# WLAN Analysis with Wireshark & AirPcap

Wednesday – June 15th, 2010

**Keith R. Parsons**

Managing Director | Wireless LAN Professionals.com

**SHARK**FEST **'10**
Stanford University
June 14-17, 2010

# Wireless LAN Analysis

A Little Review of Wireless LANs

Hands On Exercises

# WLAN Review

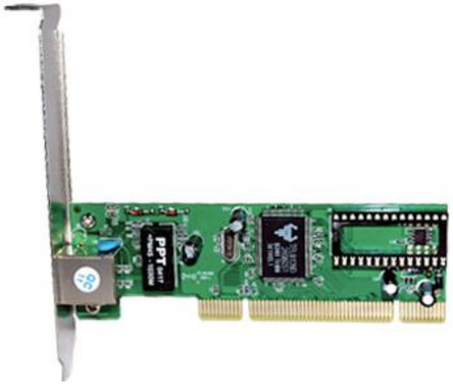
- How WLAN NICs work
- Three Types of Wireless LAN Frames
  - Management/Control/Data
    - Only Data Crosses Wired/Wireless Boundary
- Know what to look for
- Associating & DS Bits

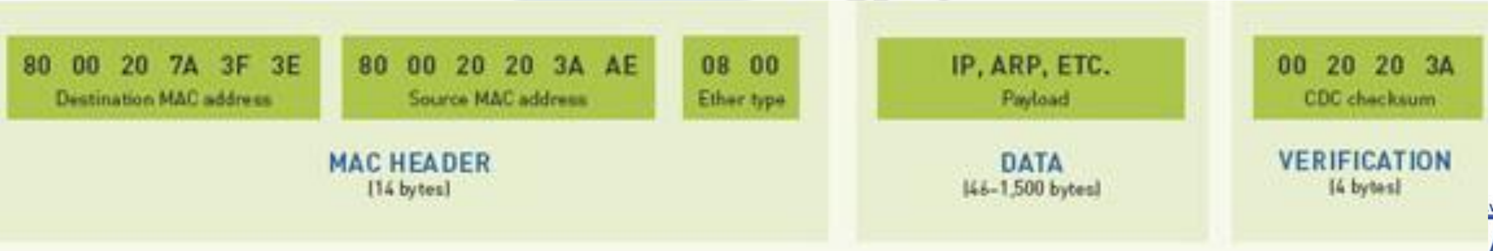
# Wired .vs Wireless NICs

- Copper .vs Radio Frequencies
- How they process bits
- Where Radio Tap Header Comes From

# How a Wired NIC Works

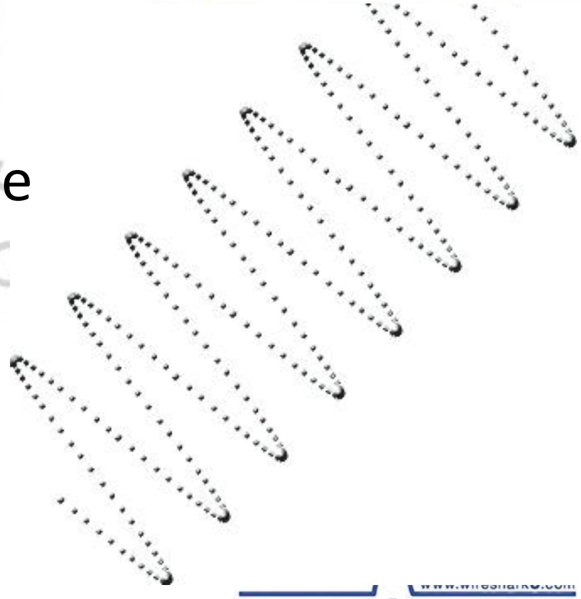
- Converts electrical energy via modulation scheme to Bits
- Preamble, Header, Frame Body, FCS
- Check Destination MAC Address
- Check for CRC Error
- Forward to OS Protocol Stack





# How a WLAN NIC Works

- Antenna – blocks all RF but 2.4GHz
- Modulation Filter – blocks all but 802.11
- Preamble, Header Frame Body, FCS
- Adds new information
  - Time Stamp, Channel Stamp, RSSI, Noise
- Check Destination MAC Address
- Check for CRC Error
- Forward on to OS Protocol Stack



