

#WiFiDesignDay

by ekahau

Wi-Fi Support Lifecycle

DESIGN – VERIFY – TEST – MONITOR – TROUBLESHOOT – REPEAT

My stake in the Wireless game

18 Years involved with network, testing and troubleshooting

Worked (and continue to work) with many test & analysis vendors

- Spirent Communications
- Fluke Networks -> NETSCOUT -> NetAlly -> ??
- OPNET (now part of Riverbed)
- Gold Partner with Ekahau
- In-country distributor for Nyansa & Efficient IP

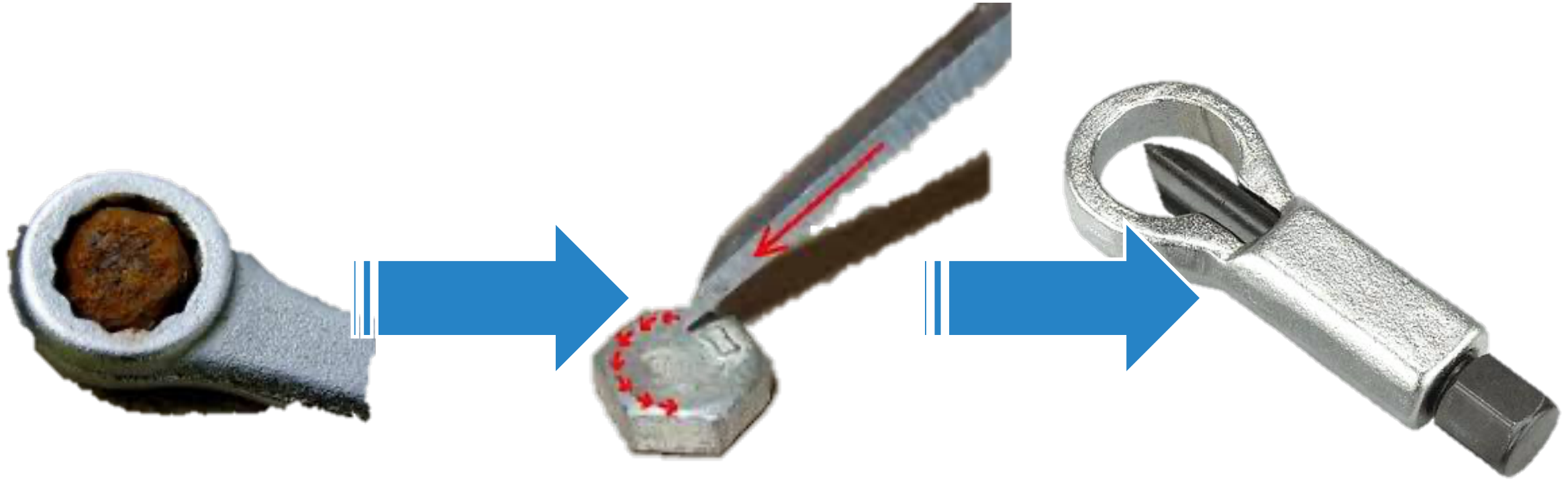
Technologies across wired & wireless networks, application performance, security, DDI....

Dom Fitzgibbon
@fit70z
dom.fitzgibbon@plexnet.com.au
www.plexnet.com.au



#WiFiDesignDay
by ekahau

Using the Right equipment

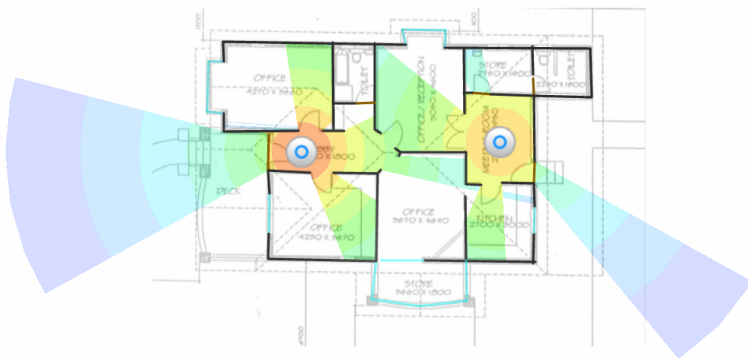


But I can use FREE tools....

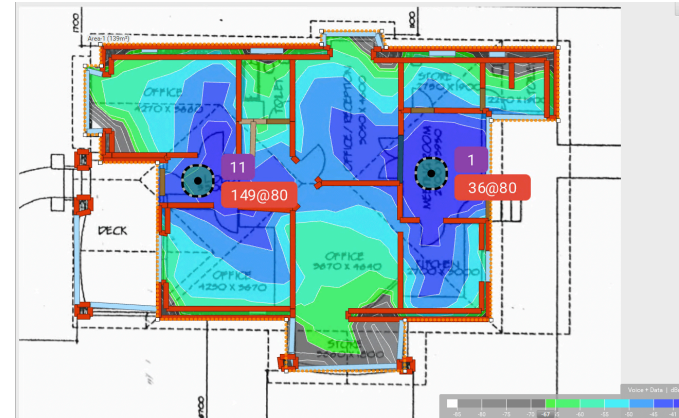
There are literally loads around and to be fair some great ones and ones that should be part of your everyday kit!

Wireless tools for Android / iPhone are great for a quick check.

AP vendors have in-built design tools



VS



Done	Scan
pl3x 7A:8A:20:D5:69:19 RSSI -62 dBm Channel 100	> 13:50:11
OPTUSVD3669468 10:0D:7F:E6:AE:3D RSSI -82 dBm Channel 1	> 13:50:11
TPG-3NTX C8:51:95:3B:89:60 RSSI -84 dBm Channel 2	> 13:50:11
MADHU 88:CE:FA:7D:0E:74 RSSI -84 dBm Channel 4	> 13:50:11
Blackvue650S-838A91 00:25:42:83:8A:91 RSSI -84 dBm Channel 6	> 13:50:11
Vinnies_Staff 0C:BD:DB:C4:F8:3B RSSI -85 dBm Channel 1	> 13:50:11

BUT IF THEY WERE SO GOOD THEN TEST VENDORS WOULD GO OUT OF BUSINESS

So why do we care?

Last year Keith said this:

