Introduction to WLAN Analysis

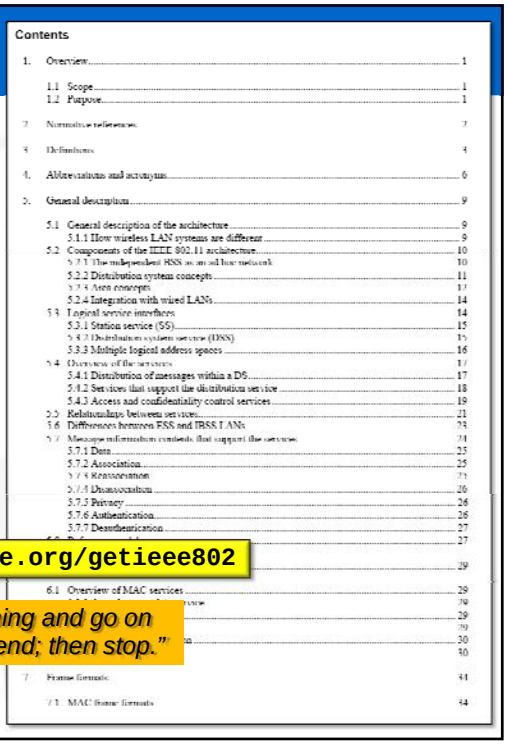
Tuesday, April 1, 2008

Joe Bardwell
Chief Scientist | Connect802 Corporation
www.Connect802.com joe@Connect802.com

SHARKFEST **'08**
Foothill College
March 31 - April 2, 2008

The 802.11 Standards

- Today we'll overview what the IEEE 802.11 standards tell us about how Wi-Fi should behave
- You need to understand the expected behavior of the protocols before you can identify anomalies
  - *"If you don't know where you're going then any road will take you there."*
    Lewis Carroll


Contents

1. Overview 1
   1.1 Scope 1
   1.2 Purpose 1
2. Normative references 2
3. Definitions 4
4. Abbreviations and acronyms 6
5. General description 9
   5.1 General description of the architecture 9
      5.1.1 How wireless LAN systems are different 9
   5.2 Components of the IEEE 802.11 architecture 10
      5.2.1 The independent BSS as an ad hoc network 10
      5.2.2 Distribution system concepts 11
      5.2.3 Area concepts 13
      5.2.4 Integration with wired LANs 14
   5.3 Logical service interfaces 14
      5.3.1 Station service (SS) 15
      5.3.2 Distribution system service (DSS) 15
      5.3.3 Multiple logical address spaces 16
   5.4 Overview of the services 17
      5.4.1 Distribution of messages within a DS 17
      5.4.2 Services that support the distribution service 18
      5.4.3 Access and confidentiality control services 19
   5.5 Relationships between services 21
   5.6 Differences between ESS and IBSS LANs 23
   5.7 Message information contents that support the services 24
      5.7.1 Data 25
      5.7.2 Association 25
      5.7.3 Reassociation 25
      5.7.4 Disassociation 26
      5.7.5 Privacy 26
      5.7.6 Authentication 26
      5.7.7 Deauthentication 27
   5.8 [illegible] 27
6. [illegible] 29
   6.1 Overview of MAC services 29
   [illegible] 29
   [illegible] 29
   [illegible] 30
   [illegible] 30
7. Frame formats 31
   7.1 MAC frame formats 34

http://standards.ieee.org/getieee802

"Begin at the beginning and go on till you come to the end; then stop."

The Secret Science of WLAN Analysis

- There is no secret
  - The 802.11 standards explain what the expected behavior is as Wi-Fi devices communicate
  - Wireshark shows you what the actual behavior is in the network
  - You isolate and describe how the actual behavior deviates from the expected behavior
  - You determine why the deviation has occurred
- Determining why a deviation has occurred is often the most difficult challenge
  - There's no substitute for experience when it comes to the "why"
  - There's no substitute for diligent study when it comes to isolating and describing anomolies

CACE TECHNOLOGIES Connect802 WIRESHARK UNIVERSITY

The Basis for Wireless Network Specifications

Federal Communications Commission (FCC)

- Develops regulatory and spectrum use policies
  - Sets radio equipment operating limits, and usage rules
  - Enforces violations under U.S. Federal law

International Electrical and Electronics Engineers Association (IEEE)

- Sets standards for equipment operation
  - Does NOT specify how equipment should be designed or manufactured
  - Creates engineering standards that comply with regulatory limitations

The Wireless Fidelity Alliance (Wi-Fi)

- Establishes guidelines for interoperability based on the IEEE standards
  - Does not set standards
  - Wi-Fi is an industry consortium

CACE TECHNOLOGIES Connect802 WIRESHARK UNIVERSITY

THE IEEE 802.11 STANDARD

- General description of the architecture
- Physical layer bit representation
  - Modulation Schemes: BPSK, QPSK, QAM
  - Spread Spectrum Bit Encoding: Barker, CCK
  - Orthogonal Frequency Division Multiplexing (OFDM)
- Service sets and distribution systems
  - Basic Service Set, Extended Service Set
- Authentication and Association
- Frame formats and fields
- Wired Equivalent Privacy (WEP)
- Distributed Coordination Function (DCF)
- Point Coordination Function (PCF)
- Fragmentation and defragmentation
- Power management

The Core 802.11 Architectural Standards

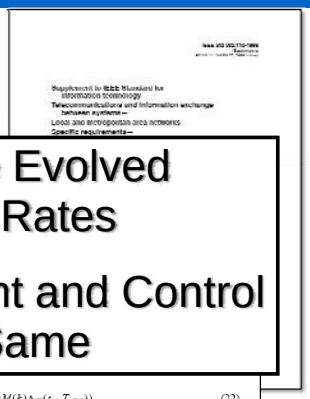
- 802.11
  - 1 and 2 Mb/sec DSSS, FHSS, and IrDA
  - BPSK and QPSK with Barker Coding
- 802.11b
  - Fall 1999
  - 2.4 GHz ISM band
  - 5.5 and 11 Mb/sec CCK+QPSK DSSS in 2.4 GHz band
- 802.11a
  - Fall 2001
  - 5.8 GHz U-NII band, 8 non-overlapping channels
  - 6-54 Mb/sec, OFDM+(BPSK,QPSK or QAM) in the 5.8 GHz band

The Core 802.11 Architectural Standards

- 802.11g
  - 11g is “11a in the ISM band”
  - The FCC (in response to a petition by Cisco) removed the requirement mandating only Spread Spectrum in the ISM band
  - Summer 2003
  - 6-54 Mb/sec, OFDM+(BPSK,QPSK or QAM) in the 2.4 GHz band
- 802.11n
  - Finalization expected in 2009
  - MIMO using 40MHz channels with STBC (Space-Time Block Code)
- 802.11y
  - Finalization expected in 2008
  - 11y is “high-power 11a in the licensed 3.7 GHz band”

The PHY Standards Differ Dramatically

- 802.11b, 802.11g, 802.11a, 802.11n…



18.4.6.5 Spreading sequences and modulation for CCK modulation at 5.5 Mbit/s and 11 Mbit/s

The PHY Standards Have Evolved to Provide Faster Data Rates

The Standards for Management and Control Have Remained the Same

The terms: φ1, φ2, φ3, and φ4 are defined in 18.4.6.5.2 for 5.5 Mbit/s and 18.4.6

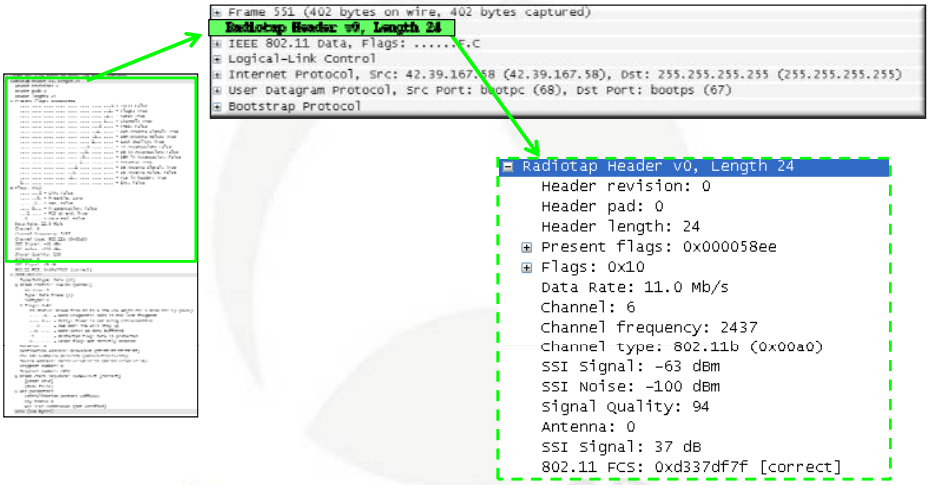
This formula creates 8 complex chips (c0 to c7), where c0 is transmitted first in

This is a form of the generalized Hadamard transform encoding, where φ1 is ad added to all odd code chips, φ3 is added to all odd pairs of code chips, and φ4 code chips.

$$r_{DATA,n}(t) = w_{TSYM}(t)\left(\sum_{k=0}^{N_{SD}-1} d_{k,n}\exp((j2\pi M(k)\Delta_F(t-T_{GI})) + p_{n+1}\sum_{k=-N_{ST}/2}^{N_{ST}/2} P_k\exp(j2\pi k\Delta_F(t-T_{GI}))\right) \quad (22)$$

where the function, $M(k)$, defines a mapping from the logical subcarrier number 0 to 47 into frequency offset index -26 to 26, while skipping the pilot subcarrier locations and the 0th (dc) subcarrier.

Radiotap Header Added by Wireshark



Possible Radiotap Header Fields

IEEE80211_RADIOTAP_TSFT
This field contains the unsigned 64-bit value, in microseconds, of the MAC's 802.11 Time Synchronization Function timer, when the first bit of the MPDU arrived at the MAC. This field should be present for received frames only.

