802.11 In-Depth

COMP3049 – Intermediate Wireless Technology

Chapters 8 & 9 - CWNA

Objectives

- Describe and apply the concepts of:
  - Frames, packets and datagrams
  - Bits, bytes and octets
  - MAC and PHY
- Explain CSMA/CA
- Compare frame types and formats
- Identify and explain frames and frame exchange sequences in the IEEE 802.11 standard
  - Active and passive scanning
  - Dynamic rate switching

2

Do you know this already?

- Which 802.11 setting can improve performance when there is interference?
- What is the purpose of Distributed Coordination Function – DCF?
- What are some of the differences between collisions in 802.3 and 802.11?
- What is the mechanism used by 802.11 to handle collisions?

3

Frames, Packets and Datagrams

Network Layer (3)	Packets or Datagrams TCP vs. UDP
Data Link Layer (2)	Frames
Physical Layer	Bits and Bytes

4

Bits, Bytes and Octets

- Bit – *Bi*nary Digi*t*
- Bytes – Group of 8 bits generally used to represent data
- Octets – Group of 8 bits used to represent data or used individually
- Computers need data to have some kind of structure (i.e.: usually 8-bits per character represented in code, such as ASCII)

5

Bits, Bytes and Octets

- When stored in memory or disk, 1 *K*ilobytes = 1024 bytes
  - Because the address is binary
- When used in datacomm, 1 *k*ilobytes = 1000 bytes

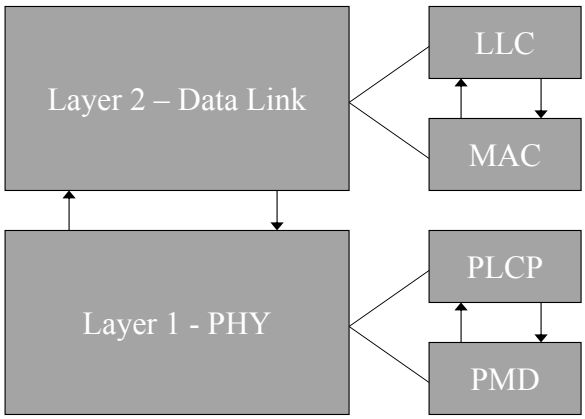
6

MAC and PHY

- MAC: acronym for *Medium Access Control*
  - Two sublayers in some technologies
    - LLC – Logical Link Control IEEE 802.2
    - MAC
  - Used in 802.11
- PHY: abbreviation of *Phy*sical layer
  - Two sublayers in 802.11 and other wireless technologies
    - PMD – Physical Medium Dependent
    - PLCP – Physical Layer Convergence Procedure

7

MAC and PHY Sublayers



8

MAC and PHY Sublayers

- MAC
  - MSDU – MAC Service Data Unit
    - Received by layer 2 via LLC or sent to layer 3
    - Headers added or removed dep. on direction
    - 2304 bytes or less (802.11 limit)
    - Expanded for encryption overhead
  - MPDU – MAC Protocol Data Unit
    - Complete MAC frame that is sent to layer 1
    - Also received from layer 1

9

MAC and PHY Sublayers

- PHY
  - PSDU – PCLP Service Data Unit
    - MPDU received from layer 2 or what is sent to layer 2
    - Preamble/header added/removed ⇔ PPDU
  - PPDU – PLCP Protocol Data Unit
    - What is actually transmitted on the medium or received from the medium

10

802.11 CSMA/CA

- CSMA/CD used in Ethernet
  - Collisions can be detected as overvoltage on the cable
- CSMA/CA used in 802.11 because transmitter cannot detect collisions
  - Collisions can happen anywhere in the Wireless Medium
  - Only failure to receive ACK is inferred as a collision

11

802.11 CSMA/CA

- Two kinds of Carrier Sense (CS)
  - CCA – Clear Channel Assessment or Physical Carrier Sense
    - "Listening" to the medium for the presence of RF energy (monitoring for a part. threshold)
  - Virtual Carrier Sensing
    - NAV – Network Allocation Vector
    - Amount of time required for frame transmission by another station to end
- Both must show that the medium is available
- Phantom frame sensing

