

# Show Me The Data

## Protocol and Spectrum Analysis

### Basics for 802.11 Wireless LAN

Robert Bartz  
robert@eightotwo.com  
@eightotwo



## Presenter - Robert Bartz

- Eight-O-Two Technology Solutions, Denver Colorado
- Engineer, Consultant, Educator, Technical Author, Speaker, CWNE
- BS Degree, Industrial Technology, California State University Long Beach, College of Engineering
- Former Aerospace Test Engineer
- 27 Years Technical Training With the Last 18 Years Specializing in Wireless Networking
- Author - CWTS Official Study Guide by Sybex – 1<sup>st</sup> and 2<sup>nd</sup> Editions
- Author - Mobile Computing Deployment and Management: Real World Skills for CompTIA Mobility+ Certification and Beyond by Sybex
- Author - CWTS, CWS, and CWT Complete Study Guide by Sybex
- E-mail: [robert@eightotwo.com](mailto:robert@eightotwo.com) Twitter: @eightotwo



# Agenda

- Common Troubleshooting Methodology
- The OSI Model (A Quick Review)
- OSI Model – The Wireless Element
- The IEEE 802.11 Frame
- Common IEEE 802.11 Frame Exchanges
- Wireless LAN Troubleshooting Tools for Layer 2 (Data Link)
- Protocol Analysis
- Wireless LAN Troubleshooting Tools for Layer 1 (Physical)
- Spectrum Analysis

# This is a no lollygagging session

lol·ly·gag

'ləlēˌgag/

*verb* North American *informal*

gerund or present participle: **lollygagging**

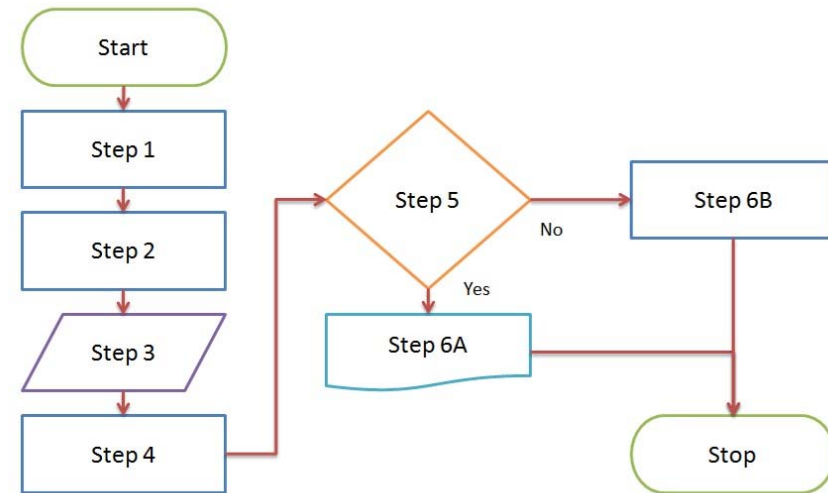
**spend time aimlessly; idle.**

"he sends her to Arizona every January to lollygag in the sun"

# Common Troubleshooting Methodology

Steps in a common troubleshooting methodology

1. Identify the problem
2. Determine the scale of the problem
3. Possible causes
4. Isolate the problem
5. Resolution or escalation
6. Corrective action / verify solution
7. Document, document and document

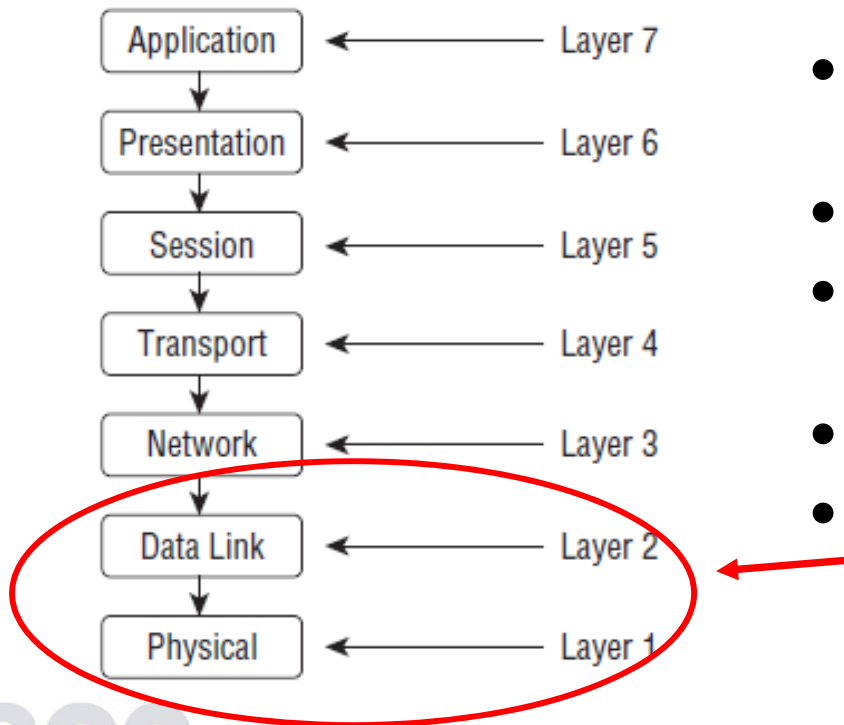


# Show Me The Data

## The OSI Model

# The OSI Model (A Quick Review)

Open Systems Interconnection (OSI)



- The basic concept of communications in the computer network environment
- Consists of seven layers
- Each layer is made up of many protocols and serves a specific function
- Data is encapsulated at some layers
- WLAN technology operates at the two lowest layers

# OSI Model – The Wireless Element

## Layer 2 – Data Link Layer (MAC)

Two sublayers

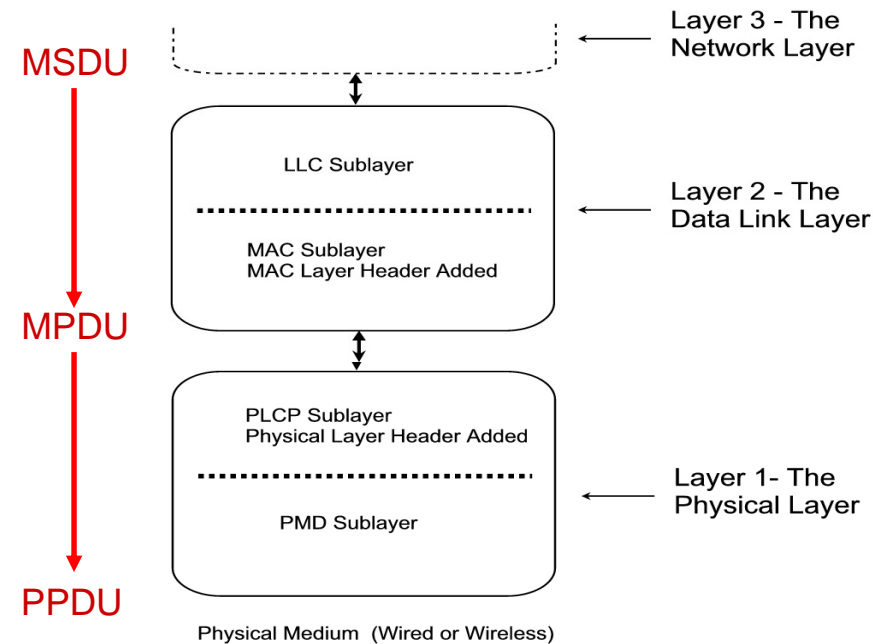
Responsible for organizing the bit-level data for communications (frames)

Detecting and correcting Physical layer errors

## Layer 1 – Physical Layer (PHY)

Two Sublayers

Bit-level data streams and computer network hardware connecting the devices together



The Media Access Control Service Data Unit (MSDU) is upper layer data that is encapsulated at the MAC and PLCP sublayers



# Show Me The Data

## The IEEE 802.11 Frame

# Famous Quotation #1

**“SHOW ME THE MONEY”**

Tom Cruise as Jerry Maguire  
in Jerry Maguire (1996)



