

Wireshark Saves the WLAN!

A WLAN Case Study

June 2009

Joseph Bardwell

Chief Scientist, Connect802 Corporation

www.Connect802.com

joe@connect802.com

SHARKFEST '09

Stanford University

June 15-18, 2009



- Connect802 was contracted to provide design, RF spectrum analysis and post-installation verification services for a client's major Cisco 802.11n deployment
- Both because 802.11n is an emerging technology and because we differentiate ourselves through our rigorous engineering methodology we were exceptionally diligent in the planning and design of the network
- We performed extensive on-site equipment testing
- We created a 3-dimensional RF CAD model of the facility
- We performed signal coverage predictions to optimize access point placement and to assure that the installed system would meet the design specifications
- We confirmed our predictive RF CAD designs through on-site testing
- Our client installed the pilot network (the first of over 100 buildings)
- The client reported that the network didn't work
- We found that signal strength remained at and above the specified levels
- The wireless LAN controller showed that all access points were operational
- Throughput testing confirmed that every three minutes the network would stop passing user traffic



Preparing for a Troubleshooting Effort



***You have to know that you know
what you think you know so you
can know how to know what
you don't know.***

Careful Quantification of Equipment and Project Specifications



DESIGN SPECIFICATIONS

For 4 GHz, 802.11b/g operation, the present design provides -75 dBm signal strength throughout the specified coverage area measured at a height of 4 feet above the floor. At this signal level, manufacturer's data sheets for the equipment indicate that it will connect at 48 Mbps 802.11b/g modulation and at least Mbps 6 modulation with 802.11n. To achieve this result, predictive RF CAD models have been created that require a target design signal strength of -62 dBm. This target signal strength is depicted on Grid Coverage Model in the present report using the color legend shown to the right.

Regulated Air Standards	802.11b/g/n
Unmuted Average Background Noise and Interference	-95 dBm
Access Point Transmit Power	14 dBm (25 mW)
Access Point Antenna Gain	3 dBi
Access Point Cable/Connector Loss	0.5 dB
Access Point Cordy Loss	3 dB
Resulting Access Point EIRP	13.5 dBm
Client Device Transmit Power	14.5 dBm (28.8 mW)
Client Device Antenna Gain	2.2 dBi
Client Device Cable/Connector Loss	0 dB
Client Device Cordy Loss	0 dB
Resulting Client Device EIRP	16.7 dBm

Specified Minimum RSSI for Real-World Implementation	-75 dBm
Resulting Signal-to-Noise-Ratio (SNR)	20 dB
Minimum Modulation Rate at Specified Minimum RSSI	48 Mbps
Coverage Cell Overlap Boundary RSSI (Calculated)	-78 dBm
Coverage Cell Overlap Percentage (Specified)	20%
Coverage Cell Overlap Factor (Calculated)	1.9 dB
Design Body Loss	3 dB
Fade Margin	10 dB
Modulation Rate in Best Case (0 dB Fading)	54 Mbps
Resulting Current Design Target RSSI for Predictive Models	-62 dBm

Color Legend:

- Red: >= 50.00 dBm
- Orange: >= 52.00 dBm
- Yellow: >= 54.00 dBm
- Light Green: >= 56.00 dBm
- Green: >= 58.00 dBm
- Dark Green: >= 60.00 dBm
- Blue: >= 62.00 dBm
- Light Blue: >= 64.00 dBm
- Medium Blue: >= 66.00 dBm
- Dark Blue: >= 68.00 dBm
- Very Dark Blue: >= 70.00 dBm
- Black: >= 72.00 dBm
- Dark Grey: >= 74.00 dBm
- Medium Grey: >= 76.00 dBm
- Light Grey: >= 78.00 dBm
- White: >= 80.00 dBm

ORIGINAL DRAWING FILES

Drawing files were provided in standard AutoCAD format. Antenna locations for the design being considered were indicated using standard CAD symbols. A 3-dimensional, virtual building model was created from these plans where each interior and exterior wall, partition, and indicated obstruction was formatted to represent its correct RF characteristics.

EQUIPMENT SPECIFICATIONS

1252 802.11a/b/g/n Access Point

designed for use with ANT2430 and ANT5140 element external antennas.

- Antenna: 802.11a, 17 dBm with 1 antenna
- Antenna: 802.11n non-HT duplicate (802.11a duplicate mode), 17 dBm with 1 antenna
- Antenna: 802.11n (HT20), 20 dBm with 1 antenna
- Antenna: 802.11n (HT40), 20 dBm with 2 antennas
- Antenna: 802.11n (HT40), 17 dBm with 1 antenna
- Antenna: 802.11n (HT40), 20 dBm with 2 antennas

Maximum Transmit Power:

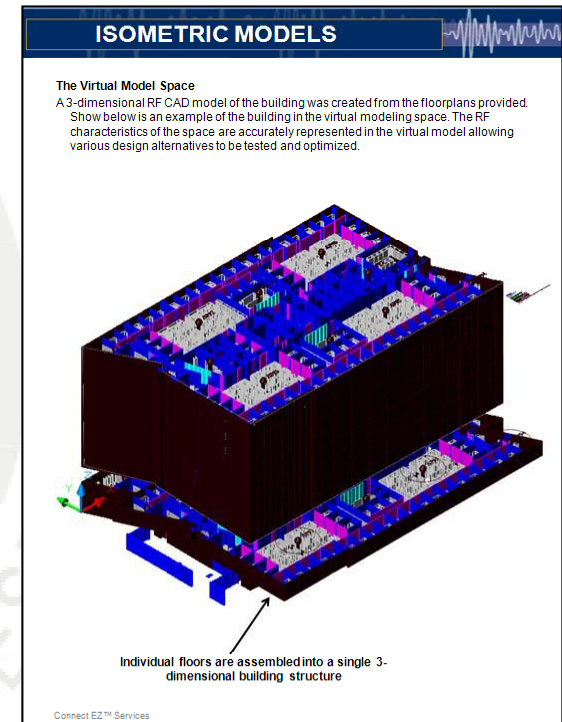
Signal	802.11a	802.11g
802.11a @ 1 Mbps	-67 dBm @ 6 Mbps	-67 dBm @ 6 Mbps
802.11a @ 2 Mbps	-65 dBm @ 9 Mbps	-65 dBm @ 9 Mbps
802.11a @ 5.5 Mbps	-62 dBm @ 12 Mbps	-62 dBm @ 12 Mbps
802.11a @ 11 Mbps	-60 dBm @ 18 Mbps	-60 dBm @ 18 Mbps
802.11g @ 6 Mbps	-61 dBm @ 24 Mbps	-61 dBm @ 24 Mbps
802.11g @ 9 Mbps	-59 dBm @ 36 Mbps	-59 dBm @ 36 Mbps
802.11g @ 12 Mbps	-57 dBm @ 54 Mbps	-57 dBm @ 54 Mbps

Supported Data Rates:

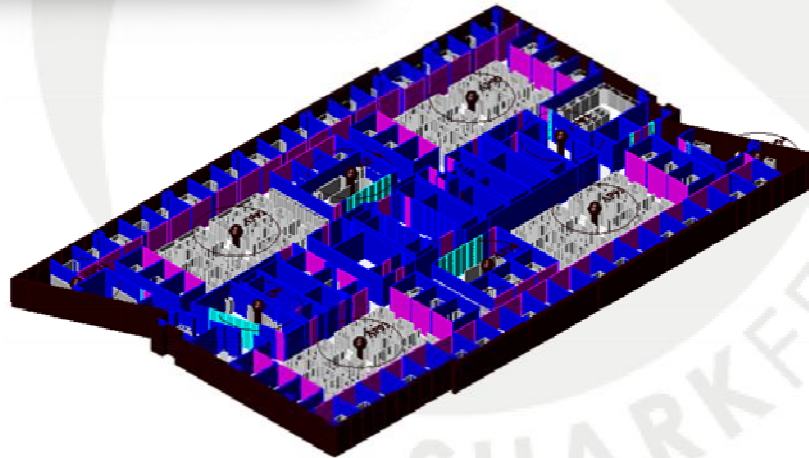
802.11a/b/g/n (2.4 GHz and 5 GHz)	QPSK	BPSK	QPSK	40 MHz Rate (Mbps)
0	0.5	13.5	7.2	15
1	1.5	4.5	14.4	30
2	16.5	48.5	21.7	45
3	26	54	28.8	60
4	36	63	43.3	90
5	52	108	57.8	120
6	58.5	121.5	65	135
7	66	135	72.2	157.5
8	73	27	14.4	30
9	26	54	28.8	60
10	36	63	43.3	90
11	52	108	57.8	120
12	58.5	121.5	65	135
13	79	162	86.7	180
14	104	216	115.9	240
15	117	243	130	270
16	135	270	144.4	300

Wireshark will report information concerning WLAN performance. You have to know whether this is good or bad, expected or unexpected.

