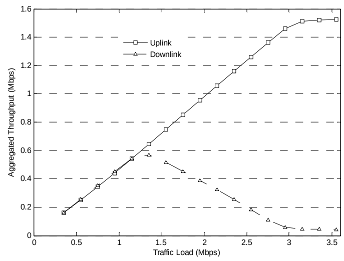


Min-max Fairness Index:
$I_{min-max} = \frac{min\{x_i\}}{max\{x_j\}}$,
where x is the rate or throughput.

802.11 Uplink/downlink starvation

- **AP has no precedence in medium access over STAs**
- **AP is responsible for all transmissions in the downlink**





- **The AP is easily starved by the uplink**
- **This problem has a large impact on TCP performance**
- **A fairness problem**

Definition of Quality of Service

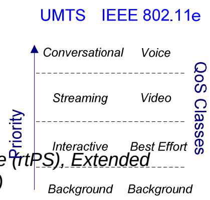
- **Applications have different QoS requirements**
  - Real time Vs. non-real time applications
  - Streaming, Web browsing, email
- **Elastic vs. Inelastic applications**
  - Tolerance of variations in throughput
- **Typical QoS parameters**
  - Throughput, Delay, Jitter. Packet loss, Bit error rate
- **Networks capable of satisfying requirements**
  - Supports quality of service
  - Not all wireless networks implement QoS support
  - IEEE 802.11 DCF has not support

Motivation: QoS in wireless networks

- **QoS is not very prioritized in wired networks**
  - Implementing QoS is difficult! Adding more hardware is easy!
  - Capacity shortage is easily solved
- **Adding more hardware in wireless**
  - Is often not an option
  - Shannon's law, one ether shared by many, limited spectrum
- **Supporting QoS in wireless is important**
  - Limited resources, maximizing resource utilization important
  - Commercial interests, user satisfaction important
  - Operators want to maximize their revenue, support new services
- **QoS guarantees in wireless is difficult**
  - Too many uncertainty factors: interference, traffic load, handover
  - May be easier to provide QoS guarantees in wired networks

Quality of Service Classes

- **Supporting arbitrary requirements is difficult**
  - One solution to this is *QoS classes*
  - Network optimizes performance according classes
  - An application belongs to a QoS class
- **Some networks utilizing QoS classes**
  - UMTS: *conversational, streaming, interactive, background*
  - IEEE 802.11e: *voice, video, Best effort, background*
  - WiMAX: *Unsolicited Grant Service (UGS), real-time Polling Service (rtPS), Extended rtPS (ertPS), Non-real-time polling service (nrtPS), Best effort (BE)*



- **Some service requirements**
  - Voice/speech: tolerates some losses sensitive to
  - delay/jitter, delay in voice < 200ms
  - Streaming: tolerates some losses, less sensitive to delay/jitter
  - Data applications: generally more sensitive to losses than delay/jitter

IEEE 802.11e (QoS support)

- **Defines the new Hybrid Coordination Function (HCF)**
  - Enhanced Distributed Channel Access (EDCA),
  - decentralized access
  - HCF Controlled Channel Access (HCCA),
  - centralized access
- **Some new mechanisms in 802.11e**
  - **User Priorities**, ranging from 0 to 7
  - **Access Categories** (AC), four per STA
  - **Arbitration Inter Frame Space** (AIFS)
  - **Transmission opportunity** (TXOP)
  - **Block Acknowledgement**, more efficient ARQ scheme
  - **Admission Control,** increases control by AP

802.11e: Priority mapping between UPs ACs.

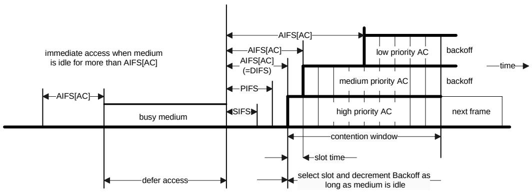
Priority	User Priorities (UP)	Access Category (AC)	Designation
lowest	1	AC_BK	Background
	2	AC_BK	Background
	0	AC_BE	Best Effort
⋮	3	AC_BE	Best Effort
	4	AC_VI	Video
	5	AC_VI	Video
	6	AC_VO	Voice
highest	7	AC_VO	Voice

802.11e: Arbitration Inter Frame Space

- **EDCA Parameters: AIFS (Arbitration Inter Frame Space)**
  - Time medium is sensed idle before an AC starts Tx or BO
  - Not fixed as in DCF instead variable value, specific to the AC