# Famous Quotation #2

## “SHOW ME THE DATA”

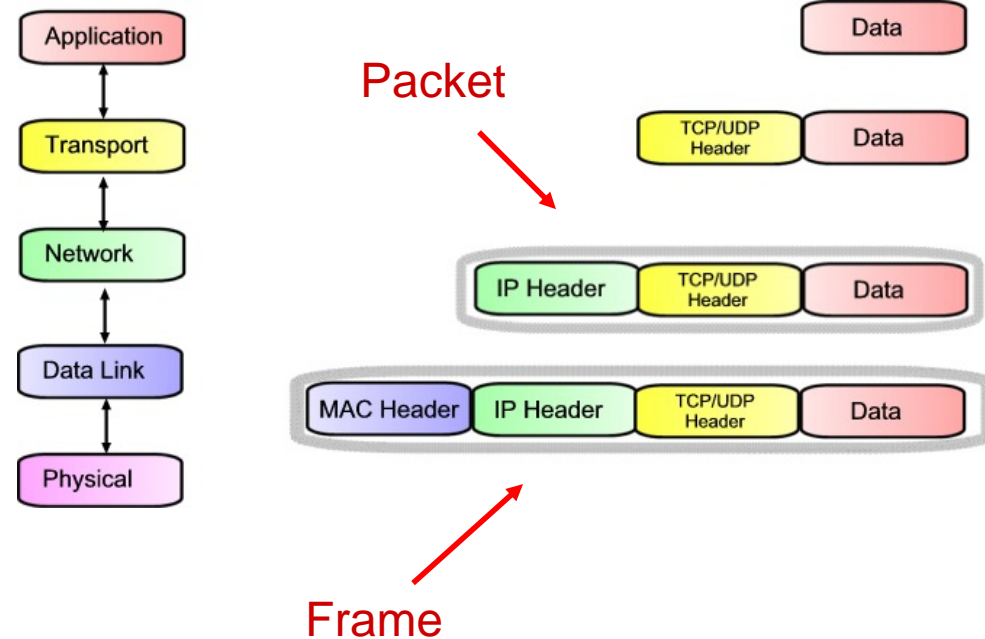
Robert Bartz as himself  
BICSI Fall Conference & Exhibition  
Las Vegas, Nevada (2019)



# The IEEE 802.11 Frame

## Packets and Frames

- Packets are at layer 3
  - Packets encapsulate data
- Frames are at Layer 2
  - Frames encapsulate packets



# The IEEE 802.11 Frame

## IEEE 802.11 - General Frame Format

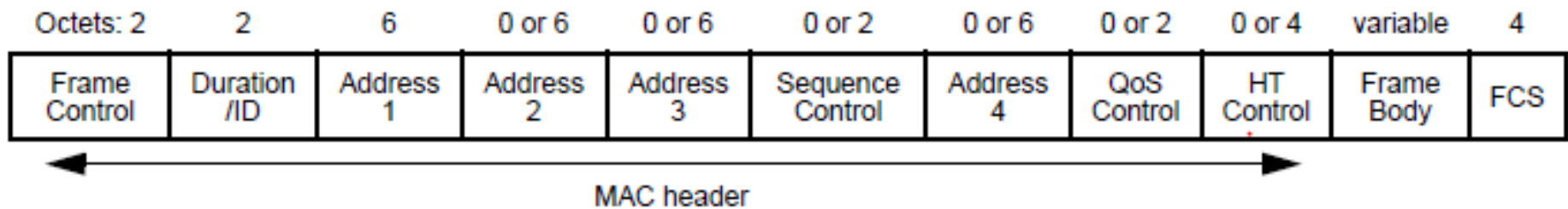


Image provided by IEEE Std 802.11™-2016

# The IEEE 802.11 Frame

## Frame Control Field

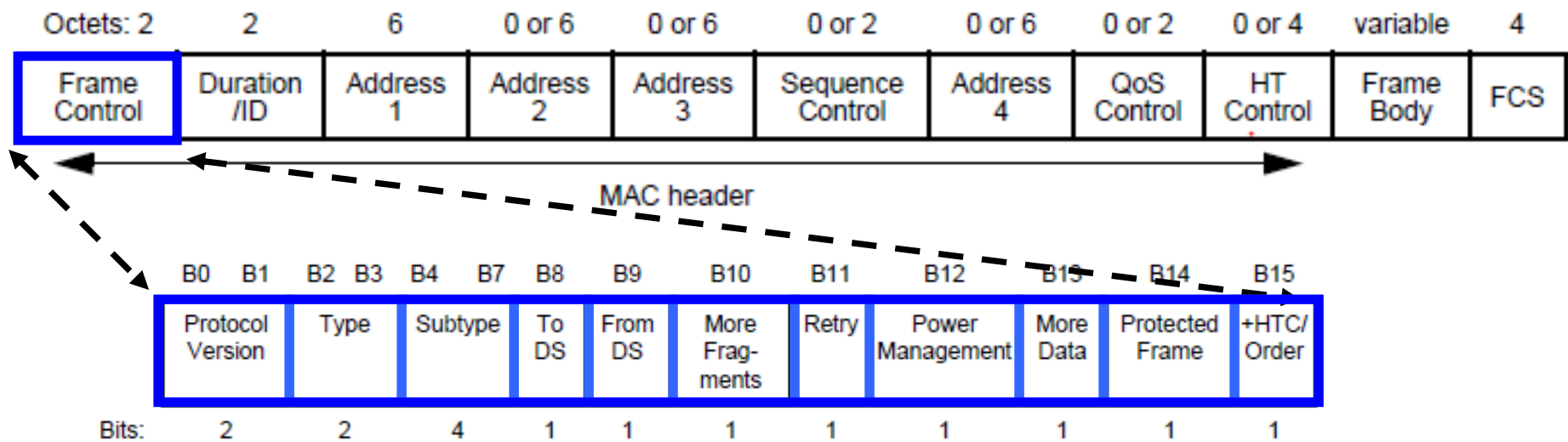


Image provided by IEEE Std 802.11™-2016

Every IEEE 802.11 Frame Has a Frame Control Field

# The IEEE 802.11 Frame

## The Three IEEE 802.11 Frame Types

- Management Frames
- Control Frames
- Data Frames

Source	Destination	BSSID	Protocol
A8:BD:27:87:D7:F1	Ethernet Broadcast	A8:BD:27:87:D7:F1	802.11 Beacon
A8:BD:27:87:D7:F1	Ethernet Broadcast	A8:BD:27:87:D7:F1	802.11 Beacon
A8:BD:27:87:D7:F1	Ethernet Broadcast	A8:BD:27:87:D7:F1	802.11 Beacon
A8:BD:27:87:D7:F1	Ethernet Broadcast	A8:BD:27:87:D7:F1	802.11 Beacon
A8:BD:27:87:D7:F1	Ethernet Broadcast	A8:BD:27:87:D7:F1	802.11 Beacon
A8:BD:27:87:D7:F1	Ethernet Broadcast	A8:BD:27:87:D7:F1	802.11 Beacon
Intel:5F:5A:B0	Ethernet Broadcast	Ethernet Broadcast	802.11 Probe Req
Intel:5F:5A:B0	Ethernet Broadcast	Ethernet Broadcast	802.11 Probe Req
A8:BD:27:87:D7:F1	Intel:5F:5A:B0	A8:BD:27:87:D7:F1	802.11 Probe Rsp
Intel:5F:5A:B0	A8:BD:27:87:D7:F1		802.11 Ack
A8:BD:27:87:D7:F1	Intel:5F:5A:B0	A8:BD:27:87:D7:F1	802.11 Probe Rsp
Intel:5F:5A:B0	A8:BD:27:87:D7:F1		802.11 Ack
ProximWire:CA:48:2C	F0:1F:AF:3E:AE:21	A8:BD:27:87:D7:F0	802.11 Encrypted ...
ProximWire:CA:48:2C	F0:1F:AF:3E:AE:21	A8:BD:27:87:D7:F0	802.11 Encrypted ...
ProximWire:CA:48:2C	F0:1F:AF:3E:AE:21	A8:BD:27:87:D7:F0	802.11 Encrypted ...
ProximWire:CA:48:2C	F0:1F:AF:3E:AE:21	A8:BD:27:87:D7:F0	802.11 Encrypted ...
ProximWire:CA:48:2C	F0:1F:AF:3E:AE:21	A8:BD:27:87:D7:F0	802.11 Encrypted ...
ProximWire:CA:48:2C	F0:1F:AF:3E:AE:21	A8:BD:27:87:D7:F0	802.11 Encrypted ...



