We’re ready. Are you?
Analysing and Fixing WiFi Issues – Cisco WLC Tools and Packet Capture Analysis Techniques

Byung Wook Cho, Wireless Escalation Sydney
Agenda

• Introduction
• Troubleshooting Methodology
• WiFi Tools
• Sample Analysis
• Conclusion
• Q & A
Introduction
Troubleshooting Methodology
Structured Troubleshooting Method

- A structured troubleshooting is an efficient way of troubleshooting
“Shoot from the Hip” Troubleshooting

- Experience can lead to faster resolution at times
“Top-Down” Troubleshooting

- Using OSI model as a guidance, troubleshoot from Application to Physical Layer

<table>
<thead>
<tr>
<th>Layer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Application</td>
</tr>
<tr>
<td>6</td>
<td>Presentation</td>
</tr>
<tr>
<td>5</td>
<td>Session</td>
</tr>
<tr>
<td>4</td>
<td>Transport</td>
</tr>
<tr>
<td>3</td>
<td>Network</td>
</tr>
<tr>
<td>2</td>
<td>Data Link</td>
</tr>
<tr>
<td>1</td>
<td>Physical</td>
</tr>
</tbody>
</table>

Problem: Client can’t browse the website but can establish TCP connection on port 80.

Conclusion: L1-L4 is okay. Therefore, not a network problem. Must be a problem with the client or the server.
“Bottom-Up” Troubleshooting

- Troubleshoot from Physical to Application Layer

Problem: Interfaces are UP and can see mac address in the CAM table but can’t ping the device.

Conclusion: L1-L2 is okay. Must be a problem on the network layer.
“Divide-and-Conquer” Troubleshooting

- Start in the middle and either move Up or Down the OSI layer

Problem: Can’t ping the device.

Conclusion: No need to troubleshoot from Application Layer. Check the mac address in the CAM table.
“Follow-the-Path” Troubleshooting

• Trace the path between source and destination to eliminate scope
"Spot-the-Difference" Troubleshooting

• Compare working vs non-working
“Move-the-Problem” Troubleshooting

- Isolate the issue by moving or changing components

Problem: User A can surf the internet but User B cannot. Unfortunately, no admin access is possible to User B.

Conclusion: Move User B to another port on the switch. If same, try swapping out the cable.
WiFi Tools
Where Are We Focusing?

• Tools that will enable you to troubleshoot in wireless space
WLCCA

- Cisco in-house built tool that is available to anyone who has a CCO user-id
- Saves you time in analysing config files from AireOS platforms as well as NGWC platforms
- Multiple controller config within same mobility group can be opened simultaneously
- Identifies Cisco best practices deviation and makes recommendations
- Provides snapshot of RF health (Neighbor AP Tx/Rx Power, Channel Utilisation, Noise/Interference, Low SNR clients and so much more) to quickly isolate cause of various issues such as frequent client disconnect or poor voice quality
- Highlights critical error messages detected by AP
WLCCA

- Works in most (if not all) Windows OS

- Collect ‘show run-config’ from AireOS platform or ‘show tech’ or ‘show tech-wireless’ from NGWC platform. Make sure to disable paging before collecting the outputs to minimise parsing errors.

- It’s a snapshot (not real time). Remember, RF constantly changes over time. Good idea to run the tool multiple times to understand RF behaviour especially after a change is made in the config.
WLCCA

Voice
(Optional) Click to enable voice related deployment checks
WLCCA - Tab 1

Device Data
This is where you’ll be spending most of your time searching for answers to your problem. Information you’ll find include:

- WLC Configuration
- AP Configuration
- RF Stats
- RF Health Details
WLCCA – Tab 1 (Best Practices)

Best Practices
Colour code gives quick summary of areas that aren’t compliant to Cisco’s best practices recommendations.

Colour Code:
Red – Bad
Orange – Not bad
Green – Good

Description field will pretty much spell out reason as to why it’s good or bad.
WLCCA - Tab 1 (RF Health)

Green
Good. No need to action anything.

