EEC173B/ECS152C, Winter 2006

Wireless LANs
- Evolution of Technology & Standards
- IEEE 802.11
  - Design Choices
  - Architecture & Protocols
  - PHY layer
  - MAC layer design

Acknowledgment: Selected slides from Prof. Schiller & Prof. A. Joseph

Wireless LANs: Design Requirements

- Global, seamless operation
  - No special permissions or licenses needed to use the LAN
  - Ad hoc networks, no planning, no wiring
- Simple MAC to support multiple PHY layers
- Mechanism to support multiple overlapping network
  - Provisions to handle interference
  - Mechanisms to handle hidden terminals
- Robust transmission technology
- Easy to use for everyone, simple management
- Low power for battery use
- Security (no one should be able to read my data), privacy (no one should be able to collect user profiles), safety (low radiation)
- Transparency concerning applications and higher layer protocols, but also location awareness if necessary

Design Choices

Q1: Which frequency range to use?

Q2: PHY layers: IR or RF?

Q3: MAC: CSMA (random access) or TDMA?

Q4: Radio Technology: Direct-sequence of frequency-hopping?

Q5: Peer to peer architecture of Base-station approach?

Evolution

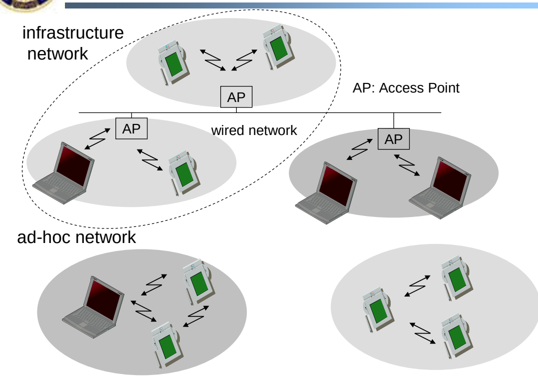
- Early experiences (1970-72): IBM, HP, Motorola
  - Abandoned due to limited performance and unavailability of frequency bands
- Early challenges:
  - Complexity and cost
  - Bandwidth
  - Coverage
  - Interference
  - Frequency administration
- Emergence of unlicensed bands
  - Release of Industrial, Scientific and Medical (ISM) bands in 1985
- Applications: military, home and enterprise networks, mobile networks, teethe less access

IEEE 802.11

- Standardization group formed in 1990, first standards completed in 1997
- IEEE 802.11 is the first WLAN standard; only one to secure a market
- IEEE 802.11b
  - Also known as wireless Ethernet and Wi-Fi
  - Operates in an unlicensed radio spectrum at 2.4 GHz
  - Wireless Ethernet access at 11 Mbps
- Other standards: 802.11a, 802.11g, 802.11e, …
- Supports both infrastructure as well as ad hoc modes

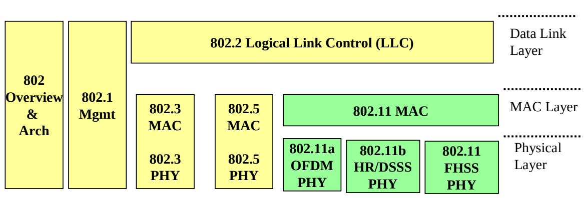
5

Comparison: infrastructure vs. ad-hoc networks



6

IEEE 802 Standards & OSI Model



- Observe 802.11 MAC is common to all 802.11 Physical Layer (PHY) standards
- 802.11 PHY is split into two sublayers
  - Physical layer convergence procedure (PLCP)
  - Physical Medium Dependent (PMD)

7

Related Standards

- Bluetooth
  - Originally intended for interconnecting computing and communication devices
- HIPERLAN
  - European standard for wireless LANs
- IEEE 802.16 Broadband Wireless
  - Addresses needs of fixed broadband wireless access replacing fibers, cables, etc.

8

Q1: Which frequency range to use?