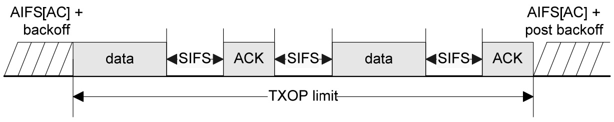
$$AIFS = AIFSN \times SlotTime + SIFS$$

  - Higher priotrity AC use smaller AIFSN
  - Minimum allowed AIFSN is 2, which makes AIFS = DIFS



802.11e: contention free bursting

- **EDCA Parameters: Transmission Oppurtunity**
  - Each AC contends for a TXOP
  - The *TXOP Limit* parameter defines its maximum length
  - If length allows, multiple frames may be transmitted
  - Consecutive transmissions are separated by SIFS
  - This is called **Contention Free Bursting**



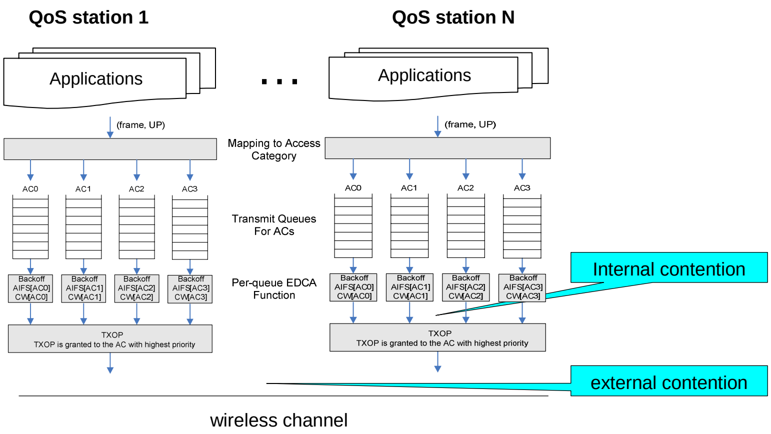
802.11e: default contention parameters

- AC Specific default contention parameters

AC	AIFSN	CW_{min}	CW_{max}
AC_VO	2	7	15
AC_VI	2	15	31
AC_BE	3	31	1023
AC_BK	7	31	1023

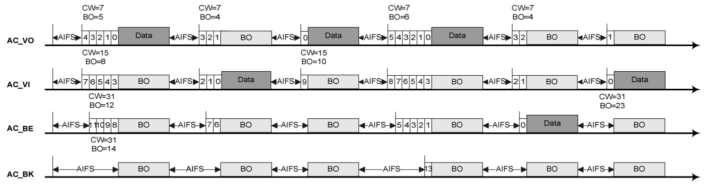
  - These values are not fixed, can be dynamically adjusted by the AP
  - No algorithm for doing so is given in the standard
  - up to manufacturers

802.11e EDCA: Basic concept



802.11e: Internal contention

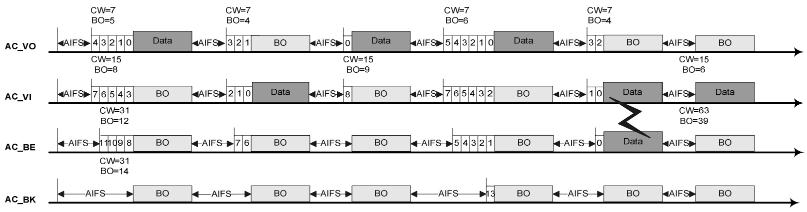
- **EDCA Access Mechanism**
  - Example: four EDCAFs contending *inside a single station*
  - Each AC acts as a virtual station inside the station



  - Each AC contends independantly from other ACs
  - Each AC uses the specific CW values: CW[AC], AIFS[AC]

802.11e: Internal contention

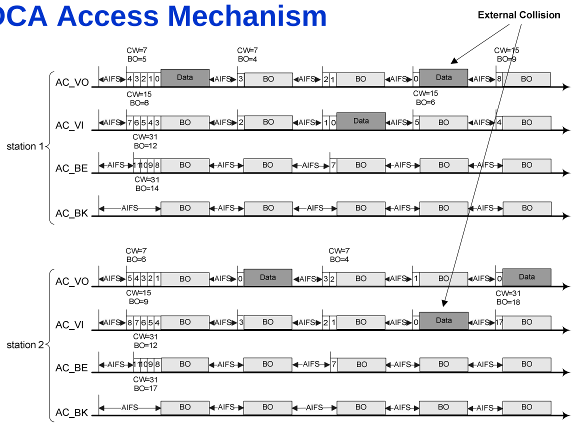
- **EDCA Access Mechanism**
  - Collisions among AC within a single STA, called Virtual Collisions