# How AirPcap Adapter Works

- Same as WLAN…
- Changes slightly with driver ‘shim’
- Promiscuous Mode (RF Monitor)
- Keeps CRC errors for Stats
- Sends data to Wireshark
  - “Data Ball”
- Slices & Dices Data
- All Data in Wireshark comes from Packets

# Management Frames

- Small
- Go at low data rate
- Travel long ways
- Always on
- Idle networks
- Have to do with getting on/off wireless network

# Control Frames

- Tiny
- Got at low data rate
- Travel a long ways
- Like to go with Data Frames
- Check Ratios of Control to Data
- Data—ACK, RTS-CTS-Data-ACK, CTS-Data-ACK, Data—Data—ACK, Retries

# Data Frames

- Carry Payload
- Large size very efficient
- Want them to go fast as possible
- Don't travel as far
- Watch Ratios with Control Frames
- Retries, and CRC errors (where you see)

# Know What You’re Looking For

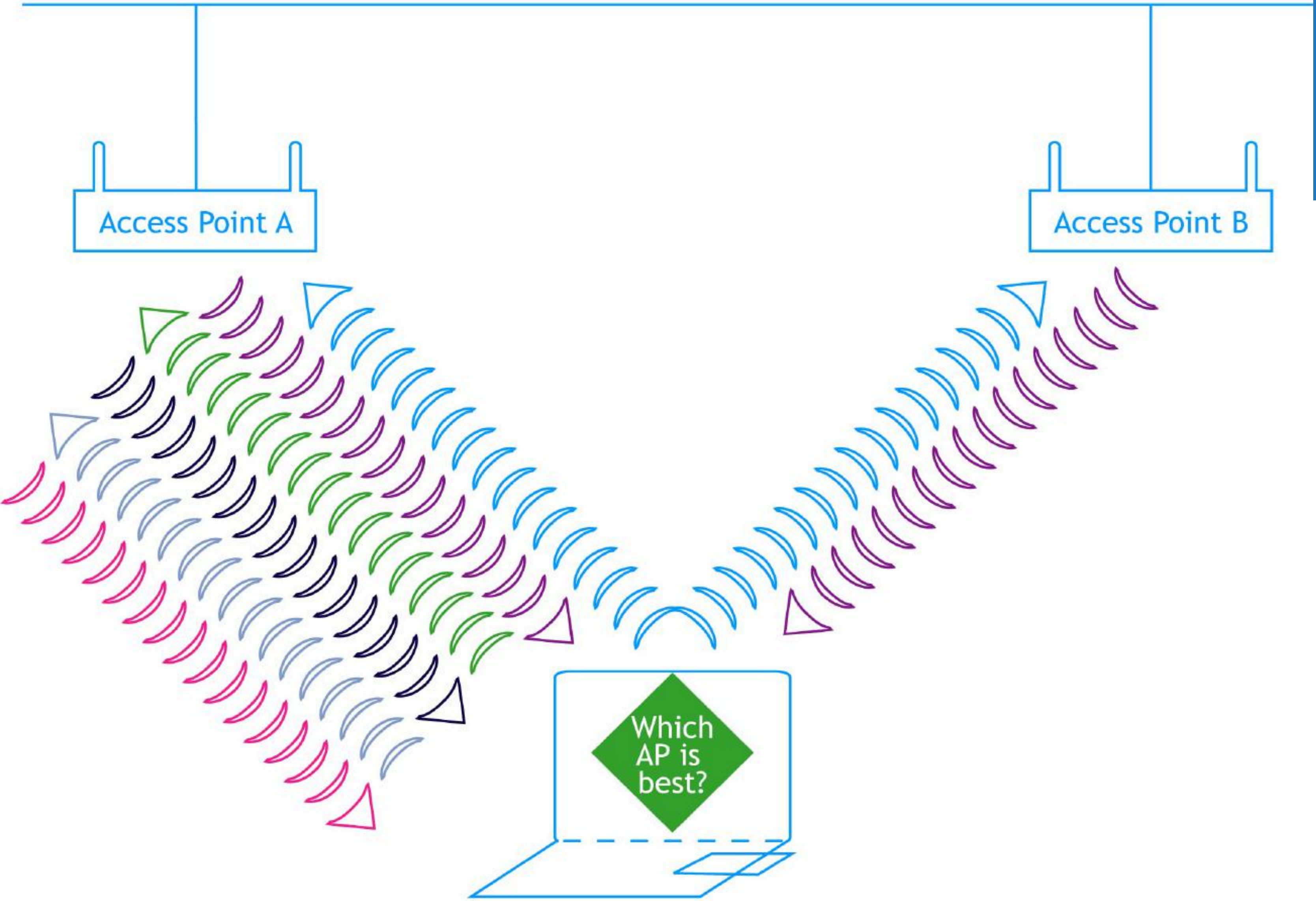
| | Management | Control | Data |
|---|---|---|---|
| Size | Small | Tiny | Huge |
| Data Rate | 1Mb | 1Mb | 54Mb |
| Distance | Far | Far | Near |
| Purpose | On/Off WLAN | Help Data | Carry Payload |
| Bridge to Wired? | No | No | Yes |
| Types | Beacon, Probes, Authenticate, Associate, DeAuth, Etc. | RTS, CTS, ACK | Data, Null Data |