802.11 Standards and Spectrum

Key Standards	Max Rate	Spectrum (U.S.)	Year
802.11	2 Mbps	2.4 GHz	1997
802.11a	54 Mbps	5 GHz	1999
802.11b (WiFi)	11 Mbps	2.4 GHz	1999
802.11g	54 Mbps	2.4 GHz	2003

- 2.4-2.5 GHz for all above except 802.11a, referred to as C-Band Industrial, Scientific, and Medical (ISM) Band
  - Microwave ovens and some cordless phones operate in the same band
- 802.11a uses Unlicensed National Information Infrastructure bands
  - 5.15-5.25 GHz, 5.25-5.35 GHz, 5.725-5.825 GHz

ISM Bands Trafeoffs

	915 MHz	2.4 GHz	5.8 GHz
Bandwidth	26 MHz	83.5 MHz	125 MHz
Availability	US/Canada	World-wide	US/Canada
Cost	Low	Medium	High
Usage	High (Very crowded)	Medium (Getting busy)	Low (Empty)

Q2: Physical Layer Alternatives (1)

- Infrared (IR) vs. Radio (RF)
- IR LAN Characteristics
  - Uses IR diodes, infrared light: 850-950 nanometers
  - Range is a function of
    - Xmit power (received optical power varies as $1/r^2$)
    - Background noise (fluorescent lights, sunlight)
    - Type of link: Directed, non-directed, line-of-sight, diffuse
    - Multiple reflections (walls, furniture etc.)
  - No Rayleigh fading (multipath effects)
  - Example Non-directed (15-75 degree capture half angle)
    - IRDA (laptops/cell phones), Rednet (alarm monitoring), ParcTab (Xerox Parc PDA)

Q2: Physical Layer Alternatives (2)

- Radio (RF)
  - Wide area instead of “spot” connectivity
  - More complicated circuitry, regulatory
  - Constraints (ISM bands) in the U.S.,
    - typically using the license free ISM band at 2.4 GHz
  - Very susceptible to Rayleigh fading and Inter-symbol interference

Comparison: Infrared vs. Radio Transmission

Infrared

- Advantages
  - Simple circuitry, cheap, available in many mobile devices
  - No regulatory constraints (no licenses needed)
  - Simple shielding possible
- Disadvantages
  - Interference by sunlight, heat sources etc.
  - Many things shield or absorb IR light
  - Low bandwidth
- Example
  - IrDA (Infrared Data Association) interface available everywhere

Radio

- Advantages
  - Experience from wireless WAN and mobile phones can be used
  - Coverage of larger areas possible (radio can penetrate walls, furniture etc.)
- Disadvantages
  - Very limited license free frequency bands
  - Shielding more difficult, interference with other electrical devices
- Example
  - WaveLAN, HIPERLAN, Bluetooth

13

IR vs. RF

	IR	RF
Cost	<$10	<$20
Regulation	None	No Licence (ISM bands)
Interference	Ambient Light	Radiators
Coverage	Spot	Wide Area
Performance	Moderate	Depends on BW
Coexistence	Limited	Possible

14

Q3: Media Access

- Why MAC? Same reason as for wired networks
  - Contention/floor control
- Media in wireless networks is shared and is scarce – access must be controlled
- Observations:
  - Contention is at the receiver, not at the sender – makes the carrier sense approach inappropriate
  - Unlike Ethernet, congestion is location-dependent
  - The media access protocol should propagate congestion information explicitly rather than having each device learn about congestion independently
  - Media access protocol should propagate synchronization information about contention periods, so that all devices can contend effectively

15

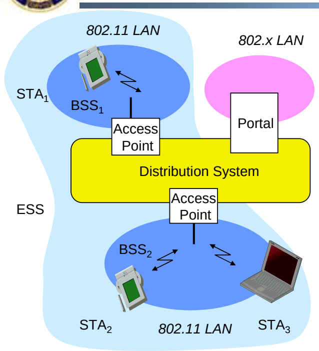
CSMA vs. TDMA

- TDMA (controlled access)
  - Simple remote stations (unless remotes can be both master/slave)
  - High power saving potential thru scheduling
  - Bluetooth approach
- CSMA (random access)
  - Can be implemented on an Ethernet chipset
  - QoS issues (uneven delays)
  - IEEE 802.11 uses a modified version of this

*** *More about this later after we introduce the IEEE 802.11 architecture and protocol stacks*

16

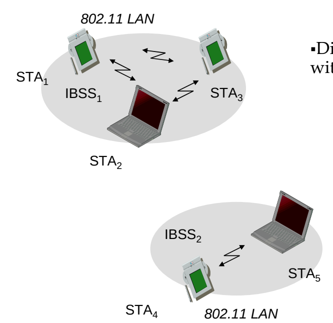
802.11 - Architecture of an Infrastructure Network



- Station (STA)
  - Terminal with access mechanisms to the wireless medium and radio contact to the access point
- Basic Service Set (BSS)
  - Group of stations using the same radio frequency
- Access Point
  - Station integrated into the wireless LAN and the distribution system
- Portal
  - Bridge to other (wired) networks
- Distribution System
  - Interconnection network to form one logical network (EES: Extended Service Set) based on several BSS