  - **Virtual collisions**: solved by grating the highest AC access
  - Other colliding ACs act as external collisions: doubling CW and backoff

802.11e: external contention

- **EDCA Access Mechanism**



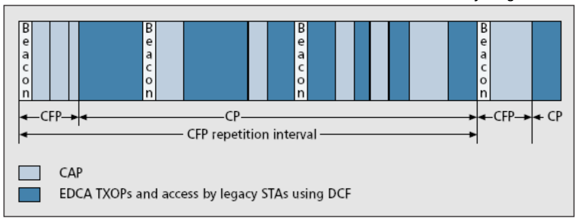
- Collisions among AC within a two STA may arise, real collisions

802.11e: HCF controlled channel access

- Similar to the legacy PCF, HCCA provides polled access to the wireless medium. In particular, HCCA uses a QoS-aware hybrid coordinator (HC), which is typically located at the QoS access point (QAP) in infrastructure WLANs.
- HC uses PIFS to gain control of the channel and then allocates TXOPs to QSTAs, which are referred as HCCA TXOPs or polled TXOPs.
- Unlike PCF, HCCA can poll the QSTAs during contention periods (CPs), and HCCA takes into account QSTAs' specific flow requirements in packet scheduling.
- Controlled access phase (CAP) is defined as the time period when HC maintains control of the medium.
- After grabbing the channel, the HC polls QSTAs in turn according to its polling list.
- In order to be included in the polling list of the HC, a QSTA must send a QoS reservation request using the special QoS management frame, and each individual flow needs one particular reservation request.

802.11e: HCF controlled channel access

D. Gao *et. Al.* “Admission Control in IEEE802.11e Wireless LAN”, IEEE Network, July/August, 2005



- **CAP** **Controlled Access Phase**
- **CP** **Contention Period**
- **CFP** **Contention Free Period**

59

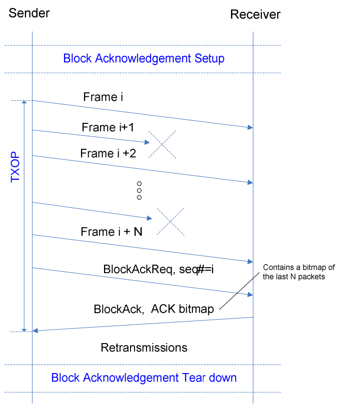
802.11e: Admission Control mechanism

- **Gives the AP better controll over the resource**
  - Contention based Admission Control
  - Goal is to protect sensitive flows from ACs AC_VO and AC_VI
  - not to violate servie commitments made earlier to granted flows
  - AP signals in the Beacon if adm. control is mandatory for ACs
    - New ACs/STAs must make explicit requests to the AP and
    - provide the AP with: packet size, mean data rate, min PHY rate etc
  - Based on this info a new AC is granted access with a response
    - How to make this decission is non trivial and not defined in the standard
    - The response contains the *medium time* allowed for the spcific AC
    - The actual admission control algorithm is not specified in the standard

60

802.11e: Block Acknowledgement Mode

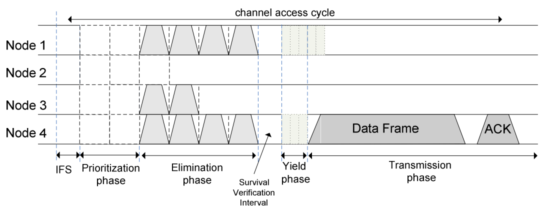
- **802.11 has inefficient ARQ**
  - Stop and wait, imediate ACK scheme
  - Purpose is two-fold: detect lost packets, adjust CW
  - Overhead is large, a significat share of the capacity is waisted
- **Two new config. for ARQ**
  - No ARQ, Block Acknowledgement mode
  - Block Acknowledgement mode is a type of selective repeat
  - May be used in contention free busrsting
  - A new problem.. How to adjust CW when immediate feedback is lost?



61

EY-NPMA (MAC for HiperLAN 1)

- **Elimination Yield Non-preemptive Priority Multiple Access**
  - MAC for HiperLAN Type 1, p2p ad-hoc mode, some QoS support, 23 Mbps



  - ***Prioritization phase***: nodes listen for a number of slots according to their priorities.
  - ***Elimination phase***: length is sampled from a *truncated geometric distribution* (max length = *m),* The probability of selecting a burst of length *k* is:

$$P(k) \overset{p=0.5}{=} \begin{cases} p^k(1-p) & \text{if } 0 \leq k < m \\ p^m & \text{if } k = m, \end{cases}$$

62

EY-NPMA (MAC for HiperLAN 1)