# Know What To Expect

| Type | Management | Control | Data |
|---|---|---|---|
| Idle Network | Lots and Lots | Little | Little |
| Good Network | Is what it is | 1:1 Ratio to Data | Data, ACK |
| Bad Network | Is what it is | 1:2 or Higher Ratio | Data, Data, ACK |
| Hidden Node | Is what is is | 3:1 Ratio to Data | RTS, CTS, Data, ACK |
| b/g Protection | Is what it is | 2:1 Ratio to Data | CTS, Data, ACK |

# Associating is a 'Link Light'

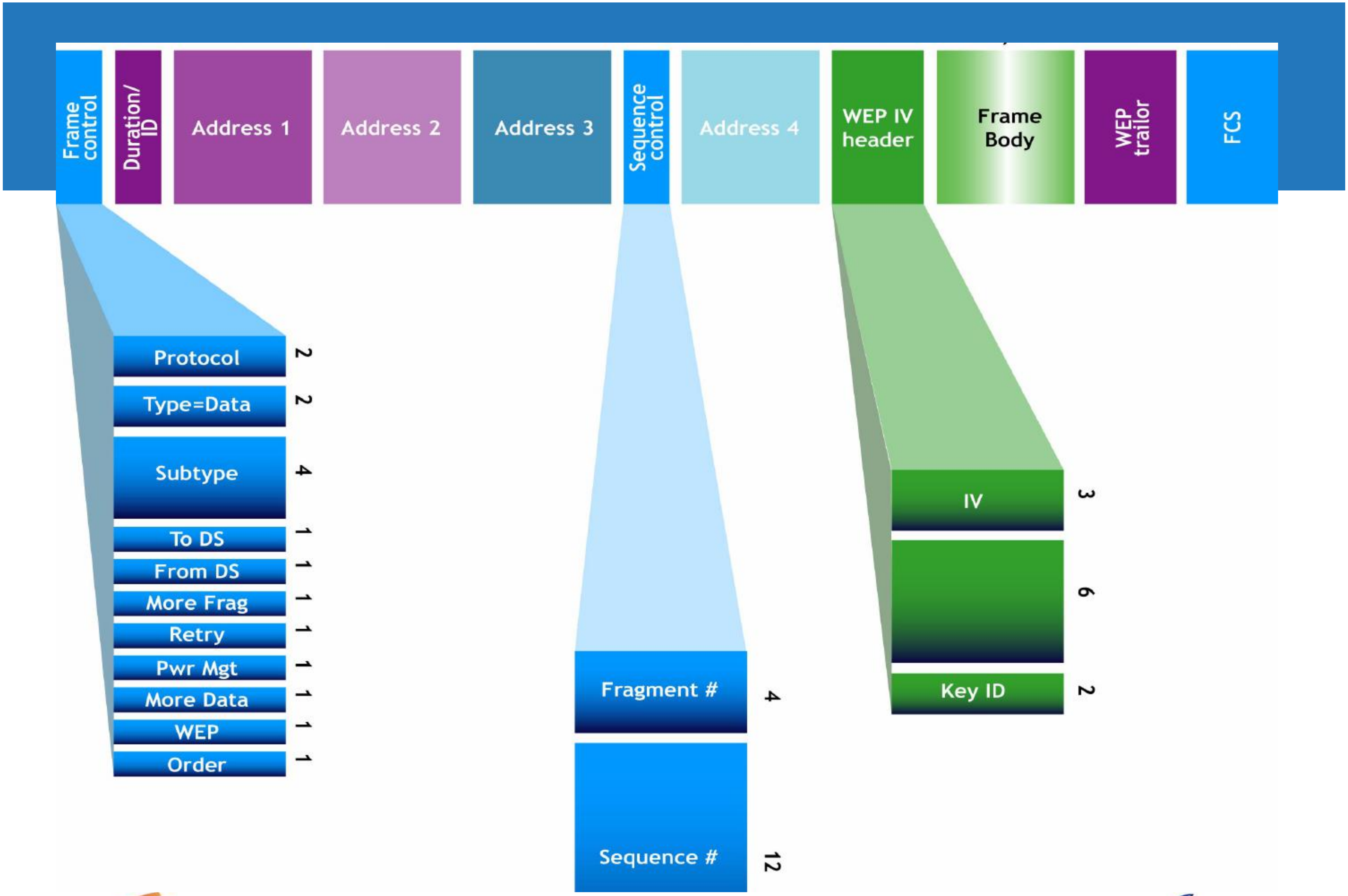
- Association
  - Beacons
  - Probe Requests/Responses
  - Authentication Request/Response
  - Association Request/Response
- How we can tell Associations
- Addresses of these frames?



