



AIRHEADS

meetup

aruba
a Hewlett Packard
Enterprise company

TAC Troubleshooting Best Practices Operational Troubleshooting

Shawn Adams, Principal Network Engineer Aruba EMEA ERT

2 November 2018

Objectives

Objectives:

Review problem reporting challenges & improvements

Understand Data Types and Sources

Understand 4-Zone method approach to troubleshooting

Efficient problem determination speeds and streamlines resolution

Why ?

Efficient problem resolution: (Do you earn money troubleshooting?)

- lowers operational costs - fewer hours troubleshooting, escalation handling

- raises profit margin

- makes the customer happy

Agenda

Preparation & Tools

Problem Reporting

Types of Data

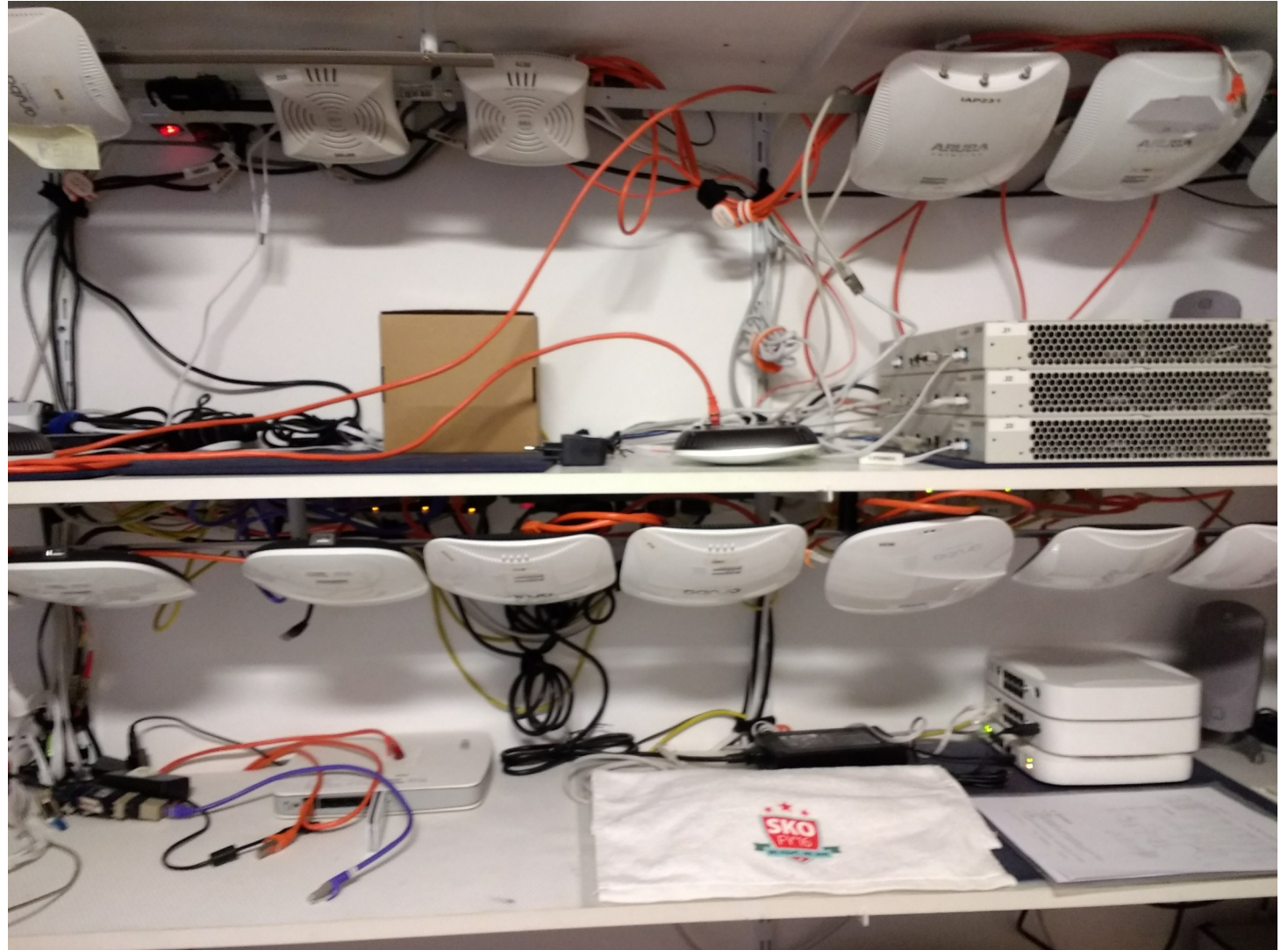
Data Sources

4-Zone Model

Preparation & Tools

Preparation & Tools

- “If it’s wireless, how come there are
- so many wires ?”
- We are replacing a low-variable cable
- with -
- air, people, obstacles and variables.
- no cat (Einstein)



Preparation & Tools

- Goal is to quickly, efficiently solve problems
 - Tasks: shortest common failure path, prove, solve
 - Being well-prepared is key to effective troubleshooting and customer service
 - The act of preparing is more valuable than the actual preparations
 - Preparation costs less than reaction
-
- “To be prepared is half the victory”
 - Miguel De Cervantes
 - “In preparing for battle I have always found that plans are useless, but planning is indispensable. “
 - Dwight D. Eisenhower
 - “If you fail to plan, you are planning to fail!”
 - Benjamin Franklin & Others

Preparation & Tools

Do you have contractually mandated and defined problem reporting procedures for your customer ?