IEEE80211_RADIOTAP_FLAGS
This field contains a single unsigned 8-bit value, containing a bitmap of flags specifying properties of the frame being transmitted or received.

IEEE80211_RADIOTAP_RATE
This field contains a single unsigned 8-bit value, which is the data rate in use in units of 500Kbps.

IEEE80211_RADIOTAP_CHANNEL
This field contains two unsigned 16-bit values. The first value is the frequency upon which this PDU was transmitted or received. The second value is a bitmap containing flags which specify properties of the channel in use. These are documented within the header file, <net80211/ieee80211_radiotap.h>.

IEEE80211_RADIOTAP_FHSS
This field contains two 8-bit values. This field should be present for frequency-hopping radios only. The first byte is the hop set. The second byte is the pattern in use.

IEEE80211_RADIOTAP_DBM_ANTSIGNAL
This field contains a single signed 8-bit value, which indicates the RF signal power at the antenna, in decibels difference from 1mW.

IEEE80211_RADIOTAP_DBM_ANTNOISE
This field contains a single signed 8-bit value, which indicates the RF noise power at the antenna, in decibels difference from 1mW.

IEEE80211_RADIOTAP_LOCK_QUALITY
This field contains a single unsigned 16-bit value, indicating the quality of the Barker Code lock. No unit is specified for this field. There does not appear to be a standard way of measuring this at this time; this quantity is often referred to as ``Signal Quality" in some datasheets.

IEEE80211_RADIOTAP_TX_ATTENUATION
This field contains a single unsigned 16-bit value, expressing transmit power as unitless distance from maximum power set at factory calibration. 0 indicates maximum transmit power. Monotonically nondecreasing with lower power levels.

IEEE80211_RADIOTAP_DB_TX_ATTENUATION
This field contains a single unsigned 16-bit value, expressing transmit power as decibel distance from maximum power set at factory calibration. 0 indicates maximum transmit power. Monotonically nondecreasing with lower power levels.

IEEE80211_RADIOTAP_DBM_TX_POWER
Transmit power expressed as decibels from a 1mW reference. This field is a single signed 8-bit value. This is the absolute power level measured at the antenna port.

IEEE80211_RADIOTAP_ANTENNA
For radios which support antenna diversity, this field contains a single unsigned 8-bit value specifying which antenna is being used to transmit or receive this frame. The first antenna is antenna 0.

IEEE80211_RADIOTAP_DB_ANTSIGNAL
This field contains a single unsigned 8-bit value, which indicates the RF signal power at the antenna, in decibels difference from an arbitrary, fixed reference.

IEEE80211_RADIOTAP_DB_ANTNOISE
This field contains a single unsigned 8-bit value, which indicates the RF noise power at the antenna, in decibels difference from an arbitrary, fixed reference.

IEEE80211_RADIOTAP_RX_FLAGS
An unsigned 16-bit bitmap indicating properties of received frames.

IEEE80211_RADIOTAP_TX_FLAGS
An unsigned 16-bit bitmap indicating properties of transmitted frames.

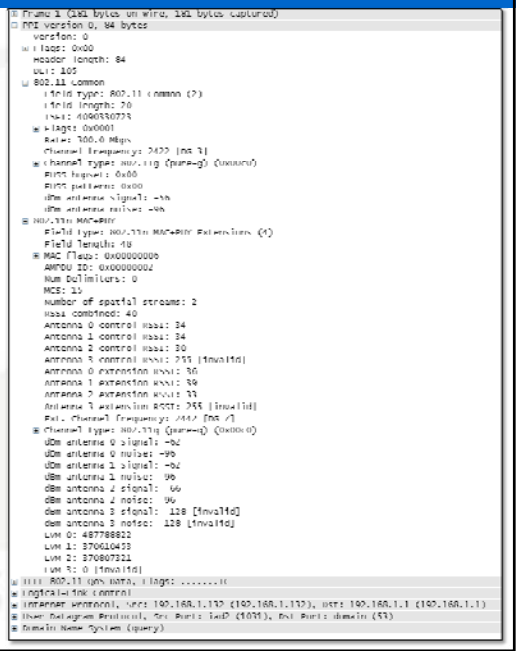
IEEE80211_RADIOTAP_RTS_RETRIES u_int8_t data
Unsigned 8-bit value indicating how many times the NIC retransmitted the Request to Send (RTS) in an RTS/CTS handshake before receiving an 802.11 Clear to Send (CTS).

IEEE80211_RADIOTAP_DATA_RETRIES
Unsigned 8-bit value indicating how many times the NIC retransmitted a unicast data packet before receiving an 802.11 Acknowledgement.

IEEE80211_RADIOTAP_EXT
This bit is reserved for any future extensions to the radiotap structure. A driver sets IEEE80211_RADIOTAP_EXT to extend the it_present bitmap by another 64 bits. The bitmap can be extended by multiples of 32 bits to 96, 128, 160 bits or longer, by setting IEEE80211_RADIOTAP_EXT in the extensions. The bitmap ends at the first extension field where IEEE80211_RADIOTAP_EXT is not set.

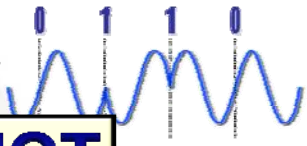
802.11n MAC+PHY PPI Header

- 802.11n is as much an architecture as it is an engineering standard
- MIMO can be implemented with 2 or 3 radios
  - Referred to as:
    2 X 2, 2 X 3, 3 X 3
- The "Per-Packet Information" (PPI) header is prepended instead of the Radiotap header to convey MIMO information beyond what Radiotap can provide

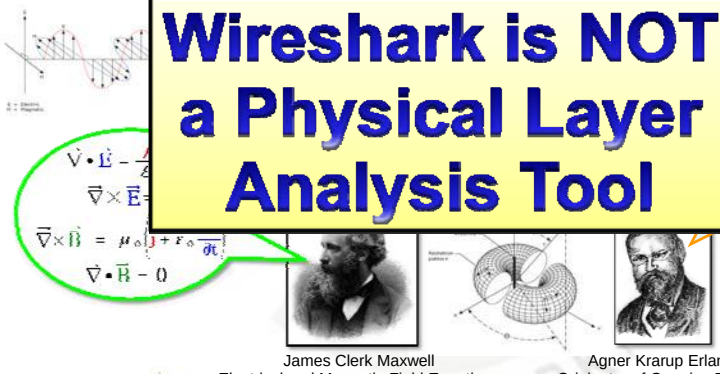


Electromagnetic Signals at the Physical Layer

- The 802.11 Physical Layer comprises the realm of **electromagnetic signal propagation**
- In this realm it's the skill set of the RF engineer that predominates



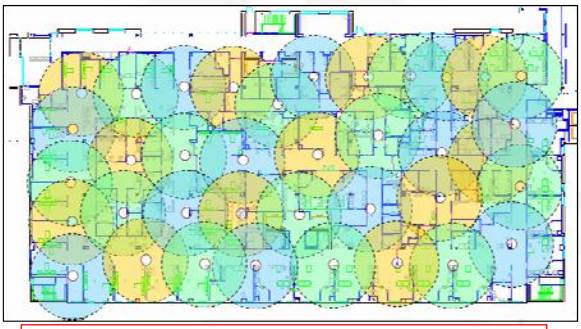
Wireshark is NOT a Physical Layer Analysis Tool



James Clerk Maxwell
Electrical and Magnetic Field Equations
(Applied to 802.11 Signal Strength Considerations)

Agner Krarup Erlang
Originator of Queuing Theory
(Applied to 802.11 Oversubscription Calculations)

RF Signals Do Not Propagate In Circular Paths



NO CIRCLES !

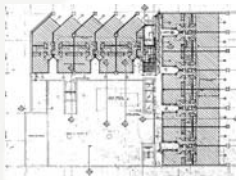
CACE TECHNOLOGIES

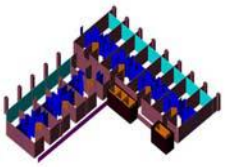
Connect802

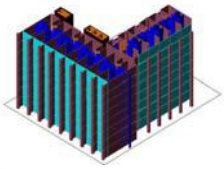
WIRESHARK UNIVERSITY

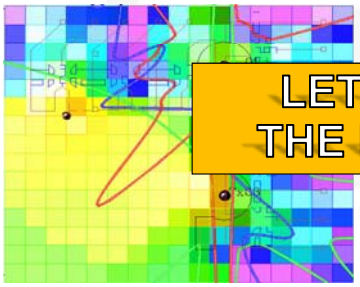
Addressing the Complexities of RF Design

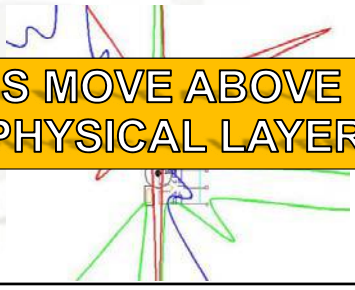
- Connect802 Utilizes 3-Dimensional RF CAD Modeling to Consider RF Engineering Complexities in a System Design
  - You provide a building (or outdoor area) plan
  - We create a 3-dimensional CAD model of the space
  - Wi-Fi signal coverage is determined accurately





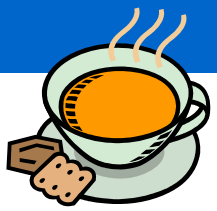






LET'S MOVE ABOVE THE PHYSICAL LAYER

More of the 802.11 Alphabet Soup



- 802.11c – Bridge Operation Procedures
  - These standards form the basis for WDS (Wireless Distribution System) implementation in the creation of a Microcell to be discussed
- 802.11d – PHY requirements to satisfy non-US regulatory requirements
  - The 5 GHz band is used differently outside the U.S.
- 802.11e – QoS to optimize/prioritize traffic for voice and video
  - Anticipated firmware upgrades will provide backward compatibility
- 802.11f – Inter Access Point Protocol
  - Communication between Access Points for multi-vendor interoperable roaming support