17

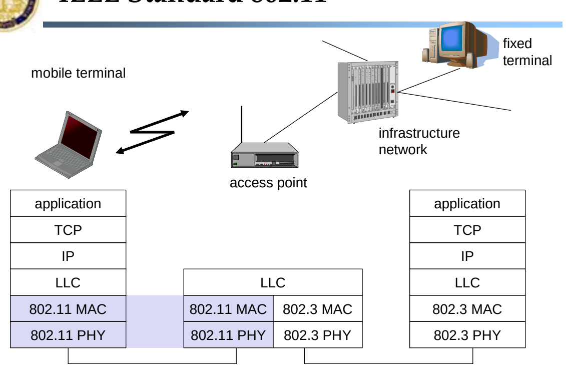
802.11 - Architecture of an Ad-hoc Network



- Direct communication within a limited range
  - Station (STA): terminal with access mechanisms to the wireless medium
  - Independent Basic Service Set (IBSS): group of stations using the same radio frequency

18

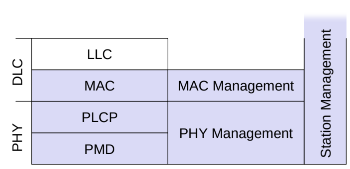
IEEE Standard 802.11



19

802.11 - Layers and functions

- MAC
  - Access mechanisms, fragmentation, encryption
- MAC Management
  - Synchronization, roaming, MIB, power management
- PLCP (Physical Layer Convergence Protocol)
  - Clear channel assessment signal (carrier sense)
- PMD (Physical Medium Dependent)
  - Modulation, coding
- PHY Management
  - channel selection, MIB (management information base)



- Station Management
  - Coordination of all management functions

20

PHY Layer

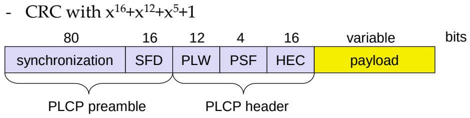
- When the MAC protocol data unit (MPDU) arrive at the PLCP layer, a header is attached that is designed specifically for the PMD
- The PLCP packet is then transmitted by the PMD according to specification of the signaling techniques
- IEEE 802.11 defines three PLCP packet formats: 2 radio (typ. 2.4 GHz), 1 IR
  - FHSS (frequency hopping spread spectrum)
  - DSSS (direct sequence spread spectrum)
  - DFIR (diffused infrared)

FHSS

- PMD hops over 78 channels of 1 MHz each in the center of 2.44 GHz ISM bands
- Spreading, d-espreading, typically, 1 Mbit/s
  - Min. 2.5 frequency hops/s (USA), two-level GFSK modulation
- Each BSS can select one of the three patterns of 26 hops:
  - (0, 3, 6, 9, …, 75)
  - (1, 4, 7, 10, …, 76)
  - (2, 5, 8, 11, …, 77)
- IEEE 802.11 specifies specific random hopping pattern for each of these frequency groups that facilitates multivendor interpretability
- Multiple BSS can co-exist in the same area by up to three APs using different frequency groups

FHSS PHY packet format

- Synchronization
  - Synch with 010101... pattern
- SFD (Start Frame Delimiter)
  - 0000110010111101 start pattern
- PLW (PLCP_PDU Length Word)
  - Length of payload incl. 32 bit CRC of payload, PLW < 4096
- PSF (PLCP Signaling Field)
  - Data of payload (1 or 2 Mbit/s)
- HEC (Header Error Check)
  - CRC with $x^{16}+x^{12}+x^5+1$



DSSS

- DSSS communicates using non-overlapping pulses at 11 Mcps
- The ISM band at 2.4 GHz is divided into 11 overlapping channels spaced at 5 MHz
  - A PHY layer managemnet sublayer of AP covering a BSS can select one of the choices
- Because of wider bandwidth, DSSS provides a better coverage and a more stable signal
- DBPSK modulation for 1 Mbit/s (Differential Binary Phase Shift Keying), DQPSK for 2 Mbit/s (Differential Quadrature PSK)
- Preamble and header of a frame is always transmitted with 1 Mbit/s, rest of transmission 1 or 2 Mbit/s
- Chipping sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code)
- Max. radiated power 1 W (USA), 100 mW (EU), min. 1mW