How do your customers report problems ?

Easily repeatable acceptance tests defined ?

Can the customer easily discern network from application problems ?

Most Aruba TAC cases opened do not have enough information for TAC to propose a solution

More than 50% of cases opened do not have any technical data included

Preparation & Tools

What's in your "toolbox" ?

SSH workstation

TFTP Server (Files from controllers to server)

FTP Server (Files from controllers to server)

SCP Server (Files from controllers to server)

Wireshark PC (AP and datapath packet-captures)

Syslog Server

SNMP Trap Server

802.11 Wireless Packet Capture

AP Console Cables (order now - do not wait)

Aruba Utilities (BT)

Remote Access

Large File Upload

Preparation & Tools - Remote Sessions

Remote Sessions

Majority of sessions show improvement potential

- highly focused tasks - avoid inefficient basic problem determination via remote session
- Better success noted when Partner takes ownership and leadership of remote sessions
- Narrate/Summarize steps
- Coffee Breaks
- Require a plan in advance, be prepared - some actions require preparation/permissions
 - Port mirror
 - Packet Capture & related Sniffer PCs
 - Client reproduction
 - Client logging enabled
 - SSH/HTTPS controller connection
 - In some cases a temporary admin password is advisable



Thank You

Preparation & Tools - Reference Material

Information Sources

Aruba Products: User, CLI, System Message Guides

<http://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Default.aspx?EntryID=12930>

Aruba Knowledge Base:

<http://support.arubanetworks.com/KnowledgeBase/tabid/133/Default.aspx>

Aruba Airheads Community:

<http://community.arubanetworks.com>

Aruba Educational Videos:

http://community.arubanetworks.com/http://www.arubanetworks.com/v/?v=/case-studies/SpectrumVideo_H264.mov&width=720&height=405&t=Spectrum%20Analyzer%20User%20Interface

<http://www.arubanetworks.com/products/networking/aruba-instant/instant-training/>

Introduction to problem determination

https://www.ibm.com/support/knowledgecenter/SSESK4_6.1.4/com.ibm.storage.csm.help.doc/frp_r_ts_overview.html

Case Opening Guidelines

https://support.arubanetworks.com/Portals/0/uploads/614/Aruba_Networks_TAC_Case_Guideline.pdf



Problem Reporting

Problem Reporting

“Hello, BMW ? Yes, I just purchased a new car from you, very expensive.”

“Well, it no longer runs and I’m angry. “

“When did it stop running? I don’t exactly know – maybe 3 weeks ago.”

“Where did it stop running ? I think it was after a meeting in Frankfurt, I’m really not sure, don’t you have experts to figure that out ?”

“I really can’t tell you more, but I am very angry, and it’s important that the car run, I have important appointments to attend. If you don’t make the car run soon, I want my money back, and will purchase a new car from your competitor !”

Problem Reporting

Facts:

- car no longer runs, very expensive
- stopped about 3 weeks prior
- stopped after a meeting
- Problem existed in Frankfurt
- Expects Partner/TAC to solve everything
- Very Angry
- Threatening, not constructive
- Wants a Car that runs

Problem Reporting

Facts:

- car no longer runs, very expensive
- stopped about 3 weeks prior
- stopped after a meeting
- Problem existed in Frankfurt
- Expects Partner/TAC to solve everything
- Very Angry
- Threatening, not constructive
- Wants a Car that runs

The new BMW didn't run any longer because the customer had driven it into the Rhine river after a meeting in Frankfurt.

Problem Reporting

What are ways we can improve the problem reporting path with existing customers, presuming we cannot change the contract ?

Where do you start troubleshooting when the customer calls saying “It hurts!” ?

Methods you’ve used successfully ?

Proactive meet with customers

Do they have the tools they need in place ? Acceptance Tests ?

Problem reporting path ?

Remote Access ?

How can we help the customer prepare and avoid expensive last-second activities ?

Problem Reporting

Suggestions:

define agreed written problem reporting process

simple end-user app/web page to report problems - date/location/username/etc... 5 data points

practical, simple, repeatable acceptance tests

- isolate between network and application issues
- before/after change comparison
- VOIP ideal

Aruba/HPE Case Opening Guidelines

Types of Data

Static, Transient, and Dependent Data

Types of Data

Static, Transient, and Dependent Data

Static Data is operational data that is not likely to change during the problem event

- Controller SW version, AP Model Number

Transient Data is data that is likely to change during the problem event

- Frame counters - Delta during the symptoms
- Reachability of Nodes - if the problem is sporadic, 5 ICMPs are not enough !
- Wireless Connections (replacing cable with air)

Dependent Data is data that is not usable by itself - we need correlated data to make use thereof

- user-debug logs without association data - 802.11 capture - obtain association sequence
- datapath session data without Wireless connection data

Types of Data

Controller tech-support files and Tech-support bundles contain both static and transient

Only One Sample is often inconclusive

Historical logs contain events - but not usually what happens between the events

The client is connected, then disconnected - what happened between ?

Frame loss through an AP - why ? Only the AP can tell us

Are logs and simultaneous captures needed ?

Are simultaneous packet captures at 2 points in the problem path ?

Types of Data

Tech-support will only contain general info, **will not contain AP, Mesh or Client specific data.**

There will be client data samples, but not details of last Thursday morning.