More of the 802.11 Alphabet Soup

- 802.11h – Automatic configuration extensions to 802.11a
  - Dynamic Channel/Frequency Selection (DCS/DFS)
  - Transmit Power Control (TPC)
- 802.11i – Strong security (foreshadowed by WPA)
  - Utilizes 802.1x Authentication with RADIUS (Remote Authentication Dial-In User Service)
    - 802.1x has been in place for wired authentication for many years
  - WPA and 802.11i correct the security flaws in WEP (Wired Equivalent Privacy)
  - Wi-Fi networks can now be designed with strong security
  - (802.11i and WPA will be discussed in more detail)
- 802.11j – 802.11a in the 4.9 GHz band for Japan

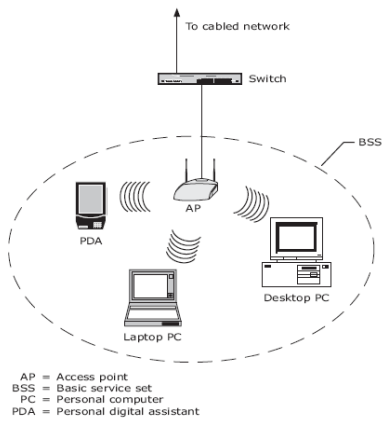
More of the 802.11 Alphabet Soup

- 802.11k – Radio Resource Management: measurement interrogation standards for Access Point and client self management to auto-provision large networks
  - Signal and Noise metrics
  - Channel use information
  - Hidden node discovery
  - Individual client statistics
  - Transmit Power Control (TPC)
- 802.11l – (Typographically unsound ☺)
- 802.11m – Maintenance of existing standards
- 802.11p – Wireless Access in the Vehicular Environment (WAVE) operating in the Intelligent Transportation Systems (ITS) licensed 5.9 GHz band.
- 802.11r – Fast roaming between Access Points

Understanding 802.11 Network Architecture

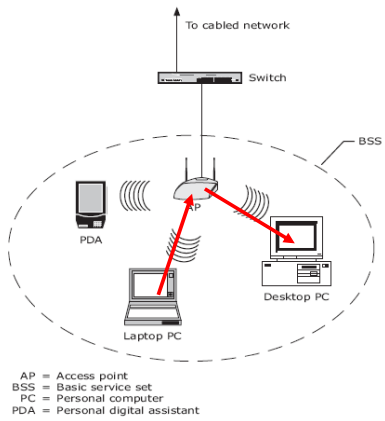
- **Access Point (AP)** – A "*Station" (device)* that provides access to the *Distribution System*
- **Distribution System (DS)** – The network that connects BSS-s together into an *ESS*
- **Station (STA)** – Any device with an 802.11 radio
  - Includes laptops, VoIP phones, PDAs, etc…
- **Basic Service Set (BSS)** – Exactly one AP and all of its client stations
- **Extended Service Set (ESS)** – One or more BSS-s sharing the same *ESSID*
  - *Commonly referred to as the "SSID"*
  - *This is the Network Name*

The Basic Service Set (BSS)



- Contains exactly one AP
- Uniquely identified by the *BSSID*, which is essentially always the same as the MAC address of the AP's wireless interface
- All clients are *associated* with the AP
- A client can only be a member of a single BSS at a time

Traffic Flow in a BSS

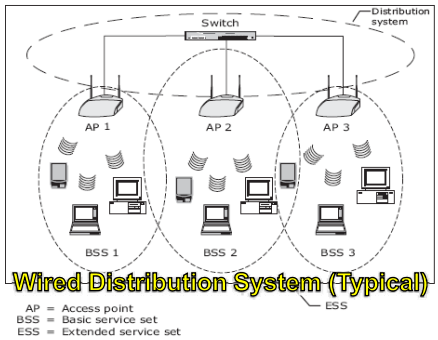


- Traffic in a BSS <u>always</u> flows from STA to AP or from AP to STA
- If both the source and destination STA are in the same BSS, this results in packet duplication
- Available throughput is cut in half
- Fortunately, wireless stations usually talk to wired stations

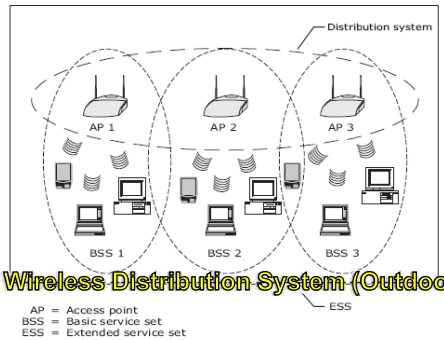
The Extended Service Set (ESS)

- Access Points are configured with an *ESSID*
  - Term is often shortened to just *SSID (or "Network Name")*
  - This is what you see in your "Available Wireless Networks"
- All Access points with the same ESSID are part of an ESS
  - ESSID identifies the group of APs as a whole, not any specific AP
  - BSSID is what identifies the specific APs
- Stations can roam within an ESS without losing connection
  - The specifications for roaming are pragmatic and not optimal
    - 802.11e and 802.11r cover fast roaming for multimedia applications
  - Access Point comprising a single ESS must be part of the same Layer 2 Broadcast Domain
    - Connected to the same Layer 2 switched network or all configured on the same VLAN.
      - Mobile IP can mitigate these requirements

Distribution System



Wired Distribution System (Typical)



Wireless Distribution System (Outdoor)

- The Extended Service Set is the identification for the Layer 2 network that interconnects all the Access Points
- Wired or wireless interconnectivity
  - "Client Access Wi-Fi" versus "Wireless Distribution System" (WDS)

Frame Formats That You'll See With Wireshark

- 802.11 frames are structured differently from Ethernet frames
- Additional addressing is used in Wi-Fi 802.11 data transfer
- A comparison between the headers of 802.3 frames and the similarly named 802.11 headers will actually reveal that in reality, they are significantly different

Ethernet

Dest Address	Src Address	Length	LLC Header

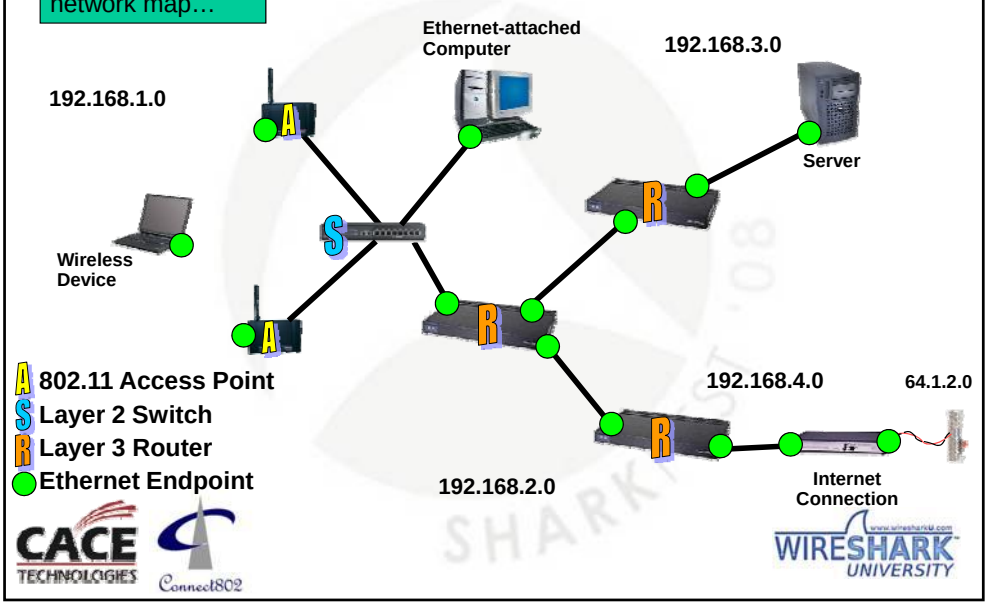
802.11

Frame Ctrl	Duration / ID	Addr. 1	Addr. 2	Addr. 3	Seq.	Addr. 4	LLC Header

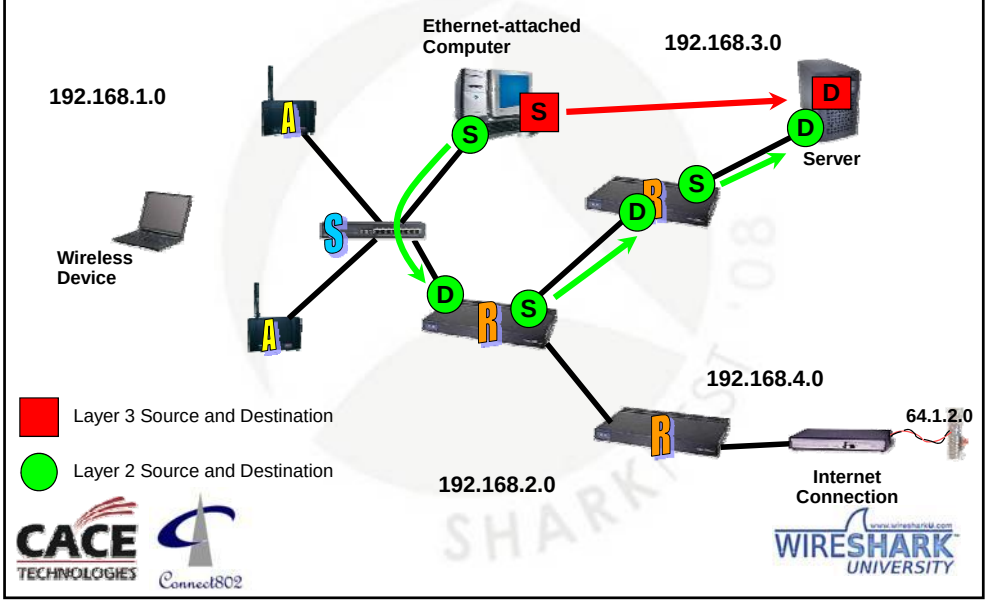
"Why are there four Data Link Layer addresses in 802.11?"