# The IEEE 802.11 Frame

## Management Frame Types in IEEE 802.11 Networking

- Common Management Frames
  - Beacon
    - Passive Scanning
  - Probe Request / Response
    - Active Scanning
  - IEEE 802.11 Authentication
    - Open System
  - IEEE 802.11 Association Request / Response
    - Capabilities

```
802.11 Management - Association Response
  Capability Info: %0000010000010001 [24-25]
    0..... Immediate Block Ack Not Allowed
    .0..... Delayed Block Ack Not Allowed
    ..0..... DSSS-OFDM is Not Allowed
    ...0.... No Radio Measurement
    ....0... APSD is not supported
    .....1.. G Mode Short Slot Time [9 microseconds]
    .....0.. QoS is Not supported
    .....0.. Spectrum Mgmt Disabled
    .....0.. Channel Agility Not Used
    .....0.. PBCC Not Allowed
    .....0.. Short Preamble Not Allowed
    .....1... Privacy Enabled
    .....0... CF Poll Not Requested
    .....0.. CF Not Pollable
    .....0.. Not an IBSS Type Network
    .....1 ESS Type Network
  Status Code: 0 Successful [26-27]
  Association ID: 1 [28-29 Mask 0x3FFF]
  Supported Rates
    Element ID: 1 Supported Rates [30]
    Length: 8 [31]
    Supported Rate: 6.0 Mbps (BSS Basic Rate) [32]
    Supported Rate: 9.0 Mbps (Not BSS Basic Rate) [33]
    Supported Rate: 12.0 Mbps (BSS Basic Rate) [34]
    Supported Rate: 18.0 Mbps (Not BSS Basic Rate) [35]
    Supported Rate: 24.0 Mbps (BSS Basic Rate) [36]
```



# The IEEE 802.11 Frame

## Control Frame Types in IEEE 802.11 Networking

- Common Control Frames
  - RTS – Request to Send
    - Reserves the medium
  - CTS – Clear to Send
    - Response to an RTS
  - IEEE 802.11 ACK
    - Acknowledges unicast frames
  - PS Poll
    - Legacy power save mode

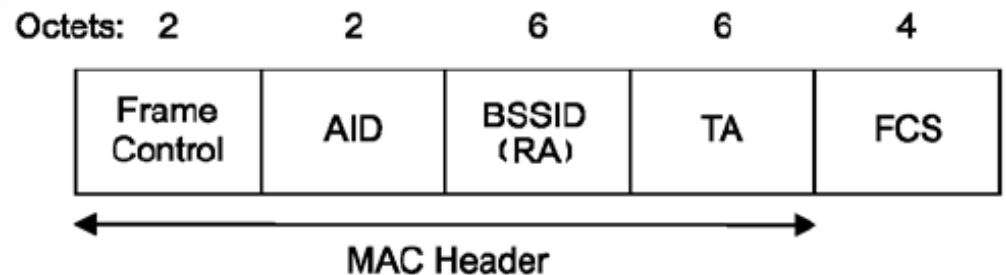


Image provided by IEEE Std 802.11™-2016

# The IEEE 802.11 Frame

## Data Frame Types in IEEE 802.11 Networking

- Two Types of Data Frames
  - Data
  - Null Data

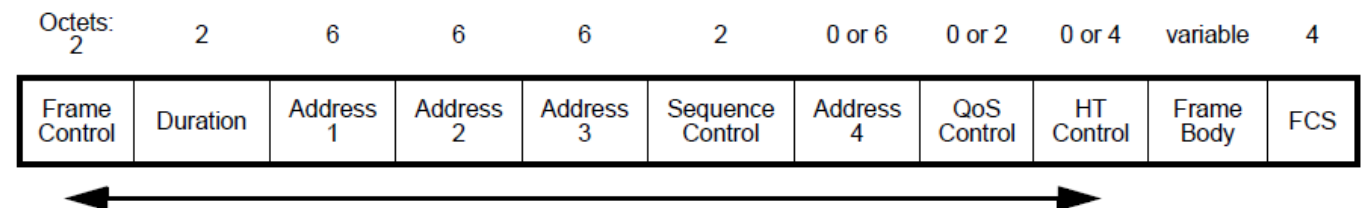
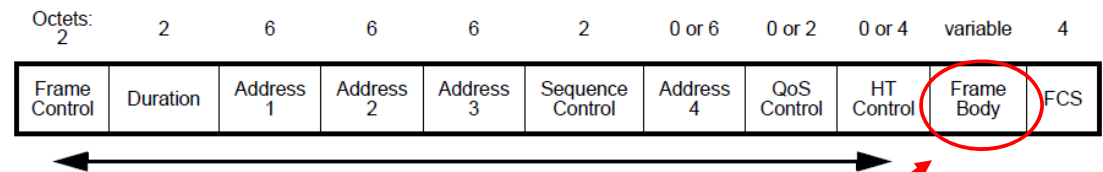


Image provided by IEEE Std 802.11™-2016

# The IEEE 802.11 Frame

## Data Frames Types in IEEE 802.11 Networking

- Data
  - Carry data payload



Data (MSDU) is in the frame body

Image provided by IEEE Std 802.11™-2016

# The IEEE 802.11 Frame

## Data Frames Types in IEEE 802.11 Networking

- Null Data
  - Does not carry data payload
  - Power management
  - Channel scanning
  - Maintaining an association

```
802.11 MAC Header
  Version: 0 [0 Mask 0x03]
  Type: %10 Data [0 Mask 0x0C]
  Subtype: %1100 QoS NULL (No Data) [0 Mask 0xF0]
  Frame Control Flags: %00010001 [1]
    0... .. Non-strict order
    .0.. .. Non-Protected Frame
    ..0. .. No More Data
    ...1 .. Power Management - power save mode
    .... 0... This is not a Re-Transmission
    .... .0.. Last or Unfragmented Frame
    .... ..0. Not an Exit from the Distribution System
    .... ...1 To the Distribution System
```

Power Management Bit

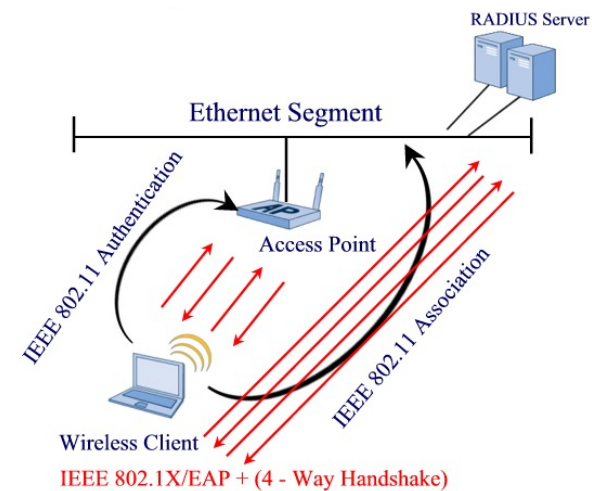
# Show Me The Data

## Common IEEE 802.11 Frame Exchanges

# IEEE 802.11 Frame Types

## Common IEEE 802.11 Frame Exchanges

- IEEE 802.11 Authentication and Association
- IEEE 802.11 Pre-Shared Key Authentication
- IEEE 802.1X/EAP Authentication



# IEEE 802.11 Frame Types

## IEEE 802.11 Authentication and Association

Packet	Source	Destination	BSSID	Protocol
9	Intel:5F:5A:B0	Ethernet Broadcast	Ethernet Broadcast	802.11 Probe Req
10	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	802.11 Probe Rsp
11	Intel:5F:5A:B0	A8:BD:27:87:D7:F0		802.11 Ack
12	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	A8:BD:27:87:D7:F0	802.11 Auth
13	A8:BD:27:87:D7:F0	Intel:5F:5A:B0		802.11 Ack
14	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	802.11 Auth
15	Intel:5F:5A:B0	A8:BD:27:87:D7:F0		802.11 Ack
16	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	A8:BD:27:87:D7:F0	802.11 Assoc Req
17	A8:BD:27:87:D7:F0	Intel:5F:5A:B0		802.11 Ack
18	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	802.11 Assoc Rsp
19	Intel:5F:5A:B0	A8:BD:27:87:D7:F0		802.11 Ack