DSSS PHY packet format

- Synchronization
  - synch., gain setting, energy detection, frequency offset compensation
- SFD (Start Frame Delimiter): 1111001110100000
- Signal
  - Data rate of the payload (0A: 1 Mbit/s DBPSK; 14: 2 Mbit/s DQPSK)
- Service
  - future use, 00: 802.11 compliant
- Length of the payload
- HEC (Header Error Check)
  - protection of signal, service and length, $x^{16}+x^{12}+x^5+1$

128	16	8	8	16	16	variable	bits
synchronization	SFD	signal	service	length	HEC	payload	
PLCP preamble		PLCP header					

25

DFIR (diffused infrared)

- Infrared
  - 850-950 nm, diffuse light
  - Typically 10 m range
  - Carrier detection, energy detection, Synchonization

26

802.11 - MAC layer

- Functions:
  - Control media access for reliable data delivery
  - Support roaming, authentication, power conservation
- Basic services provided by MAC layer
  - Asynchronous Data Service (mandatory)
    - Exchange of data packets based on "best-effort"
    - Support of broadcast and multicast
  - Time-Bounded Service (optional)
    - implemented using PCF (Point Coordination Function)

27

Reliable Data Delivery

- High degree of unreliability and large timers for retransmissions used in higher layers motivates to deal with errors at the MAC layer
- Each transmission is followed by an ACK as an atomic unit. Retransmission is done if the ACK is not received

28

DFWMAC

- MAC mechanisms are also called distributed foundation wireless medium access control (DFWMAC)
- Three access methods has been defined
  1. Mandatory basic method based on CSMA/CA
     - Collision avoidance via randomized "back-off" mechanism
     - Minimum distance between consecutive packets
     - ACK packet for acknowledgements (not for broadcasts)
  2. Optional contention-free method w/ RTS/CTS
     - Avoids hidden terminal problem
  3. Optional contention-free method for time-bounded service
     - Access point polls terminals according to a list
- Method 1 + 2: Distributed Coordination Function (DCF)
- Method 3: Point Coordinated Function (PCF) Centralized

29

Carrier Sense Multiple Access (CSMA appropriateness?)

- Carrier sense provides information about potential collision at the sender, but not at the receiver
- Since the receiver and sender are not collocated, carrier sense does not provide adequate information for collision avoidance – interference at the sender does not imply interference at the receiver

30

Carrier Sensing

- Carrier sensing in IEEE 802.11 is performed physically or virtually
- PHY sensing is through the clear channel assignment (CCA) signal produced by PLCP
- CCA is generated by sensing detected bits or by checking the radio subsystem
- Virtual carrier sensing is done based on a network allocation vector (NAV)
  - Used in combination of RTS/CTS
  - More later …

31

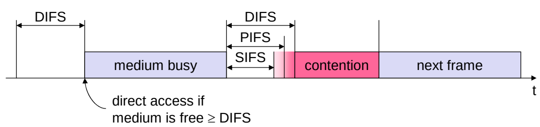
MAC: Time Slots & Inter-Frame Spacing

- All access methods use concept of "slots"
  - Slot time is derived from medium propagation delay, transmitter delay, and other PHY dependent paramters
  - 50 μs for FHSS and 20 μs for DSSS
- Medium can be busy or idle (detected by CCA)
- Use different parameters to control the waiting time before medium access, or *Inter-Frame Spacing*
  - i.e., how long should one wait when the medium is "free" before accessing the channel

32

Priorities of Medium Access

- Priorities defined through different inter frame spaces
  - no guaranteed, hard priorities
- SIFS (Short Inter Frame Spacing)
  - Highest priority, for ACK, CTS, polling response
- PIFS (PCF IFS), typically SIFS + 1 slot time
  - Medium priority, for time-bounded service using PCF
- DIFS (DCF IFS), typically SIFS + 2 slot time
  - Lowest priority, for asynchronous data service



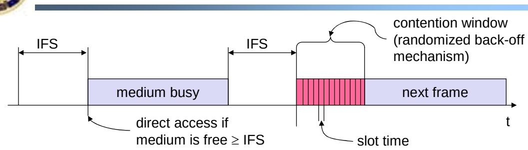
33

IEEE 802.11 DCF

- DCF sublayer makes use CSMA/CA
  - Contention-based random access
  - Collision detection not possible while a node is transmitting
  - Collision avoidance
    - Nodes stay silent when carrier sensed busy (physical/virtual)
    - Backoff intervals used to reduce collision probability
- Uses RTS-CTS exchange to avoid hidden terminal problem
  - Any node overhearing a CTS cannot transmit for the duration of the transfer
  - Any node receiving the RTS cannot transmit for the duration of the transfer
    - To prevent collision with ACK when it arrives at the sender
- Uses ACK to achieve reliability