802.11 and Ethernet Addressing

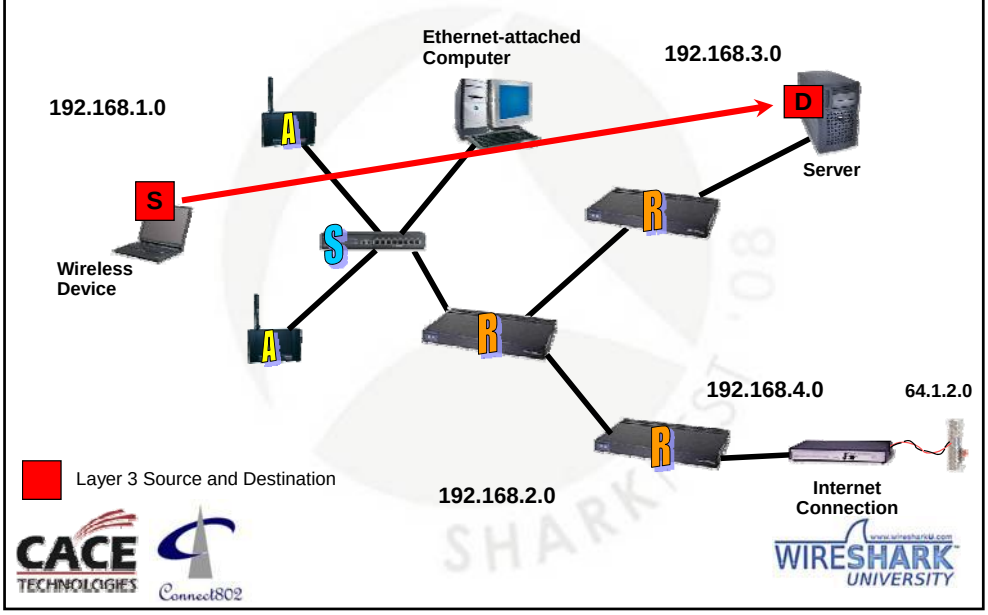
Consider this network map…



Wired to Wired Addressing

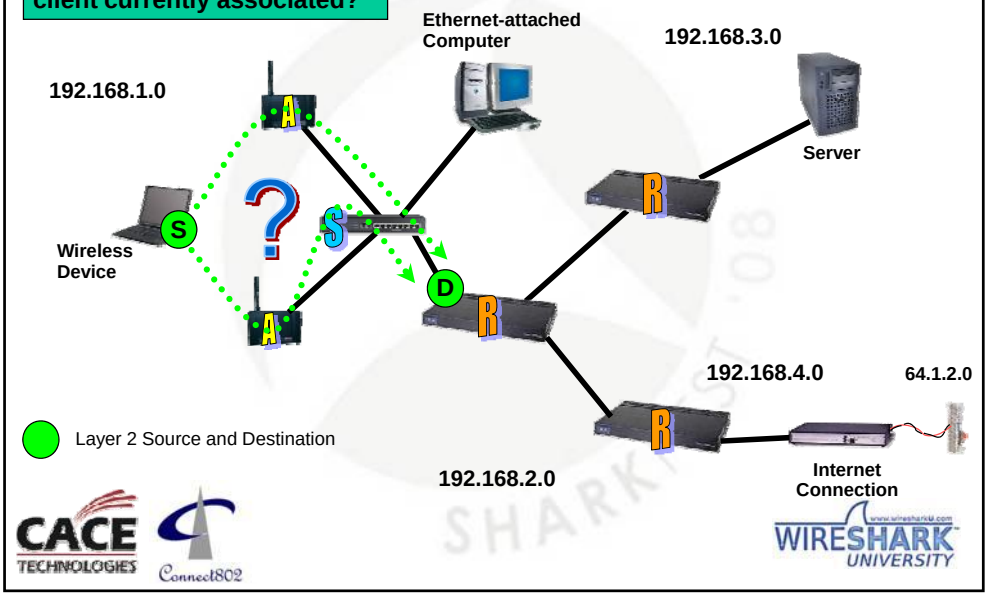


Wireless to Wired Addressing

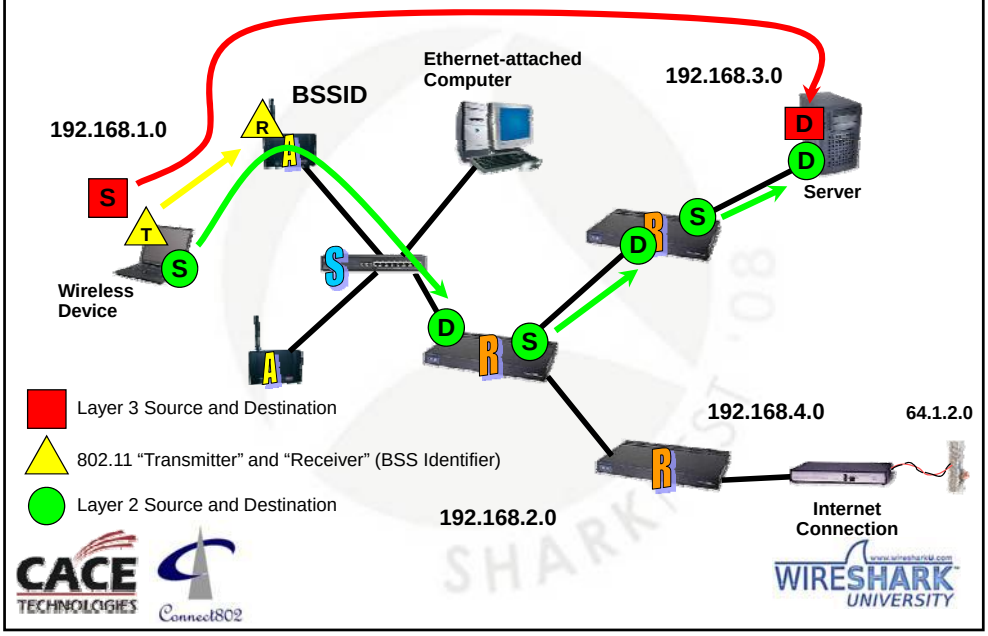


Wireless Addressing Requires More

To which access point is the client currently associated?



802.11 Adds Address Fields To The Packet



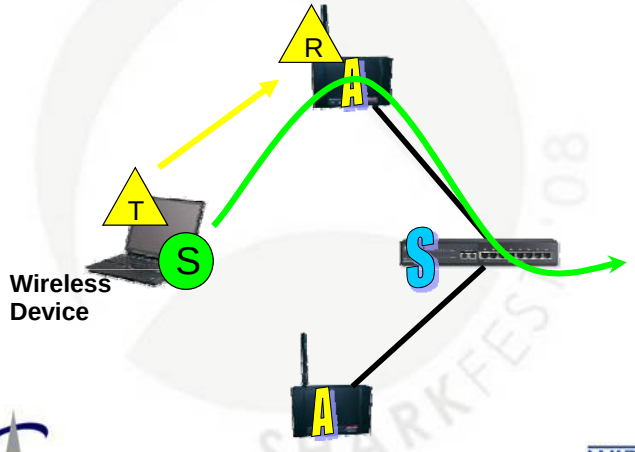
Effects of 802.11 Addressing (1)

- 802.11's transmitter and receiver fields use the same MAC addresses as the source and destination fields
- The "BSS Id" field is Address 3
  - This is the MAC address of the Access Point
  - Address 4 would only be present in a Wireless Distribution System frame

```
⊞ Frame 2841 (146 bytes on wire, 146 bytes captured)
⊞ Radiotap Header v0, Length 24
⊟ IEEE 802.11 Data, Flags: .p....F..
    Type/Subtype: Data (0x20)
  ⊟ Frame Control: 0x4208 (Normal)
      Version: 0
      Type: Data frame (2)
      Subtype: 0
    ⊞ Flags: 0x42
    Duration: 0
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    BSS Id: Globalsu_01:12:c8 (00:03:2f:01:12:c8)
    Source address: Micro-St_f3:85:34 (00:13:d3:f3:85:34)
    Fragment number: 0
    Sequence number: 3041
  ⊞ Frame check sequence: 0x7f7dd64c
⊞ Logical Link Control
⊞ Data (90 bytes)
```

Effects of 802.11 Addressing (2)

- The transmitter and receiver address allow an 802.11 client to specify which access point a packet should go through, even when that client is within range of multiple access points



Effects of 802.11 Addressing (3)

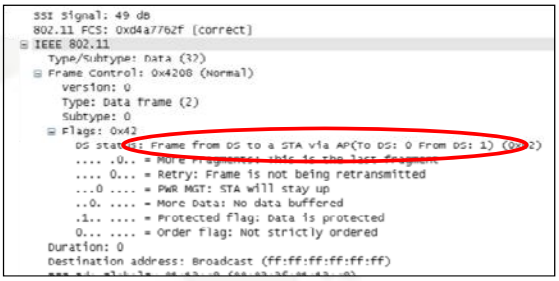
- A client will "associate" with a single access point, then send all packets through that access point
  - If necessary, a client may decide to roam to a new access point, but clients will not change APs on a packet-by-packet basis, even though 802.11's addressing could support this
- 802.11 transmitter and receiver addresses are only carried in 802.11 packets, not in Ethernet packets
  - Although the same MAC addresses may be used for transmitter/receiver and source/destination, Ethernet frames don't have fields for transmitter/receiver (nor do they need them)
- 802.11 source and destination addresses are identical to Ethernet source and destination packets
  - Source and destination addresses don't change when packets go through an AP
  - In terms of source and destination addressing, the AP acts just like an Ethernet switch—packets pass through it transparently

Normally, Only the Access Point BSSID Will Be Present

This is not the case when packets are exchanged in a Wireless Distribution System