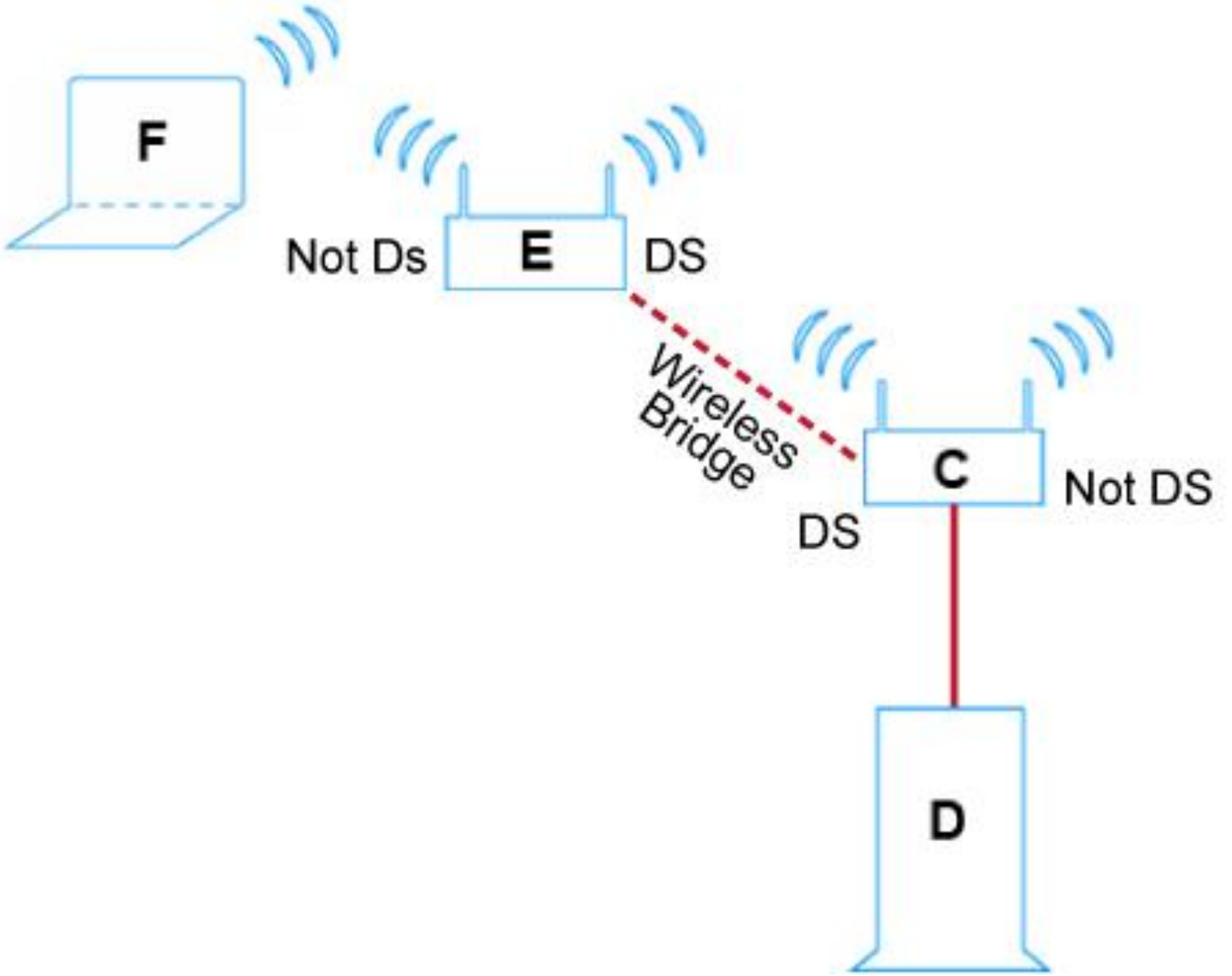
1. Client sends probe request.
2. All access points send probe response.
3. Client evaluates access point response, selects best access point.
4. Access Point A confirms authentication and registers client.
5. Client sends association request to selected Access Point (B).
6. Access Point B confirms association and registers client.