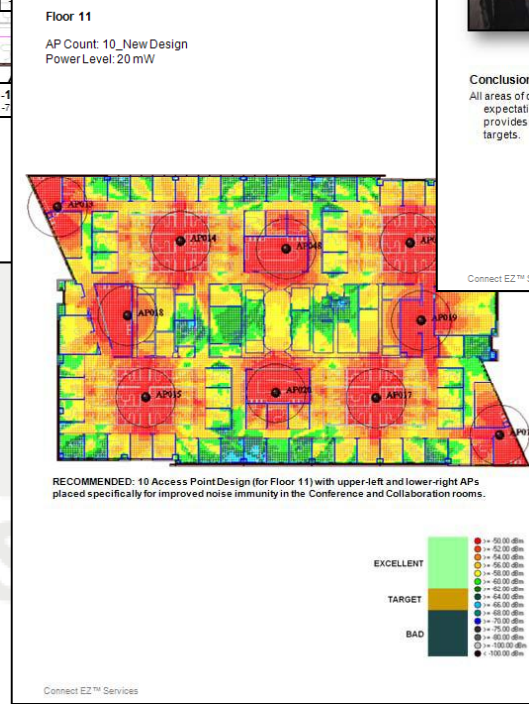
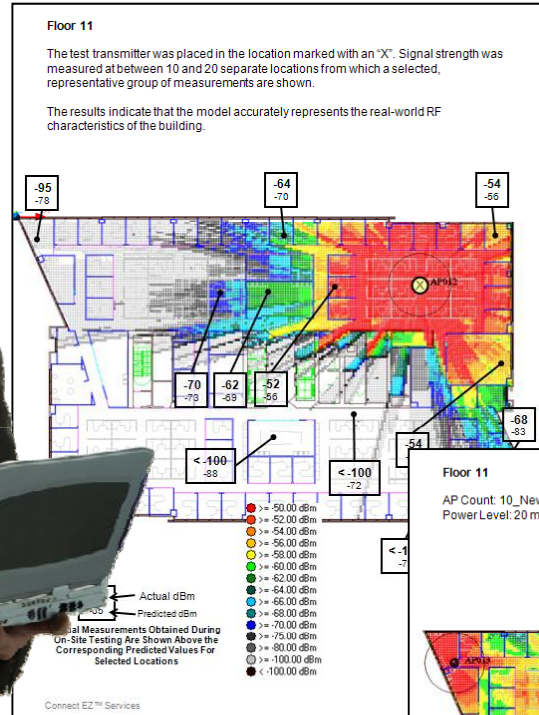
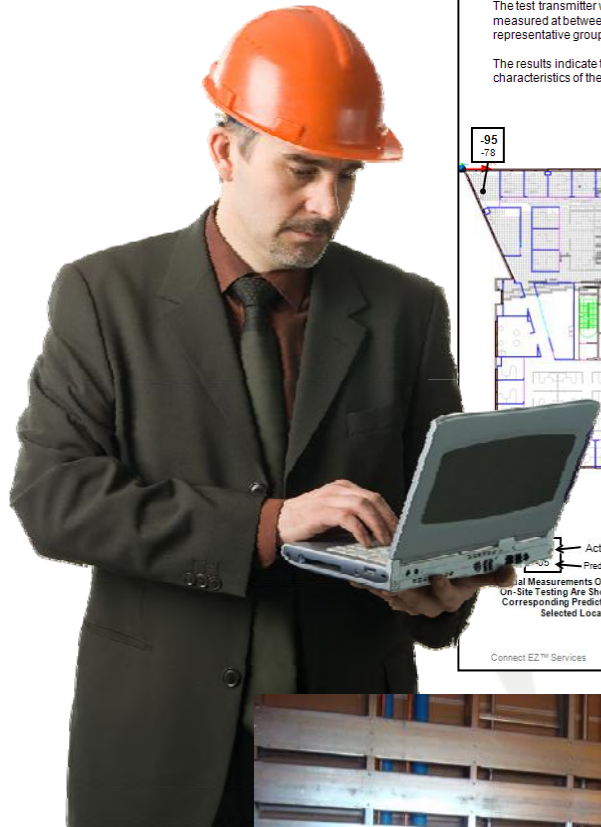
3-Dimensional RF CAD Modeling and Simulation



You have to be sure that your WLAN design will perform as expected.



Real-World Testing and Design Calibration



CISCO 1252 REAL-WORLD TESTING

The Portable Test Rig

As shown in the photo to the right, a portable test rig was assembled to allow moving a Cisco 1252 access point with a horizontally-mounted ANT5140 5.8 GHz antenna to various test locations in the building.

The access point was configured in Autonomous Mode with a test SSID so that it could be readily identified during scanning and signal strength measurement.

Shown below is the testing rig in a cubicle area while the on-site engineer evaluated signal coverage in areas of concern.

Conclusions

All areas of concern were examined and found to have signal coverage that exceeded the expectations for the design. This confirms the accuracy of the RF predictive CAD models and provides additional confirmation that the installed system will meet or exceed the design targets.

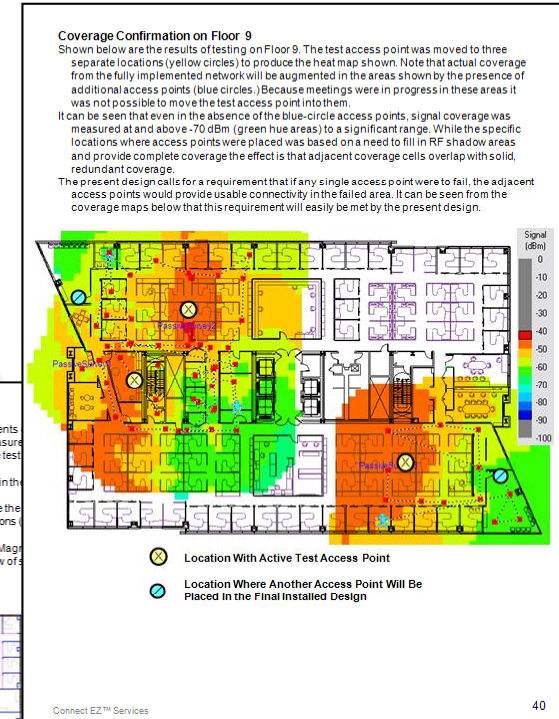
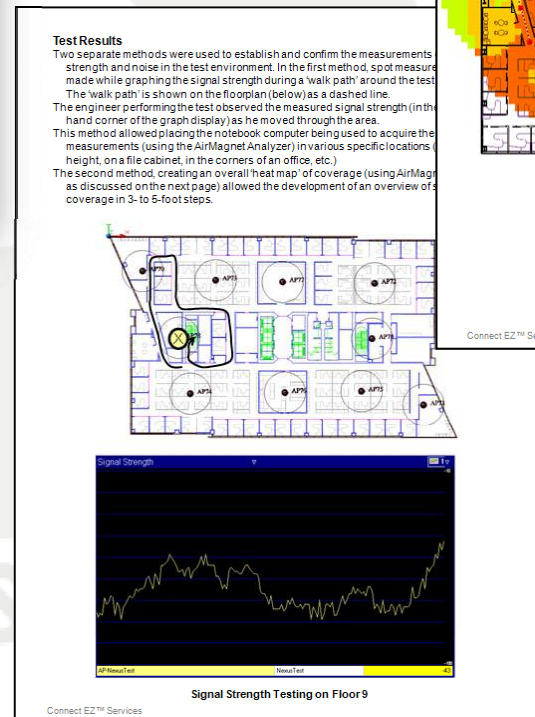
Connect EZ™ Services



Design Review with Client



Stakeholders must be on-board with the system and design specifications so that you have a “line-in-the-sand” to differentiate acceptable versus unacceptable behavior and performance.




Careful On-Site Spectrum Analysis

You have to be sure that background noise or interference isn't going to impact the behavior of your network. Wireshark will show you 802.11 retransmissions and packets with CRC errors – both indicative of RF noise or interference problems.

ORIGINAL DRAWING FILES

Drawing files were provided in standard AutoCAD format. Antenna locations for the design being considered were indicated using standard CAD symbols.

A 3-dimensional, virtual building model was created from these plans where each interior and exterior wall, partition, and indicated obstruction was formatted to represent its correct RF characteristics.



