EEC173B/ECS152C, Spring 2009

IEEE 802.11 (Cont'd)

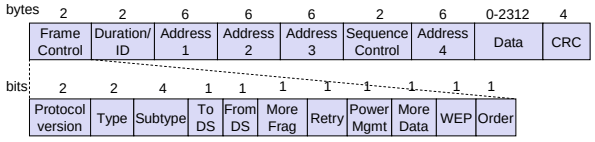
- 802.11 Frame format
- 802.11 MAC management
  - Synchronization, Handoffs, Power
- Advanced Topics
  - Security
  - QoS
  - Throughput

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

802.11 - Frame format

- Frame Types
  - Data: unicast (ACKed); broadcast/multicast (not ACKed)
  - Control: RTS/CTS, ACKs
  - Management (beacon, probe request/response, authentication, association, etc)
- Sequence numbers
  - Important against duplicated frames due to lost ACKs
- Addresses
  - Receiver, transmitter (physical), BSS identifier, sender (logical)
- Miscellaneous
  - Sending time, checksum, frame control, data

802.11 - Frame format



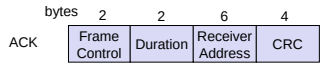
MAC Address Format

scenario	to DS	from DS	address 1	address 2	address 3	address 4
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure network, from AP	0	1	DA	BSSID	SA	-
infrastructure network, to AP	1	0	BSSID	SA	DA	-
infrastructure network, within DS	1	1	RA	TA	DA	SA

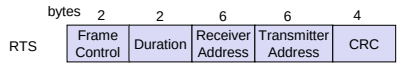
DS: Distribution System
AP: Access Point
DA: Destination Address
SA: Source Address
BSSID: Basic Service Set Identifier
RA: Receiver Address
TA: Transmitter Address

Special Frames: ACK, RTS, CTS

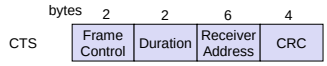
- Acknowledgement



- Request To Send



- Clear To Send



5

EEC173B/ECS152C, Spring 2009

Wireless LANs
- Evolution of Technology & Standards
- IEEE 802.11
  - Design Choices
  - Architecture & Protocols
  - PHY layer
  - MAC layer design
  - 802.11 Frame format
  - 802.11 MAC management
    - Synchronization, Handoffs, Power

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

802.11 - MAC Management Sublayer

- Registration/Synchronization
  - Try to find a LAN, try to stay within a LAN
  - Timer, etc.
- Handoff: Association/Reassociation
  - Integration into a LAN
  - Roaming, i.e. change networks by changing access points
  - Scanning, i.e. active search for a network
- Power management
  - Sleep-mode without missing a message
  - Periodic sleep, frame buffering, traffic measurements
- Security
- MIB - Management Information Base
  - Managing, read, write

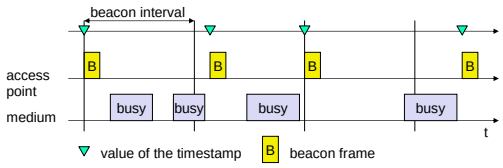
7

Registration

- A management frame called beacon is transmitted periodically by the AP to establish the timing synchronization function (TSF)
- TSF contains: BSS id, timestamp, traffic indication map (TIM), power management, and roaming information
- RSS measurements are done on the beacon message
- Association: process by which an MS registers with an AP

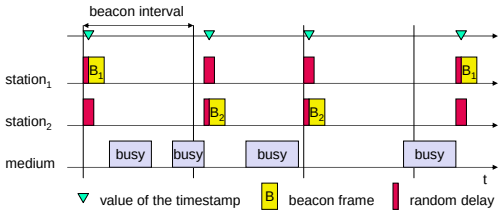
8

Synchronization using a Beacon (infrastructure)



9

Synchronization using a Beacon (ad-hoc)



10

Handoff

- Mobility Types:
  - No transition – MS is static or moving within a BSA
  - BSS transition – MS moves from one BSS to another within the same ESS (extended service set)
  - ESS transition – MS moves from one BSS to another BSS which belong to a different ESS (not supported)
- BSSs in an ESS communicate via Distribution System
- Reassociation service is used when an MS moves from one BSS to another within the same ESS

11

802.11 - Roaming

- No or bad connection? Then perform:
- Scanning
  - Scan the environment, i.e., listen into the medium for beacon signals or send probes into the medium and wait for an answer
- Reassociation Request
  - Station sends a request to one or several AP(s)
- Reassociation Response
  - Success: AP has answered, station can now participate
  - Failure: continue scanning
- AP accepts Reassociation Request
  - Signal the new station to the distribution system
  - The distribution system updates its data base (i.e., location information)
  - Typically, the distribution system now informs the old AP so it can release resources