# DS Bits

- DS Bits change which Address carry which information
- BSSID is *always* available in header
- Except when an AP is in Bridging Mode
- Can tell who's associated to whom and direction of travel of frame on/off WLAN

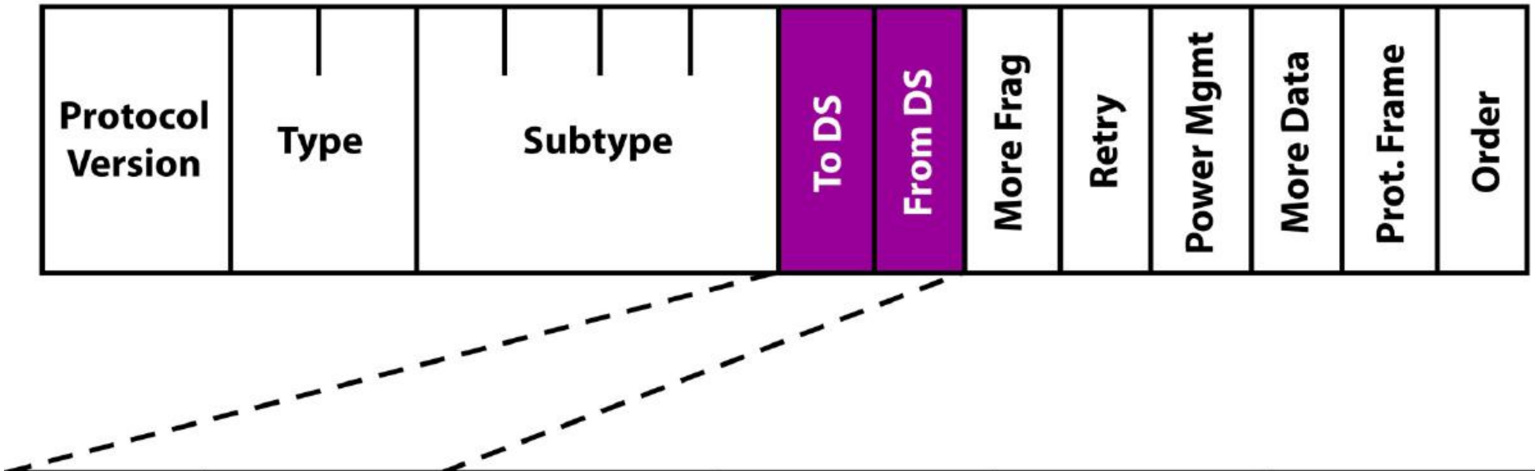

Frame control
Duration/ ID
Address 1
Address 2
Address 3
Sequence control
Address 4
WEP IV header
Frame Body
WEP trailor
FCS
Protocol
2
Type=Data
2
Subtype
4
To DS
1
From DS
1
More Frag
1
Retry
1
Pwr Mgt
1
More Data
1
WEP
1
Order
1
Fragment #
4
Sequence #
12
IV
3
6
Key ID
2