# IEEE 802.11 Frame Types

## IEEE 802.11 Pre-Shared Key Authentication

Packet	Source	Destination	BSSID	Protocol
1	Intel:5F:5A:B0	Ethernet Broadcast	Ethernet Broadcast	802.11 Probe Req
2	Intel:5F:5A:B0	Ethernet Broadcast	Ethernet Broadcast	802.11 Probe Req
3	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	802.11 Probe Rsp
4	Intel:5F:5A:B0	A8:BD:27:87:D7:F0		802.11 Ack
5	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	802.11 Probe Rsp
6	Intel:5F:5A:B0	A8:BD:27:87:D7:F0		802.11 Ack
7	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	A8:BD:27:87:D7:F0	802.11 Auth
8	A8:BD:27:87:D7:F0	Intel:5F:5A:B0		802.11 Ack
9	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	802.11 Auth
10	Intel:5F:5A:B0	A8:BD:27:87:D7:F0		802.11 Ack
11	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	A8:BD:27:87:D7:F0	802.11 Assoc Req
12	A8:BD:27:87:D7:F0	Intel:5F:5A:B0		802.11 Ack
13	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	802.11 Assoc Rsp
14	Intel:5F:5A:B0	A8:BD:27:87:D7:F0		802.11 Ack
15	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	EAPOL-Key
16	Intel:5F:5A:B0	A8:BD:27:87:D7:F0		802.11 Ack
17	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	A8:BD:27:87:D7:F0	EAPOL-Key
18	A8:BD:27:87:D7:F0	Intel:5F:5A:B0		802.11 Ack
19	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	EAPOL-Key
20	Intel:5F:5A:B0	A8:BD:27:87:D7:F0		802.11 Ack
21	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	A8:BD:27:87:D7:F0	EAPOL-Key
22	A8:BD:27:87:D7:F0	Intel:5F:5A:B0		802.11 Ack
23	Intel:5F:5A:B0	Ethernet Broadcast	A8:BD:27:87:D7:F0	802.11 Encrypted ...



# IEEE 802.11 Frame Types

## IEEE 802.1X/EAP Authentication

35	Intel:5F:5A:B0	Ethernet Broadcast	Ethernet Broadcast	802.11 Probe Req
36	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	802.11 Probe Rsp
37	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	A8:BD:27:87:D7:F0	802.11 Ack
38	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	A8:BD:27:87:D7:F0	802.11 Auth
39	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	802.11 Ack
40	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	802.11 Auth
41	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	A8:BD:27:87:D7:F0	802.11 Ack
42	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	A8:BD:27:87:D7:F0	802.11 Assoc Req
43	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	802.11 Ack
44	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	802.11 Assoc Rsp
45	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	A8:BD:27:87:D7:F0	802.11 Ack
46	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	802.11 Assoc Rsp
47	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	A8:BD:27:87:D7:F0	802.11 Ack
48	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	EAP Request
49	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	A8:BD:27:87:D7:F0	802.11 Ack
50	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	A8:BD:27:87:D7:F0	EAPOL-Start
51	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	802.11 Ack

Packet	Source	Destination	BSSID	Protocol
93	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	EAP Request
94	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	A8:BD:27:87:D7:F0	802.11 Ack
95	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	A8:BD:27:87:D7:F0	EAP Response
96	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	802.11 Ack
97	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	A8:BD:27:87:D7:F0	EAP Response
98	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	802.11 Ack
99	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	EAP Request
100	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	A8:BD:27:87:D7:F0	802.11 Ack
101	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	A8:BD:27:87:D7:F0	EAP Response
102	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	802.11 Ack
103	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	EAP Success
104	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	A8:BD:27:87:D7:F0	802.11 Ack
105	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	EAPOL-Key
106	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	A8:BD:27:87:D7:F0	802.11 Ack
107	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	A8:BD:27:87:D7:F0	EAPOL-Key
108	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	802.11 Ack
109	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	EAPOL-Key
110	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	A8:BD:27:87:D7:F0	802.11 Ack
111	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	A8:BD:27:87:D7:F0	EAPOL-Key
112	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	802.11 Ack
113	Intel:5F:5A:B0	Ethernet Broadcast	A8:BD:27:87:D7:F0	802.11 Encrypted ...
114	A8:BD:27:87:D7:F0	Intel:5F:5A:B0	A8:BD:27:87:D7:F0	802.11 Ack

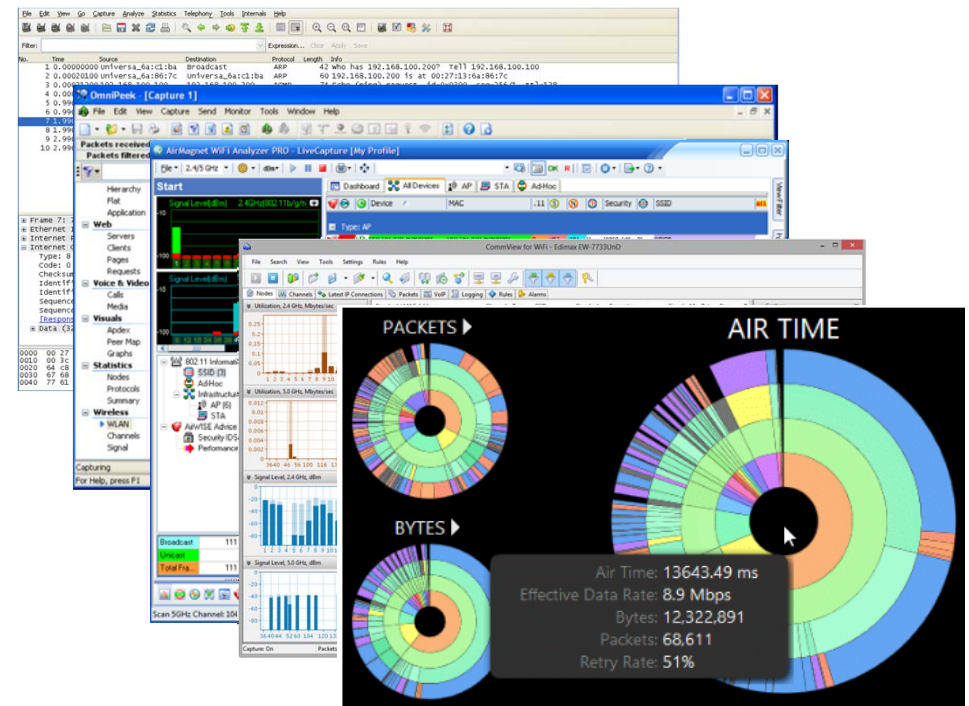
# Show Me The Data

Common Layer 2 Data Link aka (MAC Layer)  
Troubleshooting Tools

# Layer 2 Data link Layer (MAC) - Troubleshooting Tools

## Protocol (Packet) Analyzers

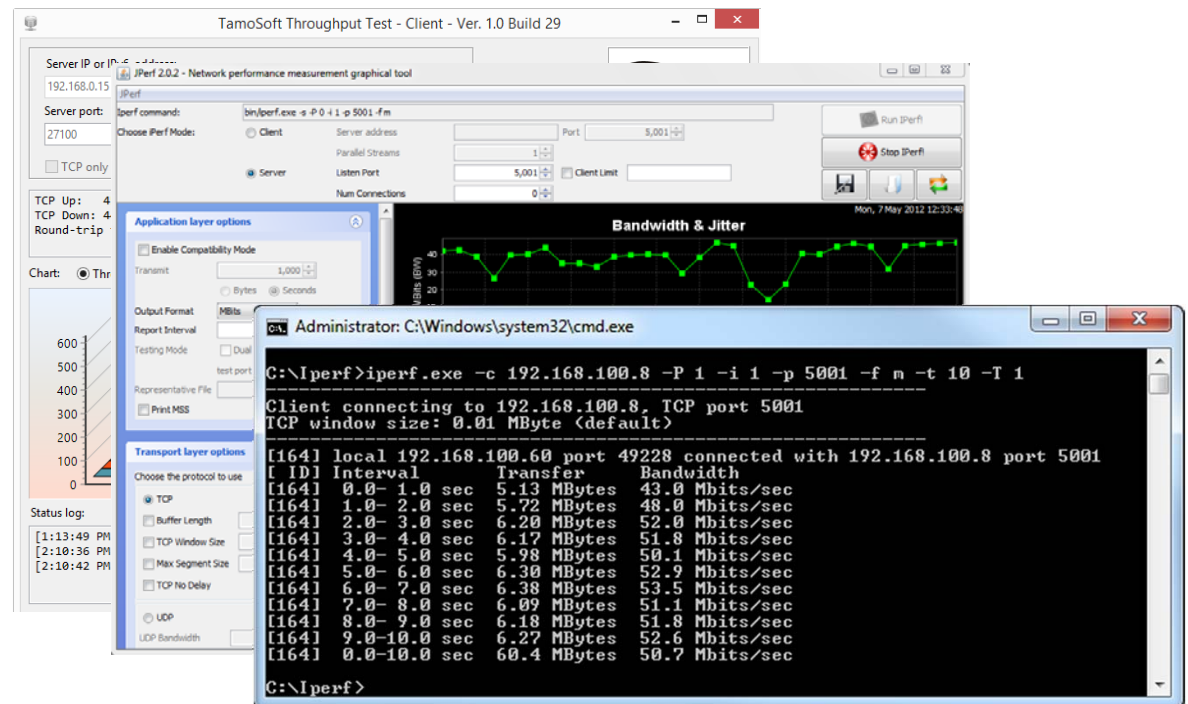
- Wireshark
- LiveAction Omnipcap
- Netscout Wi-Fi Analyzer
- Tamosoft CommView for Wi-Fi
- MetaGeek Eye P.A.