To DS and From DS

- These flags within the 802.11 frame indicate where the packet is going
  - From an AP to a client STA?
  - From a client STA to an AP?
  - From an AP to another AP within the DS?
- Wireshark provides a plain-text explanation of the bits, as shown to the right

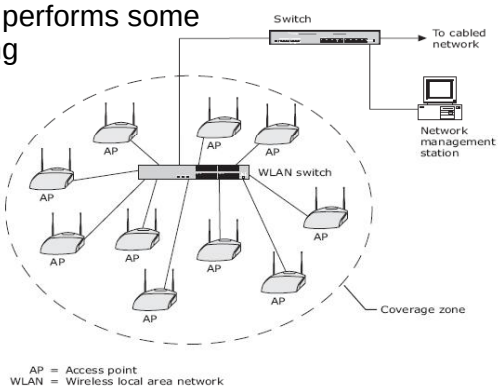


The Wireless Distribution System (WDS)

```
⊞ Frame 52 (98 bytes on wire, 98 bytes captured)
⊟ Radiotap Header v0, Length 24
    Header revision: 0
    Header pad: 0
    Header length: 24
  ⊞ Present flags: 0x000058ee
  ⊞ Flags: 0x10
    Data Rate: 11.0 Mb/s
    Channel frequency: 2437 [BG 6]
  ⊞ Channel type: 802.11b (0x00a0)
    SSI Signal: -77 dBm
    SSI Noise: -100 dBm
    Signal Quality: 5
    Antenna: 0
    SSI Signal: 23 dB
    802.11 FCS: 0xeffae3b4 [incorrect, should be 0xd6bbadf6]
⊟ IEEE 802.11 Unrecognized (Reserved frame), Flags: ..m.R.FT.
    Type/Subtype: Unknown (0x3d)
  ⊟ Frame Control: 0x2BDD (Normal)
      Version: 1
      Type: Unknown (3)
      Subtype: 13
    ⊟ Flags: 0x2B
        DS status: Frame part of WDS from one AP to another AP (To DS: 1 From DS: 1) (0x03)
        .... .0.. = More Fragments: This is the last fragment
        .... 1... = Retry: Frame is being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..1. .... = More Data: Data is buffered for STA at AP
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    Duration: 20693
  ⊟ Frame check sequence: 0xeffae3b4 [incorrect, should be 0xd6bbadf6]
      [Good: False]
      [Bad: True]
```

One More Architecture: Wireless LAN Switching

- The central switch controller performs some or all of the packet processing
  - Authentication
  - Encryption
  - Probe Response
  - Beacon Transmission
- The "Access Point" can be thought of as a "radio head"
- The central switch controller can automatically adjust channel and power settings

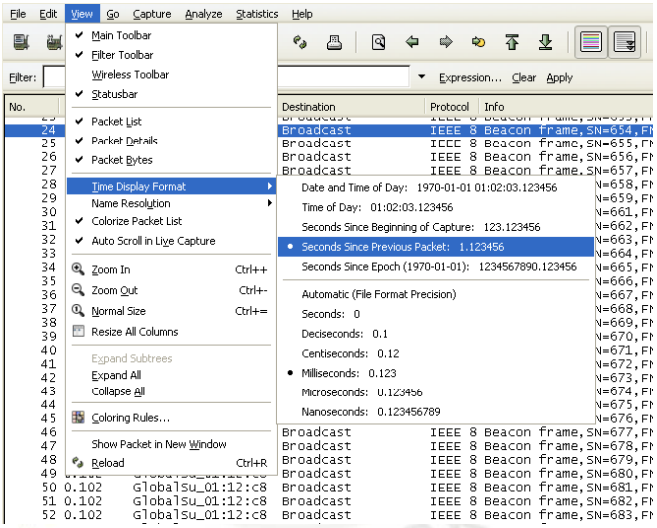


- Real-Time Location Services (RTLS) can be implemented
- The entire system could be a single BSS with the MAC of the controller used as the target for wireless packets (Address 3)

"All together now…."

- Class 1 Frames
  - Beacon
  - Probe
    - ACK
  - Probe Response
    - ACK
- Class 2 Frames
  - Authenticate
    - ACK
  - Authenticate (Response)
    - ACK
  - Association Request
    - ACK
  - Associated Response
    - ACK
- Class 3 Frames
  - All Data
  - ACK

Setup for Milliseconds Since Previous Packet



Beacon Frames Every 10 ms

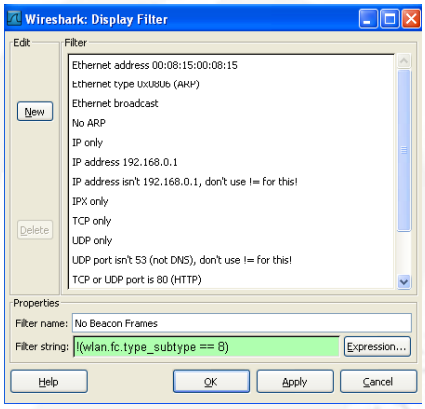
No.	Time	Source	Destination	Protocol	Info
27	0.102	Globalsu_01:12:c8	Broadcast	IEEE 8	Beacon frame,SN=657,FN=0,BI=100, SSID: "pintado476"
28	0.102	Globalsu_01:12:c8	Broadcast	IEEE 8	Beacon frame,SN=658,FN=0,BI=100, SSID: "pintado476"
29	0.102	Globalsu_01:12:c8	Broadcast	IEEE 8	Beacon frame,SN=659,FN=0,BI=100, SSID: "pintado476"
30	0.204	Globalsu_01:12:c8	Broadcast	IEEE 8	Beacon frame,SN=661,FN=0,BI=100, SSID: "pintado476"
31	0.102	Globalsu_01:12:c8	Broadcast	IEEE 8	Beacon frame,SN=662,FN=0,BI=100, SSID: "pintado476"
32	0.102	Globalsu_01:12:c8	Broadcast	IEEE 8	Beacon frame,SN=663,FN=0,BI=100, SSID: "pintado476"
33	0.102	Globalsu_01:12:c8	Broadcast	IEEE 8	Beacon frame,SN=664,FN=0,BI=100, SSID: "pintado476"
34	0.102	Globalsu_01:12:c8	Broadcast	IEEE 8	Beacon frame,SN=665,FN=0,BI=100, SSID: "pintado476"
35	0.102	Globalsu_01:12:c8	Broadcast	IEEE 8	Beacon frame,SN=666,FN=0,BI=100, SSID: "pintado476"
36	0.102	Globalsu_01:12:c8	Broadcast	IEEE 8	Beacon frame,SN=667,FN=0,BI=100, SSID: "pintado476"
37	0.102	Globalsu_01:12:c8	Broadcast	IEEE 8	Beacon frame,SN=668,FN=0,BI=100, SSID: "pintado476\a-" [Malformed Packet]
38	0.102	Globalsu_01:12:c8	Broadcast	IEEE 8	Beacon frame,SN=669,FN=0,BI=100, SSID: "pintado476"
39	0.102	Globalsu_01:12:c8	Broadcast	IEEE 8	Beacon frame,SN=670,FN=0,BI=100, SSID: "pintado476"
40	0.102	Globalsu_01:12:c8	Broadcast	IEEE 8	Beacon frame,SN=671,FN=0,BI=100, SSID: "pintado476"
41	0.102	Globalsu_01:12:c8	Broadcast	IEEE 8	Beacon frame,SN=672,FN=0,BI=100, SSID: "pintado476"[Malformed Packet]
42	0.102	Globalsu_01:12:c8	Broadcast	IEEE 8	Beacon frame,SN=673,FN=0,BI=100, SSID: "pintado476"
43	0.102	Globalsu_01:12:c8	Broadcast	IEEE 8	Beacon frame,SN=674,FN=0,BI=100, SSID: "pintado476"
44	0.102	Globalsu_01:12:c8	Broadcast	IEEE 8	Beacon frame,SN=675,FN=0,BI=100, SSID: "pintado476"
45	0.102	Globalsu_01:12:c8	Broadcast	IEEE 8	Beacon frame,SN=676,FN=0,BI=100, SSID: "pintado476"
46	0.102	Globalsu_01:12:c8	Broadcast	IEEE 8	Beacon frame,SN=677,FN=0,BI=100, SSID: "pintado476"

```
⊞ Present flags: 0x000058ee
⊟ Flags: 0x10
    .... ...0 = CFP: False
    .... ..0. = Preamble: Long
    .... .0.. = WEP: False
    .... 0... = Fragmentation: False
    ...1 .... = FCS at end: True
    ..0. .... = Data Pad: False
  Data Rate: 1.0 Mb/s
  Channel: 6
  Channel frequency: 2437
  Channel type: 802.11b (0x0040)
  SSI Signal: -54 dBm
  SSI Noise: -100 dBm
  Signal Quality: 88
  Antenna: 0
  SSI Signal: 46 dB
  802.11 FCS: 0x6304fdc3 [Incorrect, should be 0x2b186a3f]
⊞ IEEE 802.11
⊞ IEEE 802.11 Wireless LAN management frame
  [Malformed Packet: IEEE 802.11]
```