# Example of DS/Not DS



# DS Bits

Frame Control Field



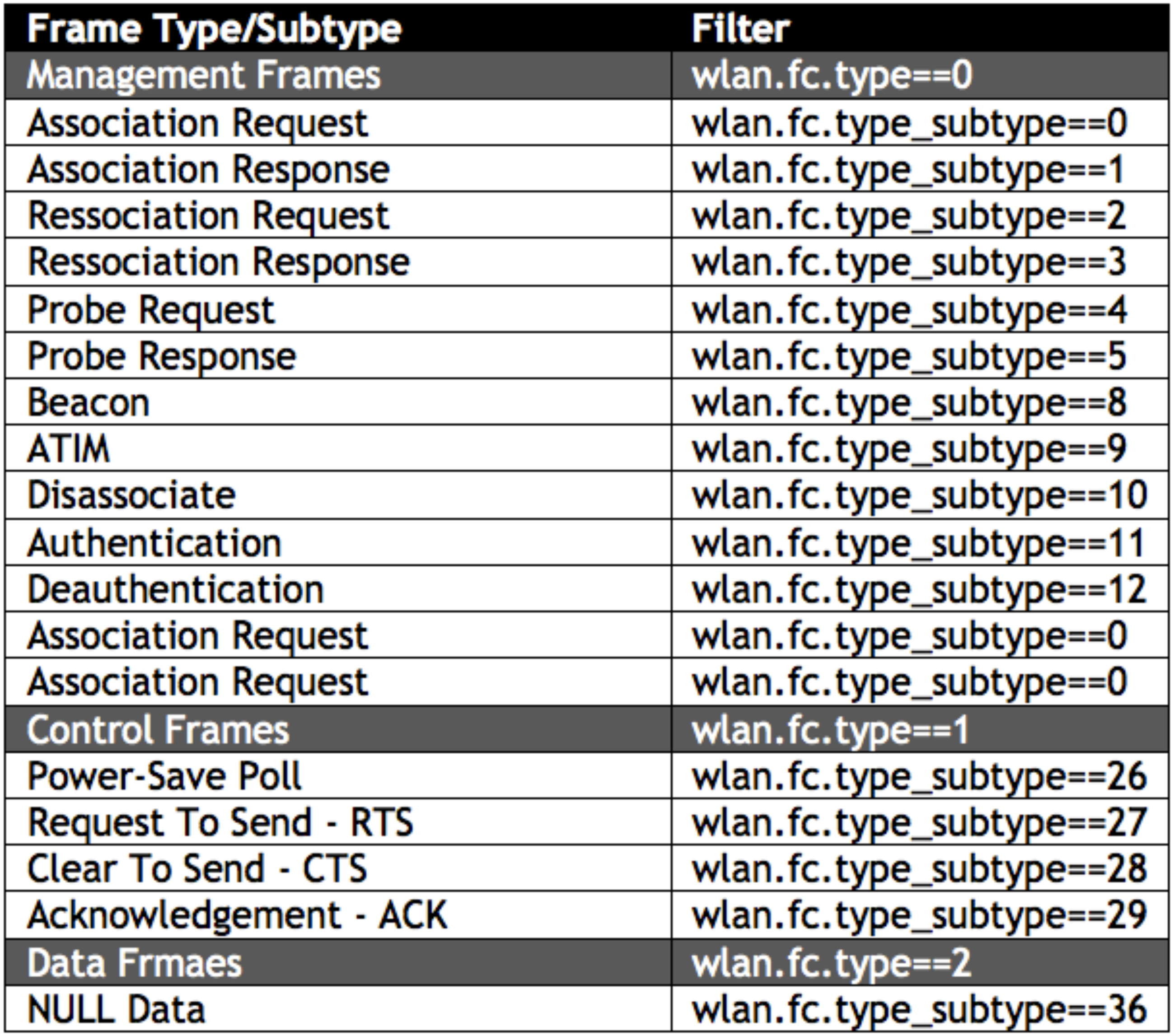
| To DS | From DS | Address 1 | Address 2 | Address 3 | Address 4 |
|---|---|---|---|---|---|
| 0 | 0 | RA/DA | TA/SA | BSSID | n/a |
| 0 | 1 | RA/DA | TA/BSSID | SA | n/a |
| 1 | 0 | RA/BSSID | TA/SA | DA | n/a |
| 1 | 1 | RA | TA | DA | SA |