Logs will only contain historical EVENT information - **but not the frames between the EVENTS.**

Commands “show ap” almost always query the AP directly - AP specific data

Tech-support bundles do not contain much AP specific data - “show ap tech-support”

Tech-support bundles do not contain much client-specific data “show tech-support user”

Data Sources

Sources of Data to Visualize the Network

Data Sources

What data helps us visualize the network or symptoms ?

Examine potential sources of data that help visualize

What facts do we know ?

- Who ? when ?
- What ? Data ? VOIP ? Both ?
- Wired ? Wireless ? both ?
- Particular Clients ?
- Stationary or Roaming ?

Data Sources

Questions and Answers (Keough, other systematic approaches)

Centralized Monitoring

Controller Dashboard/CLI/SNMP

AP Data

Client Data (data,logs, traces)




802.11 Air Captures

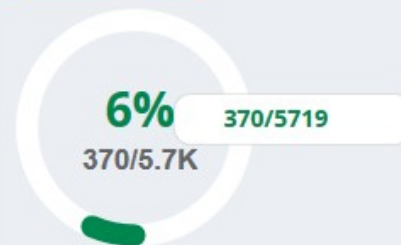
The first task is to isolate down to a failure path for reproduction, or discover unique data-points that reflect the symptoms.

Data Sources

Airwave Clarity provides
historical overview
Comparative Data



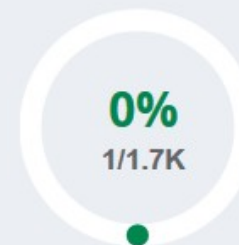
2h 1d 1w 2w   



ASSOCIATION



AUTHENTICATION
































DHCP



DNS




Summary



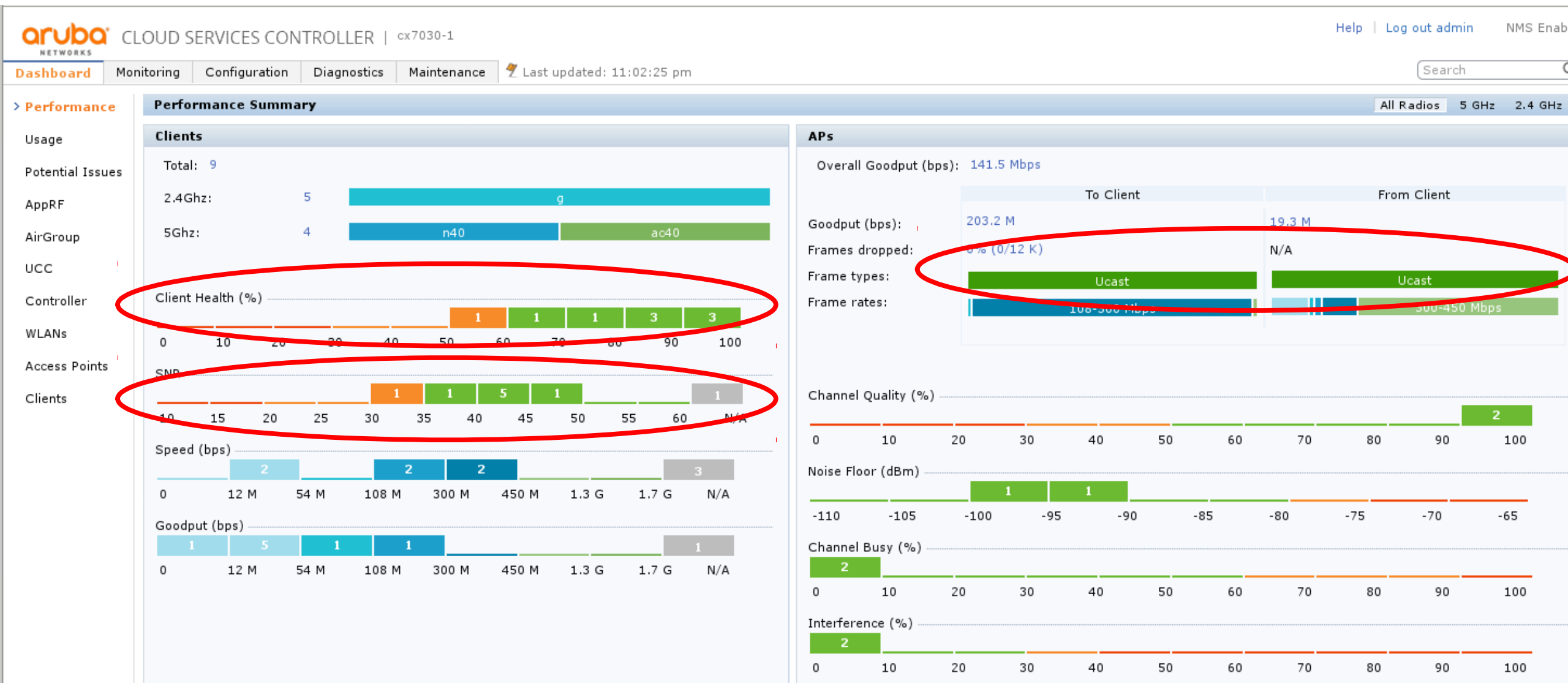
AP NAME	ASSOCIATION	AUTHENTICAT...	DHCP	
1322w-AP2				
1322w-AP05				
1322w-AP5				
8-1322w-AP08...				
1322w-AP08				
1322w-AP09				
1322w-AP08				
1322w-AP10				
1322w-AP08				