Red
This is bad. Fix it ASAP.

Yellow
Not bad. Could be better though.

The Health score represents the lowest score achieved by an AP across different RF parameters instead of using the average score. This ensures that we are not masking an issue.
WLCCA - Tab 1

• Definitions:
  • **Health** – Overall score that represents RF quality of an AP. This is the lowest score achieved from all RF metrics.
  • **Neighbor Channel Capacity** – RF score that represents impact caused by neighboring APs of an AP.
  • **Neighbor Overlap Avoidance** – RF score that represents co-channel interference of an AP.
  • **Neighbor Impact Side Channel** – Impact caused by neighboring APs on the side channel of an AP.
  • **AP Channel Capacity** – Channel Utilisation of an AP.
  • **Noise Same Channel** – Noise detected on the same channel of an AP.
  • **Interference Same Channel** – Interference detected on the same channel of an AP.
  • **Low SNR Clients** – Minimum of 5 clients with low SNR detected on an AP.
WLCCA – Tab 2 (AP Neighbor)

AP Nearby Info

This is where you'll be spending second most of your time searching for answers to your problem.

Gives details on how many APs we are hearing at what power and what channel from the selected AP perspective. Will give ultimate answer to whether there is too much or too little APs for the environment.
Voice Messages
This is where you’ll find error messages relating to voice.

| AP-2052-09 | Config Error | 40022. Voice: SSID W2052 Platinum QoS settings are not set to 802.1p, check in Controller QoS Profiles |
| AP-2052-09 | Config Error | 40030. Voice: WLAN with EAP, without CCKM, roaming would be disrupted, WLAN:W2052 |
Global Messages
This is where you’ll find error messages logged in the WLC.

Different Category gives different level of details. But RED means you need to fix it.

| WA-SS-CWLC02 | Best Practices | 120003, Security: It is recommended to monitor all channels for rogue detection. Band: 5 GHz |
| WA-SS-CWLC02 | Best Practices | 120003, Security: It is recommended to monitor all channels for rogue detection. Band: 2.4 GHz |
WLCCA - Tab 5 (AP)

AP Messages

This is where you’ll find error messages logged in the AP.

AP-2052-44 Informational 60015:RF AP detected a persistent device with duty cycle higher of 100, type Video Camera on band 2.4...
WLCCA - Tab 6 (Parsing)

Parsing Errors
This is where you’ll find error messages that resulted in WLCCA failing to interpret the data correctly.

| WA-SS-CWLC02 | Parsing Error | 10011, Exception catch parsing file | Possible wrong date format during AP Checks in AP: AP-2052-58 |
Need more info?

• More info can be found at Cisco Support Community for WLCCA available at https://supportforums.cisco.com/community/12168506/wireless-lan-controller-config-analyser-wlcca

• WLCCA is an internal tool only to share with the community

• Want to use this tool? Send your request to wlc-conf-app-dev@cisco.com along with your CCO user-id.

• Found a bug? Report it to wlc-conf-app-dev@cisco.com

• Have a great idea you’d like to suggest as an enhancement to the tool? Report it to wlc-conf-app-dev@cisco.com
Wireshark Capture Using NGWC

• A built-in tool that can be used for wireless capture (via CAPWAP tunnel)
• Requires 3.3.0 IOS-EX or higher
• Feature also available in 3850, 3650 and 5760 model
• Can capture multiple CAPWAP tunnels simultaneously
• Captures are stored in either local flash or USB drive (in .pcap file format)
• Can use CLI to analyse the captures but much easier to export the captures (via FTP, HTTP, HTTPS, TFTP) and use PC Wireshark
Wireshark Capture Using NGWC

```
C3650#monitor capture ?
   WORD  Name of the Capture

C3650#monitor capture wifi ?
   access-list   access-list to be attached
   buffer       Buffer options
   class-map    class name to attached
   clear        Clear Buffer
   control-plane Control Plane
   export       Export Buffer
   file         Associated file attributes
   interface    Interface
   limit        Limit Packets Captured
   match        Describe filters inline
   start        Enable Capture
   stop         Disable Capture
   vlan         Vlan
```
Wireshark Capture Using NGWC