# Layer 2 Data link Layer (MAC)- Troubleshooting Tools

## Throughput Test Tools

- Tamosoft - Free
- jPerf - Free
- iPerf - Free



# Layer 2 Data link Layer (MAC) - Troubleshooting Tools

## Throughput test tools are not just for throughput testing

- Get data moving for various testing purposes

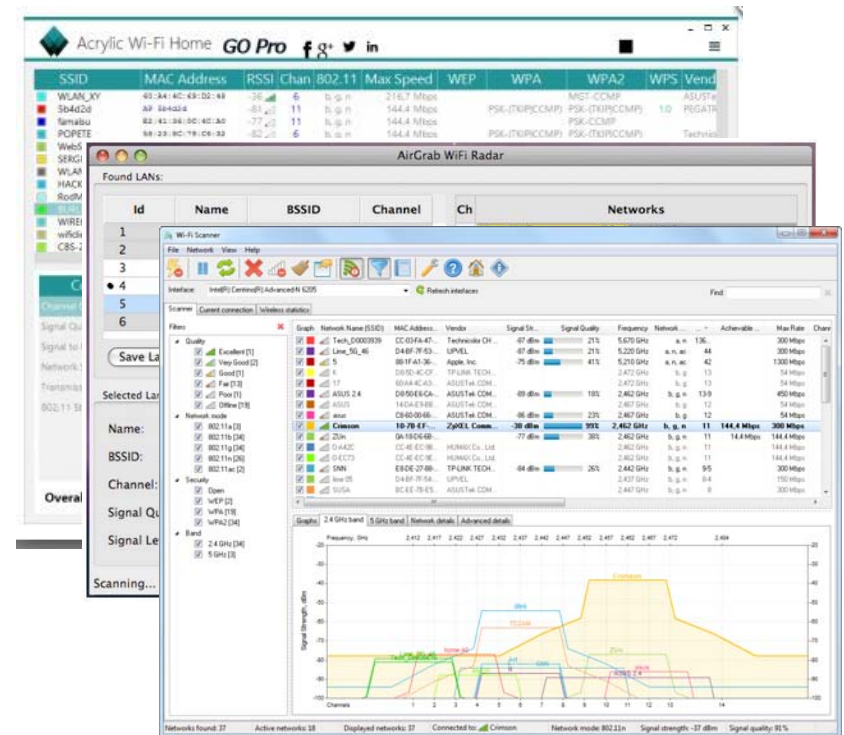
	Protocol	Summary
27:87:D7:F0	802.11 Encrypted ...	
27:87:D7:F0	802.11 WEP Data	
27:87:D7:F0	802.11 Encrypted ...	
27:87:D7:F0	802.11 Encrypted ...	
27:87:D7:F0	802.11 Encrypted ...	
27:87:D7:F0	802.11 Encrypted ...	
27:3B:1C:12	802.11 Encrypted ...	
27:87:D7:F0	802.11 Encrypted ...	
27:87:D7:F0	802.11 Encrypted ...	
27:87:D7:F0	802.11 Encrypted ...	
27:87:D7:F0	802.11 Encrypted ...	
27:87:D7:F0	802.11 Encrypted ...	
	802.11 BA	FC=.....
	802.11 Ack	FC=.....
27:87:D7:F0	802.11 Encrypted ...	FC=.F....W.,SN=3215,FN= 0
	802.11 BA	FC=.....
27:87:D7:F0	802.11 Encrypted ...	
27:87:D7:F0	802.11 Encrypted ...	
1F:3E:AE:21	802.11 Encrypted ...	
27:87:D7:F0	802.11 Encrypted ...	
27:87:D7:F0	802.11 Encrypted ...	
27:87:D7:F0	802.11 Encrypted ...	
27:87:D7:F0	802.11 Encrypted ...	
27:87:D7:F0	802.11 Encrypted ...	
27:87:D7:F0	802.11 Encrypted ...	
27:87:D7:F0	802.11 Encrypted ...	
27:87:D7:F0	802.11 Encrypted ...	



# Additional Software Troubleshooting Tools

## Wi-Fi Discovery Tools

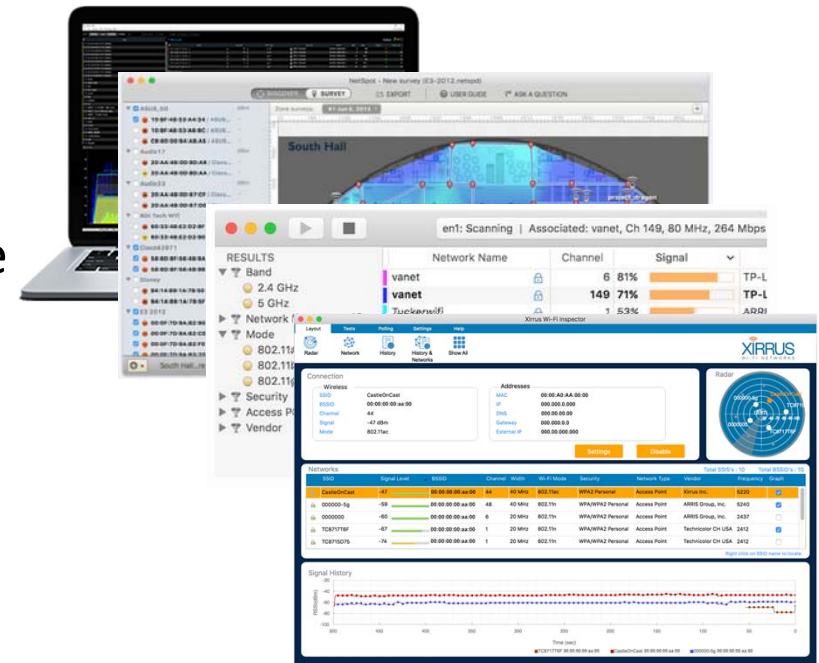
- Acrylic WiFi Home (Windows) - Free
- AirGrab WiFi Radar (Mac OSX) - Free
- LizardSystems Wi-Fi Scanner (Windows) - Free and purchase version



# Additional Software Troubleshooting Tools

## Wi-Fi Discovery Tools

- MetaGeek InSSIDer Office - Purchase
- NetSpot (Windows and Mac)
- WiFi Explorer (Mac) – Free and purchase version
- Xirrus (Riverbed) W-Fi Inspector (Windows and Mac) - Free



# Hardware Troubleshooting Tools

## Wi-Fi Test Tools

- Netscout LinkSprinter
- Netscout AirCheck G2
- Berkeley Varitronics Yellowjacket-BANG
- Netscout OptiView XG