Beacon Frames Tend to Clutter a Trace

13	0.102	Cisco_4b:dc:10	Broadcast	129	IEEE 8 Beacon frame,SN=311,FN=0,BI=100, SSID: "JXP", Name: "WAP-B7"
14	0.102	Cisco_4b:dc:10	Broadcast	129	IEEE 8 Beacon frame,SN=312,FN=0,BI=100, SSID: "JXP", Name: "WAP-B7"
15	0.140	20:09:9e:db:df:ff	4e:7c:fb:6a:fe:ff	78	LLC I P, N(R)=119, N(S)=87; DSAP Ungermann-Bass Group, SSAP 0x68 Command
16	0.064	Cisco_4b:dc:10	Broadcast	129	IEEE 8 Beacon frame,SN=314,FN=0,BI=100, SSID: "JXP", Name: "WAP-B7"
17	0.204	Cisco_4b:dc:10	Broadcast	129	IEEE 8 Beacon frame,SN=317,FN=0,BI=100, SSID: "JXP", Name: "WAP-B7"
18	0.102	Cisco_4b:dc:10	Broadcast	129	IEEE 8 Beacon frame,SN=318,FN=0,BI=100, SSID: "JXP", Name: "WAP-B7"
19	0.102	Cisco_4b:dc:10	Broadcast	129	IEEE 8 Beacon frame,SN=320,FN=0,BI=100, SSID: "JXP", Name: "WAP-B7"
20	2.287	Cisco-Li_32:9a:8d	Broadcast	91	IEEE 8 Beacon frame,SN=2128,FN=0,BI=100, SSID: "\000\000\000\000\000\000\000
21	0.204	Cisco-Li_32:9a:8d	Broadcast	91	IEEE 8 Beacon frame,SN=2130,FN=0,BI=100, SSID: "\000\000\000\000\000\000\000
22	0.102	Cisco-Li_32:9a:8d	Broadcast	91	IEEE 8 Beacon frame,SN=2131,FN=0,BI=100, SSID: "\000\000\000\000\000\000\000
23	0.102	Cisco-Li_32:9a:8d	Broadcast	91	IEEE 8 Beacon frame,SN=2132,FN=0,BI=100, SSID: "\000\000\000\000\000\000\000
24	0.102	Cisco-Li_32:9a:8d	Broadcast	91	IEEE 8 Beacon frame,SN=2133,FN=0,BI=100, SSID: "\000\000\000\000\000\000\000
25	0.204	Cisco-Li_32:9a:8d	Broadcast	91	IEEE 8 Beacon frame,SN=2135,FN=0,BI=100, SSID: "\000\000\000\000\000\000\000
26	0.102	Cisco-Li_32:9a:8d	Broadcast	91	IEEE 8 Beacon frame,SN=2136,FN=0,BI=100, SSID: "\000\000@\346\366\377\237WF"
27	0.102	Cisco-Li_32:9a:8d	Broadcast	91	IEEE 8 Beacon frame,SN=2137,FN=0,BI=100, SSID: "\000\000\000\000\000\000\000
28	1.296	Cisco_4b:dc:10	Broadcast	129	IEEE 8 Beacon frame,SN=368,FN=0,BI=100, SSID: "JXP", Name: "WAP-B7"
29	0.102	Cisco_4b:dc:10	Broadcast	129	IEEE 8 Beacon frame,SN=369,FN=0,BI=100, SSID: "JXP", Name: "WAP-B7"
30	0.102	Cisco_4b:dc:10	Broadcast	129	IEEE 8 Beacon frame,SN=370,FN=0,BI=100, SSID: "JXP", Name: "WAP-B7"
31	0.102	01:22:40:96:5e:2e	7f:5b:37:05:bf:ff	129	IEEE 8 Beacon frame,SN=742,FN=0,BI=200, SSID: "\224\260\240\002\020\004", Na
32	0.204	Cisco_4b:dc:10	Broadcast	129	IEEE 8 Beacon frame,SN=373,FN=0,BI=100, SSID: "JXP", Name: "WAP-B7"
33	0.102	Cisco_4b:dc:10	Broadcast	129	IEEE 8 Beacon frame,SN=374,FN=0,BI=100, SSID: "JXP", Name: "WAP-B7"
34	0.102	Cisco_4b:dc:10	Broadcast	129	IEEE 8 Beacon frame,SN=375,FN=0,BI=100, SSID: "JXP", Name: "WAP-B7"
35	0.102	Cisco_4b:dc:10	Broadcast	129	IEEE 8 Beacon frame,SN=376,FN=0,BI=100, SSID: "JXP", Name: "WAP-B7"
36	0.102	Cisco_4b:dc:10	Broadcast	129	IEEE 8 Beacon frame,SN=377,FN=0,BI=100, SSID: "JXP", Name: "WAP-B7"
37	0.102	Cisco_4b:dc:10	Broadcast	129	IEEE 8 Beacon frame,SN=378,FN=0,BI=100, SSID: "JXP", Name: "WAP-B7"
38	0.102	Cisco_4b:dc:10	Broadcast	129	IEEE 8 Beacon frame,SN=379,FN=0,BI=100, SSID: "JXP", Name: "WAP-B7"
39	0.102	Cisco_4b:dc:10	Broadcast	129	IEEE 8 Beacon frame,SN=380,FN=0,BI=100, SSID: "JXP", Name: "WAP-B7"
40	0.102	Cisco_4b:dc:10	Broadcast	129	IEEE 8 Beacon frame,SN=381,FN=0,BI=100, SSID: "JXP", Name: "WAP-B7"
41	0.102	Cisco_4b:dc:10	Broadcast	129	IEEE 8 Beacon frame,SN=382,FN=0,BI=100, SSID: "JXP", Name: "WAP-B7"
42	0.102	Cisco_4b:dc:10	Broadcast	129	IEEE 8 Beacon frame,SN=383,FN=0,BI=100, SSID: "JXP", Name: "WAP-B7"
43	2.289	Cisco-Li_32:9a:8d	Broadcast	91	IEEE 8 Beacon frame,SN=2187,FN=0,BI=100, SSID: "\000\000\000\000\000\000\000
44	0.103	Cisco-Li_32:9a:8d	Broadcast	91	IEEE 8 Beacon frame,SN=2188,FN=0,BI=100, SSID: "\000\000\000\000\000\000\000
45	0.100	Cisco-Li_32:9a:8d	Broadcast	91	IEEE 8 Beacon frame,SN=2189,FN=0,BI=100, SSID: "\000\000\000\000\000\000\000
46	0.102	Cisco-Li_32:9a:8d	Broadcast	91	IEEE 8 Beacon frame,SN=2190,FN=0,BI=100, SSID: "\000\000\000\000\000\000\000
47	0.102	Cisco-Li_32:9a:8d	Broadcast	91	IEEE 8 Beacon frame,SN=2191,FN=0,BI=100, SSID: "\000\000\000\000\000\000\000
48	0.102	Cisco-Li_32:9a:8d	Broadcast	91	IEEE 8 Beacon frame,SN=2192,FN=0,BI=100, SSID: "\000\000\000\000\000\000\000
49	0.102	Cisco-Li_32:9a:8d	Broadcast	91	IEEE 8 Beacon frame,SN=2193,FN=0,BI=100, SSID: "\000\000\000\000\000\000\000
50	0.204	Cisco-Li_32:9a:8d	Broadcast	91	IEEE 8 Beacon frame,SN=2195,FN=0,BI=100, SSID: "\000\000\000\000\000\000\000
51	0.102	Cisco-Li_32:9a:8d	Broadcast	91	IEEE 8 Beacon frame,SN=2196,FN=0,BI=100, SSID: "\000\000\000\000\000\000\000

Get Rid of Those Beacon Frames



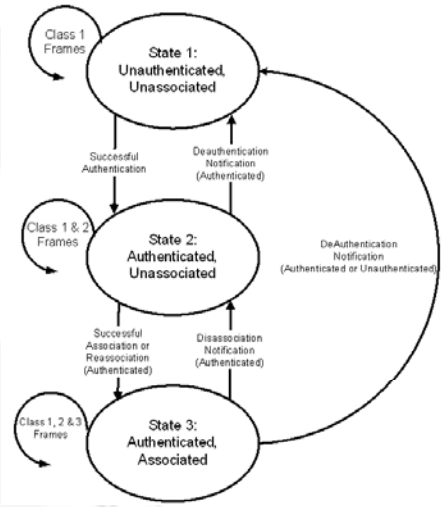
Where the Action Starts

- **Probe**
- **Authenticate**
- **Associate**

452	0.057	00:1b:77:68:7c:5b	Broadcast	IEEE 8 Probe Request,SN=0,FN=0, SSID: "pintado476"
453	0.001	GlobalSu_01:12:c8	00:1b:77:68:7c:5b	IEEE 8 Probe Response,SN=2368,FN=0,BI=100, SSID: "pintado476"
454	0.000		GlobalSu_01:12:c8	IEEE 8 Acknowledgement
455	0.013	00:1b:77:68:7c:5b	GlobalSu_01:12:c8	IEEE 8 Authentication,SN=0,FN=0
456	0.000		00:1b:77:68:7c:5b	IEEE 8 Acknowledgement
457	0.000	GlobalSu_01:12:c8	00:1b:77:68:7c:5b	IEEE 8 Authentication,SN=2369,FN=0
458	0.000		GlobalSu_01:12:c8	IEEE 8 Acknowledgement
459	0.000	00:1b:77:68:7c:5b	GlobalSu_01:12:c8	IEEE 8 Association Request,SN=1,FN=0, SSID: "pintado476"
460	0.000		00:1b:77:68:7c:5b	IEEE 8 Acknowledgement
461	0.000	GlobalSu_01:12:c8	00:1b:77:68:7c:5b	IEEE 8 Association Response,SN=2370,FN=0
462	0.000		GlobalSu_01:12:c8	IEEE 8 Acknowledgement

The 802.11 State Machine

- The “State Machine” and its “Classes” is just a complicated way of saying:
- **“You can’t send data through the AP until you authenticate yourself”**
- General flow is:
  1. Find a BSS
  2. Authenticate to the BSS
  3. Associate with the BSS
- <u>Must be in that order</u>
- Can only Associate with One AP at a time