Once this buffer is full, any further packets will not be captured.
Wireshark Capture Using NGWC

```
C3650#dir flash:wifi.pcap
Directory of flash:/wifi.pcap

  80816  -rw-   249781 Jan 29 2016 23:37:27 +11:00  wifi.pcap

1562509312 bytes total (415440896 bytes free)
C3650#dir flash:wifi.pcap
Directory of flash:/wifi.pcap

  80816  -rw-   274623 Jan 29 2016 23:37:31 +11:00  wifi.pcap

1562509312 bytes total (415412224 bytes free)
```
Wireshark Capture Using NGWC

```
<table>
<thead>
<tr>
<th>C3650#show monitor capture file flash:wifi.pcap brief</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  0.000000 00:00:00:00:00:00:00:00 $00000000</td>
</tr>
<tr>
<td>2  0.429030 64:d9:89:42:29:70 $00000000</td>
</tr>
<tr>
<td>3  1.400025 fe80::c6ea:1dff:fe12:37f4 $00000000</td>
</tr>
<tr>
<td>4  1.400025 fe80::c6ea:1dff:fe12:37f4 $00000000</td>
</tr>
<tr>
<td>5  2.445021 fe80::c6ea:1dff:fe12:37f4 $00000000</td>
</tr>
<tr>
<td>6  2.552025 fe80::2acf:e9ff:fe20:f883 $00000000</td>
</tr>
<tr>
<td>7  4.500026 00:00:00:00:00:00:00:00 $00000000</td>
</tr>
<tr>
<td>8  7.182034 192.168.24.16 $00000000</td>
</tr>
<tr>
<td>9  8.457029 192.168.24.16 $00000000</td>
</tr>
<tr>
<td>10 9.500026 00:00:00:00:00:00:00:00 $00000000</td>
</tr>
<tr>
<td>12 12.813013 64:d9:89:42:29:70 $00000000</td>
</tr>
<tr>
<td>13 14.000000 00:00:00:00:00:00:00:00 $00000000</td>
</tr>
</tbody>
</table>

--More--
```
Wireshark Capture Using NGWC

C3650#show monitor capture file flash:wifi.pcap detail
Frame 1: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
  Arrival Time: Jan 29, 2016 12:31:06.843950000 UTC
  Epoch Time: 1454070666.843950000 seconds
  [Time delta from previous captured frame: 0.000000000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Frame Length: 122 bytes (976 bits)
Capture Length: 122 bytes (976 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
Wireshark Capture Using NGWC

C3650#show monitor capture file flash:wifi.pcap detail | section Frame 1
Frame 1: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
  Arrival Time: Jan 29, 2016 12:31:06.843950000 UTC
  Epoch Time: 1454070666.843950000 seconds
  [Time delta from previous captured frame: 0.000000000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 0.000000000 seconds]
  Frame Number: 1
  Frame Length: 122 bytes (976 bits)
  Capture Length: 122 bytes (976 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
Frame 10: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
  Arrival Time: Jan 29, 2016 12:31:16.343976000 UTC
Wireshark Capture Using NGWC

```
C3650#show monitor capture file flash:wifi.pcap detail | count Probe
Number of lines which match regexp = 284
C3650#show monitor capture file flash:wifi.pcap brief | exclude DTLS

1 0.000000 00:00:00:00:00:00:00:00 -> 64:d9:89:42:29:70 IEEE 802.11 Probe Request, SN=0
2 0.429030 64:d9:89:42:29:70 -> 64:d9:89:42:29:70 WLCCP U, func=UI; SNAP, OUI 0x0
3 1.400025 fe80::c6ea:1dff:fe12:37f4 -> fe80::462a:60ff:ff6:5a32 ICMPv6 Neighbor
4 1.400025 fe80::462a:60ff:ff6:5a32 -> fe80::c6ea:1dff:fe12:37f4 ICMPv6 Neighbor
5 2.445021 fe80::c6ea:1dff:fe12:37f4 -> fe80::2acf:e9ff:fe20:f883 ICMPv6 Neighbor
6 2.552025 fe80::2acf:e9ff:fe20:f883 -> fe80::c6ea:1dff:fe12:37f4 ICMPv6 Neighbor
7 4.500026 00:00:00:00:00:00:00:00 -> 64:d9:89:42:29:70 IEEE 802.11 Probe Request, SN=0
10 9.500026 00:00:00:00:00:00:00:00 -> 64:d9:89:42:29:70 IEEE 802.11 Probe Request, SN=0
13 14.000000 00:00:00:00:00:00:00:00 -> 64:d9:89:42:29:70 IEEE 802.11 Probe Request, SN=0
15 18.500026 00:00:00:00:00:00:00:00 -> 64:d9:89:42:29:70 IEEE 802.11 Probe Request, SN=0
```
Wireshark Capture Using NGWC