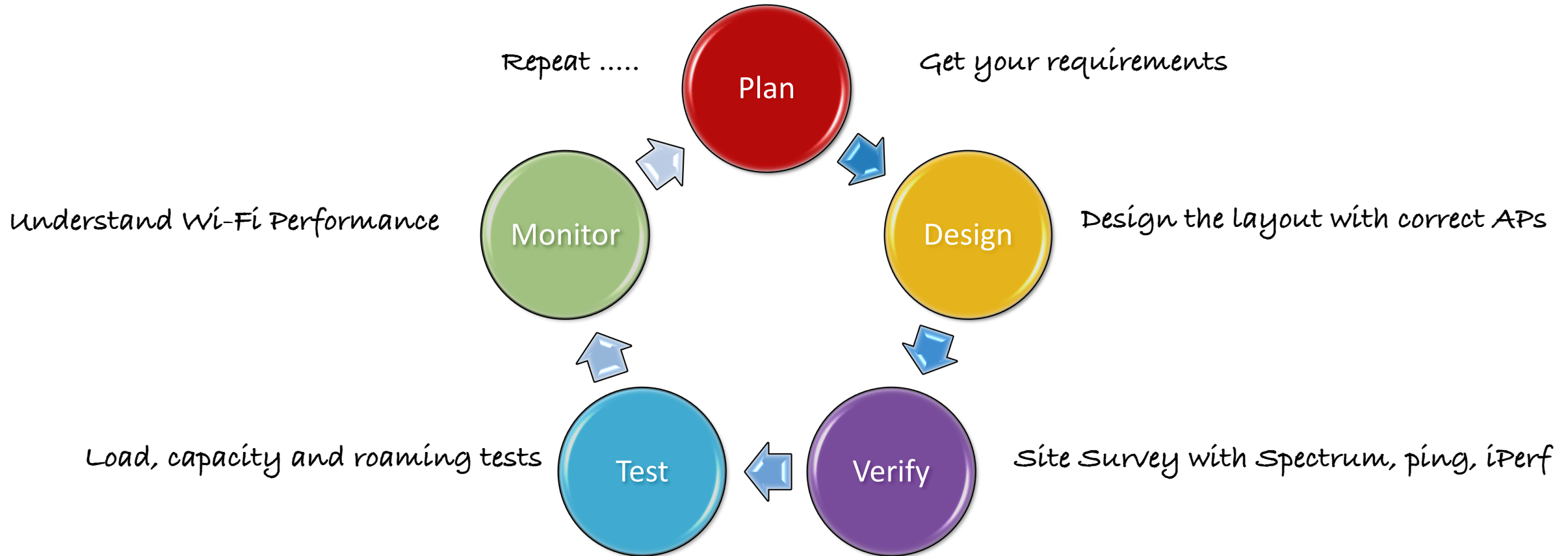
**Difference between
Wi-Fi that**

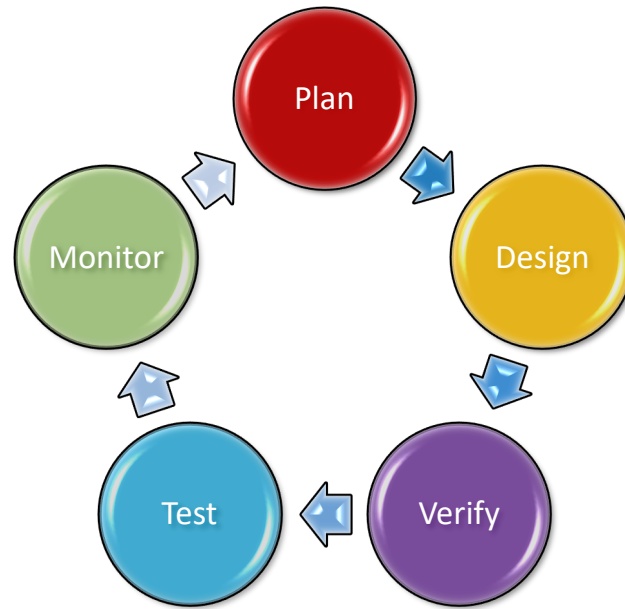
BUT IT CAN SUCK !!!

Wi-Fi Always Works...

#WiFiDesignDay

Have a Lifecycle Support Plan





Lifecycle Support Plan

MITIGATE...



Areas of Interest

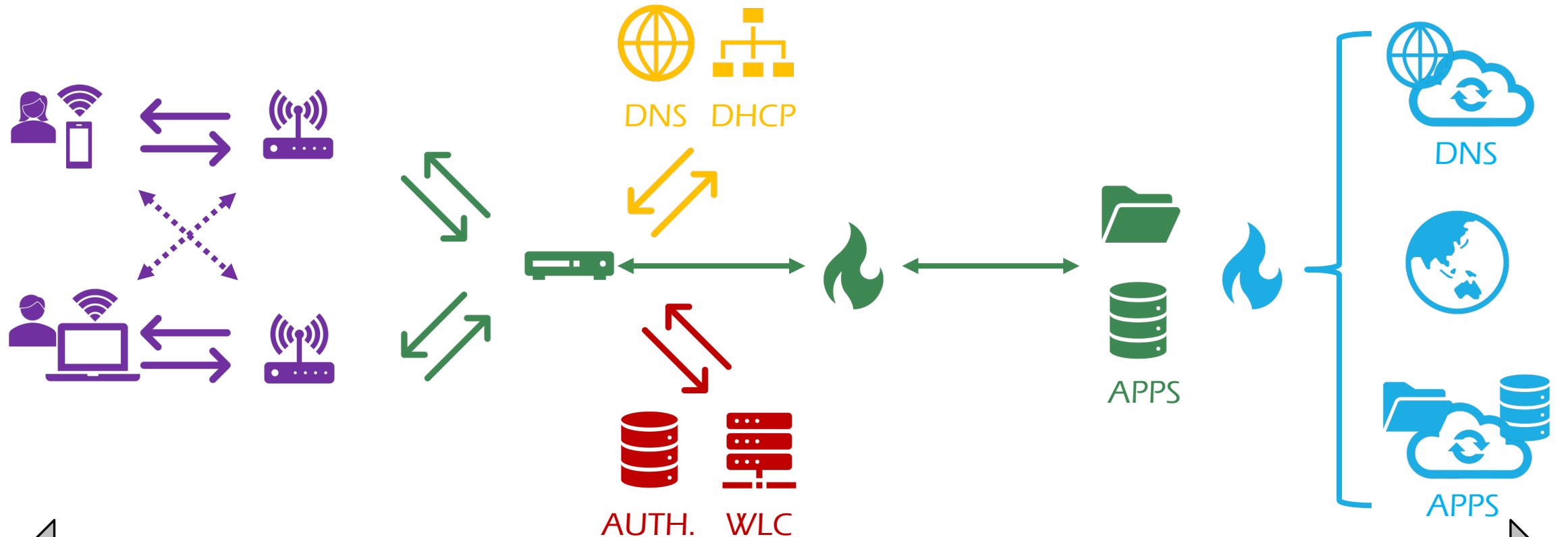
Wireless Medium

Network / Apps

Authentication & Control

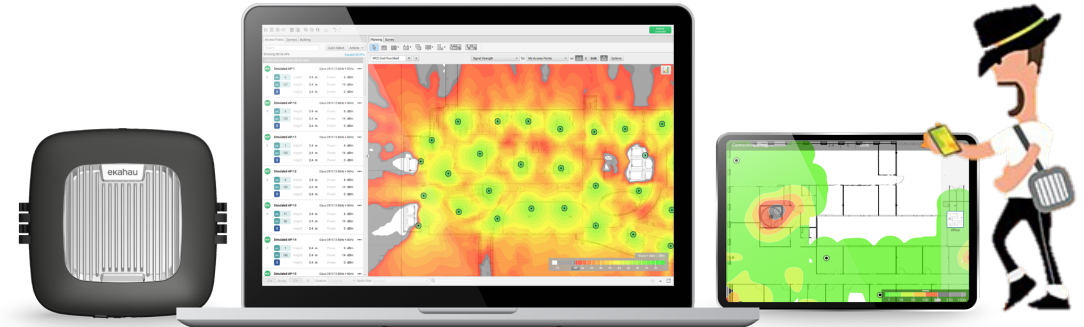
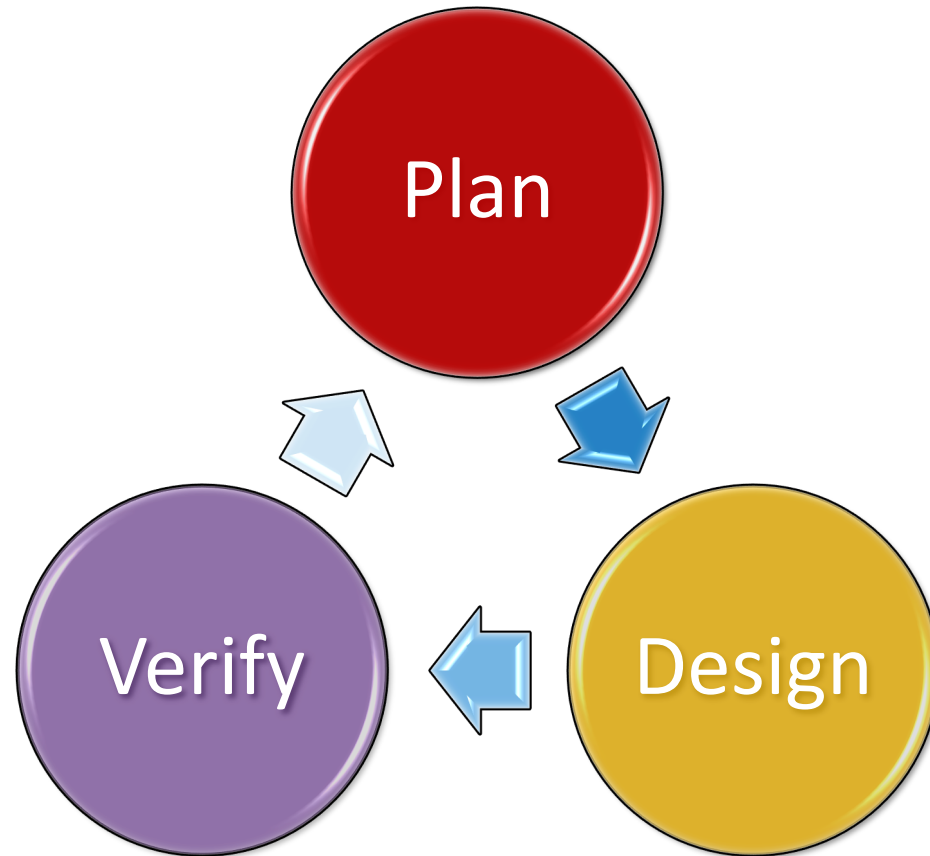
Network Services