12

Management Operations: Scanning

- Passive scanning
  - Listen to BS beacons
- Active scanning
  - MS sends probe request
  - BS responds to probe

13

Power Management (1)

- How to power-off during idle periods?
- Idea: switch the transceiver off if not needed
- States of a station: sleep and awake
- IEEE 802.11 buffers data at the AP, and sends the data when the MS is awakened
- Timing Synchronization Function (TSF)
  - Using TSF, all MSs are synchronized – they wake up at the same time to listen to beacon
- With every beacon a Traffic Indication Map (TIM) is sent that has a list of stations having buffered data
- An MS learns that it has buffered data by checking beacon and TIM

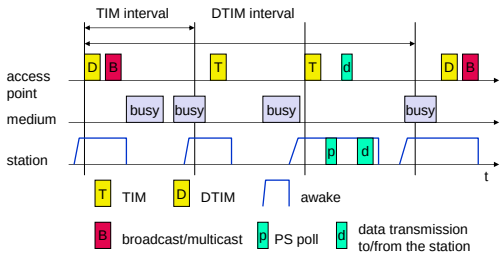
14

Power Management (2)

- Infrastructure
  - Traffic Indication Map (TIM)
    - List of unicast receivers transmitted by AP
  - Delivery Traffic Indication Map (DTIM)
    - List of broadcast/multicast receivers transmitted by AP
- Ad-hoc
  - Ad-hoc Traffic Indication Map (ATIM)
    - Announcement of receivers by stations buffering frames
    - More complicated - no central AP
    - Collision of ATIMs possible (scalability?)

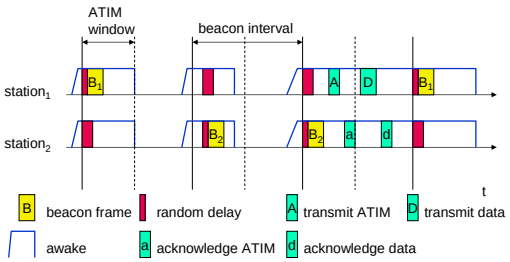
15

Power saving with wake-up patterns (infrastructure)



16

Power saving with wake-up patterns (ad-hoc)



17

Wifi - IEEE 802.11b (1)

- Data rate
  - 1, 2, 5.5, 11 Mbit/s, depending on SNR
  - User data rate max. approx. 6 Mbit/s
- Transmission range
  - 300m outdoor, 30m indoor
  - Max. data rate ~10m indoor
- Frequency
  - Free 2.4 GHz ISM-band
- Security
  - Limited, WEP insecure, SSID
- Cost
  - $20-$100 base station, dropping
- Availability
  - Many products, many vendors

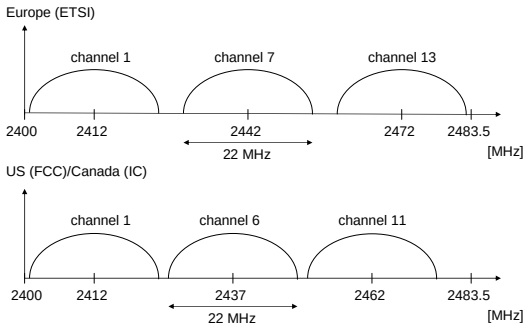
18

Wifi - IEEE 802.11b (2)

- Connection set-up time
  - Connectionless/always on
  - Typ. Best effort, no guarantees (unless polling is used, limited support in products)
- Quality of Service
- Manageability
  - Limited (no automated key distribution, sym. Encryption)
- Special Advantages
  - Many installed systems, lot of experience, available worldwide, free ISM-band, many vendors, integrated in laptops, simple system
- Disadvantages
  - Heavy interference on ISM-band, no service guarantees, slow relative speed only

19

Channel Selection (Non-overlapping)



20

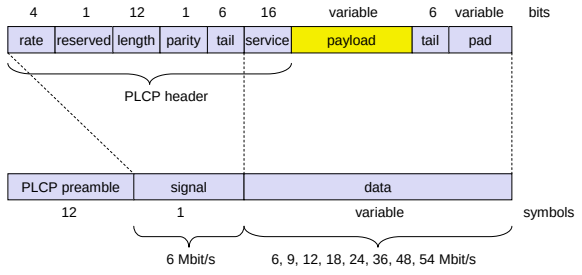
IEEE 802.11a (1)