Connect EZ™ Services

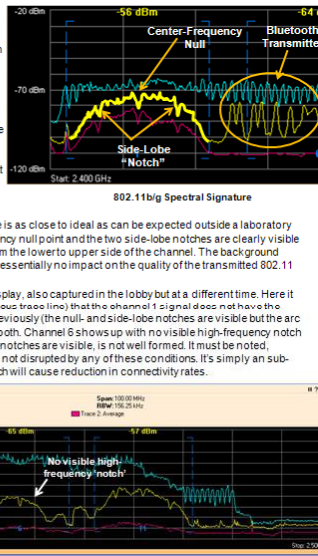
Assessing the 802.11 Spectral Signature

To the right is a detailed inset taken from the FFT display presented previously. Although the Bluetooth transmitter has a higher maximum signal strength than the 802.11 transmitter the 802.11 transmission is actually optimal.

An IEEE 802.11b/g network is comprised of periodic access point beacon packets. These are transmitted using the least-common-denominator modulation technique consistent with 802.11b. As such, the spectral signature for the network is well known.

The spectral signature seen above is as close to ideal as can be expected outside a laboratory environment. The center-frequency null point and the two side-lobe notches are clearly visible across an even arc of signal from the lower to upper side of the channel. The background noise, in this specific case, had essentially no impact on the quality of the transmitted 802.11 signal.

Shown below is a different FFT display, also captured in the lobby but at a different time. Here it can be seen (yellow, instantaneous trace line) that the channel 1 signal does not have the same level of quality as it did previously (the null- and side-lobe notches are visible but the arc of transmission is no longer smooth. Channel 6 shows up with no visible high-frequency notch and channel 11, while the three notches are visible, is not well formed. It must be noted, however, that communication is not disrupted by any of these conditions. It's simply an sub-optimal signal environment which will cause reduction in connectivity rates.



IMPORTANT NOTE: This information is being presented as a perspective on the RF environment and to present the methodology and analytical rigor applied to the analysis. Nothing presented here is indicative of a problematic condition demanding specific mitigation.

Connect EZ™ Services

2.4 GHz in Conference Room – Floor 11

Cordless Phone Interference

In the conference room near the elevator lobby the RF spectrum was consistent with that observed in the main building lobby. There is a cordless phone visible as the sawtooth blue spiking across the top and the 802.11 'humps' are poorly formed. Noise (particularly the Bluetooth and cordless phones) is causing performance problems in the 2.4 GHz frequency band.



As shown and discussed for the ground floor lobby area, the 802.11a spectrum on the 11th floor remained very noise and interference free. The trace to the right shows the FFT display from the 11th floor Main Conference Room.

Floor 11 5.8 GHz 802.11a/n Band

Connect EZ™ Services

Knowing What You Know...

- You have to understand how RF issues can impact WLAN performance and operation
- You have to understand 802.11 protocol behavior
 - Client Association
- You have to understand L2 and L3 initialization behavior
 - DHCP (and possibly VLAN to SSID mapping)
 - RADIUS Authentication (EAP)
 - Possibility of Captive Portal Authentication
- Once the client is Associated and Authenticated, everything else is conventional Ethernet packet analysis



An Idle 802.11 Wireless LAN

No.	Time	Source	Destination	Bytes	Protocol	Info
267	0.102	GlobalSu_01:12:c8	Broadcast	91	IEEE 802.11	Beacon frame, SN=2187, FN=0, Flags=.....C, BI=100, SSID="pintado476"
268	0.102	GlobalSu_01:12:c8	Broadcast	91	IEEE 802.11	Beacon frame, SN=2188, FN=0, Flags=.....C, BI=100, SSID="pintado476"
269	0.102	GlobalSu_01:12:c8	Broadcast	91	IEEE 802.11	Beacon frame, SN=2189, FN=0, Flags=.....C, BI=100, SSID="pintado476"
270	0.102	GlobalSu_01:12:c8	Broadcast	91	IEEE 802.11	Beacon frame, SN=2190, FN=0, Flags=.....C, BI=100, SSID="pintado476"
271	0.102	GlobalSu_01:12:c8	Broadcast	91	IEEE 802.11	Beacon frame, SN=2191, FN=0, Flags=.....C, BI=100, SSID="pintado476"
272	0.102	GlobalSu_01:12:c8	Broadcast	91	IEEE 802.11	Beacon frame, SN=2192, FN=0, Flags=.....C, BI=100, SSID="pintado476"
273	0.102	GlobalSu_01:12:c8	Broadcast	91	IEEE 802.11	Beacon frame, SN=2193, FN=0, Flags=.....C, BI=100, SSID="pintado476"
274	0.102	GlobalSu_01:12:c8	Broadcast	91	IEEE 802.11	Beacon frame, SN=2194, FN=0, Flags=.....C, BI=100, SSID="pintado476"
275	0.102	GlobalSu_01:12:c8	Broadcast	91	IEEE 802.11	Beacon frame, SN=2195, FN=0, Flags=.....C, BI=100, SSID="pintado476"
276	0.102	GlobalSu_01:12:c8	Broadcast	91	IEEE 802.11	Beacon frame, SN=2196, FN=0, Flags=.....C, BI=100, SSID="pintado476"
277	0.102	GlobalSu_01:12:c8	Broadcast	91	IEEE 802.11	Beacon frame, SN=2197, FN=0, Flags=.....C, BI=100, SSID="pintado476"
278	0.102	GlobalSu_01:12:c8	Broadcast	91	IEEE 802.11	Beacon frame, SN=2198, FN=0, Flags=.....C, BI=100, SSID="pintado476"
279	0.102	GlobalSu_01:12:c8	Broadcast	91	IEEE 802.11	Beacon frame, SN=2199, FN=0, Flags=.....C, BI=100, SSID="pintado476"
280	0.102	GlobalSu_01:12:c8	Broadcast	91	IEEE 802.11	Beacon frame, SN=2200, FN=0, Flags=.....C, BI=100, SSID="pintado476"
281	0.102	GlobalSu_01:12:c8	Broadcast	91	IEEE 802.11	Beacon frame, SN=2201, FN=0, Flags=.....C, BI=100, SSID="pintado476"
282	0.102	GlobalSu_01:12:c8	Broadcast	91	IEEE 802.11	Beacon frame, SN=2202, FN=0, Flags=.....C, BI=100, SSID="pintado476"
283	0.102	GlobalSu_01:12:c8	Broadcast	91	IEEE 802.11	Beacon frame, SN=2203, FN=0, Flags=.....C, BI=100, SSID="pintado476"
284	0.102	GlobalSu_01:12:c8	Broadcast	91	IEEE 802.11	Beacon frame, SN=2204, FN=0, Flags=.....C, BI=100, SSID="pintado476"

```
Frame 1 (91 bytes on wire, 91 bytes captured)
Radiotap Header v0, Length 24
IEEE 802.11 Beacon frame, Flags: .....C
  Type/Subtype: Beacon frame (0x08)
    Frame Control: 0x0080 (Normal)
      Version: 0
      Type: Management frame (0)
      Subtype: 8
      Flags: 0x0
        DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x00)
          .... 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)
        Source address: GlobalSu_01:12:c8 (00:03:2f:01:12:c8)
        BSS Id: GlobalSu_01:12:c8 (00:03:2f:01:12:c8)
        Fragment number: 0
        Sequence number: 1928
      Frame check sequence: 0xe518a114 [correct]
    IEEE 802.11 wireless LAN management frame
      Fixed parameters (12 bytes)
        Timestamp: 0x0000008c15540258
        Beacon Interval: 0.102400 [Seconds]
      Capability Information: 0x0011
      Tagged parameters (27 bytes)
        SSID parameter set: "pintado476"
        Supported Rates: 1.0(B) 2.0(B) 5.5(B) 11.0(B)
        DS Parameter set: Current Channel: 6
        Traffic Indication Map (TIM): DTIM 0 of 2 bitmap empty
```

Checking RF Characteristics with Wireshark

```
[-] Radiotap Header v0, Length 24
  Header revision: 0
  Header pad: 0
  Header length: 24
  Present flags: 0x000058ee
  Flags: 0x10
  Data Rate: 1.0 Mb/s
  Channel frequency: 2437 [BG 6]
  Channel type: 802.11b (0x00a0)
  SSI Signal: -52 dBm
  SSI Noise: -100 dBm
  Signal Quality: 100
  Antenna: 0
  SSI Signal: 48 dB
  802.11 FCS: 0xb2331546 [correct]
```