Internet / Cloud

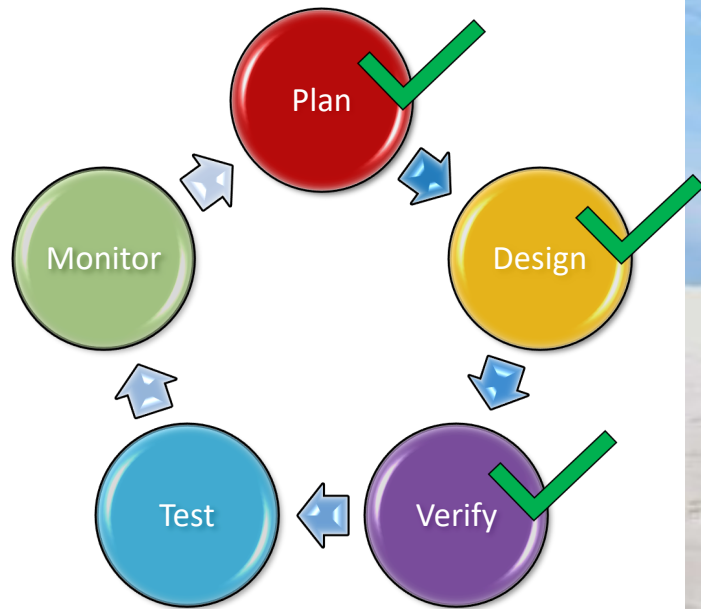


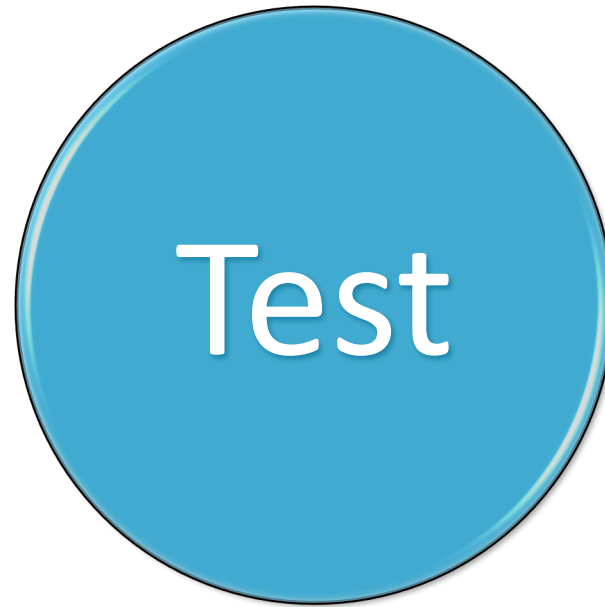
END USER EXPERIENCE

Plan, Design, Verify



Testing & Monitoring



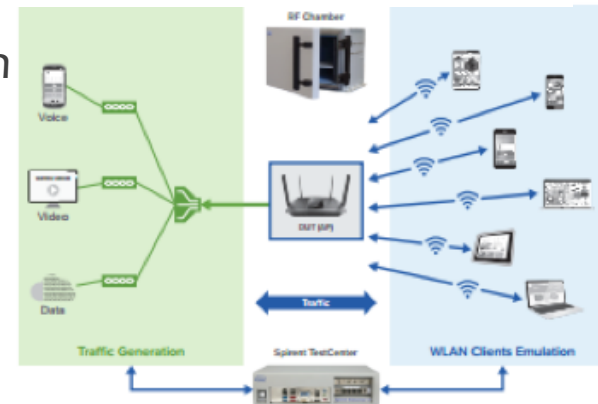
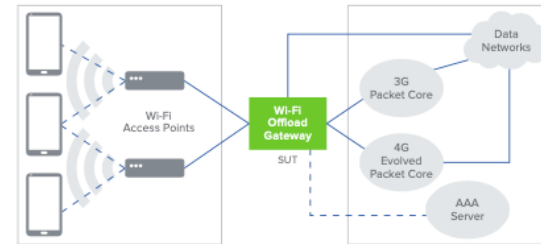


Testing

Wireless Load and Capacity Testing

What to Test?

- AP Authentication WPA/WPA2/WPA3, 802.1x
- Average and maximum client capacity loading
- AP stability
- AP interoperability with legacy 802.11 mode
- Benchmark L2-L7 throughput, Rate vs Range
- Features: Roaming, Band Steering, Multi-AP mesh
- 802.11ax (Wi-Fi 6) network readiness
- Wi-Fi Offload (AP/Hotspots to LTE/5G)



Testing

Testing with Real Traffic & Sessions



Test Configuration | Command Sequence | Network Devices | RF Interface | L3-7

Available 802.11 Interfaces and Settings

Interface	Include	Type	Band(s)	BW	Power Level	Antenna 1	Antenna 2	Antenna 3	MCS Index
wlan0	<input type="checkbox"/>	802.11ac	5.0GHz	20MHz	Auto	On	On	On	Auto
wlan1	<input type="checkbox"/>	802.11ac	5.0GHz	20MHz	Auto	On	On	On	Auto
wlan2	<input type="checkbox"/>	802.11ac	5.0GHz	20MHz	Auto	On	On	On	Auto
wlan3	<input type="checkbox"/>	802.11ac	5.0GHz	20MHz	Auto	On	On	On	Auto
wlan4	<input checked="" type="checkbox"/>	802.11ac	5.0GHz	40MHz	Auto	On	On	On	Auto

Access Points | SSIDs/BSSIDs

AP #	Access Point Name
1	AP1
2	AP2

UE Group Settings

Number of UE Groups: 1

UE Group	Name	Subscriber Range
1	Group1	From 1 to 50

Group Name: Group1

Number of UEs: 50

Assigned Interface: wlan4

Next Hop IP Address:

SSID: ciscoPEAP

BSSID: AP2

Authentication Type: 802.1x-EAP

Link Established Poll Rate (ms): 100

Link Established Timeout (intervals): 3000

Link Status Poll Rate (ms): 1000

Link Status Timeout (intervals): 5

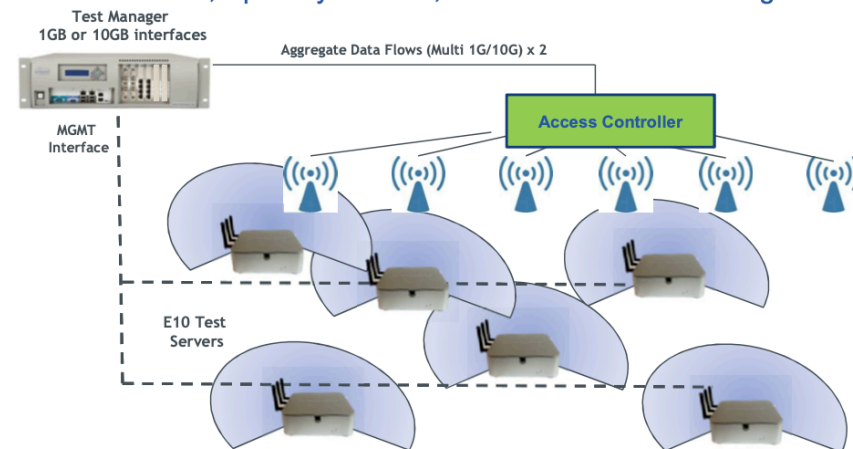
Pass Phrase: password

PMK Caching 802.11r

Opportunistic Key Caching

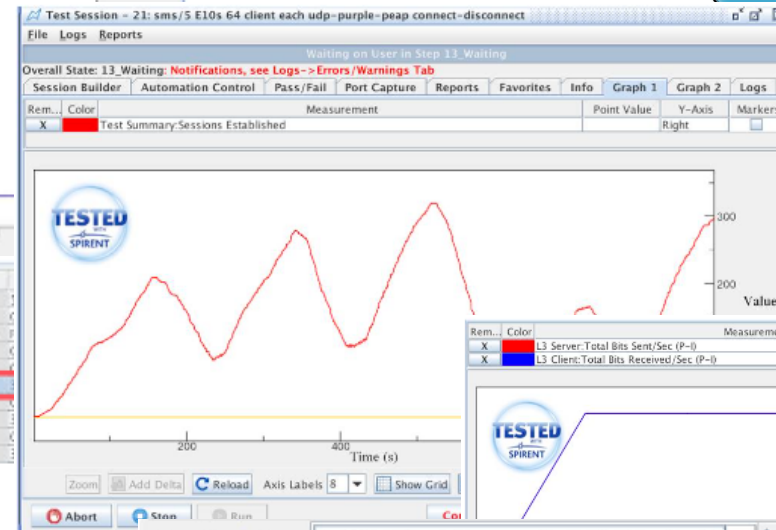
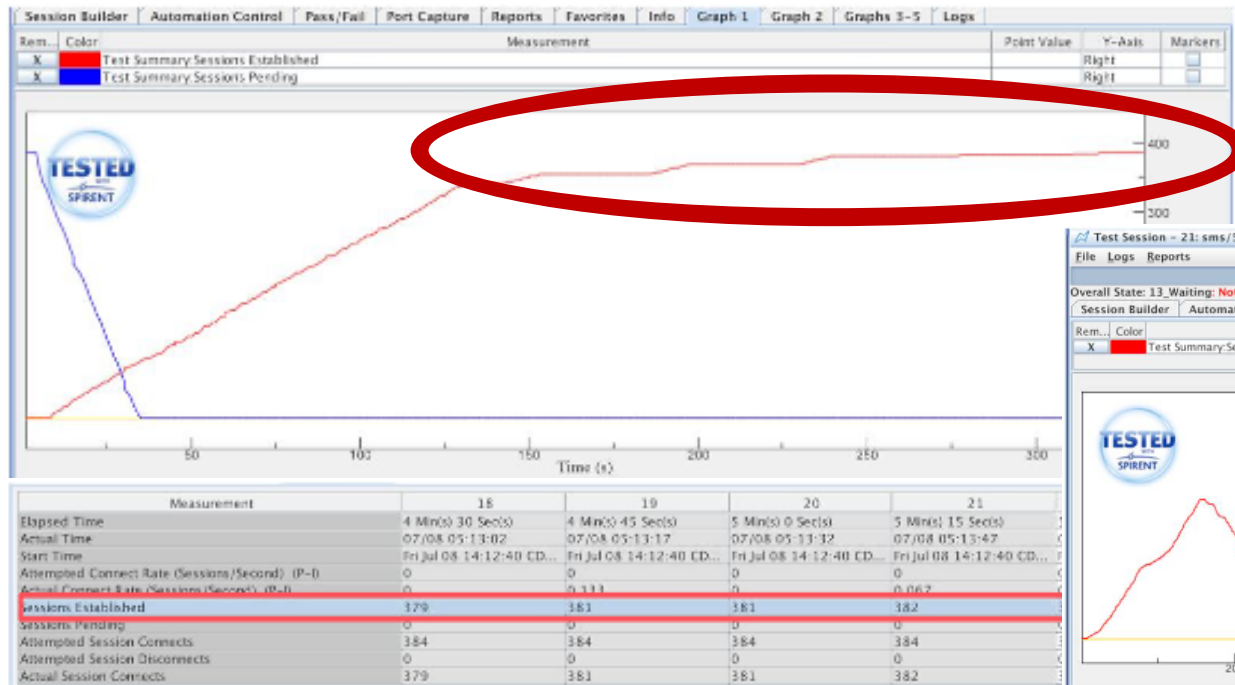
EAP Settings...

Simultaneous, Spatially Diverse, Over-The-Air Wi-Fi testing



Testing

Understanding Load vs Connection Times



Test Case View 1 [Wifi Offload Gateway Nodal] / 1 / ts0:tc0

UE_IDX	STATUS_OF...	FREQ_MHz	SIGNAL_DELT..	TX_BIT_RATE
1	Established	5785	-44	540.0 Mbit/s VHT-MCS 8 40MHz short GI VH..

Testing

Having Historical Data for *Every* UE – Control Plane & Data Plane



Test Session - 51: sms/6 E10s 64 client each udp-purple-peap capacity- demo 1

File Logs Reports

Waiting on User in Step 8_Waiting

Overall State: 8_Waiting

Session Builder Automation Control Pass/Fail Port Capture Reports Favorites Info Graph 1 Graph 2 Graphs 3-5 Logs

Configure... Query Generate Horizontal Scrolling

Test Case View 1 [Wifi Offload Gateway Nodal]/ 1 / ts1:tc0

UE_IDX	STATUS_OF_CLIENT	FREQ_MHz	SIGNAL_DELTA_10d...	TX_BIT_RATE	IP_ADDR	MAC_ADDR	BSSID	SSID
42	Established	5785	-48	13.5 Mbit/s VHT-M...	10.1.0.42/32	00:11:22:33:44:7e	00:42:68:00:72:fb	purple-peap
43	Established	5785	-49	13.5 Mbit/s VHT-M...	10.1.0.43/32	00:11:22:33:44:7f	00:42:68:00:72:fb	purple-peap
44	Established	5785	-49	13.5 Mbit/s VHT-M...	10.1.0.44/32	00:11:22:33:44:80	00:42:68:00:72:fb	purple-peap
45	Established	5785	-48	13.5 Mbit/s VHT-M...	10.1.0.45/32	00:11:22:33:44:81	00:42:68:00:72:fb	purple-peap

UE Info Query Results for 1 [Wifi Offload Gateway Nodal]/ 1 / ts1:tc0

UE_IDX	LOGTIME	COLCHANGED	COLVALUE
45	14:14:11.959045	TX_BIT_RATE	13.5 Mbit/s VHT-MCS 0 40MHz VHT-NSS 1
45	14:13:56.959176	SSID	purple-peap
45	14:13:56.959140	TX_BIT_RATE	18.0 Mbit/s
45	14:13:56.959101	FREQ_MHz	5785
45	14:13:56.959048	SIGNAL_DELTA_10dBm	-48
45	14:13:55.959362	IP_ADDR	10.1.0.45/32
45	14:13:55.959247	BSSID	00:42:68:00:72:fb
45	14:13:55.959208	STATUS_OF_CLIENT	Established
45	14:13:55.959105	STATUS_OF_CLIENT	Authenticated
45	14:13:54.459051	STATUS_OF_CLIENT	Associated
45	14:13:05.755484	STATUS_OF_CLIENT	Authenticate
45	14:13:05.444566	MAC_ADDR	00:11:22:33:44:81
45	14:13:05.444506	STATUS_OF_CLIENT	Idle

Testing

Wireless load and Capacity testing

What about iPerf?

- Great for quick testing. Not always reliable past about 350-500 Mbps
- Will tend to detect problems more-so than a tangible throughput result
- Should not be used as a definitive test result



The collage displays various wireless testing results and hardware. On the left, three smartphone screens show iPerf test results for 'LAN of Hope and Glory' with various metrics like up/down speeds and signal strength. In the center, a terminal window shows iPerf command-line output and a table of interval-based performance data. On the right, two more smartphone screens show iPerf test results with large throughput numbers (407 and 377 Mbps) and a physical device labeled 'WLAN Pi' connected to a 'NETSCOUT TEST ACCESSORY'.

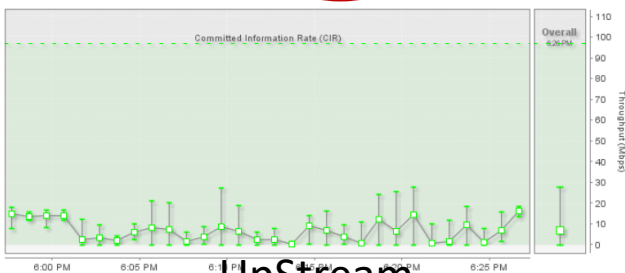
ID	Interval	Transfer	Bitrate	Retr
[5]	0.00-1.00	sec 69.6 MBytes	585 Mbits/sec	
[5]	1.00-2.00	sec 64.2 MBytes	538 Mbits/sec	
[5]	2.00-3.00	sec 59.4 MBytes	498 Mbits/sec	
[5]	3.00-4.00	sec 58.7 MBytes	492 Mbits/sec	
[5]	4.00-5.00	sec 61.1 MBytes	513 Mbits/sec	
[5]	5.00-6.00	sec 65.7 MBytes	549 Mbits/sec	
[5]	6.00-7.00	sec 70.4 MBytes	593 Mbits/sec	
[5]	7.00-8.00	sec 65.3 MBytes	548 Mbits/sec	
[5]	8.00-9.00	sec 55.2 MBytes	463 Mbits/sec	
[5]	9.00-10.00	sec 63.6 MBytes	533 Mbits/sec	

Testing

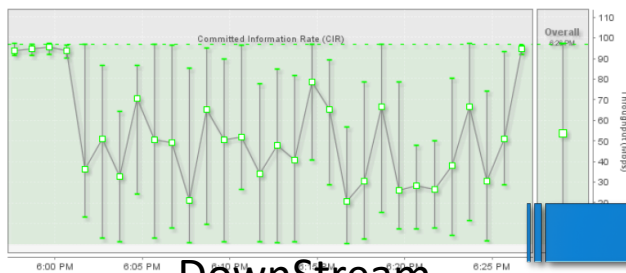
When it Goes Wrong – Y.1564 Tests Help!