- Best to export the capture and analyse using PC wireshark

```
C3650#copy flash:wifi.pcap ftp:
Address or name of remote host []? 192.168.24.14
Destination filename [wifi.pcap]?
!!!
515074 bytes copied in 0.400 secs (1287685 bytes/sec)
C3650#
*Jan 29 13:06:18.416: Writing wifi.pcap
```
Wireshark Capture Using NGWC

• Here’s how it looks like in PC wireshark

No Radiotap

Frame 1: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
User Datagram Protocol, Src Port: 80 (HTTP), Dst Port: 5000 (HTTP)
Control And Provisioning of Wireless Access Points – Data
IEEE 802.11 Probe Request, Flags: ........
IEEE 802.11 wireless LAN management frame
Packet Dump In AireOS
Packet Dump Using AireOS

• Can capture over the air traffic for a specific client remotely
• Not supported in 32MB radio platforms (ie. 1130, 1240)
• Only captures packet header information (ie. no radiotap)
• Captures are streamed to an external FTP server (*.pcap format only) which can then be opened using 3rd party application such as Wireshark or Omnipeek
• FTP server must be reachable by the AP during the capture period
• If FTP transfer time is slower than the packet rate, some of the packets will be missed
Packet Dump Using AireOS

• Before starting the capture, define initial parameters

```
(WLC) >config ap packet-dump ?

buffer-size  Set Buffer Size for Packet Capture
capture-time  Set Time for Packet Capture
classifier    Set Classifiers for Packet capture
ftp           Set FTP parameters for Packet Capture
start         Start Packet Capture at AP
stop          Stop Packet Capture
truncate      Set Packet Length after Truncating

(WLC) >config ap packet-dump ftp serverip 10.137.76.146 path / username bcho password cisco
```
Packet Dump Using AireOS And NGWC

• Define what you want to capture

(WLC) >config ap packet-dump classifier?

arp          Capture ARP Packets
broadcast    Capture Broadcast Packets
data         Capture 802.11 Data Packets
dot1x        Capture Dot1x Packets
iapp         Capture IAPP Packets
ip           Capture IP Packets
management   Capture 802.11 Management Packets
multicast    Capture Multicast Packets
tcp          Capture TCP packets
udp          Capture UDP packets

(WLC) >config ap packet-dump classifier management enable
Packet Dump Using AireOS

• More classifiers

```plaintext
(WLC) >config ap packet-dump classifier broadcast enable

(WLC) >config ap packet-dump buffer-size ?
<Size in KB>    Size of Buffer (1024 – 4096)

(WLC) >config ap packet-dump buffer-size 1024

(WLC) >config ap packet-dump capture-time ?
<Time in Min>    Time in for Packet Capture (1 - 60 Minutes)
```
Packet Dump Using AireOS