Beacon Frames are always transmitted at the lowest data rate for the air standard:

- 802.11b 1 Mbps**
- 802.11b/g Mixed Mode 1 Mbps**
- 802.11g Greenfield 6 Mbps**
- 802.11a 6 Mbps**
- 802.11b/g/n Mixed Mode 1 Mbps**
- 802.11g/n Mixed Mode 6 Mbps**

Signal-to-Noise Ratio (SNR)

The difference between Signal and Noise:

- > 30 dB Excellent!**
- > 20 dB No Worries**
- < 15 dB Worry.**
- < 10 dB Bad Thing!**

Signal Strength Indicator values provide an indication of power, not of quality:

- > -65 dBm Excellent!**
- > -75 dBm No Worries**
- > -80 dBm Acceptable for**

Web/Email

< -80 dBm

On the Edge – Be Careful



Normal Client Association Behavior

```
452 0.057 IntelCor_68:7c:5b Broadcast 80 IEEE 8(Probe Request, SN=0, FN=0, Flags=.....C, SSID="pintado476"
453 0.001 GlobalSu_01:12:c8 IntelCor_68:7c:5b 85 IEEE 8(Probe Response, SN=2368, FN=0, Flags=.....C, BI=100, SSID="pintado476"
454 0.000 GlobalSu_01:12:c8 GlobalSu_01:12:c8 38 IEEE 8(Acknowledgement, Flags=.....C
455 0.013 IntelCor_68:7c:5b GlobalSu_01:12:c8 58 IEEE 8(Authentication, SN=0, FN=0, Flags=.....C
456 0.000 IntelCor_68:7c:5b IntelCor_68:7c:5b 38 IEEE 8(Acknowledgement, Flags=.....C
457 0.000 GlobalSu_01:12:c8 IntelCor_68:7c:5b 58 IEEE 8(Authentication, SN=2369, FN=0, Flags=.....C
458 0.000 GlobalSu_01:12:c8 GlobalSu_01:12:c8 38 IEEE 8(Acknowledgement, Flags=.....C
459 0.000 IntelCor_68:7c:5b GlobalSu_01:12:c8 74 IEEE 8(Association Request, SN=1, FN=0, Flags=.....C, SSID="pintado476"
460 0.000 IntelCor_68:7c:5b IntelCor_68:7c:5b 38 IEEE 8(Acknowledgement, Flags=.....C
461 0.000 GlobalSu_01:12:c8 IntelCor_68:7c:5b 64 IEEE 8(Association Response, SN=2370, FN=0, Flags=.....C
462 0.000 GlobalSu_01:12:c8 GlobalSu_01:12:c8 38 IEEE 8(Acknowledgement, Flags=.....C
469 0.110 Micro-St_f3:85:34 Broadcast 146 LLC I, N(R)=0, N(S)=0; DSAP ISO Network Layer Group, SSAP NULL LSAP Command
477 0.041 Micro-St_f3:85:34 Broadcast 146 LLC I, N(R)=0, N(S)=0; DSAP ISO Network Layer Group, SSAP NULL LSAP Command
503 0.021 IntelCor_68:7c:5b Broadcast 396 LLC I, N(R)=0, N(S)=0; DSAP 0x1e Group, SSAP NULL LSAP Command
```

Probe / Probe-Response / Ack

Authentication Request / Ack

Authentication Response / Ack

Association Request / Ack

Association Response / Ack

Data (Which could be AAA credential exchange and verification)

Raw Captured Data from the Troubleshooting Scenario

```
1529 0.000 Cisco_78:cc:8a Apple_d8:c9:c4 (R 10 IEEE 8(Acknowledgement, Flags=.....
1530 0.030 Cisco_78:cc:8a Broadcast 224 IEEE 8(Beacon frame, SN=357, FN=0, Flags=....., BI=102, SSID="test"
1531 0.014 Apple_d8:c9:c4 (T Cisco_78:cc:8a (R 16 IEEE 8(Request-to-send, Flags=.....
1532 0.000 Apple_d8:c9:c4 (R 10 IEEE 8(Clear-to-send, Flags=.....
1533 0.000 Apple_d8:c9:c4 IPv6mcast_00:00:0 106 LLC I, N(R)=16, N(S)=0; DSAP 0xa4 Group, SSAP NULL LSAP Command
1534 0.000 Cisco_78:cc:8a (T Apple_d8:c9:c4 (R 28 IEEE 8(802.11 Block Ack, Flags=.....
1535 0.000 Apple_d8:c9:c4 Cisco_78:cc:8a 24 IEEE 8(Null function (No data), SN=512, FN=0, Flags=.....T
1536 0.000 Apple_d8:c9:c4 (R 10 IEEE 8(Acknowledgement, Flags=.....
1537 0.089 Cisco_78:cc:8a Broadcast 224 IEEE 8(Beacon frame, SN=358, FN=0, Flags=....., BI=102, SSID="test"
1538 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8(Beacon frame, SN=359, FN=0, Flags=....., BI=102, SSID="test"
1539 0.043 Apple_d8:c9:c4 Cisco_78:cc:8a 24 IEEE 8(Null function (No data), SN=513, FN=0, Flags=...P...T
1540 0.000 Apple_d8:c9:c4 (R 10 IEEE 8(Acknowledgement, Flags=.....
1541 0.002 Cisco-Li_a7:24:f6 Broadcast 139 IEEE 8(Probe Request, SN=3, FN=0, Flags=....., SSID="\327m\0330F\362P\204\263\261DR\210\267\341\2
1542 0.030 Cisco-Li_a7:24:f6 Broadcast 139 IEEE 8(Probe Request, SN=4, FN=0, Flags=....., SSID="\327m\0330F\362P\204\263\261DR\210\267\341\2
1543 0.027 Cisco_78:cc:8a Broadcast 224 IEEE 8(Beacon frame, SN=360, FN=0, Flags=....., BI=102, SSID="test"
1544 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8(Beacon frame, SN=361, FN=0, Flags=....., BI=102, SSID="test"
1545 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8(Beacon frame, SN=362, FN=0, Flags=....., BI=102, SSID="test"
1546 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8(Beacon frame, SN=363, FN=0, Flags=....., BI=102, SSID="test"
1547 0.103 Apple_d8:c9:c4 (T Cisco_78:cc:8a (R 16 IEEE 8(Request-to-send, Flags=.....
1548 0.000 Apple_d8:c9:c4 (R 10 IEEE 8(Clear-to-send, Flags=.....
1549 0.000 Apple_d8:c9:c4 Cisco_39:9b:40 1538 LLC I, N(R)=16, N(S)=0; DSAP 0xa6 Individual, SSAP NULL LSAP Command
1550 0.000 Apple_d8:c9:c4 Cisco_78:cc:8a 24 IEEE 8(Null function (No data), SN=514, FN=0, Flags=.....T
1551 0.000 Apple_d8:c9:c4 (R 10 IEEE 8(Acknowledgement, Flags=.....
1552 0.000 Cisco_78:cc:8a Broadcast 224 IEEE 8(Beacon frame, SN=364, FN=0, Flags=....., BI=102, SSID="test"
1553 0.000 Apple_d8:c9:c4 (T Cisco_78:cc:8a (R 16 IEEE 8(Request-to-send, Flags=.....
1554 0.000 Apple_d8:c9:c4 (R 10 IEEE 8(Clear-to-send, Flags=.....
1555 0.000 Cisco_78:cc:8a (T Apple_d8:c9:c4 (R 28 IEEE 8(802.11 Block Ack, Flags=.....
1556 0.003 Cisco_39:9b:40 Apple_d8:c9:c4 1538 LLC I, N(R)=16, N(S)=0; DSAP 0x56 Individual, SSAP NULL LSAP Command
1557 0.000 Apple_d8:c9:c4 (T Cisco_78:cc:8a (R 28 IEEE 8(802.11 Block Ack, Flags=.....
1558 0.205 Cisco_78:cc:8a Broadcast 224 IEEE 8(Beacon frame, SN=366, FN=0, Flags=....., BI=102, SSID="test"
1559 0.048 Apple_d8:c9:c4 Cisco_78:cc:8a 24 IEEE 8(Null function (No data), SN=515, FN=0, Flags=...P...T
1560 0.000 Apple_d8:c9:c4 (R 10 IEEE 8(Acknowledgement, Flags=.....
1561 0.056 Cisco_78:cc:8a Broadcast 224 IEEE 8(Beacon frame, SN=367, FN=0, Flags=....., BI=102, SSID="test"
1562 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8(Beacon frame, SN=368, FN=0, Flags=....., BI=102, SSID="test"
1563 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8(Beacon frame, SN=369, FN=0, Flags=....., BI=102, SSID="test"
1564 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8(Beacon frame, SN=370, FN=0, Flags=....., BI=102, SSID="test"
1565 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8(Beacon frame, SN=371, FN=0, Flags=....., BI=102, SSID="test"
1566 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8(Beacon frame, SN=372, FN=0, Flags=....., BI=102, SSID="test"
1567 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8(Beacon frame, SN=373, FN=0, Flags=....., BI=102, SSID="test"
1568 0.054 Apple_d8:c9:c4 (T Cisco_78:cc:8a (R 16 IEEE 8(Request-to-send, Flags=.....
1569 0.000 Apple_d8:c9:c4 (R 10 IEEE 8(Clear-to-send, Flags=.....
1570 0.000 Apple_d8:c9:c4 Cisco_39:9b:40 1538 LLC I, N(R)=16, N(S)=0; DSAP 0xa6 Group, SSAP NULL LSAP Command
1571 0.000 Cisco_78:cc:8a (T Apple_d8:c9:c4 (R 28 IEEE 8(802.11 Block Ack, Flags=.....
1572 0.000 Apple_d8:c9:c4 Cisco_78:cc:8a 24 IEEE 8(Null function (No data), SN=516, FN=0, Flags=.....T
1573 0.000 Apple_d8:c9:c4 (R 10 IEEE 8(Acknowledgement, Flags=.....
```