12

IFS – Inter-Frame Spacing

- Time intervals in which frames cannot be transmitted
- Ensures that frames do not overlap each other
- Used to proritize the transmission of certain key types of frames
  - RTS/CTS, etc.
  - Not at all related to QoS

13

IFS Types

- SIFS – Short interframe spacing
  - ACK frames for data
  - CTS frames sent as a response to RTS
  - Data that immediately follows CTS
  - All frame exchanges made in PCF mode
  - All fragment frames that are part of a fragment burst

14

SIFS Interval

- Defined as:
  - "The time interval from the end of the last symbol of the previous frame to the beginning of the first symbol of the preamble of the subsequent frame as seen in the medium"

FHSS	28 μs
DSSS	10 μs
OFDM	16 μs
HR/DSSS	10 μs
ERP	10 μs

15

IFS Types

- PIFS – (PCF) Point (Coordination Function) Interframe Spacing
  - PCF has not been widely implemented
- DIFS – (DCF) Distributed (Coordination Function) Interframe Spacing
  - One of the two longest IFS = SIFS + 2x slot time
  - DSSS PHY = 50 μs; OFDM = 34 μs
  - Period of time when no stations are allowed to transmit except when *bursting*

16

IFS Types

- EIFS – Extended Interframe Spacing
  - Used in case of reception error (incomplete or corrupted frame is received), before next frame is transmitted
  - Equal to: SIFS + (8x ACKsize) + Preamble Length + PLCP Header Length +DIFS

17

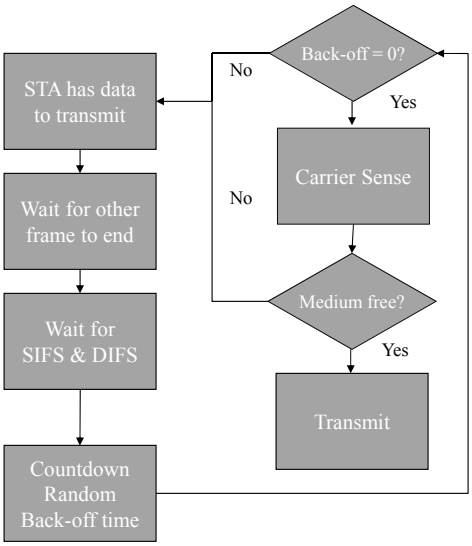
Contention Window

- After IFSs stations must still wait before transmitting
- STAs initiate a random back-off algorithm and then contend for the WM
- Random Back-off time = random no. of slot times

Slot Times	
FHSS	50 µs
DSSS	20 µs
OFDM	9 µs
HR/DSSS	20 µs
ERP Long	20 µs
ERP Short (802.11b compatible)	9 µs

18

Contention Window



19

Contention Window

- Used only with DSSS and in DCF mode
- It may appear some stations will get very few chances to transmit
- However, the back-off time is random for each transmission.
- STAs count down back-off time while others are transmitting
- Collisions may still occur; ACK or its absence is used to detect them

20

Frame Types and Formats Compared

- IEEE Project 802 frames have similar structures
- Similarity makes for easier conversion from 802.3 to 802.11
- APs convert 802.3 frames to 802.11 and vice-versa
- Because APs are used in TCP/IP Ethernet networks, majority of 802.11 frames will be 1500 bytes

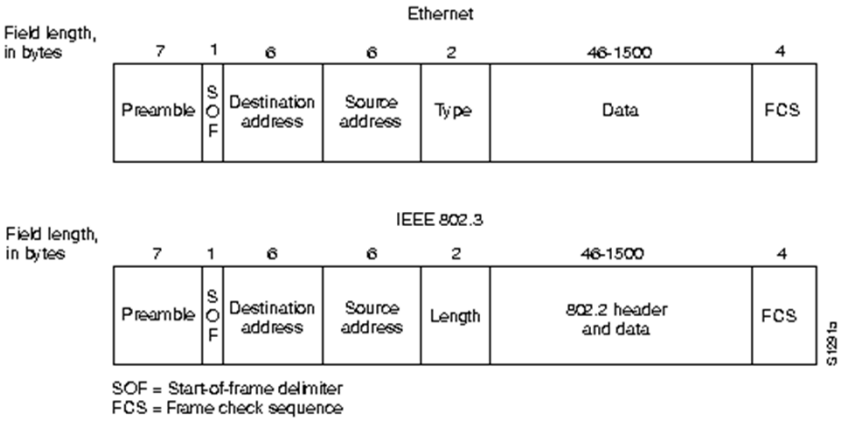
21

Problem #1

- You need to extend your network beyond 100 m
- You decide to use a 802.11 repeater (AP)
- Frames are sent back and forth, but how do they get to their destinations?
- What are the potential problems, if any?
- See 802.3 frame…