Overall Results

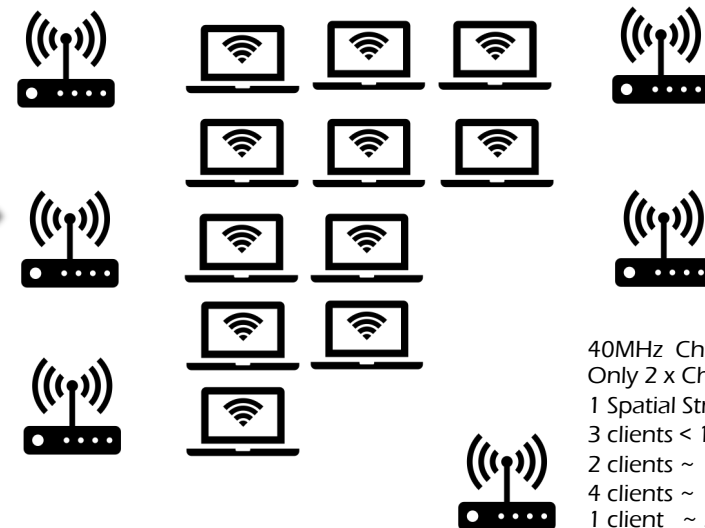
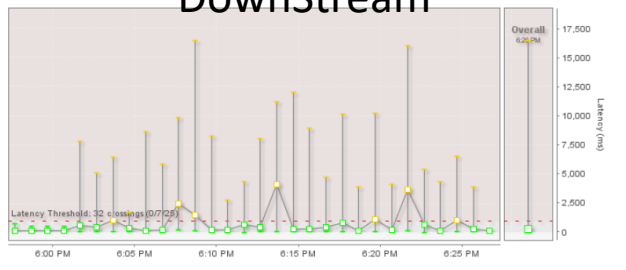
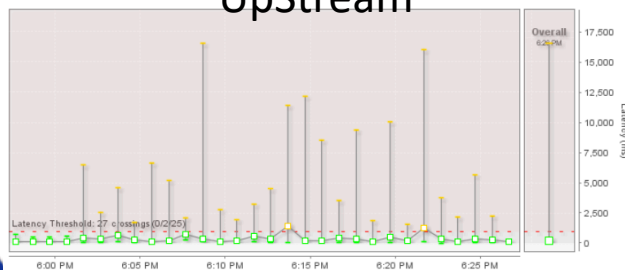
Overall Status	Throughput (Mbps)			Frame Loss		Latency (ms)				Jitter (ms)				Avail %	Unavail Seconds
	Min	Avg	Max	Count	Ratio	Min	Avg	Max	%	Min	Avg	Max	%		
Service (Upstream) Started at: 07/16 05:56:41 PM - Finished at: 07/16 06:26:42 PM															
Overall Results	0	6.806867	27.797494	33,889,541	0.9309157	2	194	16565	98.65147	0	1.325	25989.521	99.87363	0	1800
Service (Downstream) Started at: 07/16 05:56:41 PM - Finished at: 07/16 06:26:42 PM															
Overall Results	0.186474	53.382265	97.223491	16,380,661	0.4499061	1	259	16463	97.41963	0	0.132	4943.778	99.99535	48.83	921



UpStream



DownStream



40MHz Channels
 Only 2 x Channels Used
 1 Spatial Stream
 3 clients < 10Mbps
 2 clients ~ 10Mbps
 4 clients ~ 15Mbps
 1 client ~ 20Mbps

Security Testing

Pen Testing / Data Breach Assessment Approach

What about my Security Posture?

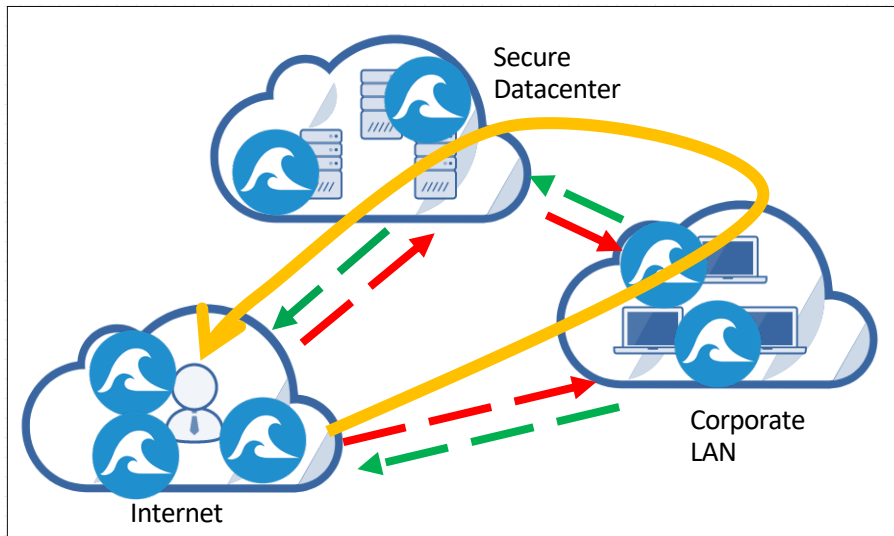
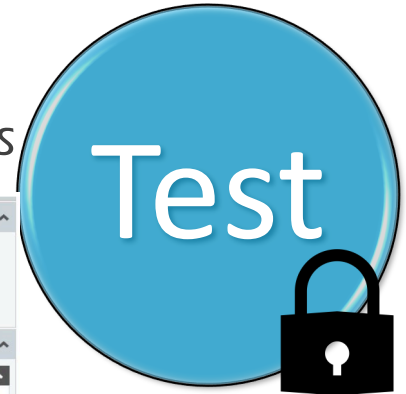
- Can a hacker jump from Guest Wi-Fi to Corporate Wi-Fi or Internal DMZ?
- Are there vulnerabilities in DHCP servers can be exploited?
- Are switches, routers, firewalls all adequately patched?
- Is corporate Wi-Fi easy to get into? Poor authentication security.



Security Testing

24/7 Situational Assessments

Tools are available to have devices constantly doing security assessments



Results Summary

Findings: Critical 4, High 2, Medium 8, Low 13, Malware 5, Sensitive 7

Zones: Corp LAN, Internal DMZ, Guest WiFi

Devices: My DUT1, My DUT3

Attack Plan Data

My DUT1: Corp LAN: 5 Scenarios, Internal DMZ

Blocked (70) 60% / 40% Not Blocked (70)

Scenario Name (S)	Category/CVE ID	Start Time	Attacker IP	Target IP	First Reported	Issue Status	Severity	Result	Event	Actions
App name here	Microsoft	2019-01-21 11:30	1.1.1.11	1.1.1.10	N/A	N/A	N/A	Blocked	Matched	
Attack name here	2012-0391	2019-01-21 11:40	1.1.1.11	1.1.1.10	N/A	N/A	Critical	Blocked	Matched	
Attack name here	2012-0391	2019-01-21 11:50	1.1.1.11	1.1.1.10	New	Not Submitted	High	Not Blocked	Not Matched	
Sensitive Data here	2012-0391	2019-01-21 11:55	1.1.1.11	1.1.1.10	2019-01-21 11:20:01	Open	Sensitive	Not Blocked	Not Matched	
Malware name here	Malware	2019-01-21 11:20:01	1.1.1.11	1.1.1.10	2019-01-21 11:20:01	Reopened	Malware	Not Blocked	Not Matched	

My DUT2: Guest WiFi: 5 Scenarios, Internal DMZ

Blocked (70) 60% / 40% Not Blocked (70)