Filtering to Select Only Beacon Frames

No. -	Time	Source	Destination	Bytes	Protocol	Info
1529	0.000		Apple_d8:c9:c4 (R	10	IEEE 8	(Acknowledgement, Flags=.....
1530	0.030	Cisco_78:cc:8a	Broadcast	224	IEEE 8	(Beacon frame, SN=357, FN=0, Flags=....., BI=102, SSID="test'
1531	0.014	Apple_d8:c9:c4 (T	Cisco_78:cc:8a (R	16	IEEE 8	(Request-to-send, Flags=.....
1532	0.000		Apple_d8:c9:c4 (R	10	IEEE 8	(Clear-to-send, Flags=.....
1533	0.000	Apple_d8:c9:c4	IPv6mcast_00:00:0	106	LLC	I, N(R)=16, N(S)=0; DSAP 0xa4 Group, SSAP NULL LSAP Command
1534	0.000	Cisco_78:cc:8a (T	Apple_d8:c9:c4 (R	28	IEEE 8	(802.11 Block Ack, Flags=.....
1535	0.000	Apple_d8:c9:c4	Cisco_78:cc:8a	24	IEEE 8	(Null function (No data), SN=512, FN=0, Flags=.....T
1536	0.000		Apple_d8:c9:c4 (R	10	IEEE 8	(Acknowledgement, Flags=.....
1537	0.089	Cisco_78:cc:8a	Broadcast	224	IEEE 8	(Beacon frame, SN=358, FN=0, Flags=....., BI=102, SSID="test'
1538	0.104	Cisco_78:cc:8a	Broadcast	224	IEEE 8	(Beacon frame, SN=359, FN=0, Flags=....., BI=102, SSID="test'
1539	0.043	Apple_d8:c9:c4	Cisco_78:cc:8a	24	IEEE 8	(Null function (No data), SN=513, FN=0, Flags=...P...T
1540	0.000		Apple_d8:c9:c4 (R	10	IEEE 8	(Acknowledgement, Flags=.....
1541	0.002	Cisco-Li_a7:24:f6	Broadcast	139	IEEE 8	(Probe Request, SN=3, FN=0, Flags=....., SSID="\327m\0330F\3f
1542	0.030	Cisco-Li_a7:24:f6	Broadcast	139	IEEE 8	(Probe Request, SN=4, FN=0, Flags=....., SSID="\327m\0330F\3f
1543	0.027	Cisco_78:cc:8a	Broadcast	224	IEEE 8	(Beacon frame, SN=360, FN=0, Flags=....., BI=102, SSID="test'
1544	0.104	Cisco_78:cc:8a	Broadcast	224	IEEE 8	(Beacon frame, SN=361, FN=0, Flags=....., BI=102, SSID="test'
1545	0.104	Cisco_78:cc:8a	Broadcast	224	IEEE 8	(Beacon frame, SN=362, FN=0, Flags=....., BI=102, SSID="test'
1546	0.104	Cisco_78:cc:8a	Broadcast	224	IEEE 8	(Beacon frame, SN=363, FN=0, Flags=....., BI=102, SSID="test'
1547	0.103	Apple_d8:c9:c4 (T	Cisco_78:cc:8a (R	16	IEEE 8	(Request-to-send, Flags=.....
1548	0.000		Apple_d8:c9:c4 (R	10	IEEE 8	(Clear-to-send, Flags=.....

Frame 1538 (224 bytes on wire, 224 bytes captured)

IEEE 802.11 Beacon frame, Flags:

Type/Subtype: Beacon frame (0x08)

Frame Control: 0x0080 (Normal)

Version: 0

Type: Management frame (0)

Subtype: 8

Flags: 0x0

DS status: Not leaving DS or network is open

.... .0.. = More Fragments: This is the last

.... 0... = Retry: Frame is not being retr

...0 = PWR MGT: STA will stay up

..0. = More Data: No data buffered

.0.. = Protected flag: Data is not prot

0... = Order flag: Not strictly order

Duration: 0

Destination address: Broadcast (ff:ff:ff:ff:ff:ff)

Source address: Cisco_78:cc:8a (00:23:5e:78:cc:8a)

BSS Id: Cisco_78:cc:8a (00:23:5e:78:cc:8a)

Fragment number: 0

Sequence number: 359

IEEE 802.11 wireless LAN management frame

Fixed parameters (12 bytes)

- Expand Subtrees
- Expand All
- Collapse All
- Apply as Filter
- Prepare a Filter
- Colorize with Filter
- Follow TCP Stream
- Follow UDP Stream
- Follow SSL Stream
- Copy
- Export Selected Packet Bytes...
- Wiki Protocol Page
- Filter Field Reference
- Protocol Preferences...
- Decode As...
- Disable Protocol...
- Resolve Name
- Go to Corresponding Packet

- Selected
- Not Selected
- ... and Selected
- ... or Selected
- ... and not Selected
- ... or not Selected

From DS: 0) (0x00)

Configure to View Time Since Previous Displayed Packet

The screenshot shows the Wireshark interface with the 'View' menu open. The 'Time Display Format' submenu is also open, showing various time display options. The option 'Seconds Since Previous Displayed Packet: 1.123456' is selected, indicating the time displayed for each packet is relative to the previous packet shown in the list.

No.	Destination	Bytes	Protocol	Info
4476	Broadcast	224	IEEE 802.11	Beacon
4477	Broadcast	224	IEEE 802.11	Beacon
4478	Broadcast	224	IEEE 802.11	Beacon
4479	Broadcast	224	IEEE 802.11	Beacon
4480	Broadcast	224	IEEE 802.11	Beacon
4481	Broadcast	224	IEEE 802.11	Beacon
4482	Broadcast	224	IEEE 802.11	Beacon
4494	Broadcast	224	IEEE 802.11	Beacon
4495	Broadcast	224	IEEE 802.11	Beacon
4502	Broadcast	224	IEEE 802.11	Beacon
4503	Broadcast	224	IEEE 802.11	Beacon
4512	Broadcast	224	IEEE 802.11	Beacon
4513	Broadcast	224	IEEE 802.11	Beacon
4514	Broadcast	224	IEEE 802.11	Beacon
4515	Broadcast	224	IEEE 802.11	Beacon
4516	Broadcast	224	IEEE 802.11	Beacon
4527	Broadcast	224	IEEE 802.11	Beacon
4528	Broadcast	224	IEEE 802.11	Beacon
4529	Broadcast	224	IEEE 802.11	Beacon
4532	Broadcast	224	IEEE 802.11	Beacon
4533	Broadcast	224	IEEE 802.11	Beacon
4534	Broadcast	224	IEEE 802.11	Beacon
4535	Broadcast	224	IEEE 802.11	Beacon
4536	Broadcast	224	IEEE 802.11	Beacon

Export the Resulting Trace File

The screenshot shows the Wireshark application window with the 'File' menu open and the 'Export' option selected. The 'Export' dialog box is open, showing the following settings:

- File name: Wireless Troubleshooting Data.csv
- Save as type: CSV (Comma Separated Values summary) (*.csv)
- Packet Range: All packets (6076 captured, 1537 displayed)
- Packet Format: Packet summary line, Packet details (As displayed)