- Optional parameters to limit how much to capture

```
(WLC) >config ap packet-dump capture-time 3

(WLC) >config ap packet-dump truncate ?
<Length in Bytes> Length of Packet after Truncation (20 - 1500)

(WLC) >config ap packet-dump truncate 1500
```
Packet Dump Using AireOS

- Checking status of the capture

```
(WLC) > show ap packet-dump status

Packet Capture Status....................... Stopped
FTP Server IP Address....................... 10.137.76.146
FTP Server Path.............................. /
FTP Server Username......................... bcho
FTP Server Password........................ *******
Buffer Size for Capture..................... 1024 KB
Packet Capture Time......................... 3 Minutes
Packet Truncate Length...................... 1500 Bytes
Packet Capture Classifier................... 802.11 Management
Packet Capture Classifier................... Broadcast
```
Packet Dump Using AireOS

• Start the capture

(WLC) >config ap packet-dump start ?

<MAC addr>  Set Client Mac Address for Packet Capture

(WLC) >config ap packet-dump start d0:22:be:73:d3:d0 ?

<Cisco AP>  Enter the name of the Cisco AP.

(WLC) >config ap packet-dump start d0:22:be:73:d3:d0 AP2702I-AS-1

Client Mac Address.........................  d0:22:be:73:d3:d0
FTP Server IP...............................  10.137.76.146
FTP Server Path.............................  /
FTP Server Username.......................  bcho
Buffer Size for Capture...................  1024 KB
Packet Capture Time.......................  3 Minutes
Packet Truncate Length....................  1500 Bytes
Packet Capture Classifier...............  802.11 Management
Packet Capture Classifier...............  802.11 Broadcast

Are you sure you want to start capture? (y/N) y
Packet Dump Using AireOS

• If all goes well...

(WLC) >*emWeb: Jan 22 09:40:38.918: Encode AP Packet Dump payload in a buffer
*emWeb: Jan 22 09:40:38.919: Capwap message to AP 74:a0:2f:fc:52:00 for Packet capture
*emWeb: Jan 22 09:40:38.919: Packet Capture Started in AP AP2702I-AS-1
*emWeb: Jan 22 09:40:38.919: Started timer for AP Packet capture 3 minutes

AP2702I-AS-1#
*Jan 21 22:40:38.779: PAKDUMP EVENT: Set parameters for Packet capture client d022.be73.d3d0 pakCap Status 1
*Jan 21 22:40:38.779: PAKDUMP EVENT: userId bcho serverIp 10.137.76.146 path Desktop
*Jan 21 22:40:38.779: PAKDUMP EVENT: classifier 1311 udpPort 0 tcpPort 0 bufferSize 4096 truncateLength 1500
*Jan 21 22:40:38.927: PAKDUMP EVENT: FTP Init time is 148 msecs
*Jan 21 22:40:38.927: PAKDUMP EVENT: dtdls_data_encrypted 0
*Jan 21 22:40:38.939: PAKDUMP EVENT: Started Packet capture for client d022.be73.d3d0
*Jan 21 22:40:59.043: PAKDUMP EVENT: ftp_send bytes_sent 13690 size 13690 dummyPktSize 590
Packet Dump Using AireOS

- If all goes well...

<table>
<thead>
<tr>
<th>File Path</th>
<th>Size</th>
<th>Date</th>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/Desktop/bcho$ ls -l *.pcap</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-r--r-- 1 bcho staff 28498 22 Jan 09:06 AP2702I-AS-1vWLC-BCHO-021012016_220354.pcap</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-r--r-- 1 bcho staff 10992974 22 Jan 09:43 AP2702I-AS-1vWLC-BCHO-021012016_224038.pcap</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-r-xr-x 1 bcho staff 849242 16 Sep 09:41 Test-#21_Filtered.pcap</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-r--r-- 1 bcho staff 25147 13 Oct 13:11 airtool_test.pcap</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw------- 1 bcho staff 6809811 18 Jan 15:36 ap-sniffer-mode-test-capture.pcap</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Packet Dump Using AireOS