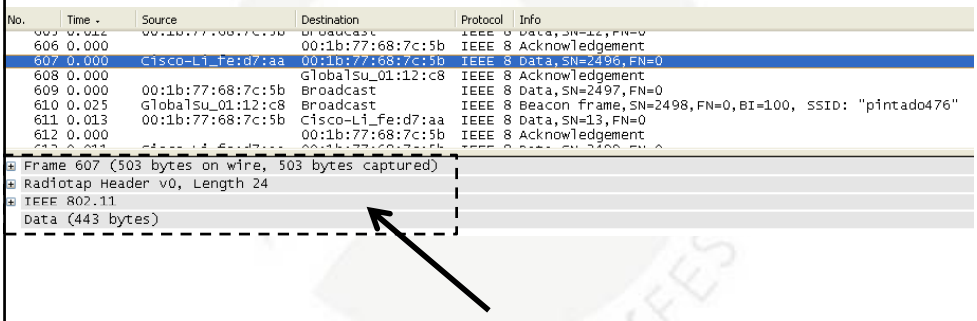
Our Old Friend, the TCP 3-Way Handshake

- Each TCP Data frame is followed by an 802.11 ACK
- If the ACK is not received then the originating station retransmits the frame
- This happens roughly 10 times faster than TCP would recognize

No.	Time	Source	Destination	Bytes	Protocol	Info
6	0.431	192.168.0.11	192.216.124.4	80	TCP	1059 > http [SYN] Seq=0 Len=0 MSS=1460
7	0.000		SymbolTe_9b:b9:aa	10	IEEE 8	Acknowledgement
9	0.094	192.216.124.4	192.168.0.11	80	TCP	http > 1059 [SYN, ACK] Seq=0 Ack=1 Win=8760 Len=0 MSS=1460
10	0.000		SymbolTe_8b:20:1f	10	IEEE 8	Acknowledgement
11	0.001	192.168.0.11	192.216.124.4	72	TCP	1059 > http [ACK] Seq=1 Ack=1 Win=17520 Len=0
12	0.000		SymbolTe_9b:b9:aa	10	IEEE 8	Acknowledgement
13	0.001	192.168.0.11	192.216.124.4	289	HTTP	GET / HTTP/1.1
14	0.000		SymbolTe_9b:b9:aa	10	IEEE 8	Acknowledgement
16	0.098	192.216.124.4	192.168.0.11	78	TCP	http > 1059 [ACK] Seq=1 Ack=218 Win=8760 Len=0
17	0.000		SymbolTe_8b:20:1f	10	IEEE 8	Acknowledgement

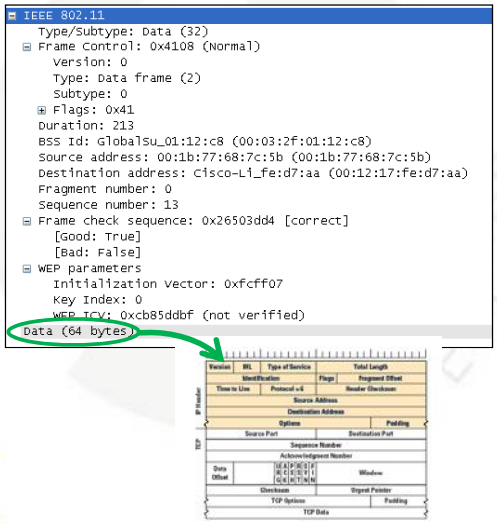
A TCP/IP Data Frame

- The TCP/IP "stuff" is carried by the 802.11 header in exactly the same way it would have been carried by an 802.3 Ethernet header on a wired network
  - The "Frame" and "Radiotap" headers are prepended by Wireshark



IEEE 802.11 Layer 2 Header

- Encrypted data is carried by the unencrypted 802.11 header
  - Addresses are always transmitted as unencrypted data over the air



LLC Is Carried on 802.11 Instead of 802.3

- Unencrypted frames look very much like their Ethernet counterparts

```
⊞ Frame 11 (72 bytes on wire, 72 bytes captured)
⊞ IEEE 802.11
⊞ Logical-Link Control
⊟ Internet Protocol, Src: 192.168.0.11 (192.168.0.11), Dst: 192.216.124.4 (192.216.124.4)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 40
    Identification: 0x0281 (641)
  ⊞ Flags: 0x04 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (0x06)
  ⊞ Header checksum: 0xfabe [correct]
    Source: 192.168.0.11 (192.168.0.11)
    Destination: 192.216.124.4 (192.216.124.4)
⊟ Transmission Control Protocol, Src Port: 1059 (1059), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0
    Source port: 1059 (1059)
    Destination port: http (80)
    Sequence number: 1    (relative sequence number)
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x10 (ACK)
    Window size: 17520
  ⊞ Checksum: 0xa4cd [correct]
  ⊞ [SEQ/ACK analysis]
```

Same Frame – This Time It's Encrypted

```
⊞ Frame 11 (80 bytes on wire, 80 bytes captured)
⊟ IEEE 802.11
    Data Rate: 11.0 Mb/s
    Channel: 11
    Signal Strength: 84%
    Type/Subtype: Data (32)
  ⊞ Frame Control: 0x4108 (Normal)
    Duration: 314
    BSS Id: SymbolTe_8b:20:1f (00:a0:f8:8b:20:1f)
    Source address: SymbolTe_9b:b9:aa (00:a0:f8:9b:b9:aa)
    Destination address: zywelcom_a2:0d:a8 (00:a0:c5:a2:0d:a8)
    Fragment number: 0
    Sequence number: 118
  ⊟ WEP parameters
      Initialization Vector: 0x5d0000
      Key Index: 0
      WEP ICV: 0x80979030 (not verified)
  Data (48 bytes)
```

The Encrypted IP, TCP, and Data Portions of the Frame

```
0000  08 41 3a 01 00 a0 f8 9b  20 1f 00 a0 f8 9b b9 aa   .A:..... .......
0010  00 a0 c5 a2 0d a8 80 07  5d 00 00 00 ef ca 9a 25   ........ ]...O..%
0020  51 3c 80 8a 0f 37 cf a8  28 28 f8 77 b1 8b 6c 71   Q<...%.. (.w..l.
0030  55 ef fe c9 f6 52 8d 56  7b a4 35 67 b0 55 16 00   U....R.V {.5g.U..
0040  01 d1 22 4d 5e cc de 4d  a0 c7 94 52 80 97 30 30   ..."M^..M ...R..F0
```

Dissecting the Key 802.11 Information

- Radiotap Header
  - SSI Levels
  - Channel
  - Data Rate
- 802.11 Header
  - Addresses
  - Sequence Number
  - DS Status
  - Retry
  - Power Management

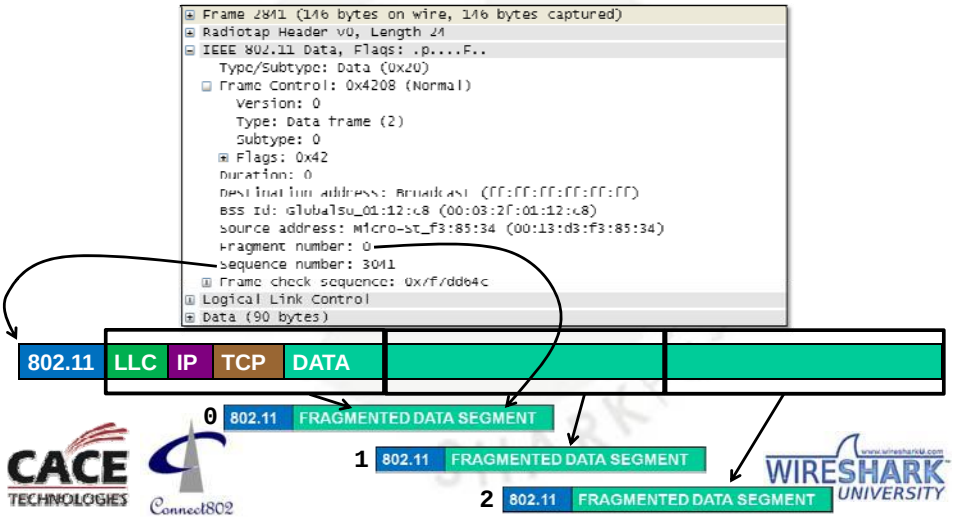
```
⊞ Frame 1162 (138 bytes on wire, 138 bytes captured)
⊟ Radiotap Header v0, Length 24
    Header revision: 0
    Header pad: 0
    Header length: 24
  ⊞ Present flags: 0x000058ee
  ⊞ Flags: 0x10
    Data Rate: 2.0 Mb/s
    Channel: 6
    Channel frequency: 2437
    Channel type: 802.11b (0x00a0)
    SSI Signal: -82 dBm
    SSI Noise: -100 dBm
    Signal Quality: 58
    Antenna: 0
    SSI Signal: 18 dB
    802.11 FCS: 0xa337eb3d [correct]
⊟ IEEE 802.11
    Type/Subtype: Data (32)
  ⊟ Frame Control: 0x0208 (Normal)
      Version: 0
      Type: Data frame (2)
      Subtype: 0
    ⊟ Flags: 0x2
        DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x02)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    Duration: 0
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    BSS Id: MS-NLB-PhysServer-32_a6:b6:9f:10 (02:20:a6:b6:9f:10)
    Source address: 42.39.167.58 (00:12:f0:ed:d2:27)
    Fragment number: 0
    Sequence number: 3736
  ⊞ Frame check sequence: 0xa337eb3d [correct]
⊞ Logical-Link Control
⊞ Internet Protocol, Src: 42.39.167.58 (42.39.167.58), Dst: 42.39.167.59 (42.39.167.59)
⊞ User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
```

Fragmentation

- 802.11 has the ability to fragment frames into smaller chunks before transmission
- Fragments are reassembled by the receiving radio (AP or client)
- Fragmentation specifically addresses cases of intermittent interference, such as microwave ovens
  - Microwaves generate interference in pulses that cycle with the 60 Hz AC current that powers them
  - Fragmented 802.11 frames can slip between these pulses and not be corrupted
- Fragmentation can be enabled in the client utilities or drivers
  - Enabled on AP and/or client individually
  - No functionality to automatically enable/disable, so only enable it on stations that are consistently in the presence of interference

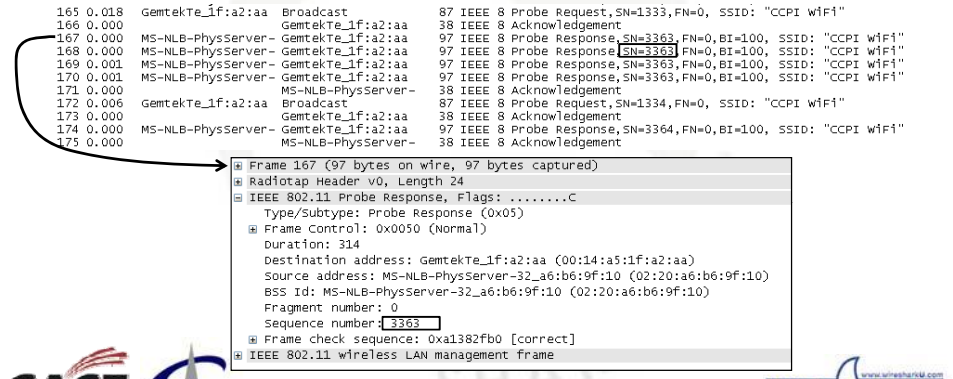
Analyzing Fragmentation with Wireshark

- Each entire TCP/IP frame is assigned a Sequence Number
- Each fragment is assigned a Fragment Number



The 802.11 Retransmission Mechanism

- An ACK is needed to confirm receipt of a frame
- Beacon frames get no ACK
- You don't always see the ACK
  - Or, sometimes all you see is the ACK !