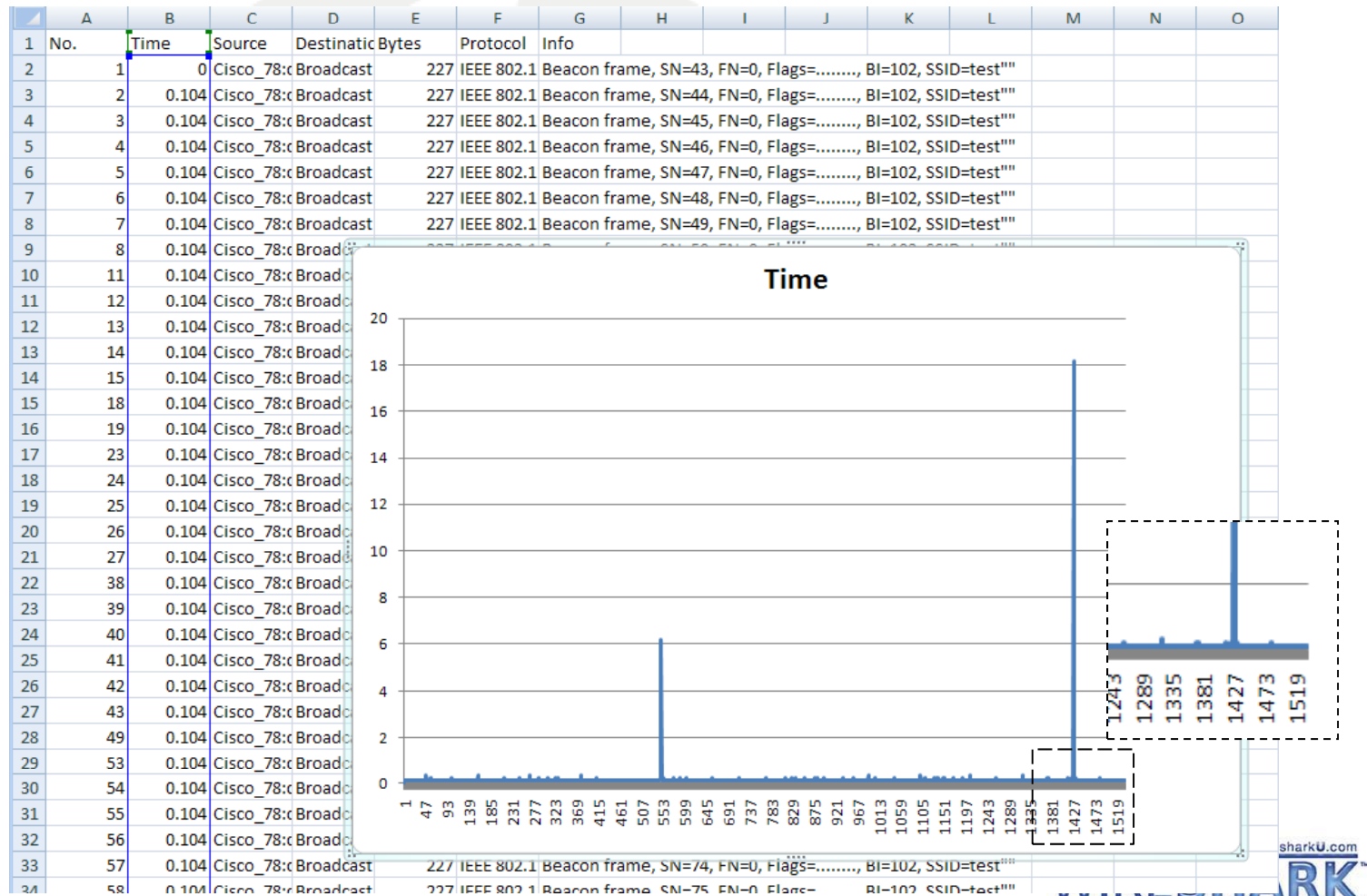
The background shows a packet capture table with columns for Time, IP, and Destination. The destination column contains 'Broadcas' and 'Cisco_78:'.

Graphing the Results in Excel

Open the .CSV file in Excel

Select the Time Column

Insert Line Chart

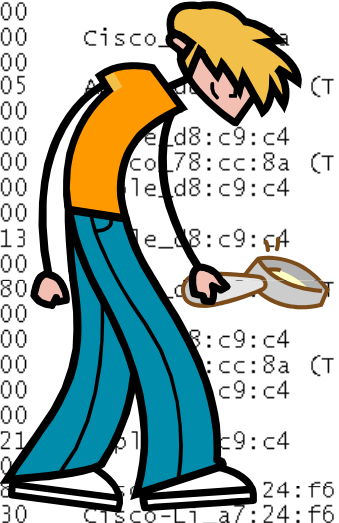


Identifying the Anomaly

```
4824 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8( Beacon frame,  
4825 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8( Beacon frame,  
4829 0.208 Cisco_78:cc:8a Broadcast 224 IEEE 8( Beacon frame,  
4830 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8( Beacon frame,  
4831 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8( Beacon frame,  
4832 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8( Beacon frame,  
4833 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8( Beacon frame,  
4834 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8( Beacon frame,  
4844 0.208 Cisco_78:cc:8a Broadcast 224 IEEE 8( Beacon frame,  
4847 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8( Beacon frame,  
4848 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8( Beacon frame,  
4849 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8( Beacon frame,  
4850 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8( Beacon frame,  
4854 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8( Beacon frame,  
5190 18.173 Cisco_78:cc:8a Broadcast 224 IEEE 8( Beacon frame,  
5191 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8( Beacon frame,  
5192 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8( Beacon frame,  
5222 0.104 Cisco_78:cc:8a Broadcast 224 IEEE 8( Beacon frame,  
5239 0.208 Cisco_78:cc:8a Broadcast 227 IEEE 8( Beacon frame,  
5242 0.104 Cisco_78:cc:8a Broadcast 227 IEEE 8( Beacon frame,  
5245 0.104 Cisco_78:cc:8a Broadcast 227 IEEE 8( Beacon frame,
```

Evaluate the Behavior

No. -	Time	Source	Destination	Bytes	Protocol	Info
4852	0.000	Cisco_78:cc:8a	Cisco-Li_a7:24:f6	218	IEEE 802.11	8(Probe Response, SN=2836, FN=0, Flags=....R..., BI=102, SSID="test")
4853	0.000	Cisco_78:cc:8a	Cisco_78:cc:8a (R)	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4854	0.011	Cisco_78:cc:8a	Broadcast	224	IEEE 802.11	8(Beacon frame, SN=1538, FN=0, Flags=....., BI=102, SSID="test")
4855	0.018	Cisco-Li_a7:24:f6	Broadcast	47	IEEE 802.11	8(Probe Request, SN=4, FN=0, Flags=....., SSID=Broadcast)
4856	0.000	Cisco_78:cc:8a	Cisco-Li_a7:24:f6	218	IEEE 802.11	8(Probe Response, SN=2837, FN=0, Flags=....R..., BI=102, SSID="test")
4857	0.000	Cisco_78:cc:8a	Cisco_78:cc:8a (R)	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4858	0.000	Cisco_78:cc:8a	Cisco-Li_a7:24:f6	218	IEEE 802.11	8(Probe Response, SN=2837, FN=0, Flags=....R..., BI=102, SSID="test")
4859	0.000	Cisco_78:cc:8a	Cisco_78:cc:8a (R)	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4860	0.305	Cisco_78:cc:8a	Cisco_78:cc:8a (R)	16	IEEE 802.11	8(Request-to-send, Flags=.....)
4861	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4862	0.000	Apple_d8:c9:c4	Cisco_39:9b:4	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4863	0.000	Cisco_78:cc:8a	Apple_d8:c9:c4	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4864	0.000	Apple_d8:c9:c4	Cisco_78:cc:8a	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4865	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4866	0.213	Apple_d8:c9:c4	Cisco_78:cc:8a	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4867	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4868	0.780	Cisco_78:cc:8a	Cisco_78:cc:8a	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4869	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4870	0.000	Apple_d8:c9:c4	Cisco_39:9b:4	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4871	0.000	Cisco_78:cc:8a	Apple_d8:c9:c4	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4872	0.000	Apple_d8:c9:c4	Cisco_78:cc:8a	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4873	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4874	0.221	Apple_d8:c9:c4	Cisco_78:cc:8a	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4875	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4876	0.188	Cisco-Li_a7:24:f6	Broadcast	47	IEEE 802.11	8(Probe Request, SN=4, FN=0, Flags=....., SSID=Broadcast)
4877	0.030	Cisco-Li_a7:24:f6	Broadcast	47	IEEE 802.11	8(Probe Request, SN=4, FN=0, Flags=....., SSID=Broadcast)
4878	0.567	Apple_d8:c9:c4	Cisco_78:cc:8a	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4879	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4880	0.000	Apple_d8:c9:c4	Cisco_39:9b:4	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4881	0.000	Cisco_78:cc:8a	Apple_d8:c9:c4	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4882	0.000	Apple_d8:c9:c4	Cisco_78:cc:8a	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4883	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4884	0.212	Apple_d8:c9:c4	Cisco_78:cc:8a	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4885	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4886	0.084	Apple_d8:c9:c4	Broadcast	111	IEEE 802.11	8(Probe Request, SN=872, FN=0, Flags=....., SSID=Broadcast)
4887	0.107	Apple_d8:c9:c4	Cisco_78:cc:8a	24	IEEE 802.11	8(Null function (No data), SN=881, FN=0, Flags=.....)
4888	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4889	0.047	Apple_d8:c9:c4	Cisco_78:cc:8a	10	IEEE 802.11	8(Null function (No data), SN=882, FN=0, Flags=.....)
4890	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4891	0.146	Apple_d8:c9:c4	Cisco_78:cc:8a	10	IEEE 802.11	8(Null function (No data), SN=892, FN=0, Flags=.....)
4892	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE 802.11	8(Acknowledgement, Flags=.....)
4893	0.053	Apple_d8:c9:c4	Cisco_78:cc:8a	10	IEEE 802.11	8(Null function (No data), SN=893, FN=0, Flags=...P...T)
4894	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE 802.11	8(Acknowledgement, Flags=.....)