Scenario Name (S)	Category/CVE ID	Start Time	Attacker IP	Target IP	First Reported	Issue Status	Severity	Result	Event	Actions
App name here	Microsoft	2019-01-21 11:30	1.1.1.11	1.1.1.10	N/A	N/A	N/A	Blocked	Matched	
Attack name here	2012-0391	2019-01-21 11:40	1.1.1.11	1.1.1.10	N/A	N/A	Critical	Blocked	Matched	
Attack name here	2012-0391	2019-01-21 11:50	1.1.1.11	1.1.1.10	New	Not Submitted	High	Not Matched	Not Matched	
Sensitive Data here	2012-0391	2019-01-21 11:55	1.1.1.11	1.1.1.10	2019-01-21 11:20:01	Open	Sensitive	Not Matched	Not Matched	
Malware name here	Malware	2019-01-21 11:20:01	1.1.1.11	1.1.1.10	2019-01-21 11:20:01	Reopened	Malware	Running	Running	



Monitoring

People in the past have spent >\$ 1M in network monitoring tools

- There are a plethora of vendors with solutions that address networks, applications, dev ops etc.
- It is commonplace to monitor a network, even if it is something as rudimentary as SNMP or Flow based metrics
- Wi-Fi is a very different scenario

AP vendors have their in-house tools

- Depending on what they are they vary in quality and information
- AP vendors don't play well with other AP vendors!

Being able to have an historical, correlated view is becoming critical



Monitoring

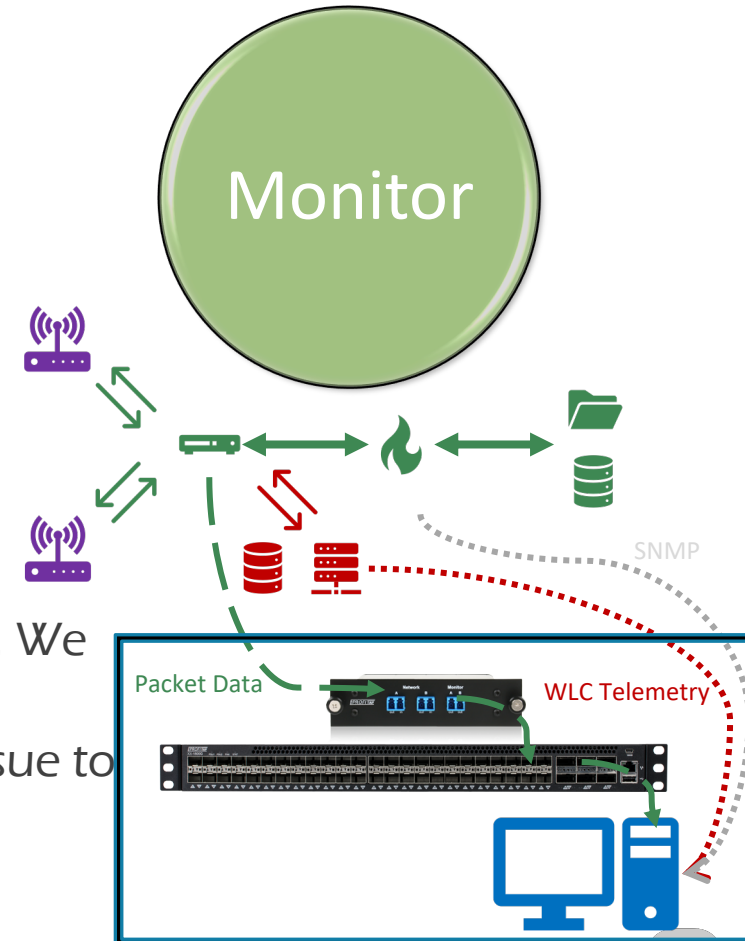
How best to monitor Wi-Fi?

Multiple sources of information is key:

- Telemetry data from Wireless LAN Controllers is important
- SNMP
- NetFlow, jFlow, sFlow, whateverFlow, etc is also useful
- Packet data is critical !!
- So is the ability to look at these metrics in a correlated view

Why

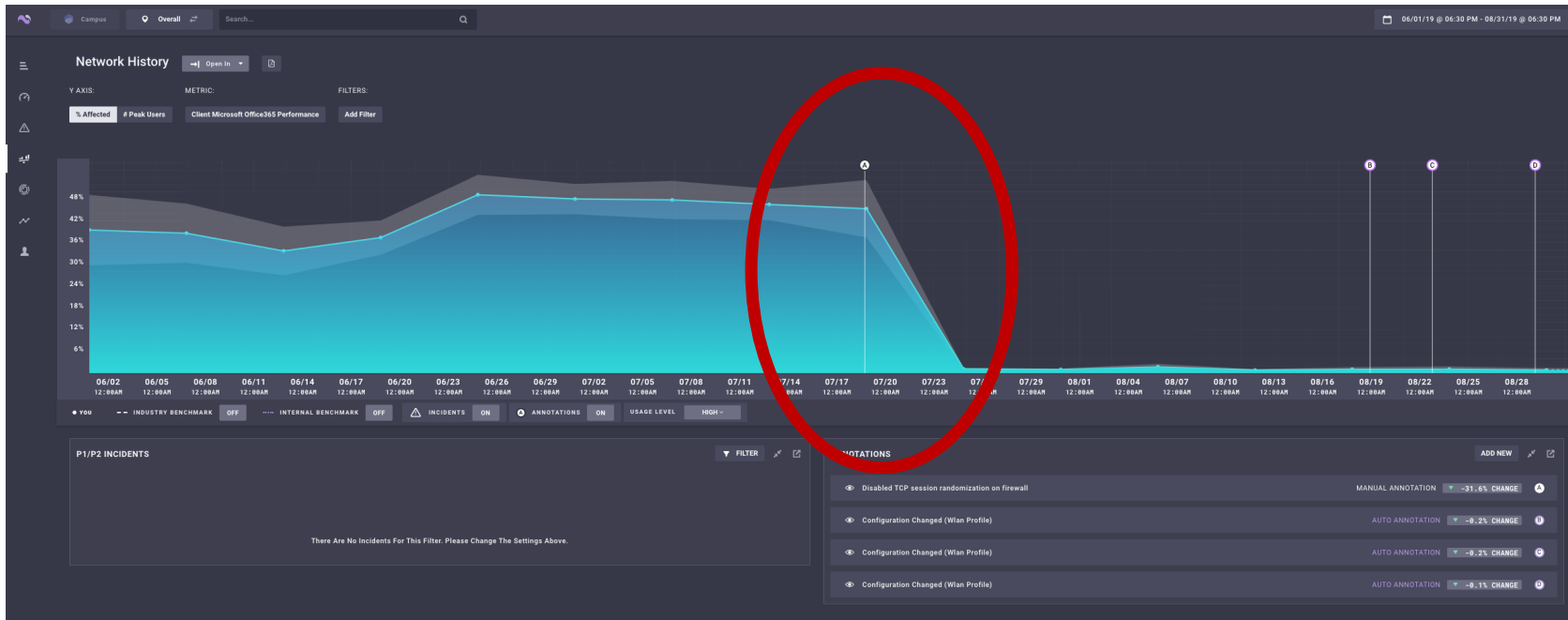
- Traditional networking tools treat the Wireless medium as a black hole. We know there is a problem but don't really know why
- With the types of wireless networks it would be great to pinpoint an issue to a floor or even a single AP
- There are a lot of additional issues around wireless environments