Total Records: 25

Details

Authentication				
SERVICES	TYPE	AUTH. FAILUR...	AUTH. TIME(
10.0.0.10.22	MAC Auth	21% (5/23)	3621	
10.11.14.140.1...	Dot1x	8% (107/1226...	2717	
10.11.1.87	Dot1x	31% (411/130...	1294	
10.11.1.201	WPA 4-Way H...	1% (22/1205)	135	
10.11.1.211	WPA 4-Way H...	0% (4/632)	114	
10.11.1.19	WPA 4-Way H...	1% (16/1279)	84	
Total Records: 6				
Details				

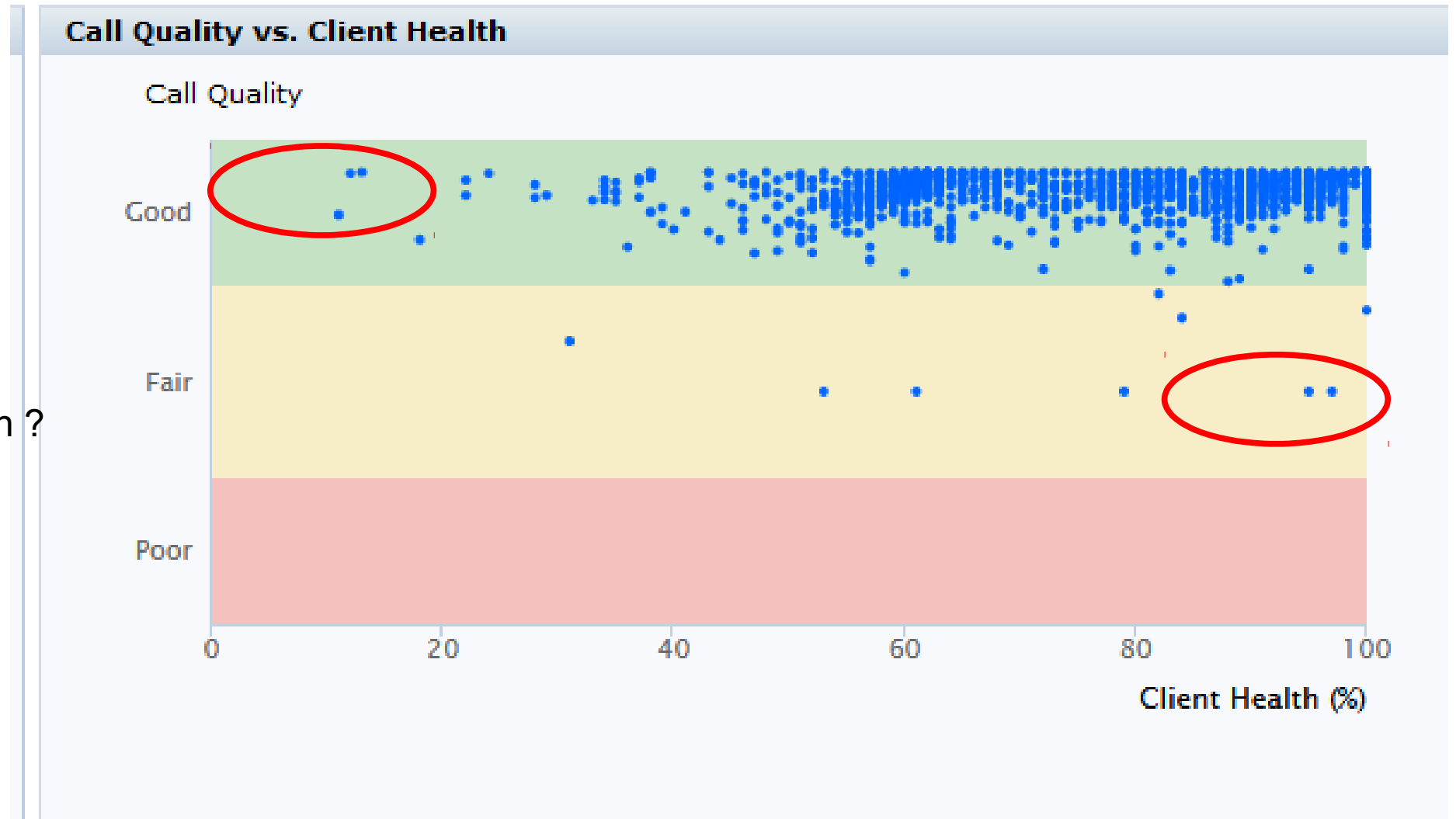
Data Sources



Data Sources

Depicts both WIFI and
Application health

Can VOIP be used
as a good indication
for general network health ?



Data Sources

What can the controller tell us about it's own operational health ?

- SNMP Traps
- Syslog messages
- core dumps
- AMON Data - readable via Network Dashboard or Airwave
- Remember: APs direct Syslog to the controller

What can it *not* tell us ?

- Think about a routing loop. Each router in the path “thinks” it is routing a legitimate packet
- Will these packets show in any log file ?
- error counter ?