1. Walk through the trace, frame-by-frame
2. Ask yourself:
 - Why was this frame transmitted?
 - What is the expected response?
 - Did the expected response occur?
3. When you find the departure from the expected response you've either found a manifestation of the problem or you've discovered something that was outside your protocol analysis experience.

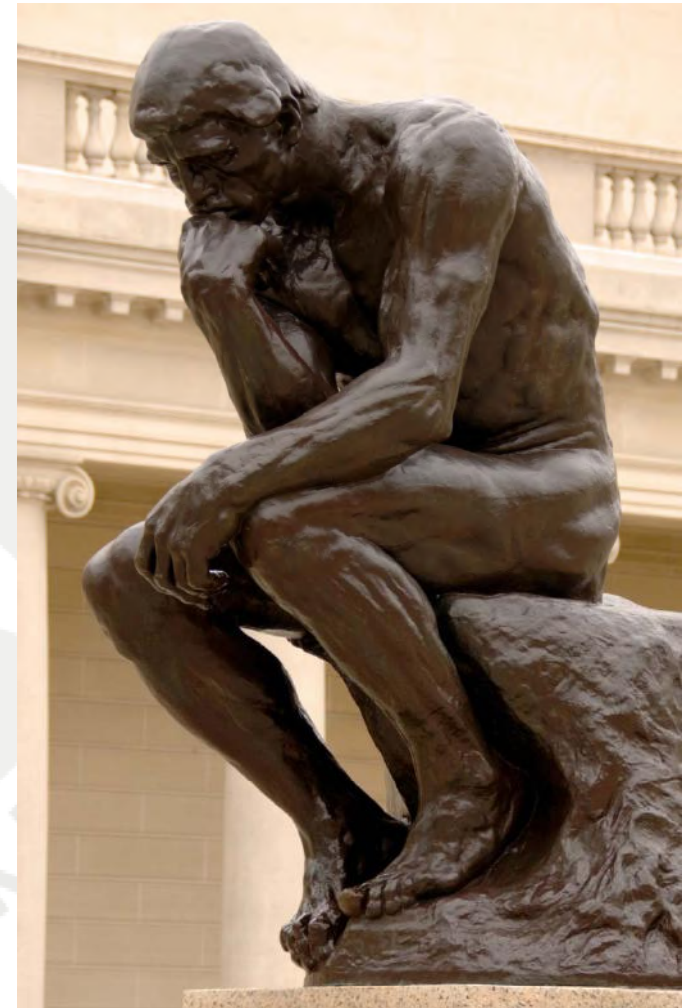


Evaluate the Behavior

No. -	Time	Source	Destination	Bytes	Protocol	Info
4852	0.000	Cisco_78:cc:8a	Cisco-Li_a7:24:f6	218	IEEE802.11	8(Probe Response, SN=2836, FN=0, Flags=....R..., BI=102, SSID="test")
4853	0.000	Cisco_78:cc:8a	Cisco_78:cc:8a	10	IEEE802.11	8(Acknowledgement, Flags=.....)
4854	0.011	Cisco_78:cc:8a	Broadcast	224	IEEE802.11	8(Beacon frame, SN=1538, FN=0, Flags=....., BI=102, SSID="test")
4855	0.018	Cisco-Li_a7:24:f6	Broadcast	47	IEEE802.11	8(Probe Request, SN=4, FN=0, Flags=....., SSID=Broadcast)
4856	0.000	Cisco_78:cc:8a	Cisco-Li_a7:24:f6	218	IEEE802.11	8(Probe Response, SN=2837, FN=0, Flags=....R..., BI=102, SSID="test")
4857	0.000	Cisco_78:cc:8a	Cisco_78:cc:8a	10	IEEE802.11	8(Acknowledgement, Flags=.....)
4858	0.000	Cisco_78:cc:8a	Cisco-Li_a7:24:f6	218	IEEE802.11	8(Probe Response, SN=2837, FN=0, Flags=....R..., BI=102, SSID="test")
4859	0.000	Cisco_78:cc:8a	Cisco_78:cc:8a	10	IEEE802.11	8(Acknowledgement, Flags=.....)
4860	0.305	Apple_d8:c9:c4	Cisco_78:cc:8a	16	IEEE802.11	8(Request-to-send, Flags=.....)
4861	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE802.11	8(Clear-to-send, Flags=.....)
4862	0.000	Apple_d8:c9:c4	Cisco_39:9b:40	1538	LLC	I, N(R)=16, N(S)=0; DSAP 0x38 Individual, SSAP NULL LSAP Response
4863	0.000	Cisco_78:cc:8a	Apple_d8:c9:c4	28	IEEE802.11	8(802.11 Block Ack, Flags=.....)
4864	0.000	Apple_d8:c9:c4	Cisco_78:cc:8a	24	IEEE802.11	8(Null function (No data), SN=866, FN=0, Flags=.....T)
4865	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE802.11	8(Acknowledgement, Flags=.....)
4866	0.213	Apple_d8:c9:c4	Cisco_78:cc:8a	24	IEEE802.11	8(Null function (No data), SN=867, FN=0, Flags=...P...T)
4867	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE802.11	8(Acknowledgement, Flags=.....)
4868	0.780	Apple_d8:c9:c4	Cisco_78:cc:8a	16	IEEE802.11	8(Request-to-send, Flags=.....)
4869	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE802.11	8(Clear-to-send, Flags=.....)
4870	0.000	Apple_d8:c9:c4	Cisco_39:9b:40	1538	LLC	I, N(R)=16, N(S)=0; DSAP 0x38 Group, SSAP NULL LSAP Response
4871	0.000	Cisco_78:cc:8a	Apple_d8:c9:c4	28	IEEE802.11	8(802.11 Block Ack, Flags=.....)
4872	0.000	Apple_d8:c9:c4	Cisco_78:cc:8a	24	IEEE802.11	8(Null function (No data), SN=868, FN=0, Flags=.....T)
4873	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE802.11	8(Acknowledgement, Flags=.....)
4874	0.221	Apple_d8:c9:c4	Cisco_78:cc:8a	24	IEEE802.11	8(Null function (No data), SN=869, FN=0, Flags=...P...T)
4875	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE802.11	8(Acknowledgement, Flags=.....)
4876	0.181	Cisco-Li_a7:24:f6	Broadcast	47	IEEE802.11	8(Probe Request, SN=21, FN=0, Flags=....., SSID=Broadcast)
4877	0.030	Cisco-Li_a7:24:f6	Broadcast	47	IEEE802.11	8(Probe Request, SN=22, FN=0, Flags=....., SSID=Broadcast)
4878	0.567	Apple_d8:c9:c4	Cisco_78:cc:8a	16	IEEE802.11	8(Request-to-send, Flags=.....)
4879	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE802.11	8(Clear-to-send, Flags=.....)
4880	0.000	Apple_d8:c9:c4	Cisco_39:9b:40	1538	LLC	I, N(R)=16, N(S)=0; DSAP 0x3a Individual, SSAP NULL LSAP Response
4881	0.000	Cisco_78:cc:8a	Apple_d8:c9:c4	28	IEEE802.11	8(802.11 Block Ack, Flags=.....)
4882	0.000	Apple_d8:c9:c4	Cisco_78:cc:8a	24	IEEE802.11	8(Null function (No data), SN=870, FN=0, Flags=.....T)
4883	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE802.11	8(Acknowledgement, Flags=.....)
4884	0.212	Apple_d8:c9:c4	Cisco_78:cc:8a	24	IEEE802.11	8(Null function (No data), SN=871, FN=0, Flags=...P...T)
4885	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE802.11	8(Acknowledgement, Flags=.....)
4886	0.084	Apple_d8:c9:c4	Broadcast	111	IEEE802.11	8(Probe Request, SN=872, FN=0, Flags=....., SSID="test")
4887	0.107	Apple_d8:c9:c4	Cisco_78:cc:8a	24	IEEE802.11	8(Null function (No data), SN=881, FN=0, Flags=.....T)
4888	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE802.11	8(Acknowledgement, Flags=.....)
4889	0.047	Apple_d8:c9:c4	Cisco_78:cc:8a	24	IEEE802.11	8(Null function (No data), SN=882, FN=0, Flags=...P...T)
4890	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE802.11	8(Acknowledgement, Flags=.....)
4891	0.146	Apple_d8:c9:c4	Cisco_78:cc:8a	24	IEEE802.11	8(Null function (No data), SN=892, FN=0, Flags=.....T)
4892	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE802.11	8(Acknowledgement, Flags=.....)
4893	0.053	Apple_d8:c9:c4	Cisco_78:cc:8a	24	IEEE802.11	8(Null function (No data), SN=893, FN=0, Flags=...P...T)
4894	0.000	Apple_d8:c9:c4	Apple_d8:c9:c4	10	IEEE802.11	8(Acknowledgement, Flags=.....)