Monitoring

Application Performance on wireless clients is poor but it isn't Wi-Fi

- Without Packet Data (or intelligent metadata) it's hard to work out the issue



Monitoring

Benchmark your Environment

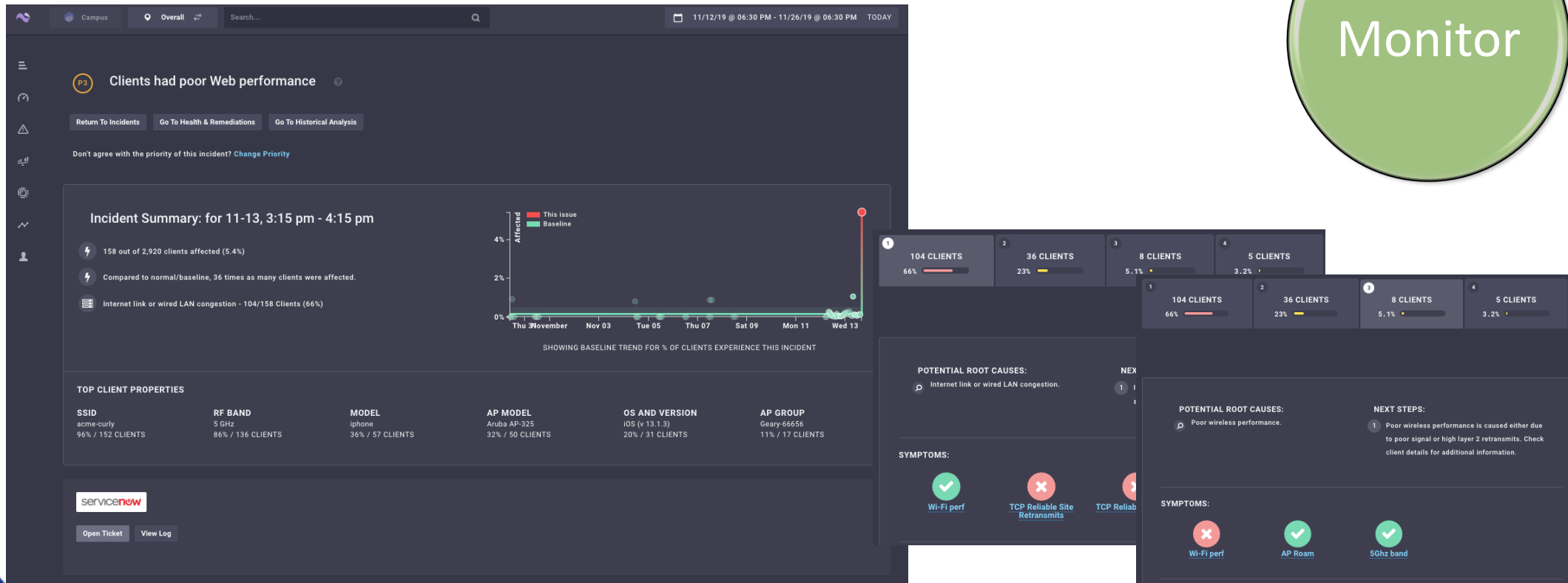
- From new, before/after an upgrade (ie. 802.11ac to 802.11ax migration)



Monitoring

Understand what is providing poor performance

- Know the group, the SSID, the AP, what type of clients...



The screenshot displays a network monitoring dashboard with the following components:

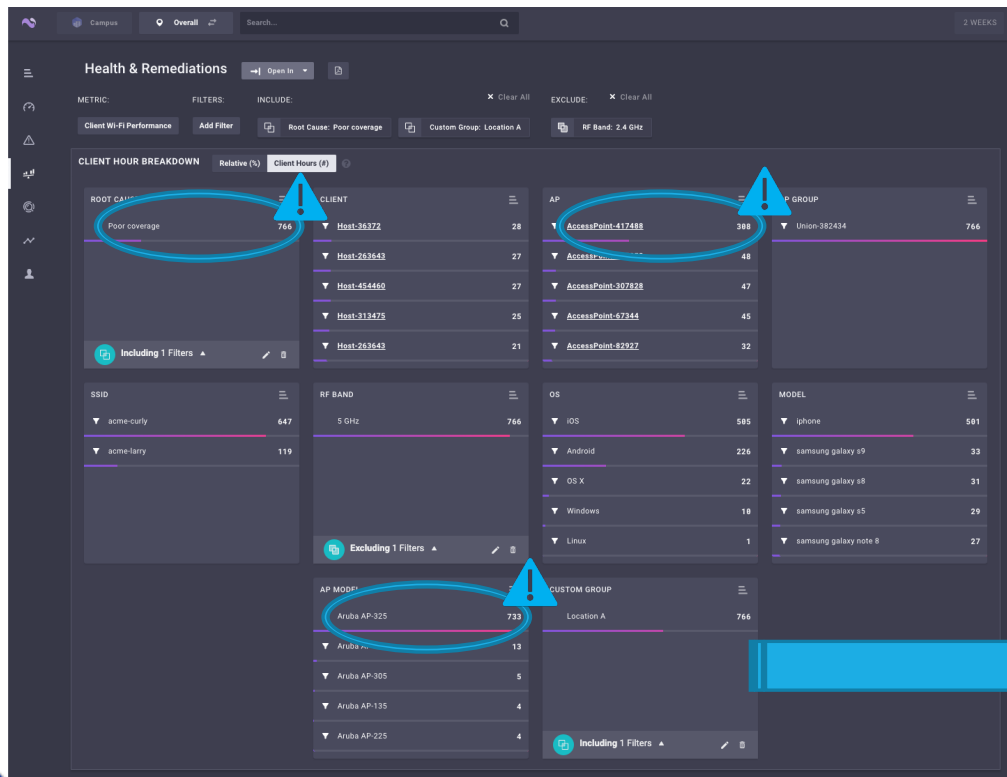
- Incident Summary:** for 11-13, 3:15 pm - 4:15 pm. 158 out of 2,920 clients affected (5.4%). Compared to normal/baseline, 36 times as many clients were affected. Internet link or wired LAN congestion - 104/158 Clients (66%).
- Graph:** A line graph showing the percentage of affected clients over time. The y-axis is labeled 'Affected' (0% to 4%). The x-axis shows dates from Thursday, November 1st to Wednesday, November 13th. A red line represents 'This issue' and a green line represents 'Baseline'. A sharp spike in the red line occurs on Wednesday, November 13th.
- Client Properties Table:**

SSID	RF BAND	MODEL	AP MODEL	OS AND VERSION	AP GROUP
acme-curlly	5 GHz	iphone	Aruba AP-325	iOS (v 13.1.3)	Geary-66656
96% / 152 CLIENTS	86% / 136 CLIENTS	36% / 57 CLIENTS	32% / 50 CLIENTS	20% / 31 CLIENTS	11% / 17 CLIENTS
- Potential Root Causes:** Internet link or wired LAN congestion.
- Symptoms:** Wi-Fi perf (green checkmark), TCP Reliable Site Retransmits (red X), TCP Reliab (red X).
- Next Steps:** Poor wireless performance is caused either due to poor signal or high layer 2 retransmits. Check client details for additional information.
- Client Counts:** 104 CLIENTS (66%), 36 CLIENTS (23%), 8 CLIENTS (5.1%), 5 CLIENTS (3.2%).
- Additional Symptoms:** Wi-Fi perf (red X), AP Roam (green checkmark), 5Ghz band (green checkmark).

