



EEEC173B/ECS152C, Winter 2006

Wireless LANs

- ◆ 802.11 Frame format
- ◆ 802.11 MAC management
 - Synchronization, Handoffs, Power

Acknowledgment: Selected slides from Prof. Schiller

Chuah Winter 2006



Key Points from Last Lecture

- MAC methods: DCF & PCF
- CSMA/CA with positive ACK
 - Exponential backoff
 - "Prioritized" access via different IFS values
- Hidden/exposed terminal problems
 - RTS/CTS clearing
 - Virtual sensing using received NAV

2



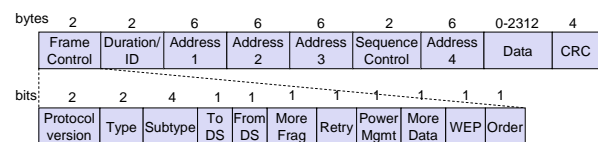
802.11 - Frame format

- 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

3



802.11 - Frame format



4



MAC Address Format

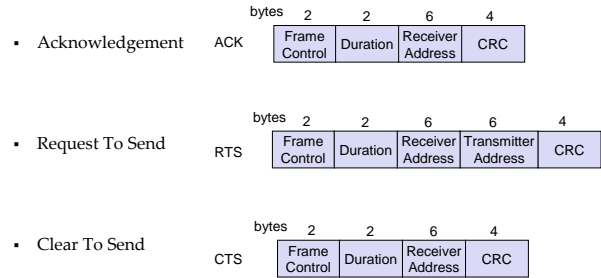
scenario	to DS	from DS	address 1	address 2	address 3	address 4
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure network, from AP	0	1	DA	BSSID	SA	-
infrastructure network, to AP	1	0	BSSID	SA	DA	-
infrastructure network, within DS	1	1	RA	TA	DA	SA

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

5



Special Frames: ACK, RTS, CTS



6



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

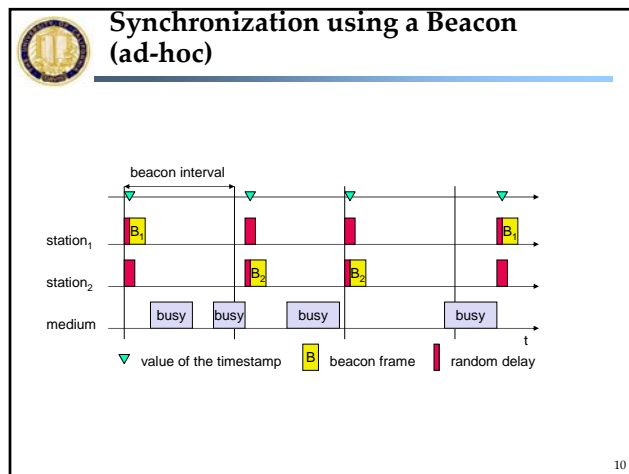
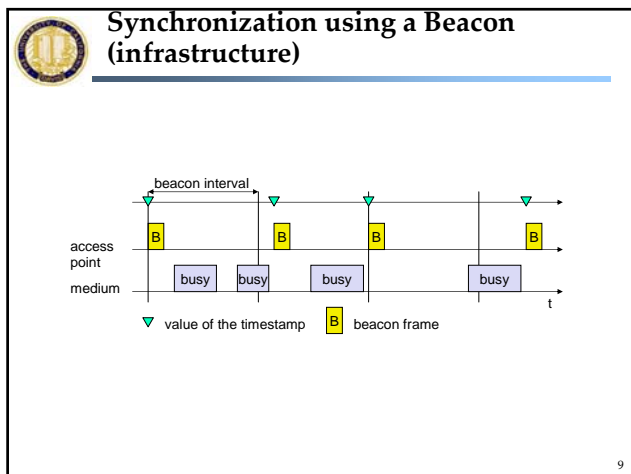
7



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



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



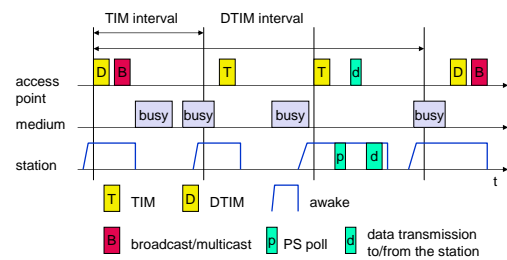
Power management (2)

- 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?)