- Open the capture in Wireshark

No Radiotap
Packet Dump Using NGWC

• Feature also available in IOSE XE 3E release

```
C3650(config)#ap packet-dump classifier control
C3650(config)#ap packet-dump ftp serverip 1.2.3.4 path /temp user test password test123
C3650(config)#exit
C3650#ap name ?
   WORD   Enter access point name

C3650#ap name AP2702I-1 packet-dump ?
   start    Start packet capture at AP
   stop     Stop packet capture at AP

C3650#ap name AP2702I-1 packet-dump start ?
   H.H.H   Set client MAC address for packet capture
```
Sniffer Mode AP
Sniffer Mode AP

- AP can be set to “sniffer mode” to capture WiFi traffic.
- AP in “sniffer mode” cannot service wireless clients
- Define a specific channel in 802.11b or 802.11a radio to capture the WiFi traffic.
- Requires external application such as Omnipeek or Wireshark to capture the traffic.
Sniffer Mode AP

- Select Sniffer mode
Sniffer Mode AP

- Select channel to listen on and specify server IP address to send traffic to for collection using Wireshark
Sniffer Mode AP

- In your remote PC running Wireshark, specify the interface and filter to only collect traffic from the AP.

Sniffer mode AP always uses UDP 5555 as source port.
Sniffer Mode AP

- Captured traffic will be displayed as UDP. Need to decode as PEEKREMOTE.
Sniffer Mode AP

- Now you can see 802.11 details

![Sniffer Mode AP Example](image.png)
Wireshark
Wireshark

• Most popular tool used in deep packet analysis (wired and wireless)
• Doesn’t require a license (ie. free for all)
• Can be used to capture WiFi traffic directly but depending on OS, maybe difficult (ie. in Windows, interaction between application and adaptor is almost impossible)
• Only certain wifi adaptors work
• Can be used to read captures from 3rd party application such as Omnipeek
Wireshark

- Sample wireshark capture

Display Filters

Frame Captures

Frame Details

Of particular interest is the radiotap which contains information such as RSSI, Noise, Channel Utilisation and QoS

Frame Info

Probes
Beacons
Authentication
Association
Power Save Polling
Encrypted Data
Wireshark

- Customize the view to quickly find what you want to see

Apply as Column

Right click on any parameters in the frame details to add as new column.

Some important columns to add for troubleshooting WiFi issues:
- RSSI (dBm)
- Noise (dBm)
- Channel
- Utilisation (%)
- DSCP/UP
Wireshark

• Use of coloring can help quickly spot frames of interest

Define the name, colour and filter that defines the frames.
Wireshark

• Apply the colour to display the frames.
Wireshark

- Display filters are your friend

Apply as Filter
Apply the selected filter or combine with other existing filters (if any)

Source address
Right click on any field to create/apply as a display filter

When combining multiple filters, you can use operators such as:
- And
- Or
- And not
- Or not
Wireshark

- Once you become familiar with filters, you can apply it directly as well.

\[
wlan.fc.type == 0
\]

Wireshark will tell you if your filter code is correct (GREEN means correct and RED means incorrect).
Wireshark

- Here are some useful filters used in wifi.

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

- Full comprehensive filters for WiFi troubleshooting can be found at https://www.wireshark.org/docs/dfref/w/wlan.html
Omnipeek
Omnipeek – What is it?