Data Sources - Controller

Controller View

Visualize OSI Model Layer 0 through 3 - Controller health, L1, L2, L3 along failure path

Learn which commands are static, which are transitory, which are visualizing L1, L2, L3

show inventory (ts)		show port status (ts) T	show ip interface brief (ts)	
show memory ecc(ts) T		show lldp T	show port stats (ts)	T
show cpu current (ts) T		show vlan status (ts) T	show ip route (ts)	T
show mem (ts) T		show datapath bridge (ts) T	show ip route-cache verbose (ts)	T
show process (ts) T		show trunk (ts)	show datapath user(ts)	T
show license (ts)		show switches(ts)	show user-table (ts)	T
show spann (ts) T		show master-local st(ts) T	show datapath session (ts)	T
show storage(ts)		show ap debug counter (ts) T		
show image version (ts)				

Data Sources - Access Point

AP View

Think about the AP as one component in the L2 failure path

Focus on AP network and RF stability

GENERAL

show ap database long (ts)

show ap active (ts)

show ap debug counters (ts)

show datapath tunnel (ts)

show datapath papi coun

show ap lldp

show crypto ipsec sa (ts)

AP SPECIFIC (requires ap-name argument)

show ap config

show ap detail adv

show ap port status

show ap debug system-status | inc Power

show ap arm rf

show ap arm hist

show datapath sess (ts)

Data Sources - Wireless Client

Client View

Controller Tech-Support contains a snapshot of a given client

Often dependent data is needed

Many commands are more useful when filtering on the client MAC/IP and or utilizing “include”

```
show ap debug client-stats 11:22:33:44:55:66 | inc etr,rop,rror,ail,Trans
```

Layer 1

```
show ap associ (ts)
show datapath stat (ts)
show ap debug client-table
show ap debug client-stats
show datapath bridge (ts)
show ap remote debug mgmt-frames
```

Layer 2

```
show datapath bridge(ts)
```

Layer 3

```
show user-table verbose (ts)
show datapath user (ts)
show datapath route-cache (ts)
show datapath session (ts)
show arp (ts)
show crypto ipsec sa (ts)
```

Data Sources - Summary

Summary

Utilize centralized Data Sources

Ask Critical Questions - Elimination by fact , deduction, or tests

Controller, AP, Client Data Sources

Understand which sources provide static, transient and dependent Data

4-Zone Model

4-Zone Model

Objectives

Aruba 4-Zone Troubleshooting Model

Data Sources for each Zone

Note intersection with OSI 7-Layer Model

4-Zone Model

The following Zone theory of approaching troubleshooting is taken from the Aruba “Advanced Troubleshooting Course”. Highly recommended. Yes, there are other methods and strategies.

- We will look at problems divided into 4 zones, and look at how we can examine each zone in more detail.
- There are a number of analysis systems that have proven to assist with the initial diagnosis, Keogh's 14-questions, the 5-W's, etc....Name a few methods you've found effective ?

W Who ?

W What works or does not work when it happens ?

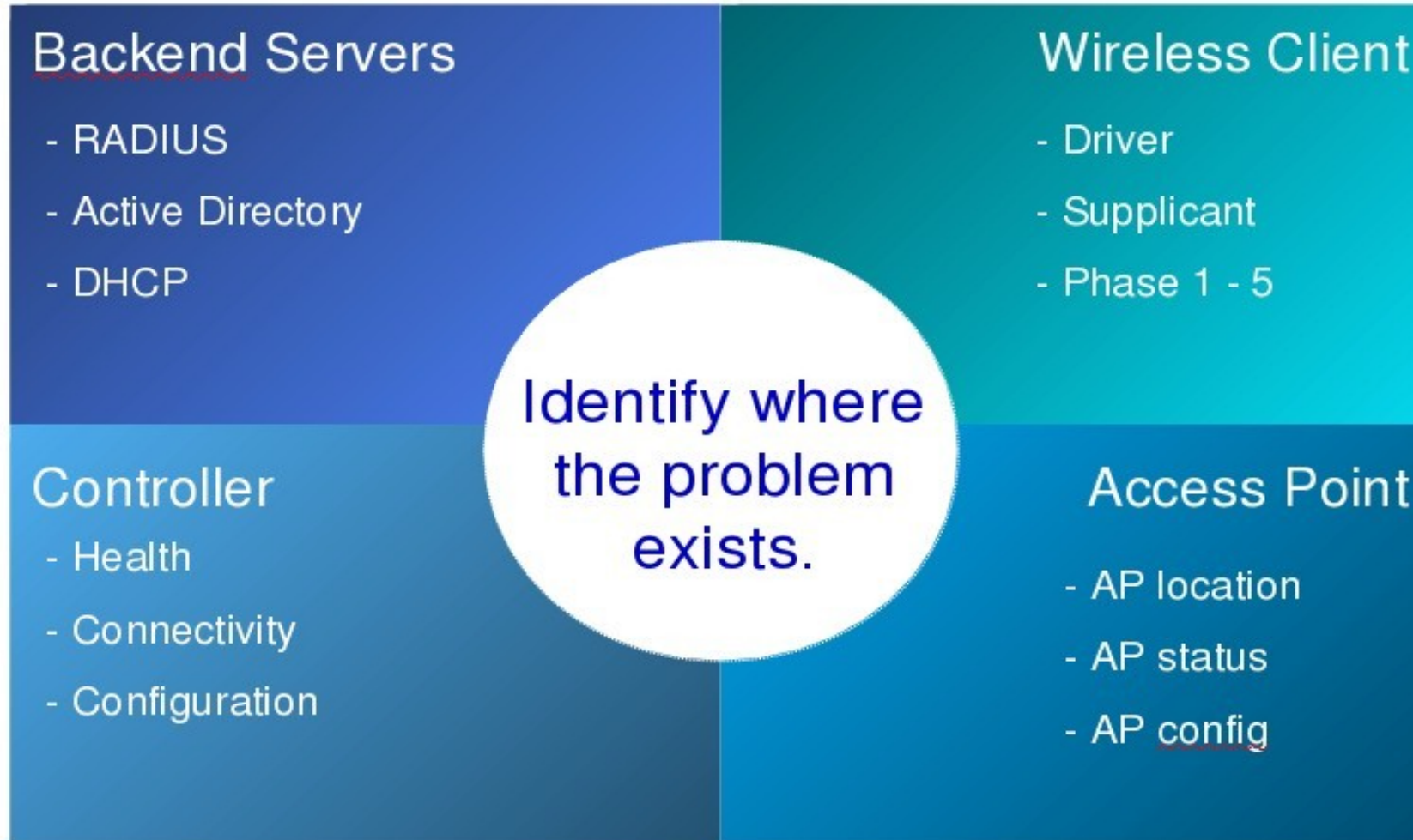
W Where does the problem happen ?