802.11 Power Management

- Low-Power Portable Devices Are Fundamental to the 802.11 Standards
  - Significant thought was put into the standards to accommodate power management
- The Power Management Process
  - When a device is going to 'sleep' it sets the Power Management bit in the last frame transmitted prior to entering Power Save Mode
  - The Access Point queues all frames destined for the device
  - The device 'wakes up' at the next Beacon interval
  - If frames are queued then a bit is set in the Beacon frame's Delivery Traffic Indication Message field (DTIM)
  - The device indicates it's now ready to receive the queued traffic
  - The Access Point sends the queued frames

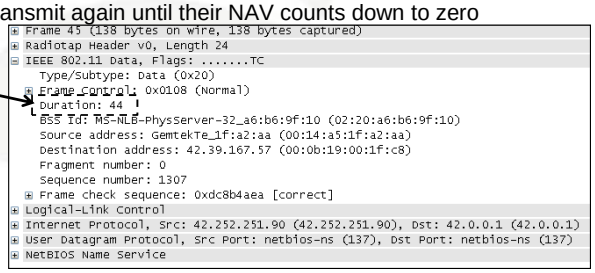
Distributed Coordination Function

- A mechanism by which 802.11 stations (and that includes access points!) coordinate their transmissions
  - If two stations transmit at the same time…
  - On the same channel…
  - Within range of each other…
  - Then corruption will result at the receiver
  - DCF is designed to prevent this from happening
- In 802.11, the DCF implements an algorithm called CSMA/CA
  - Carrier Sense
  - Multiple Access
  - With Collision Avoidance

CSMA/CA

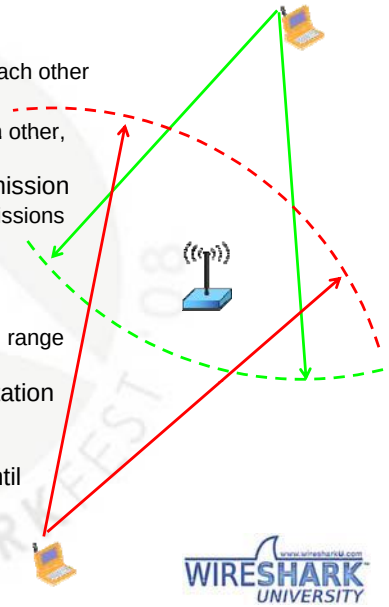
- Step 1: Sense Carrier
  - Physical Carrier Sense (Clear Channel Assessment / CCA)
    - Listen for signal energy coming in off of the radio
    - All stations in a BSS must be able to hear the AP
    - All stations in a BSS are <u>not</u> required to be able to hear each other… and usually they can't!
    - This is called the "Hidden Node Problem," and it is addressed by…
  - Virtual Carrier Sense (Network Allocation Vector / NAV)
    - A mechanism whereby stations can "reserve" the airtime for their transmissions
    - Think of it like a countdown timer
    - Transmitting station "sets" the NAV on other stations
    - Other stations won't transmit again until their NAV counts down to zero

Network Allocation Vector



Hidden Nodes and the RTS/CTS Mechanism

- Occurs in three ways
  - Distance
    - Stations are within range of the AP, but not each other
  - Obstructions
    - Obstacle prevents stations from hearing each other, but both can hear the AP
  - OFDM (802.11g) vs. DSSS (802.11b) transmission
    - 802.11b stations can't decode OFDM transmissions from 802.11g stations
- Addressed by RTS/CTS Mechanism
  - Transmitting station sends RTS frame to AP
    - This frame sets the NAV on all stations within range of the transmitting station
  - AP sends CTS frame back to Transmitting station
    - This frame sets the NAV on all stations within range of the AP
  - Now, all stations within range will be quiet until the data transmission completes



CSMA/CA

- Step 2: Interframe Spacing (IFS)
- A certain minimum period of silence must be observed between each transmission
- IFS length varies depending on the type of frame that a station is attempting to transmit
  - SIFS ("Short" IFS) – Used for frames that must immediately follow a previously-transmitted frame, such as 802.11 ACK in response to 802.11 DATA or CTS in response to RTS.
  - DIFS ("DCF" IFS) – Longer than SIFS. Used for normal data frames when operating in DCF mode
  - Others exist, but SIFS and DIFS are the major ones
- Packets that use a shorter IFS will get priority access to the network when competing against packets that use a longer IFS
  - ACK packets are sent using the SIFS interval

CSMA/CA

- Step 3: Random Backoff Timer
  - Stations' NAV timers are may expire at the same time
  - Many stations are likely to use the same IFS value
  - This means that many stations would transmit at the same time and have a 'collision' at the receiver
- After the NAV expires, after the IFS expires, stations choose a random amount of additional time and wait
- The station that chose the shortest time transmits
- All other stations pause their timer until the transmission completes, the NAV expires, and the IFS expires… again.

And Now For Something Completely Different…

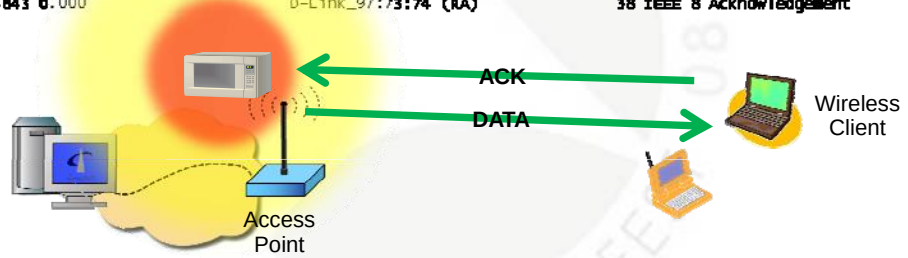
- Point Coordination Function (PCF)
  - A totally obscure supplement to DCF
  - Optional in the 802.11 standard and no manufacturers implement it (that we know of—anybody know of one?)
- The Access Point periodically orders all stations to be quiet!
  - Reserves the airtime using the NAV
- The Access Point then polls certain stations, one at a time, giving them permission to transmit data
  - This is the one case where a station can transmit when its NAV is nonzero
- PCF has the advantage that a subset of stations can get guaranteed, priority access to the network…
  - This can be as fair or unfair as the administrator wants it to be
- But since it is not typically implemented, that advantage is entirely hypothetical :-)

Isolating and Describing a Problem

Trouble Report: Poor Performance and Loss of Connectivity

We see the Data and the Ack but evidently the Access Point doesn't see the Ack

4836	0.000	D-Link_97:73:74	D-Link_4f:f2:21		108	IEEE 8 Data,SN=3946,FN=0
4837	0.000		D-Link_97:73:74	(RA)	38	IEEE 8 Acknowledgement
4838	0.000	D-Link_97:73:74	D-Link_4f:f2:21		108	IEEE 8 Data,SN=3946,FN=0
4839	0.000		D-Link_97:73:74	(RA)	38	IEEE 8 Acknowledgement
4840	0.000	D-Link_97:73:74	D-Link_4f:f2:21		108	IEEE 8 Data,SN=3946,FN=0
4841	0.000		D-Link_97:73:74	(RA)	38	IEEE 8 Acknowledgement
4842	0.001	D-Link_97:73:74	D-Link_4f:f2:21		108	IEEE 8 Data,SN=3946,FN=0
4843	0.000		D-Link_97:73:74	(RA)	38	IEEE 8 Acknowledgement



Practical WLAN Packet-Level Analysis

- Determine the channel of interest and capture from it
- Examine Beacon traffic then eliminate it with a filter
- Examine Probe/Probe-Response traffic
- Follow station authentication and association behavior
- Look for atypical configurations (PCF, non-10ms Beacons, etc.)
- Look for 802.11 retransmissions and isolate whether the data or the Ack is being lost
- Track physical packet flow to and from the distribution system (focusing on the BSSID in the ESS as compared to the Ethernet addressing
- Track and overlay the IP logical data flow on top of the physical packet flow assessment to ascertain validity (and to pay attention to TCP sequence and acknowledgment.)

Thank You !

- For more information on Connect802's services and products, please visit: www.Connect802.com/info
  - Watch a video showing how 3-dimensional RF CAD modeling is performed
  - Get sample system design reports
  - Find out more about who we are and how we might be able to be a resource for you.
- From our home page (www.Connect802.com) explore the Literature tab to find:
  - "Wi-Fi: Just the Facts"
    - Technical discussions that put 802.11 into perspective
  - The Connect802 On-Line Encyclopedia
    - A compendium of 802.11 information
  - "Wireless Connectivity Update"
    - Archives of our quarterly technical update newsletter

joe@Connect802.com
(925) 552-0802