- Data rate
  - 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s, depending on SNR
  - User throughput (1500 byte packets): 5.3 (6), 18 (24), 24 (36), 32 (54)
  - 6, 12, 24 Mbit/s mandatory
- Transmission range
  - 100m outdoor, 10m indoor
    - E.g., 54 Mbit/s up to 5 m, 48 up to 12 m, 36 up to 25 m, 24 up to 30m, 18 up to 40 m, 12 up to 60 m
- Frequency
  - Free 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz ISM-band
- Security
  - Limited, WEP insecure, SSID
- Cost
  - $100
- Availability
  - Some products, some vendors

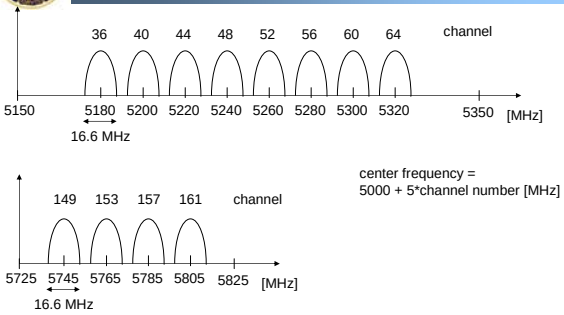
IEEE 802.11a (2)

- Connection set-up time
  - Connectionless/always on
- Quality of Service
  - Typ. best effort, no guarantees (same as all 802.11 products)
- Manageability
  - Limited (no automated key distribution, sym. Encryption)
- Special Advantages/Disadvantages
  - Advantage: fits into 802.x standards, free ISM-band, available, simple system, uses less crowded 5 GHz band
  - Disadvantage: stronger shading due to higher frequency, no QoS

IEEE 802.11a – PHY frame format

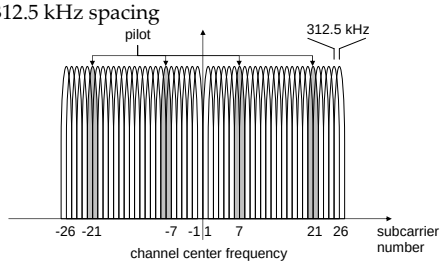


Operating channels for 802.11a / US U-NII



OFDM in IEEE 802.11a

- Orthogonal FDM with 52 used subcarriers (64 in total)
- 48 data + 4 pilot
- (plus 12 virtual subcarriers)
- 312.5 kHz spacing



Concluding Remarks

- IEEE 802.11 WLAN is becoming real popular these days
- There is still a big room to improve the current 802.11 systems
- Important to consider how any improved system co-exists with legacy systems

Characteristics of Wireless LANs

- Advantages
  - Very flexible within the reception area
  - Ad-hoc networks without previous planning possible
  - (Almost) no wiring difficulties (e.g. historic buildings, firewalls)
  - More robust against disasters like, e.g., earthquakes, fire - or users pulling a plug...

Characteristics of Wireless LANs

- Disadvantages
  - Typically very low bandwidth compared to wired networks (1-10 Mbit/s)
  - Many proprietary solutions, especially for higher bit-rates, standards take their time (e.g. IEEE 802.11)
  - Products have to follow many national restrictions if working wireless, it takes a vary long time to establish global solutions like, e.g., IMT-2000

Advanced Topics

IEEE 802.11 Future Development

- Security
- QoS
- Throughput

IEEE 802.11 – Ongoing/Future Developments

- 802.11d: Regulatory Domain Update
- 802.11e: MAC Enhancements – QoS
  - Enhance the current 802.11 MAC to expand support for applications with Quality of Service requirements, and in the capabilities and efficiency of the protocol.
- 802.11f: Inter-Access Point Protocol
  - For data exchange via the distribution system.
- 802.11g: Data Rates > 20 Mbit/s at 2.4 GHz; 54 Mbit/s, OFDM
- 802.11h: Spectrum Managed 802.11a (DCS, TPC)
- 802.11i: Enhanced Security Mechanisms
  - Stronger encryption/authentication than WEP
- Study Groups
  - 5 GHz (harmonization ETSI/IEEE)
  - Radio Resource Measurements
  - High Throughput

30

Security in Wireless Networks

- Wireless networks are inherently insecure compared to their wired counterparts
- The broadcast nature of the channel makes it easier to be tapped
- The widely varying features and capabilities of wireless communication devices introduces several security concerns

31

Security Requirements

- In addition to the voice or data, a variety of control information (call set-up information, user id, user location, etc.) that are carried over the air should be secured
- Calling patterns should be hidden
- It is desirable to have at the least wireline equivalent privacy for all voice conversations
- Secret key algorithms with key sizes larger than 80 bits are appropriate for maintaining privacy in wireless networks
- Need for identifying and authenticating wireless devices