22

Ethernet & IEEE 802.3 Frames



23

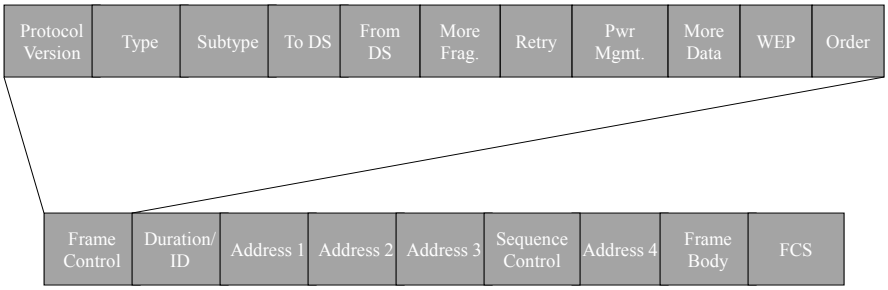
Frame Types and Formats Compared

- 802.11 frames have up to 4 MAC addresses
- These fields can contain four of the following five types:
  - BSSID
  - Destination (DA)
  - Source (SA)
  - Receiver (RA)
  - Transmitter (TA)
- Which addresses are included depends on the frame subtype

24

General 802.11 Frame and FC Field

Frame Control Field



802.11 General Frame Format

Note: Most *details* of 802.11 frame format are not part of exams

25

802.11 Frame Types and Formats

- Management Frames
  - Used to manage access and to move associations from one AP to another with an ESS
- Control Frames
  - Used to assist with the delivery of data frames
  - Must be transmitted using a modulation that can be understood by all STAs in a BSS

26

IEEE 802.11 Frame Types & Formats

- Data Frames
  - Carry application-level data
  - Can be standard data frames or QoS frames as per IEEE 802.11e
- Jumbo frame support (layer 2)
  - Can be up to 9000 bytes
  - Must be supported by the wired infrastructure components

27

IEEE 802.11 Frame Types & Formats

- Jumbo frame support (cont'd.)
  - With LW APs you may have a *split MAC architecture*
  - Part of the MAC services handled by the AP and part by the controller (usually a smart switch)
  - Many wireless controllers support jumbo frames
  - For the most part only GB capable devices support jumbo frames
  - Some Cisco devices support a protocol that allows the controller to detect whether the infrastructure supports jumbo frames

28

MTU Discovery and Functionality

- Layer 3 defines the MTU
- 802.11 MAC frames can be up to 2304 octets
- Layer 4 TCP supports MSS – Maximum Segment Size
- Actual datagram/frame sizes can always be smaller

29

802.11 Frames and Exchanges

- CWNA does not require you to know frame details
- But requires you to understand:
  - The frame exchange sequences
  - The flow of creating a WLAN
  - How to disconnect from a WLAN
  - How to find WLANs
  - Dynamic Rate Switching

30

MAC Functions

- Scanning
  - STAs must be able to find APs
- Synchronization
  - STAs update their clocks based on beacon frames
- Frame Transmission
  - STAs must abide by the frame transmission rules of the BSS (i.e.: DCF, etc)

31

MAC Functions

- Authentication
  - Must be performed before a STA can be associated with the BSS
- Association
  - Discovery of capabilities of BSS in both directions – STA ⇔ AP
- Reassociation
  - In an ESS STAs can move from one AP to another

32

MAC Functions

- Data Protection
  - Data encryption may be (should be) employed to prevent intrusion
- Power Management
  - Since 802.11 wireless devices consume a significant amount of power, STAs can *sleep* for specified periods of time