34

802.11 DCF- CSMA/CA access method (1)



- Station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
- If the medium is free for the duration of an IFS, the station can start sending (IFS depends on service type)
- If the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
  - Choose a random backoff interval in the range [0,CW]
  - CW is contention window

35

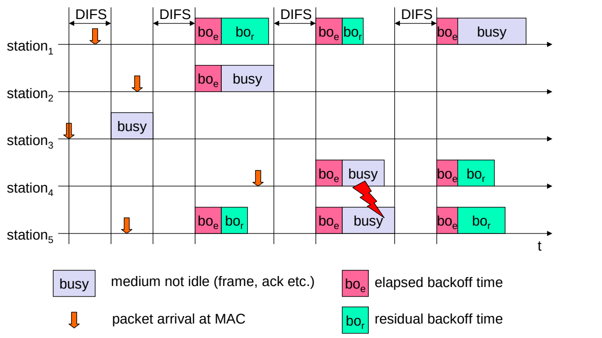
Backoff Timer for Fairness

- Basic CSMA/CA is not fair
  - Independent of the overall time a node has already waited for transmission, each node has to choose a random timer in the next cycle, and has the same chances of transmitting data
- Backoff Timer
  - Choose a random backoff interval between [0,CW]
  - Count down the backoff interval when medium is idle
  - Count-down is suspended if medium becomes busy
  - When channel is idle, continue to count down
  - When backoff interval reaches 0, transmit data

=> Stations waiting longer have advantage over stations that just entered

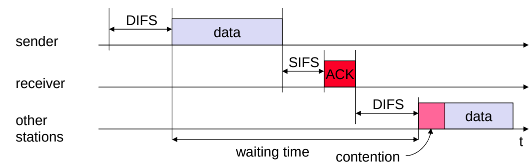
36

CSMA/CA Example - competing stations



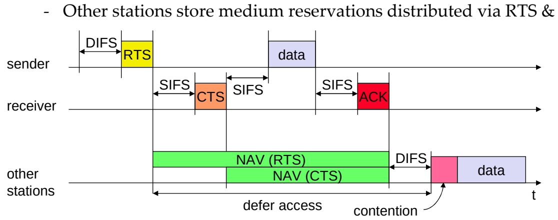
802.11 DCF CSMA/CA: ACK

- Sending unicast packets
  - Station has to wait for DIFS before sending data
  - Receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (CRC)
  - Automatic retransmission of data packets in case of transmission errors

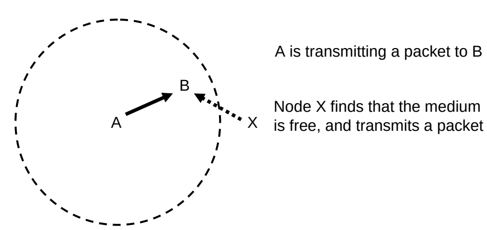


802.11 DCF-RTS/CTS

- Contention-free method
  - Station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
  - Acknowledgement via CTS after SIFS by receiver (if ready to receive)
  - Sender can now send data at once, acknowledgement via ACK
  - Other stations store medium reservations distributed via RTS & CTS

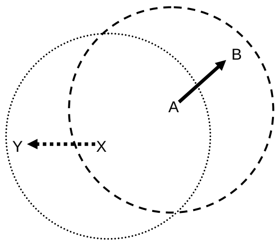


A Case for RTS/CTS: Hidden Terminal Problem



No carrier ≠OK to transmit

Exposed Terminal Problem



A is transmitting a packet to B

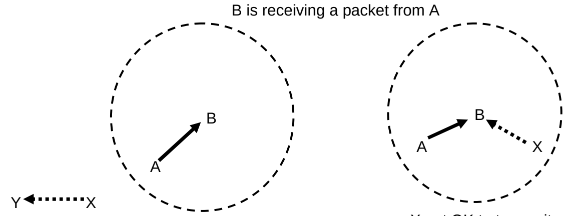
X can not transmit to Y, even though it will not interfere at B