32

Security Services

- Confidentiality or privacy
  - Provides resistance to the security attack known as interception
- Message Authentication & Integrity
  - Provides integrity of the message and authenticates sender; guards against message modification and impersonation
- Non-repudiation
  - Guards against denial by either party of creating or acknowledging a message
- Access control
  - Authorizes access; avoids masquerading
- Availability
  - Avoids denial of service attacks

33

Security Mechanisms

- Encryption can provide
  - Confidentiality
  - Message authentication
  - Nonrepudiation
  - Access control
  - Identification
- Availability cannot be guaranteed by encryption as it is powerless against signal jams, DoS, and faults
- Requirement: Maintain processing to "reasonable" levels

34

802.11 Wired Equivalent Privacy (WEP)

- WEP uses 40 bit RC4 secret key and 24 bit initialization vector (IV)
- Crucial aspect is how to create keystream using Pseudorandom Number Generator
  - Use IV and secret key to generate a pseudorandom key stream. The data is then simply XORed with the key stream to create the ciphertext
  - Receiver XOR ciphertext with keystream to recover data
- Initialization vector is sent in clear text
- Framebody and Integrity Check Value (ICV) are encrypted

35

WEP Flaws

- Need secret key distribution
- Cipher stream creation needs to be based on true random generator
- ICV collisions allows attacker to decipher
- A weak class of keys and known first byte of payload

36

QoS Issues

- Current 802.11: Lack of QoS support
  - Best-effort service with contention-based MAC
- PCF falls short of guaranteeing desired QoS due to
  - Beacon frame delays beyond target Beacon transition time (TBTT)
  - Unpredictable demand from the polled station
- Low throughput due to large overhead
  - < 5 Mbps throughput at 11 Mbps 802.11b link
- 802.11e proposes an enhanced MAC protocol

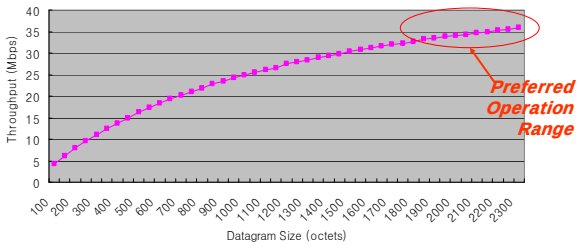
37

IEEE 802.11n Initiative

- A new standardization effort to achieve over 100 Mbps throughput over WLAN
  - Via both PHY and MAC enhancement
- Frame Size Affects Throughput
  - 802.11 MAC/PHY have big fixed overheads
    - MAC header, IFSs, ACK, and Backoff
    - PLCP preamble & header

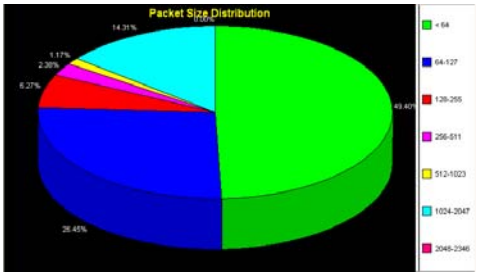
38

Theoretical Throughput for 54 Mbps



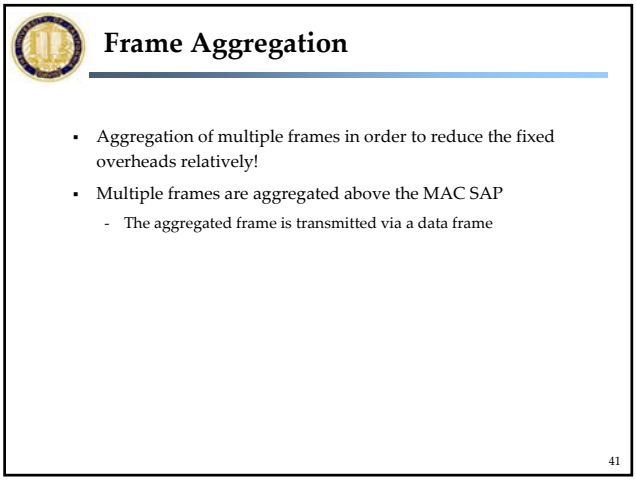
39

Packet Size Statistics



This statistics is from the measurement taken in the 802.11 standard meeting room in the morning of July 22nd 2003

40


Frame Aggregation
▪ Aggregation of multiple frames in order to reduce the fixed overheads relatively!
▪ Multiple frames are aggregated above the MAC SAP
- The aggregated frame is transmitted via a data frame
41