W When does the problem happen ?

hoW How does the problem manifest ? hoW is it visible ? hoW do we provoke it ?

4-Zone Model

Troubleshooting Zones



4-Zone Model

Centralized View - including suspect controller

- Airwave ? Central ? IMC ?
- Avoid over-focus (spyglass effect)

SNMP Trap data

Syslog Data

AMON Data

- Controller Dashboard
- Logs+Tech-support
- Focused Data - AP specific, Client Specific

4-Zone Model - Back-end

Back-end Servers

Active Directory Server

DHCP Server

DNS Server

RADIUS Server

- L3 connectivity
- Debug logs
- UDP/TCP ports open ?
- Check client auth, DHCP, DNS operations



4-Zone model - Controller

Controller

Stable ?

- CPU ?
- Memory ?
- Error messages?

L1/L2 connectivity ?

L3 connectivity ? VRRP ?

Check controller CPU, RAM, Processes

Refer back to controller-relative commands

aruba



4-Zone model - Controller

Controller View

Layer 0 - Hardware, CPU, RAM, Fans, power supplies, licenses - isolated and unique to each

show ver (ts) show clock(ts) show inv (ts) show lic (ts)
show mem (ts) show switch (ts) show cpu detail(ts)

Layer 1 - Ethernet ports - connections to the outside world

show port status[ts] show trunks (ts) show spanning (ts)

Layer 2 - MAC Layer, FDB, STP,VLANs

show datapath bwm(ts) show datapath debug dma(ts) show datapath debug trace(ts) show datapath util(ts)

Layer 3 - IP, OSPF, Routing

show ip interface (ts) show ip route (ts) show arp (ts)
show datapath route-cache verbose (ts)

Data Sources - Controller

Controller View

Visualize OSI Model Layer 0 through 3 - Controller health, L1, L2, L3 along failure path

Learn which commands are static, which are transitory, which are visualizing L1, L2, L3

show inventory (ts)		show port status (ts) T	show ip interface brief (ts)	
show memory ecc(ts) T		show lldp T	show port stats (ts)	T
show cpu current (ts) T		show vlan status (ts) T	show ip route (ts)	T
show mem (ts) T		show datapath bridge (ts) T	show ip route-cache verbose (ts)	T
show process (ts) T		show trunk (ts)	show datapath user(ts)	T
show license (ts)		show switches(ts)	show user-table (ts)	T
show spann (ts) T		show master-local st(ts) T	show datapath session (ts)	T
show storage(ts)		show ap debug counter (ts) T		
show image version (ts)				

4-Zone Model - Access Point

Access Point

Connected to controller ?

Stable ?

L3 connection ?

Application symptoms?

Power – 802.3af, 802.3.at, PoE+ , LLDP ?

ARM Changes ?

What if we suspect AP connection issues ? how can we check operations ?

show ap remote port status

show datapath tunnel heart

show datapath tunnel papi

ify where
problem
xists.

Access Point

- AP location
- AP status
- AP config

Data Sources - Access Point

AP View

Now let's widen our view to include APs.

think about the AP as one component in the L2 failure path

Focus on AP network and RF stability

- | | |
|-------------------------------|---|
| • GENERAL | AP SPECIFIC (requires ap-name argument) |
| • show ap database long (ts) | show ap config |
| • show ap active (ts) | show ap detail adv |
| • show ap debug counters (ts) | show ap port status |
| • show datapath tunnel (ts) | show ap debug system-status inc Power |
| • show datapath papi coun | show ap arm rf |
| • show ap lldp | show ap arm hist |
| • show crypto ipsec sa (ts) | show ap tech-support |
| • show datapath sess (ts) | |

4-Zone Model - Wireless Client

Wireless Client

802.11 Association ?

- 2.4Ghz or 5Ghz ?
- Specific Client Types ?
- Specific SSID Affected ?

L3 connection ?

Keep in mind the Virtual-ap operational mode - tunnel, d-tunnel, bridge, split-tunnel

Application symptoms?