33

MAC Functions

- Fragmentation
  - In case of intermittent interference, fragmentation may lead to better reception
- Request-to-Send (RTS)/Clear-to-Send (CTS)
  - A feature that helps prevent hidden node problem
  - Allows for more centralized control of the WM

34

Beacon Management Frame

Information	Description
Time Stamp	Used for synchronization
Beacon Interval	Used to specify the amount of time between beacon transmissions
Capability information	WEP requirements, PCF support, ESS or IBSS, and others
SSID	The ID or name of the network
FH parameter set	Used in FH PHYs; includes hop pattern, dwell time, and others

35

Beacon Management Frame

Information	Description
DS parameter set	Used by DS systems. Provides channel info.
CF parameter set	Only present in PCF. Provides PCF management info.
IBSS	Only present in IBSS (ad hoc networks). Contains ATIM Window for power save operations
TIM	Only present in beacons from APs. Used by STAs employing Pwr Save

36

Beacon Management Frame

Information	Description
Supported rates	Specifies up to eight data rates
Extended supported rates	Specifies any other data rates not included in above field
ERP information	Contains information that allows Clause 19 ERP PHY devices to coexist with Clause 15 DSSS PHY or Clause 18 HR/DSSS devices

37

Active Scanning (Probes)

- Clients uses probe request and probe response frames to find a WLAN
- Two methods:
  - STAs use the SSID. All APs with the same SSID in range respond
  - STAs can use wildcard SSID of "ANY" (null value)
- Intruders can just wait for a beacon frame, which contains the SSID or wait for a data frame
- Standard dictates that APs must respond to probe requests

38

Active Scanning (Probes)

- Basic process:
  1. Switch to a channel
  2. Wait for an incoming frame or for ProbeDelay timer to expire
  3. Wait for MinChannelTime to pass
     a. If WM was never busy, there is no WLAN on this channel. Move to next channel
     b. If WM was busy, wait for MaxChannelTime to expire, then process any probe response frames

39

Passive Scanning (Beacons)

- Instead of transmitting, the STAs listen for the beacons
- STAs determine the AP with best signal (RSSI)…
- Then attempt to authenticate and associate

40

Authentication and Association

- STAs must go through the Auth. and Assoc. process
- These are the second and third stages of connectivity with a WLAN
- The 802.11 State Machine
  - Unauthenticated/Unassociated
  - Authenticated/Unassociated
  - Authenticated/Associated

41

Authentication and Association

- Unauthenticated/Unassociated
  - STAs are completely disconnected from the WLAN
  - Cannot pass frames to the wired network
  - Auth. frames can be sent to the APs
  - These frames do not pass through the AP, except in a split-MAC implementation (wireless switch/controller)

42

Authentication and Association

- APs and WLAN controllers keep a list
  - Association table
  - Vendors may report status of clients differently
- Authenticated/Unassociated
  - STAs must first authenticate with the APs
  - Then send association frames
  - APs validate STAs; STAs do not validate APs

43

Authentication and Association

- Authenticated/Associated
  - Association process requires four frames
    - Association request (STA to AP)
    - ACK (AP to STA)
    - Association Response (AP to STA)
    - ACK (STA to AP)
  - Client may finally communicate between wireless/wired LAN
  - Association status codes, in Association response frames control the process

44

Authentication and Association

- Association Status Codes
  - 0 = successful association
  - 12 = association rejected for unknown reason
  - 17 = AP already servicing max. no. of STAs
  - 18 = client does not support all of the basic rates required to join BSS

45

Authentication and Association

- Open Authentication
  - No true verification of identity occurs
  - Default authentication in Clause 8 of IEEE 802.11
  - APs always respond with a positive to all authentication requests
  - WEP can be used for authentication and privacy but has weak security

46

Authentication and Association

- Open authentication (cont'd.)
  - Preferred in hotspots
  - Used with 802.1X/802.11i
- Shared Key Authentication
  - Uses Wired Equivalent Privacy (WEP)
  - STA and AP must use same key

47

Authentication and Association

1. STA xmits authentication frame indicating that Shared Key Authentication should be used
2. AP receives auth. frame and transmits ACL to STA
3. AP generates challenge text and xmits to STA
4. STA receives and ACKs challenge frame