Presence of carrier ≠ holds off transmission

41

What is needed: Busy Tone

B is receiving a packet from A



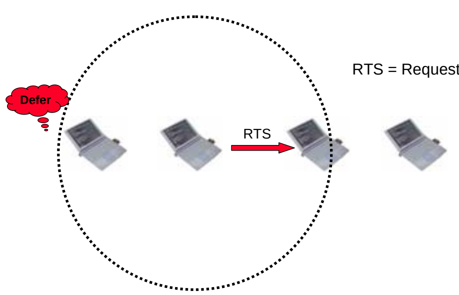
X OK to transmit

X not OK to transmit

1. Receiver transmits busy tone when receiving data
2. All nodes hearing busy tone keep silent
3. Requires a separate channel for busy tone

42

RTS/CTS Dialog (1)



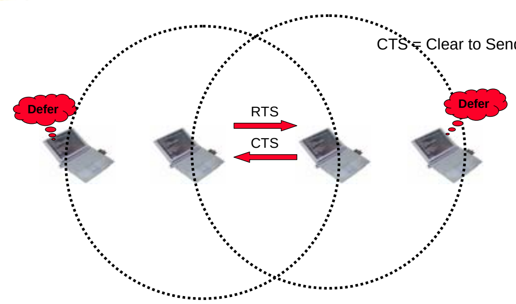
RTS = Request to Send

Any node that hears this RTS will defer medium access.

43

RTS/CTS Dialog (2)

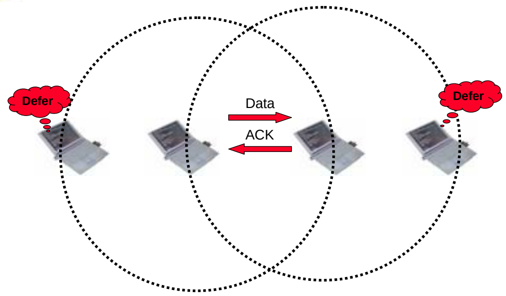
CTS = Clear to Send



Any node that hears this CTS will defer medium access.

44

RTS/CTS Dialog (3)



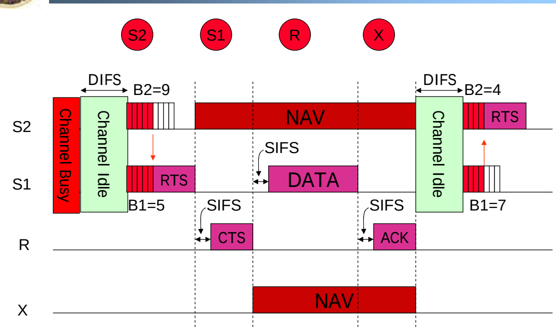
Virtual carrier sense using Network Allocation Vector (NAV)

- NAV is updated based on overheard RTS/CTS packets, each of which specified duration of a pending Data/Ack transmission

Dynamic Contention Window

- Binary Exponential Backoff in 802.11 DCF
  - When a node fails to receive CTS in response to its RTS, it increases the contention window
    - *cw* is doubled (up to an upper bound)
  - When a node successfully completes a data transfer, it restores *cw* to *Cwmin*

802.11 CSMA/CA



cw = 15

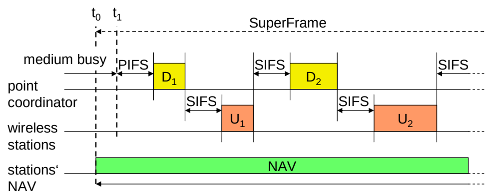
DIFS: DCF Inter-Frame Space

SIFS: Short Inter-Frame Space

802.11 Point Coordination Function (PCF)

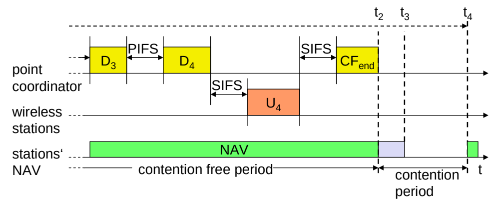
- PCF is implemented on top of DCF
- The time sensitive traffic are controlled by the PCF and the remaining traffic contend for access using CSMA/CA
- The centralized polling master (point coordinator) issues polls using PIFS
- The poll responses use SIFS
- The point coordinator could issue polls in a round robin fashion
- Seizing of the medium by the PCF is avoided by using superframes where the point coordinator is allowed to poll for a fixed duration and then idle for the rest of the superframe period to allow the asynchronous traffic to contend for the medium.

802.11 PCF Example (1)



49

802.11 PCF (2)



50