# Hands On Exercises

- First
  - Columns and Colors for Wireless LANs
    - Add Channel, RSSI, Data Rate, To/From DS Bits, Retries
    - Color Code Channels, Retries, Mgmt, Ctrl, Data
  - Capture Radio Tap Header
  - Using AirPcap Adapters

- Exercise from WLSAT Course Materials

# Display Filters for WLANs

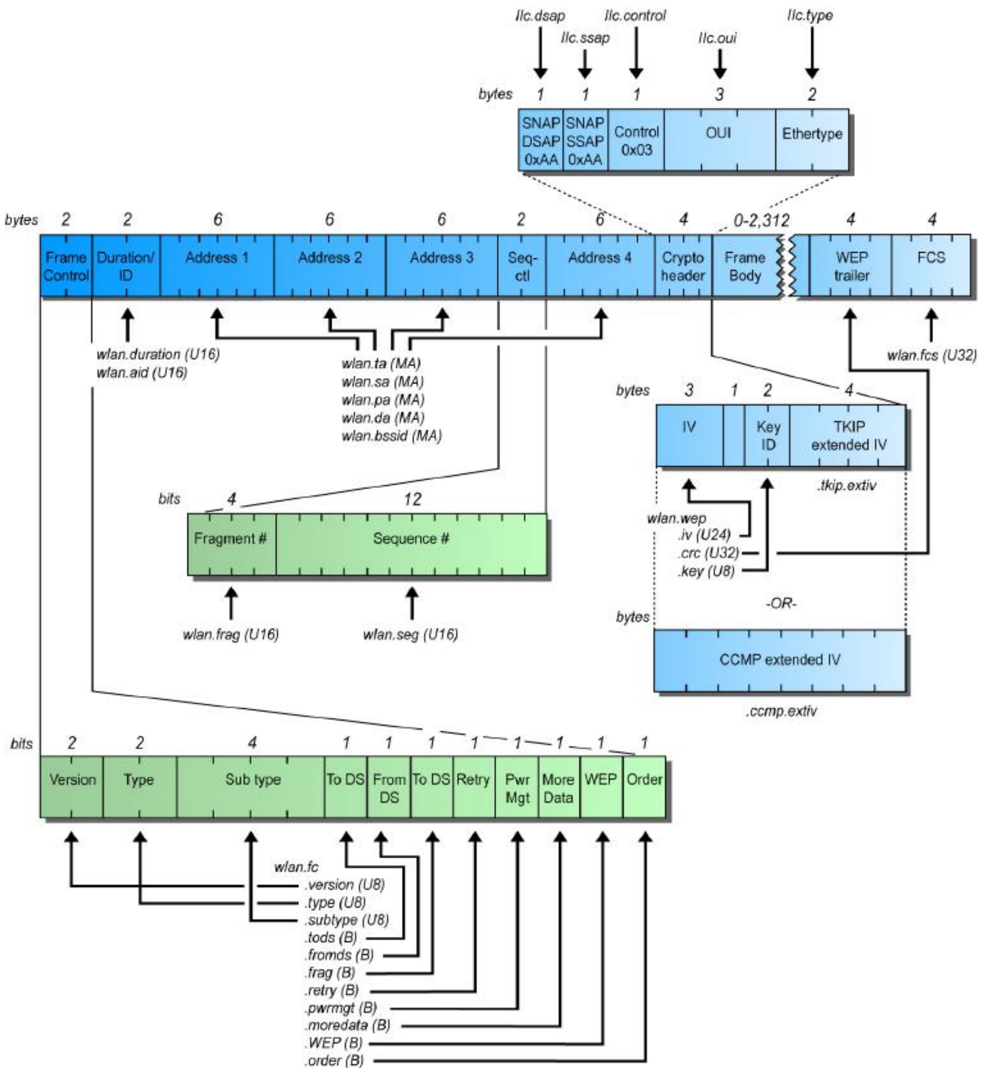


| Frame Type/Subtype | Filter |
|---|---|
| Management Frames | wlan.fc.type==0 |
| Association Request | wlan.fc.type_subtype==0 |
| Association Response | wlan.fc.type_subtype==1 |
| Ressociation Request | wlan.fc.type_subtype==2 |
| Ressociation Response | wlan.fc.type_subtype==3 |
| Probe Request | wlan.fc.type_subtype==4 |
| Probe Response | wlan.fc.type_subtype==5 |
| Beacon | wlan.fc.type_subtype==8 |
| ATIM | wlan.fc.type_subtype==9 |
| Disassociate | wlan.fc.type_subtype==10 |
| Authentication | wlan.fc.type_subtype==11 |
| Deauthentication | wlan.fc.type_subtype==12 |
| Association Request | wlan.fc.type_subtype==0 |
| Association Request | wlan.fc.type_subtype==0 |
| Control Frames | wlan.fc.type==1 |
| Power-Save Poll | wlan.fc.type_subtype==26 |
| Request To Send - RTS | wlan.fc.type_subtype==27 |
| Clear To Send - CTS | wlan.fc.type_subtype==28 |
| Acknowledgement - ACK | wlan.fc.type_subtype==29 |
| Data Frmaes | wlan.fc.type==2 |
| NULL Data | wlan.fc.type_subtype==36 |

CACE TECHNOLOGIES

www.wiresharkU.com ESHARK UNIVERSITY

# Graphic of 802.11 MAC Header



# ‘Scavenger Hunt’

- You’ve got to know what you’ve got!