- Packet analyser from Savvius (3\textsuperscript{rd} party).
- Used for troubleshooting and analysing WiFi issues.
- License is required to use this tool.
- Able to capture as well as read WiFi packet captured using ORA (Omnipeek Remote Assistance) which is provided to customers free of charge.
- ORA encrypts the captures which can only be opened using Omnipeek Enterprise which can then be converted to other file extension to open in another application such as Wireshark.
- Has many built-in WiFi attributes that can be added as extra columns or filters to assist in analysing captures
# Omnipeek – Supported Adaptors

- Full list of supported WiFi adaptor and drivers can be found at [https://techzone.cisco.com/t5/Troubleshooting-and-Tools/Adapters-and-Drivers-for-OmniPeek/ta-p/487509](https://techzone.cisco.com/t5/Troubleshooting-and-Tools/Adapters-and-Drivers-for-OmniPeek/ta-p/487509)

<table>
<thead>
<tr>
<th>Adaptor Model</th>
<th>Supported Drivers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linksys AE6000</td>
<td>MediaTek/Ralink 5.1.12.48</td>
</tr>
<tr>
<td>CB21AG</td>
<td>Atheros 4.2.2.9</td>
</tr>
<tr>
<td>AirMagnet C1060</td>
<td>Atheros 6.0.4.13</td>
</tr>
<tr>
<td>D-Link DWA-160 Rev B2</td>
<td>Ralink 3.2.4.5</td>
</tr>
<tr>
<td>Linksys WUSB600N</td>
<td>Ralink 1.4.0.18</td>
</tr>
</tbody>
</table>
Omnipeek

- Look and feel is similar to Wireshark but much more tailored to WiFi analysis

Options

Each selection provides unique analytics that can guide users in interpreting the captures easily.

Decode View

Selected packet details can be seen here.

Packet List

All 802.11 packets captured can be seen here.

Hex View

Raw format of actual captures
Omnipeek – Filters

Name
A unique name that identifies the filter.

Type
Type of filter. Select Wireless Address.

Address 1
Source mac-address of WiFi client.

Direction
Source & Destination
Omnipeek – Customisable Column

Packet List Options
Delete or add information columns as required that will help troubleshoot issue you are trying to solve.
Omnipeek – Compass

Compass
Provides various unique analytics to quickly identify possible issues
Which Tool Do I Use?

• Use Packet Dump if you don’t have a 3rd party application that can capture WiFi traffic and you are targeting a specific issue such as “WiFi client does not get an IP” or “Voice quality issues”. Remember, no radiotap header.

• Use Wireshark Capture if you don’t have a 3rd party application that can capture WiFi traffic and you want to see what’s happening from an AP point of view. No radiotap header here either.

• Sniffer Mode AP has the advantage of seeing more details about the WiFi packet (ie. radiotap header which contains info about RSSI, data rate, etc).

• Omnipeek can capture everything happening over the air.
Sample Analysis
Exporting Frames For Statistical Analysis

- Analysing large amount of wifi captures are at times very difficult
- Would be easier to graphically display the result and recognise patterns instead
- Wireshark do have a built-in graphical tool but is a bit challenging in knowing which filters to apply
- Instead, can export the filtered data to Excel which you can then easily display multiple types of graphs
- Let me show you
Exporting Frames For Statistical Analysis

• First, let’s filter the Wireshark data to observe a particular client.

Exporting Frames For Statistical Analysis

• Next, export the data to CSV format.
Exporting Frames For Statistical Analysis

- Next, import the CSV file into Excel and select the axis you want to graph.
Exporting Frames For Statistical Analysis

• Under Charts, select “Straight Marked Scatter” to ensure relative values are displayed.
Example 1 – iPhone 5S One-Way Audio

- Here’s a sample graph of a 7925 moving away from an AP (no issue).

Nice Tx at 54Mbps, ACK at 24Mbps. Sometimes Tx at 24Mbps.
Example 1 – iPhone 5S One-Way Audio

- The same 7925 at the end of the cell coverage area

<table>
<thead>
<tr>
<th>Tx Data Rate (Mbps)</th>
<th>Time (sec)</th>
</tr>
</thead>
</table>

7925 tries 54 Mbps, then fails, reverts to slower rate, gets ACK, then tries again 54 Mbps…

The 7925 also maintains a failed counter, eventually the phone gives up on the connection because of the retry count… good phone!
Example 1 - iPhone 5S One-Way Audio

• Sample graph of an iPhone 5S moving away from the same AP (one way voice).