---

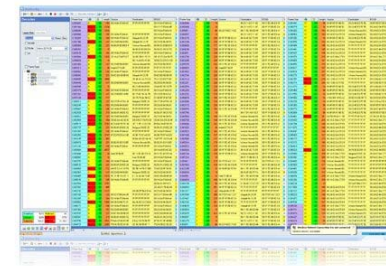
# Show Me The Data

## Protocol Analysis

# Troubleshooting Tools – Protocol Analyzers

## Types of Protocol Analyzers

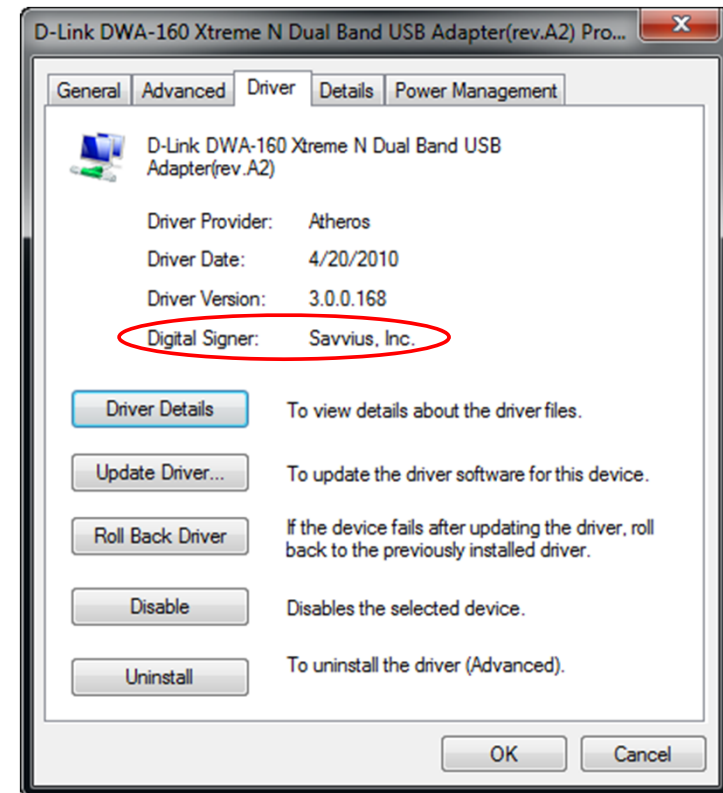
- Portable (Laptop)
- Infrastructure (Access Points)
- Distributed (Sensors)



# Troubleshooting Tools – Protocol Analyzers

## Network Adapter and Operation Modes

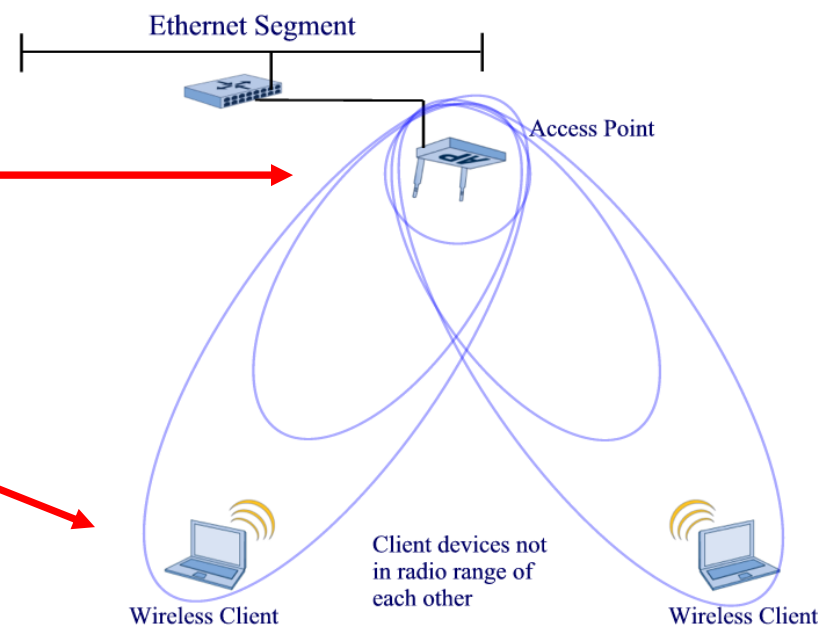
- Monitor vs Promiscuous Mode
- Supported Adapters
- Adapter Capabilities



# Troubleshooting Tools – Protocol Analyzers

## Protocol Analyzers Placement

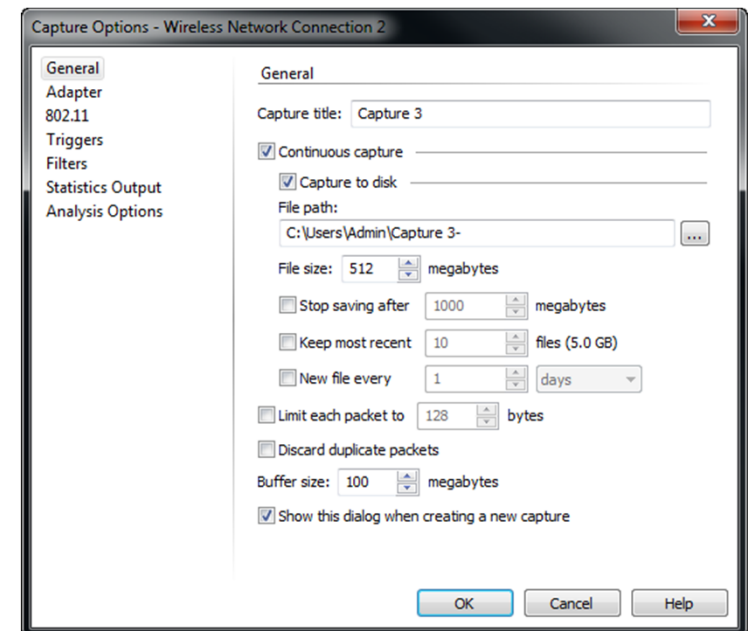
- Near Access Point?
- Near User?
- Moving?



# Troubleshooting Tools – Protocol Analyzers

## Common Protocol Analyzers Settings

- Filters
- RF Channel / Transitioning
- Save to Disk
- Naming



# Troubleshooting Tools – Protocol Analyzers

## Protocol Analyzers Packet List

- MAC Address Information
- Protocol Types
- Timing

Channel	Signal	Data Rate	Size	Relative Time	Protocol	Application	Summary
1	100%	39.0	239	0:01:35.020103	802.11 Encrypted ...		FC=T....W.,SN= 282,FN= 0
1	48%	24.0	32	0:01:35.020114	802.11 BA		FC=.....
1	14%	1.0	284	0:01:35.023376	802.11 Beacon		
1	24%	1.0	259	0:01:35.031223	802.11 Beacon		FC=.....,SN=2746,FN= 0,BI=100,..
1	12%	5.0	1502	0:01:35.049787	802.11 Encrypted ...		
1	44%	13.0	106	0:01:35.057896	802.11 Encrypted ...		FC=.F....W.,SN=1471,FN= 0
1	58%	11.0	106	0:01:35.058255	802.11 Encrypted ...		FC=.F.R..W.,SN=1471,FN= 0
1	46%	11.0	106	0:01:35.058695	802.11 Encrypted ...		FC=.F.R..W.,SN=1471,FN= 0
1	58%	5.0	20	0:01:35.058825	802.11 RTS		FC=.....
1	44%	5.0	20	0:01:35.059432	802.11 RTS		FC=.....
1	100%	5.0	14	0:01:35.059436	802.11 CTS		FC=.....
1	58%	5.0	106	0:01:35.059956	802.11 Encrypted ...		FC=.F....W.,SN=1471,FN= 0
1	100%	5.0	14	0:01:35.059959	802.11 Ack		FC=.....
1	58%	11.0	1554	0:01:35.061407	802.11 Encrypted ...		FC=.F....W.,SN=1472,FN= 0
1	100%	11.0	14	0:01:35.061410	802.11 Ack		FC=.....
1	58%	11.0	1554	0:01:35.062780	802.11 Encrypted ...		FC=.F....W.,SN=1473,FN= 0
1	100%	11.0	14	0:01:35.062784	802.11 Ack		FC=.....
1	44%	11.0	1306	0:01:35.063971	802.11 Encrypted ...		
1	100%	12.0	20	0:01:35.064540	802.11 RTS		FC=.....
1	100%	5.0	14	0:01:35.068081	802.11 Ack		FC=.....
1	44%	11.0	1554	0:01:35.069576	802.11 Encrypted ...		FC=.F....W.,SN=1475,FN= 0
1	100%	11.0	14	0:01:35.069592	802.11 Ack		FC=.....