- Fill in the missing boxes in the grid
- What else do you know?
- What clients are in the room?
- Which client is associated to ‘Keith Overdrive’?
- Is there AdHoc in the room?

# Thanks For Your Time!

- Answer Sheets are available at the front.
- Check out Laura Chappell’s Book
  - www.WiresharkBook.com

- Keith@WLANPros.com
- Podcast – Wireless LAN Weekly
- http://WirelessLANProfessionals.com

# Classroom Access Points - Configurations

| # | Brand | MAC | CH | SSID | Security | B-cast | AdHoc/ESS | Band | Data Rates | Power | Mode | Notes |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | **BC:2A** | | ! Classroom 1 | | | | | | | | |
| 2 | | **00:98** | | | | | | | | | b/g mixed | |
| 3 | | **C7:1C** | 11 | | Open | | | | | | | |
| 4 | | **00:8D** | | | | | | | 1-54 | | | |
| 5 | | **00:9E** | | | | | | | | | | b/g - WPA1 - PSK |
| 6 | | **00:2F** | | | WPA 2 - PSK | | | | | | | |
| 7 | | **32:65** | | ! Classroom 6 | | | | 5 GHz | | | | |
| 8 | | **E5:3B** | 3 | | | | | | | | b-only | |
| 9 | | **B5:F0** | | | WPA 2 - PSK | | | | | | | |
| 10 | | **53:44** | | | | Y | | | | | | |
| 11 | | **18:99** | | | | | ESS | | | | | |
| 12 | | **18:9A** | | | Open | | | | | 100% | | |
| 13 | | **18:99** | 11 | | | | | | | | | b/g/n/ mixed - 2.4 Ghz |
| 14 | | **18:9A** | | ! Classroom Guest | | | | | | | | |
| 15 | | **D6:EB** | | | | | | | | | | AdHoc |

*WEP Key is '**0123456789**'* *WPA PSK is '**password**'*

Please use your laptop and packet analysis software to fill in the missing information for each Access Point