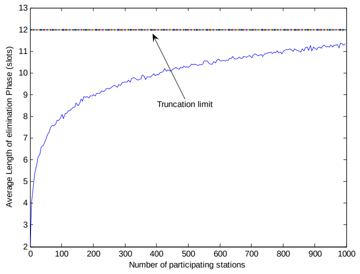
- ***The Yield phase:***
  - The remaining nodes will sense the channel for a uniformly chosen number of slots
  - *The winner:* selects the fewest number of mini slots and starts the transmission
- **Two channel access modes**
  - Access in ***channel free condition***:
    - listen to the channel for a random number of slots (*0, k*)
    - if idle transmit, Intended for lower channel loads
  - Access in ***synchronized channel condition***
    - Immediately following the previous channel access cycle
    - For higher loads

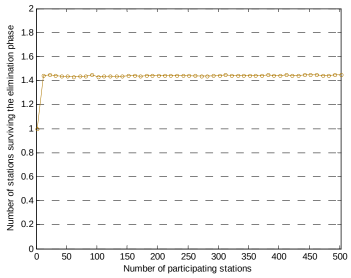
EY-NPMA (MAC for HiperLAN 1)

- **Prioritization phase**
  - Each node has a so-called channel access priority, P_i
  - Defines *h* priorities, with 0 denoting the highest priority
  - Priorities are ***non preemptive*** only nodes with highest P_i contends
  - Under high loads only the highest priorities will access the channel
- **IEEE 802.11e priorities vs. HiperLAN priorities**
  - Priorities in H1 are *non-preemptive* while *preemptive* in 802.11e
  - In 802.11e backoff performed after AIFS (additional idle time)
  - In HiperLAN a burst follows immediately after AIFS (Prio phase)

EY-NPMA performance

- **Elimination phase length**
  - The number of nodes have only an effect of the length of the elimination phase (right figure)



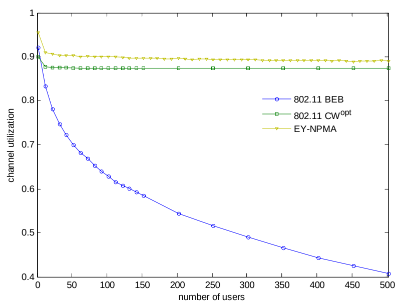


- **Elimination phase survivors**
  - the number surviving this phase is almost independent on the number of participating nodes (left figure)

65

EY-NPMA vs. 802.11 comparison

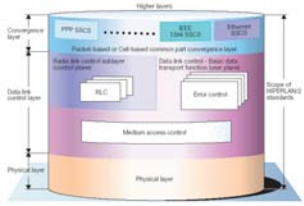
- **Simulation study**
  - Simple model of the MAC layers
  - Under saturation conditions
  - Same PHY layer as 802.11a is assumed, i.e. slot times etc.
  - All nodes have the same priorities
  - No propagation effects are modeled
- **Results from Ad hoc study**
  - EY-NPMA is a 'noise protocol'
  - Under high loads much background noise will be generated due to the elimination phase
- **802.11 vs. HiperLAN Type 1**



66

ETSI HiperLAN Type 2

- **Centralized mode with AP**
  - A complex standard published in 2000 by ETSI
  - Resemblance with a telecommunication std.
  - An ad hoc mode but requires central control
- **H2 Features**
  - High speed transmission, up to 54 Mbps
  - Connection oriented cf. IEEE 802.11
  - QoS, DFS, TPC, convergence layers
  - Mobility support, Interworking with e.g. UMTS, ATM, etc.



- **Medium Access Control (MAC)**
  - The air interface is based on TDMA: MAC frames have a fixed size and are repeated every 2ms (time slots)
  - Time Division Duplex (TDD): Uplink and downlink are multiplexed onto the same MAC frame
  - Many control channels are mapped onto the MAC frame

ETSI HiperLAN Type 2

- **Physical layer**
  - OFDM, 52 sub carriers, 54 Mbps, 5 GHz
  - Similar to 802.11a, a harmonization between the two
- **Transport Channels**
  - **Broadcast Channel (BCH)**
    Control info, reaches all MTs, for RRC functions, e.g. power levels, AP ID
  - **Frame Channel (FCH)**
    describes structure of current MAC frame, e.g. size of DL phase.
  - **Random Access Channel (RCH)**
    For MTs to request transmission resources in future frames
  - **Access Feedback Channel (ACH)**
    information on previous access attempts made in the RCH
- **Resource Control (MAC)**
  - MTs make requests in RCH using slotted Aloha, exponential backoff
  - centralized controller schedules the resource, polling