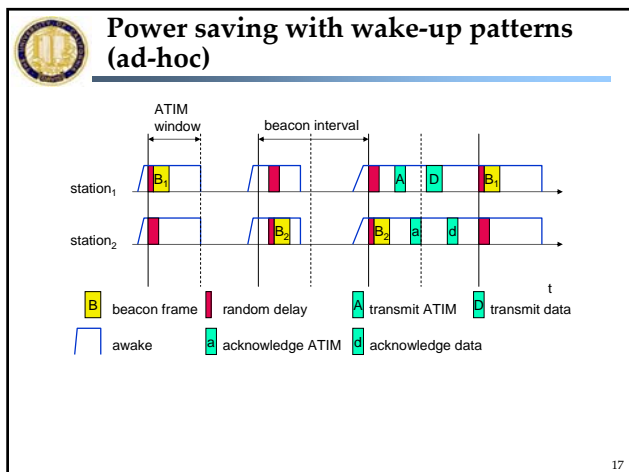
15



Power saving with wake-up patterns (infrastructure)

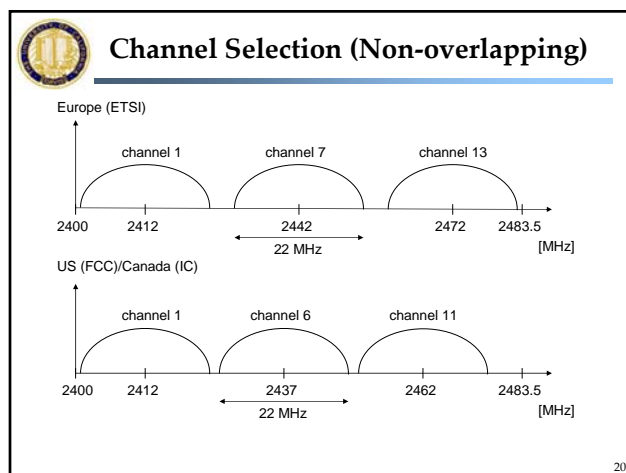


16



- ### 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





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

21



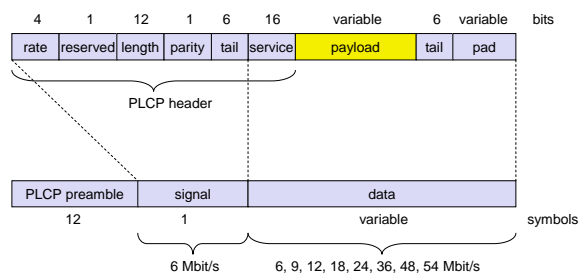
IEEE 802.11a (2)

- 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

22



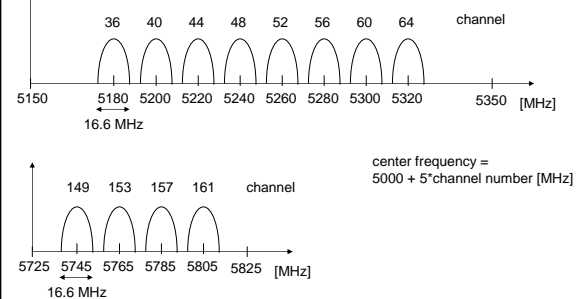
IEEE 802.11a – PHY frame format



23



Operating channels for 802.11a / US U-NII

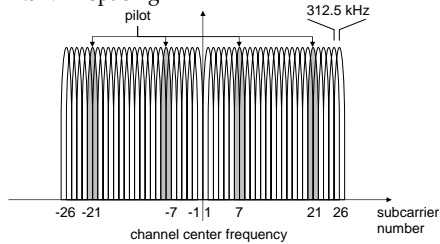


24



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



25



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

26



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...

27



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

28