Strange that the rate is increasing as distance is increasing.
Example 1 - iPhone 5S One-Way Audio

- The same iPhone 5S at the end of the cell coverage area

iPhone is in the same cell… but never tries lower than 24 Mbps… even tries higher rates sometimes

Issue: behavior is RSSI-based, not retry count
Example 1 - iPhone 5S One-Way Audio

• The roaming behavior between 7925 and iPhone 5S was different.

• 7925 kept an eye on the retry count. Once, the retry count reached a threshold, it looked for a better AP to roam to and it eventually roamed.

• iPhone 5S remained associated to the same AP even though retry count increased because it decided the RSSI was “good enough” to remain associated.

• AP Tx power was sufficient for the iPhone 5S to hear but iPhone 5S Tx power wasn’t enough for the AP to hear. Hence, the one-way audio.

• Can reduce AP Tx power or redesign cell overlap to ensure iPhone 5S sees better RSSI (8dB better than current AP) at the cell boundary so that it will roam.
Example 2 – iOS 8 MAC Randomisation

- Apple iOS 8 introduced MAC address randomisation as part of a security measure to prevent the infrastructure from being tracked by WiFi monitoring tools.

- One popular use of this type of monitoring is to track shopping habits of a user.

- Several conditions that must be met before randomisation kicks in
  - Phone is in sleep mode (display is off)
  - WiFi should be ON but NOT associated (unknown to any network)
  - Location services must be turned OFF (defeats the purpose?)

- Limited to following products only despite Apple stating it works in iOS 8
  - iPhone 5S, iPhone 5C, iPhone 6, iPhone 6 Plus
  - iPad Air, iPad Mini Retina Display
Example 2 - iOS 8 MAC Randomisation

- MAC address contains an OUI part and a host part
- OUI B2 bit always 0 for real OUIs
- B2 can be set to 1 to express “locally administered address”
- When B2 is “1”, rest of OUI does not matter
Example 2 - iOS 8 MAC Randomisation

- A sample capture of probe requests from an iPhone 6 running iOS 8 not associated, no cellular data enabled, in sleep mode and location services disabled

2 consecutive probes (20msec apart always) using real MAC
6 consecutive probes (135 or 270 seconds apart) using random MAC
Interval between real and random MAC varies between 140 seconds up to 10 minutes
Example 3 - Probing Behaviour

- Probing behavior of a device can be used to understand whether the device is happy with the current connection or not.

- Most devices don’t probe if it’s not absolutely required. Remember, more you probe the more battery life you are chewing up.

- If the device is associated, don’t necessarily have to probe unless the current connection reaches a threshold (ie. near cell edge where RSSI crosses -70dBm for iPhones). Some smartphones (ie. Samsung Galaxy) periodically probe.

- If you really want, you can induce probing by waking up the device from sleep mode (ie. black screen).

- The higher the frequency of probing, more the client is unhappy about its current connection.
Example 3 - Probing Behaviour

- Samsung Galaxy S5 when not associated and awake
Example 3 - Probing Behaviour

• Samsung Galaxy S5 when associated and awake

Burst of 2, SSID unstable SSID count changes, or probe response not received

285 s cycle can be seen

App network activity interrupts the cycle
Example 3 - Probing Behaviour

- Now let’s move back and forth between two APs.

  - **AP good signal** (no need to probe that much)
  - **AP poor signal** (need to find a better AP!)

Graph showing probe interval (seconds) vs. time (seconds).
Conclusion
“Definition of Insanity is doing the same thing over and over again and expecting different results.”
Q & A
Complete Your Online Session Evaluation

Give us your feedback and receive a **Cisco 2016 T-Shirt** by completing the Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- Visit any Cisco Live Internet Station located throughout the venue

**T-Shirts can be collected Friday 11 March at Registration**

Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations.
[www.CiscoLiveAPAC.com](http://www.CiscoLiveAPAC.com)
Thank you