# Troubleshooting Tools – Protocol Analyzers

## Protocol Analyzers Decodes

- Radiotap Header / Packet Info
- Not Layer 2 Information
- Derived from Physical Layer Header or Driver

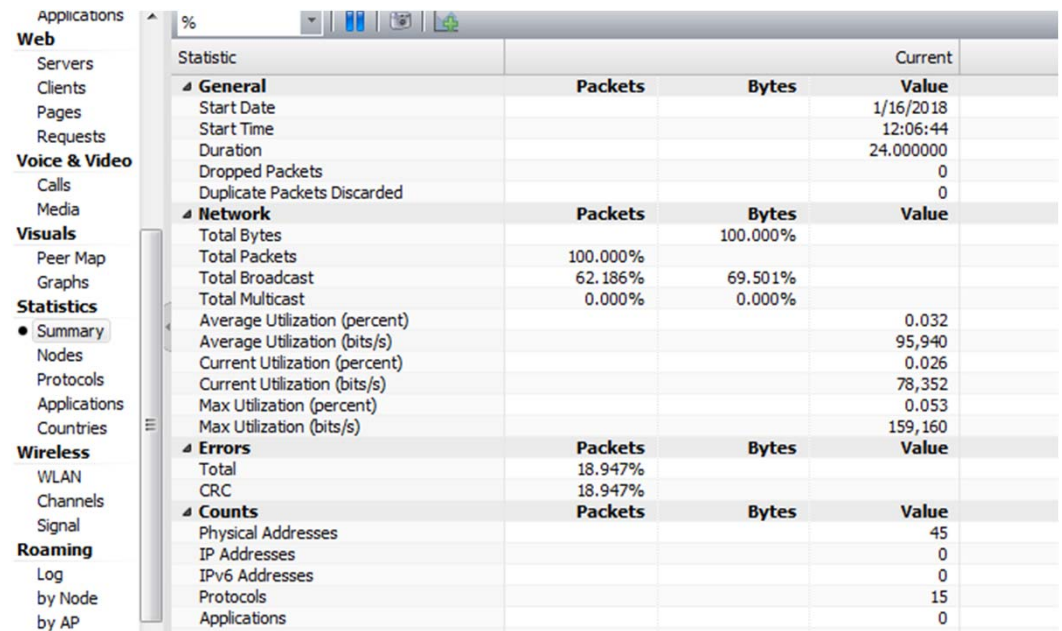
```
Packet Info
  Packet Number: 9
  Flags: 0x00000000
  Status: 0x00000000
  Packet Length: 227
  Timestamp: 12:03:33.651885900 01/16/2018
  Data Rate: 12 6.0 Mbps
  Channel: 100 5500MHz 802.11n 20MHz
  802.11 Flags: %00000000000000000000000000000000
  Signal Level: 100%
  Signal dBm: -18
  Noise Level: 0%
  Noise dBm: -127
  802.11 MAC Header
  Version: 0 [0 Mask 0x03]
  Type: %00 Management [0 Mask 0x0C]
  Subtype: %1000 Beacon [0 Mask 0xF0]
```



# Troubleshooting Tools – Protocol Analyzers

## Protocol Analyzers General Information

- Channel Information
- Statistics



The screenshot shows a software interface for a protocol analyzer. On the left is a navigation tree with categories like Web, Voice & Video, Visuals, Statistics, Wireless, and Roaming. The 'Statistics' section is expanded, showing a table of metrics. The table has columns for 'Statistic', 'Packets', 'Bytes', and 'Value'. It is divided into sections: General, Network, Errors, and Counts. The 'Current' column shows real-time values for various metrics.

Statistic	Packets	Bytes	Value	Current
<b>General</b>				
Start Date				1/16/2018
Start Time				12:06:44
Duration				24.000000
Dropped Packets				0
Duplicate Packets Discarded				0
<b>Network</b>				
Total Bytes		100.000%		
Total Packets	100.000%			
Total Broadcast	62.186%	69.501%		
Total Multicast	0.000%	0.000%		
Average Utilization (percent)				0.032
Average Utilization (bits/s)				95,940
Current Utilization (percent)				0.026
Current Utilization (bits/s)				78,352
Max Utilization (percent)				0.053
Max Utilization (bits/s)				159,160
<b>Errors</b>				
Total	18.947%			
CRC	18.947%			
<b>Counts</b>				
Physical Addresses				45
IP Addresses				0
IPv6 Addresses				0
Protocols				15
Applications				0



# Show Me The Data

So, Let's Get Physical



# Wireless LAN Troubleshooting Tools

Common Layer 1 Physical Layer (aka The PHY)  
Troubleshooting Tools

# Layer 1 Physical Layer (PHY) - Troubleshooting Tools

## Instrumentation Spectrum Analyzers

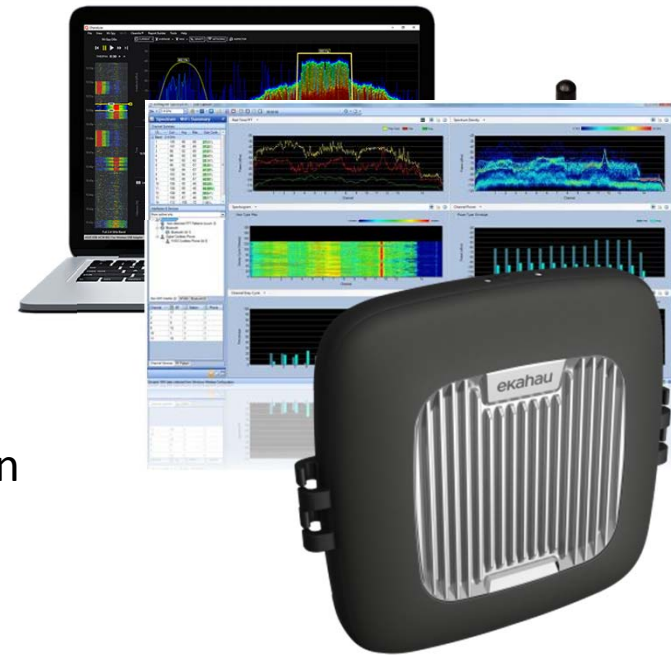
- Tektronix
- Rohde & Schwarz
- RF Explorer



# Layer 1 Physical Layer (PHY) - Troubleshooting Tools

## Wi-Fi Centric Spectrum Analyzers

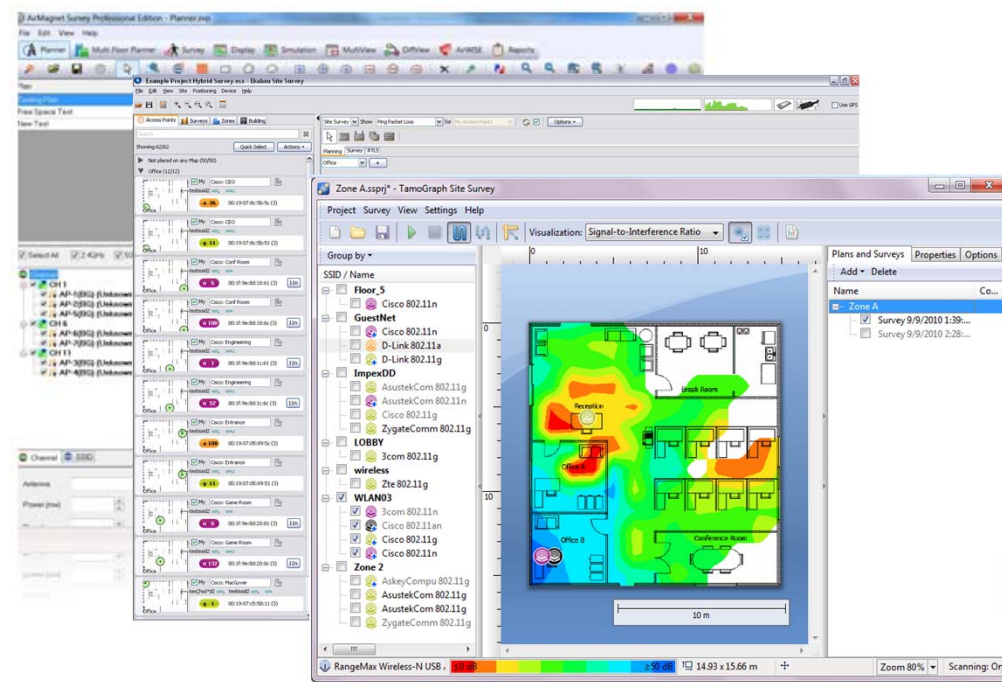
- MetaGeek Chanalyzer + Wi-Spy DBx
- Netscout Spectrum XT
- Ekahau Sidekick
- Not just for troubleshooting
  - Spectrum analyzers are also used with design