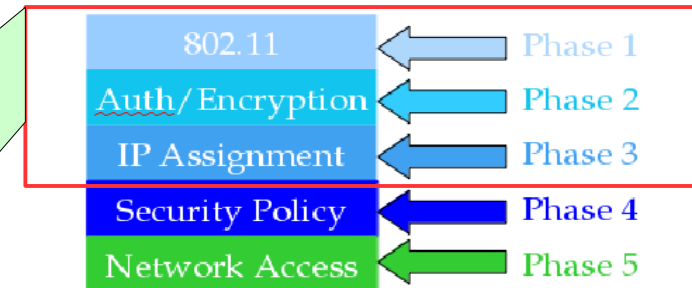
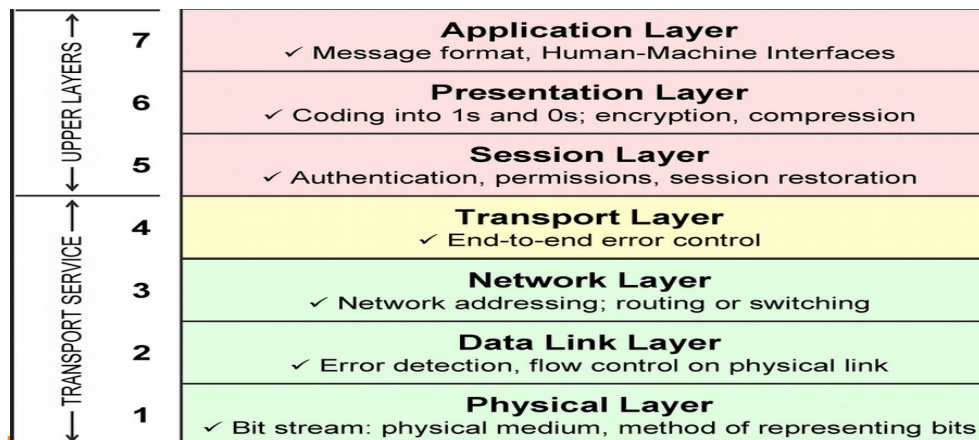
4-Zone Model - Wireless Client

Troubleshooting Aruba Networks - Wireless Client

Wireless Client:

Client to AP - RF Connection – OSI 7-Layer Model

802.11 Exists at Layer 1 and Layer 2



4-Zone Model - Wireless Client

Wireless Client

802.11 Association ?

L3 connection ?

Application symptoms?

what will the controller and AP logs tell us ?

user-debug log

AP logs

what will they not tell us ?

How can we look at the 802.11 connection ? show ap associ, show datapath sta, show ap debug mgm

How can we look at the higher layers of the connection ? show user-table verbose, show datapath user



4-Zone Model - Wireless Client

Wireless Client

- 802.11 connection
- L3 - IP connection ?
- Applications ?

Start with the tech-support bundle for an overview

Differentiate between stationary and roaming problems

Isolate between application and L1-L3 problems

802.11 packet-captures - be sure to obtain the association sequence

Keep in mind static data and transitory data

4-Zone Model - Wireless Client

If client problems are suspected , look at Layers 1 - 3

What portions of the client connection are displayed in the tech-support ?

Many commands are more useful when filtering on the client MAC/IP and or utilizing “include”