48

Authentication and Association

5. STA encrypts challenge text with WEP key and transmits to AP in challenge response frame
6. AP receives challenge response and ACKs it to the client
7. AP decrypts text and compares with original. If it matches, sends positive authentication response to STA
8. STA receives auth. response and sends ACK to AP

49

Authentication and Association

- Deauthentication
  - Advisory frame; includes address of STA and address of device with which STA is newly authenticated, if applicable
  - STA is leaving BSS or ESS
  - This effectively disassociates STA with AP
- Reassociation
  - When STA is roaming between APs in an ESS

50

Authentication and Association

- Disassociation
  - Advisory frame
  - AP cannot deny
  - Component of the MAC layer
  - See table 4.9 in course book
  - Service may be contained in the DS or in a WLAN controller

51

Regulatory Domain Requirements

- Amendments d, h, and j define a country element
- Code must be present in a beacon frame
- May indicate if AP supports multiple regulatory domains
- Defines which country an AP is operating
  - Related to which frequencies are supported

52

Data Flow Optimization

- DCF – Distributed Coordination Function
  - WM access method described previously as CSMA/CA
- PCF – Point Coordination Function
  - Included in 802.11 but not widely implemented in commercial systems
  - Centralizes access to the WM
  - APs use both DCF and PCF (when PCF implemented)
    - Alternate between contention and contention-free periods
- HCF
  - Combines features of both channel access methods above
  - Part of 802.11e (see EDCA later)

53

Data Flow Optimization

- PCF cycle
  1. AP waits for duration of PIFS
  2. AP sends beacon frame announcing CFP is about to begin
  3. CFP window begins and AP polls each STA that is participating in CFP
  4. CP window begins and STAs contend for access using DCF

54

IEEE 802.11 and WMM

- Many networking technologies require very low latency
- Works by identifying higher-priority data and making sure it gets preferential access
- PCF was a contender
- Now APs will use 802.11e
  - EDCA and HCF

55

EDCA and HCF

- Two new device types:
  - QoS APs and QoS STAs
- EDCA
  - Enhancement to DCF (Enhanced Distributed Channel Access)
  - Defines 8 traffic categories (priority levels); User Priority level
  - Higher priority traffic gains access to the WM sooner
  - Does not ensure that higher priority frame will be xmitted sooner, just increases probability
  - Uses tags identical to 802.1D (MAC level)

56

EDCA and HCF

- HCF
  - Provides preemptive capability to QoS AP (QAP)
  - AP can preempt STAs for next transmission
  - AP as centralized coordinator (*hybrid coordinator)*
- WMM
  - Wi-Fi Alliance extension
  - Based on draft 802.11e
  - Will continue to be updated and redefined for QoS and VoWLAN

57

Block Acknowledgement

- 802.11e
- Now incorporated into 802.11-2007
- Improves channel efficiency by aggregating ACKs
- Used with QoS
- Other uses defined in 802.11n

RTS/CTS & CTS-to-self

- Different from DCF and PCF
- STAs tell AP they need to communicate
  - Then wait for AP to send CTS
    1. STA sends RTS frame to AP
    2. AP sends CTS frame to STA
    3. Nearby STAs *hear* the CTS and know to stay silent
    4. Requesting STA xmits frame and hears ACK during *quiet* time
  - Other STAs set NAV timers to cooperate

59

RTS/CTS & CTS-to-self

- CTS-to-self applies to 802.11g
- STAs using ERP PHY can communicate using OFDM and faster data rates than HR/DSSS PHY
- STAs using ERP transmit CTS without a prior RTS, using modulation understood by slower STAs
- Slower STAs will go silent, honouring the duration value in the CTS frame

60

Fragmentation

- When 1500-byte frames are too large, WLAN devices can fragment frames
- Configure *fragmentatio threshold* setting
- Determines when MAC layer will break-up frames into smaller elements
- Increases overhead but also increases resilience agains interference
- WLAN administrator may have to modify this setting for optimum performance

61

Dynamic Rate Switching

- Process of reducing or increasing data rate as quality of the RF signal changes
- Signals at slower data rates are easier to demodulate
- Devices only switch between data rates supported in each mode
  - i.e.: 11 to 5.5 to 2 to 1 Mbps in 802.11b
  - 54 to 48 Mbps, etc. in 802.11g or 802.11a

62