# Layer 1 Physical Layer (PHY) - Troubleshooting Tools

## Site Survey / Design Software

- Netscout Survey Pro
- Ekahau Site Survey
- Tamosoft TamoGraph



---

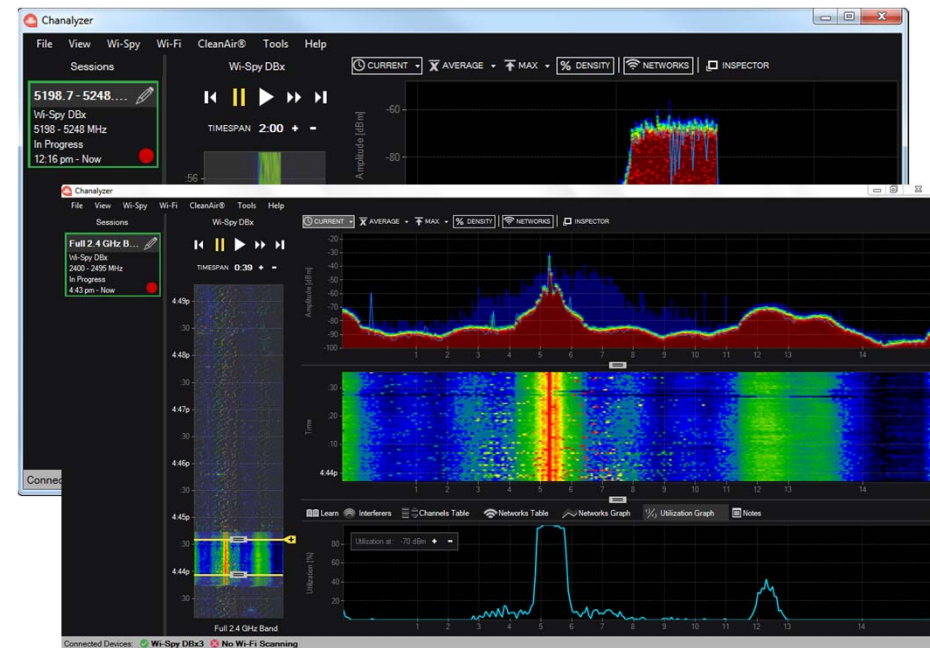
# Show Me The Data

## Spectrum Analysis

# Troubleshooting Tools – Spectrum Analyzers

## Spectrum Analysis Allows You To

- “See” Your Wi-Fi
  - Visualize Unbounded Medium
- View Interference Types
  - Both Wi-Fi and Non-Wi-Fi

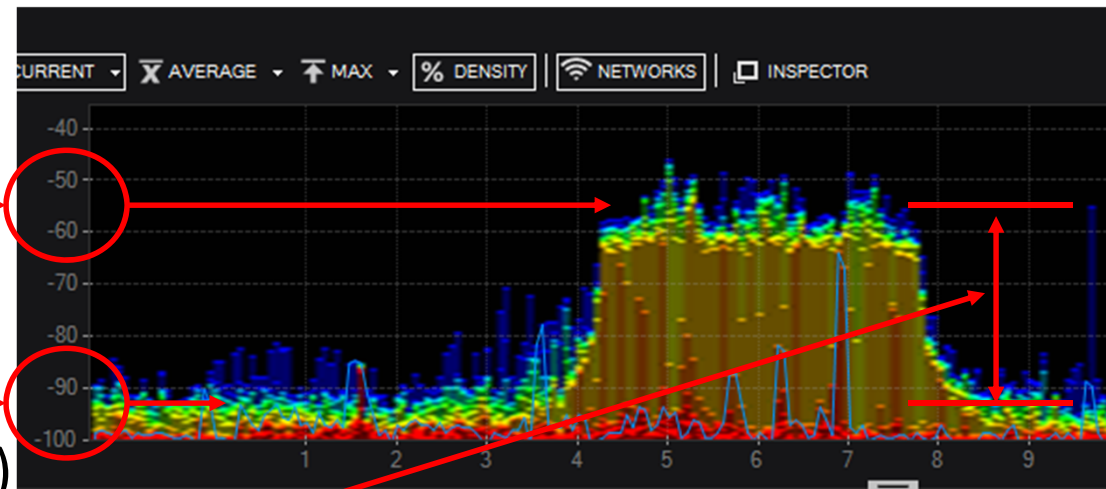




# Troubleshooting Tools – Spectrum Analyzers

## View Key Information

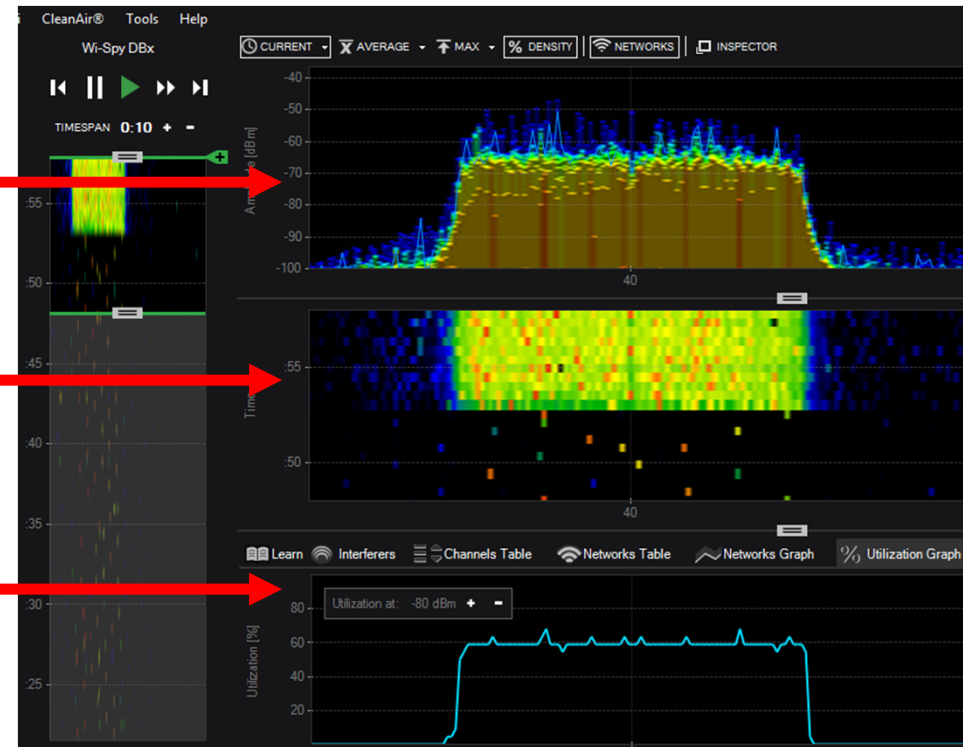
- Signal Strength
  - Received signal (-55 dBm)
- RF Noise Floor
  - Unwanted signal (-95 dBm)
- Signal to Noise Ratio (SNR)
  - Difference between signal and noise
    - »  $-55 \text{ dBm} - (-95 \text{ dBm}) = +40 \text{ dBm}$



# Troubleshooting Tools – Spectrum Analyzers

## View Key Information

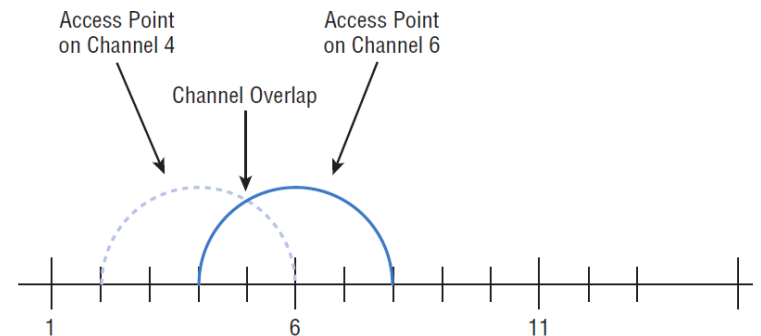
- Real Time FFT
  - Amplitude over frequency
- Waterfall
  - RF signal over a period of time
- Channel Utilization
  - RF activity on the channel



# Troubleshooting Tools – Spectrum Analyzers

## Spectrum Analysis Allows You To See

- Co-channel Interference (Wi-Fi)
- Overlapping Channel Interference (Wi-Fi)
- Non-Wi-Fi Interference
- Much More



---

# Show Me The Data

## Spectrum Analyzer Demonstration

# Thank You!

Robert Bartz

E-mail: [robert@eightotwo.com](mailto:robert@eightotwo.com)

Twitter: [@eightotwo](https://twitter.com/eightotwo)