`show ap debug client-stats 11:22:33:44:55:66 | inc etr,rop,rror,ail,Trans`

Layer 1

`show ap associ (ts)`

`show datapath stat (ts)`

`show ap debug client-table`

`show ap debug client-stats`

`show ap remote debug mgmt-frames`

`show ap remote debug mgmt-frames`

Layer 2

`show datapath bridge(ts)`

`show auth`

Layer 3

`show user-table verbose (ts)`

`show datapath user (ts)`

`show datapath route-cache (ts)`

`show datapath session (ts)`

`show arp (ts)`

`show crypto ipsec sa (ts)`

4-Zone Model - Wireless Client

(MC-LOCAL-1) #show ap debug client-table ap-name f0:5c:19:c0:bf:ba

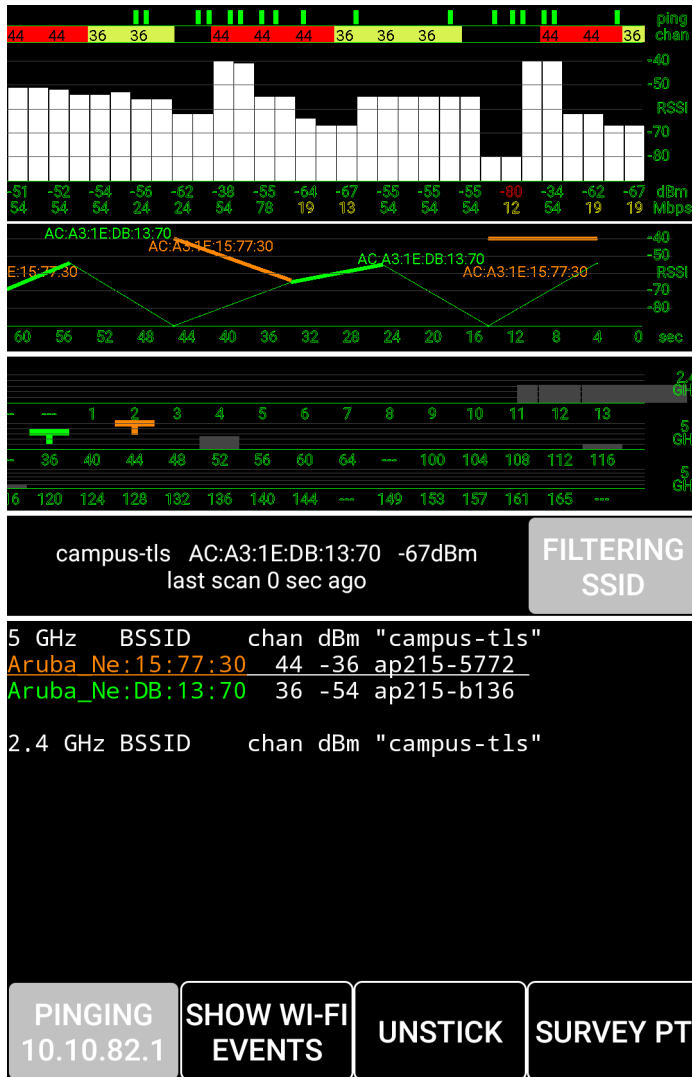
Client Table

MAC Tx_Timestamp	ESSID	BSSID Rx_Timestamp	Assoc_State MFP	HT_State Status (C,R)	AID Idle time	PS_State Client health (C/R)	UAPSD	Tx_Pkts	Rx_Pkts	PS_Qlen	Tx_Retries	Tx_Rate	Rx_Rate	Last_ACK_SNR	Last_Rx_SNR	TX_Chains	
a4:84:31:fb:e3:66 1 11:14:36 2017	k-tele (0,0)	f0:5c:19:8b:fb:b1 1	Associated	WQSS	0x1	Power-save	(0,0,0,0,N/A,0)	2152	14478	0	290	72	72	33	34	3[0x7]	Wed Mar 1 11:14:35 2017 Wed Mar

Client Table

MAC Tx_Timestamp	ESSID	BSSID Rx_Timestamp	Assoc_State MFP	HT_State Status (C,R)	AID Idle time	PS_State Client health (C/R)	UAPSD	Tx_Pkts	Rx_Pkts	PS_Qlen	Tx_Retries	Tx_Rate	Rx_Rate	Last_ACK_SNR	Last_Rx_SNR	TX_Chains	
a4:84:31:fb:e3:66 1 11:14:36 2017	k-tele (0,0)	f0:5c:19:8b:fb:b1 1	Associated	WQSS	0x1	Power-save	(0,0,0,0,N/A,0)	2152	14478	0	290	72	72	33	34	3[0x7]	Wed Mar 1 11:14:35 2017 Wed Mar
a4:84:31:fb:e3:66 11:14:37 2017	k-tele (0,0)	f0:5c:19:8b:fb:b1 0	Associated	WQSS	0x1	Awake	(0,0,0,0,N/A,0)	2154	14490	0	290	72	43	19	22	3[0x7]	Wed Mar 1 11:14:37 2017 Wed Mar 1
a4:84:31:fb:e3:66 1 11:14:39 2017	k-tele (0,0)	f0:5c:19:8b:fb:b1 1	Associated	WQSS	0x1	Power-save	(0,0,0,0,N/A,0)	2155	14498	0	290	72	72	17	19	3[0x7]	Wed Mar 1 11:14:38 2017 Wed Mar
a4:84:31:fb:e3:66 11:14:40 2017	k-tele (0,0)	f0:5c:19:8b:fb:b1 0	Associated	WQSS	0x1	Power-save	(0,0,0,0,N/A,0)	2156	14513	0	290	72	6	7	6	3[0x7]	Wed Mar 1 11:14:40 2017 Wed Mar 1

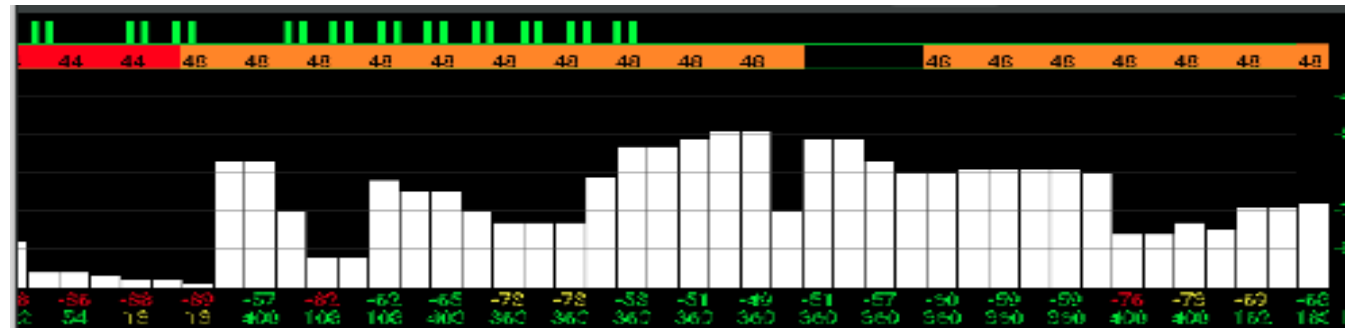
4-Zone Model - Wireless Client



This is a sample of one of the better tests for

The correlation is low departure SNR, poor performance:

- Retries
- drops
- VOIP interruptions
- Application interruptions
- Complete 802.11 disconnect



4-Zone Model - Summary

Summary

Ask Critical Questions - Elimination by fact, testing, or deduction

Based on known fact, narrow down to likely zone

Use Data Sources to visualize each zone

Summary

Summary - Takeaways

Be Prepared - Plan for failures

Enhance problem reporting flow

Use all available focused data sources