The “Think” Method

- You now must determine what problems or configuration issues result in the identified behavior.
- This is where vendor technical support and collaboration play a critical part
- In the present scenario, the question is:
“What makes an access point stop beaconing for a consistent time period at reasonably regular intervals?”
- Once you’ve isolated and described the problem and formulated a concise question the answer is often quite simple



Know Your Vendor's Products



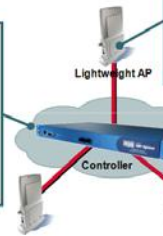
Radio Resource Management

Radio Resource Management Software - Embedded in Controllers

- | | |
|--------------------------|------------------------------------|
| Transmit Power Selection | Rogue Detection & Containment |
| User Load Management | Coverage Hole Management |
| Auto Channel Management | Interference Detection & Avoidance |

Key RF stats profiled

- AP received energy**
Total energy on each channel
- 802.11 noise**
Non-802.11 noise heard on channel
- 802.11 interference**
802.11 packets heard during sampling intervals. Described as % busy
- Utilization**
More emphasis given to APs that require more bandwidth



RF Groups

RF Group != Mobility Group
RF Group is a cluster of controllers that coordinate RRM calculations between them

RF Group can be up to 20 controllers

RF Group is identified by "RF Group Name", which acts as a shared secret between members of the group

Neighbor messages sent out by APs include a hash of the BSSID and timestamp

When controllers hear neighbor messages with the right shared secret they form the RF Group

RF Group Leader is elected:

- Controller with the highest "Group ID" number is elected
- If there is a tie, the Controller with the lowest path-loss between APs

Automatic RF Grouping

Auto-RRM negates the need to configure each AP

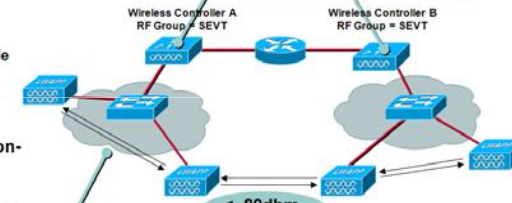
Automatic channel and power selection

- Performed in real-time
- Computed across multiple controllers
- Automatically performs ongoing configuration adjustments

Over-ride capability for non-typical installs

- On-demand RRM
- Manual channel and power configuration

Controllers elect a leader to analyze RF measurement variables and make optimal channel and power decisions for the whole system. Changes are made locally if possible. Dampening for system wide changes.



NEIGHBOR MESSAGES
Sent at full power

- Controller IP/RF Group Name
- Operating channel
- Authenticated

If APs on different controllers hear neighbor messages at -80 dBm or stronger, they group their RF domains

Channel and power then computes as a group

The Solution!

Dynamic Channel Assignment Algorithm

Channel Assignment Method	<input checked="" type="radio"/> Automatic Interval: 600 secs AnchorTime: 0 (Hour of the day)
	<input type="radio"/> On Demand <input type="button" value="Invoke Channel Update now"/>
	<input type="radio"/> OFF
Avoid Foreign AP interference	<input checked="" type="checkbox"/> Enabled
Avoid Cisco AP load	<input type="checkbox"/> Enabled
Avoid non-802.11b noise	<input checked="" type="checkbox"/> Enabled
Signal Strength Contribution	Enabled
Channel Assignment Leader	00:16:46:4b:33:40
Last Channel Assignment	467 secs ago
DCA Sensitivity Level	MEDIUM (15 dB)

Monitor Intervals (60 to 3600 secs)

Noise Measurement	180
Load Measurement	60
Neighbor Packet Frequency	60
Channel Scan Duration	180

Noise/Interference/Rogue Monitoring Channels

Channel List

Country Channels

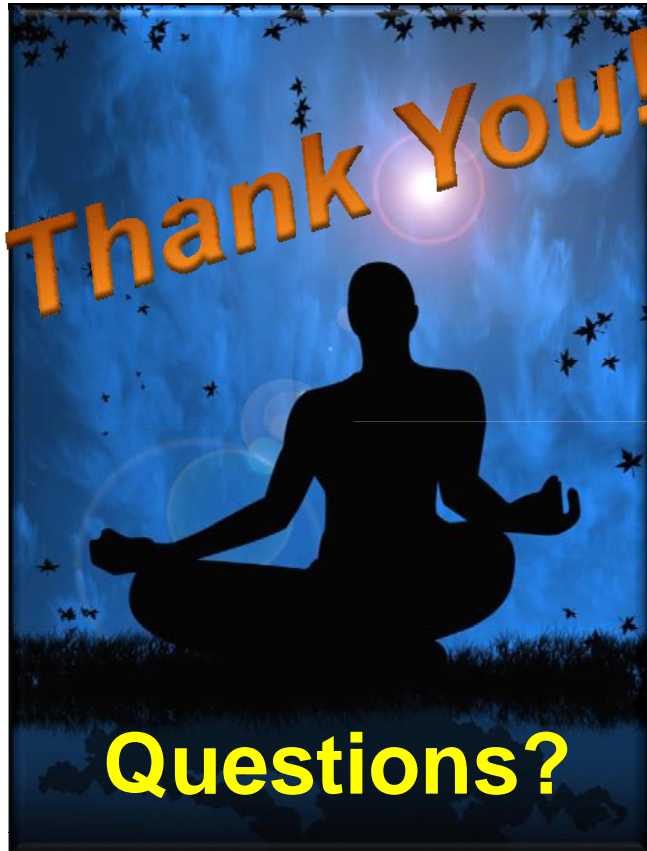
- All Channels
- Country Channels
- DCA Channels

Monitor Intervals (60 to 3600 secs)

Tx Power Level Assignment Algorithm

Power Level Assignment Method	<input checked="" type="radio"/> Automatic Every 600 secs
	<input type="radio"/> On Demand <input type="button" value="Invoke Power Update now"/>
	<input type="radio"/> Fixed 1
Power Threshold	-70 dBm
Power Neighbor Count	3
Power Update Contribution	SNI.
Power Assignment Leader	00:16:46:4b:33:40
Last Power Level Assignment	33 secs ago

Wireshark Saves the WLAN !



www.Connect802.com
joe@Connect802.com
(925) 552-0802

You have to know that you know what you think you know so you can know how to know what you don't know.

- Understand the RF design and RF signal behavior
- Understand the expected 802.11 protocol behavior
- Understand the expected L2 and L3 protocol behavior
- Capture the problem scenario with Wireshark
- Walk through the trace until the problem point is identified
- Pose a troubleshooting question to quantify the problem.