Monitoring

Health and Remediation

- Why is coverage poor, and filter down on main offenders



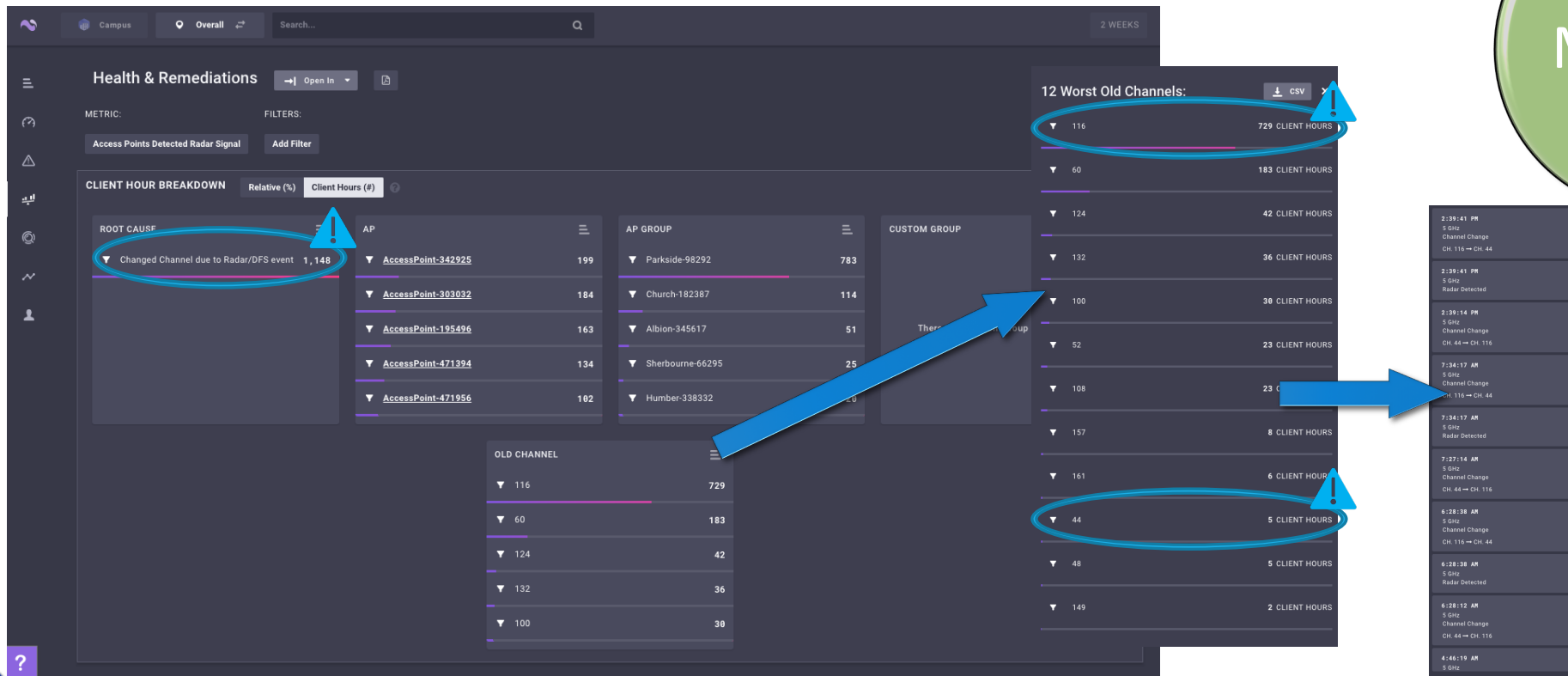
SURVEY THE PROBLEMATIC AP



Monitoring

Health and Remediation

- DFS events adversely effecting the wireless environment



Understand the Ecosystem



"There's another classic example of someone having a two-inch pipe and us having installed only one-inch piping."

CENSORED

DNS, DHCP, Auth, Backhaul

Many complaints about Wi-Fi come down to DHCP or DNS

- If you have authenticated, then it's not Wi-Fi – well not completely
- Has DHCP pool exhaustion occurred – does your DDI solution help you here?
- Are your DNS servers responding and operating efficiently. Are they sized correctly?

The screenshot displays a network management dashboard for DHCP. The left sidebar contains navigation options: Dashboards, IPAM, DHCP (selected), Servers, Groups, Scopes, Ranges, Leases, Statics, Analytics, DNS, Application, Guardian, NetChange, and Workflow. The main content area shows a DHCP treeview on the left and a detailed view of DHCP leases on the right. The lease view includes a table with columns for IP address, Full MAC address, MAC vendor, Start, End, Name, Percent, Expires in, and Status. Below the table, there is a section for 'Range' and 'Failover channel' with a 'Used' percentage and 'Status'.

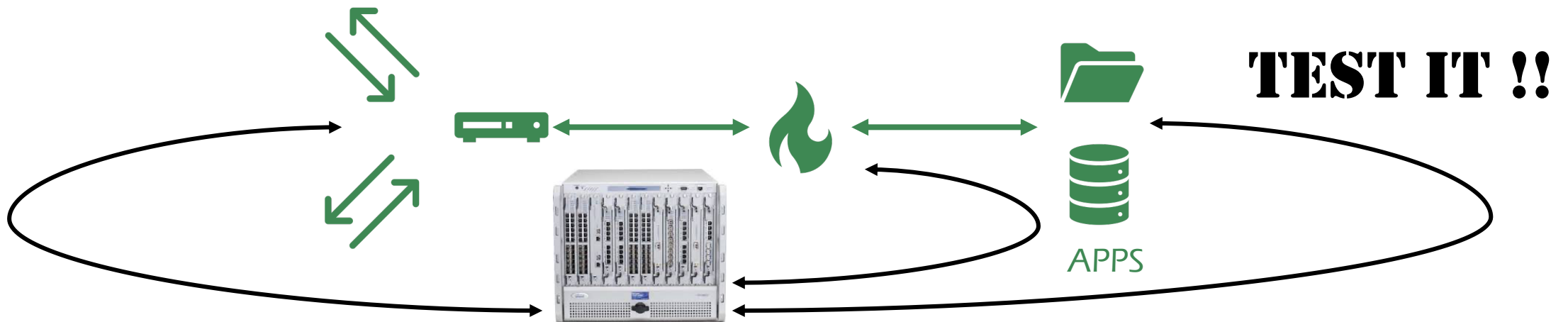
IP address	Full MAC address	MAC vendor	Start	End	Name	Percent	Expires in	Status
192.168.100.102		Texas Instruments	02/12/2019 12:44:08	03/12/2019 00:44:08		6%	0 d 11:14	OK
192.168.100.103		Ubiquiti Networks Inc.	02/12/2019 02:37:57	02/12/2019 14:37:57	Office-Rear	90%	0 d 1:8	OK
192.168.100.105			02/12/2019 08:23:37	02/12/2019 20:23:37	Galaxy-S9	42%	0 d 6:54	OK
192.168.100.106		Ubiquiti Networks Inc.	02/12/2019 02:38:13	02/12/2019 14:38:13	Office-Hall	90%	0 d 1:8	OK
192.168.100.107		Intel Corporate	02/12/2019 09:20:17	02/12/2019 21:20:17	Gloria-PC	35%	0 d 7:50	OK
192.168.100.108		Intel Corporate	02/12/2019 10:11:51	02/12/2019 22:11:51	Sergio-Thinkpad	27%	0 d 8:42	OK
192.168.100.110		Apple, Inc.	02/12/2019 12:08:27	03/12/2019 12:08:27	Atari-2600	6%	0 d 22:39	OK
192.168.100.112			02/12/2019 10:11:29	02/12/2019 22:11:29	SergioTab	27%	0 d 8:42	OK
192.168.100.114		Apple, Inc.	02/12/2019 10:38:31	02/12/2019 22:38:31	Doms-MBP-2	24%	0 d 9:9	OK
192.168.100.115		Apple, Inc.	02/12/2019 10:32:29	02/12/2019 22:32:29	Doms-iPad	25%	0 d 9:3	OK
192.168.100.117								
192.168.100.132								
192.168.100.140								
192.168.100.150								
192.168.100.157		Apple, Inc.	02/12/2019 13:24:52	03/12/2019 13:24:52	Doms-AppleWatch	0%	0 d 23:55	OK
192.168.100.198		NetScout Systems, Inc.	02/12/2019 10:22:42	02/12/2019 22:22:42		26%	0 d 8:53	OK

Range	Failover channel	Used	Status
192.168.100.100-192.168.100.199	N/A	16.0%	OK

DNS, DHCP, Auth, Backhaul

Backhaul is also starting to become of more importance

- As APs move from AC to AX the need for higher backhaul speeds are required
- Are you set up to run NBASE-T?
- Have you tested the backhaul.
 - All our testing discussion was around the wireless medium but have the wired connections been tested.
- Is the DC environment coping with increased traffic / users / applications
 - Has all this been benchmarked? Do you know the performance of your applications?



AI, Root Cause, Single Pain of Glass*

Be aware of marketing hype.....

AI is really just machine learning (ML).

- Some vendors do it very very well
- It's historically based using advanced analytics – pseudo AI!
- Can provide an 'Expert' level of information to assist where to start

Root Cause Analysis

- There is no magic bullet!
- Usually derived from multiple tools through 'fault domain isolation'

Single **Pain** of Glass

- UGH!
- Everyone uses it, but unless you have a massive screen then you won't get it.



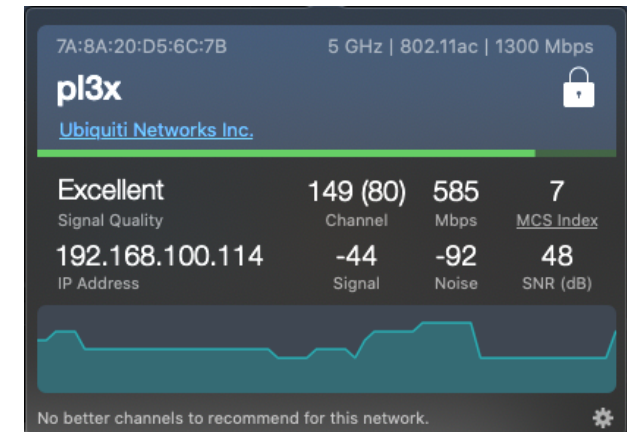
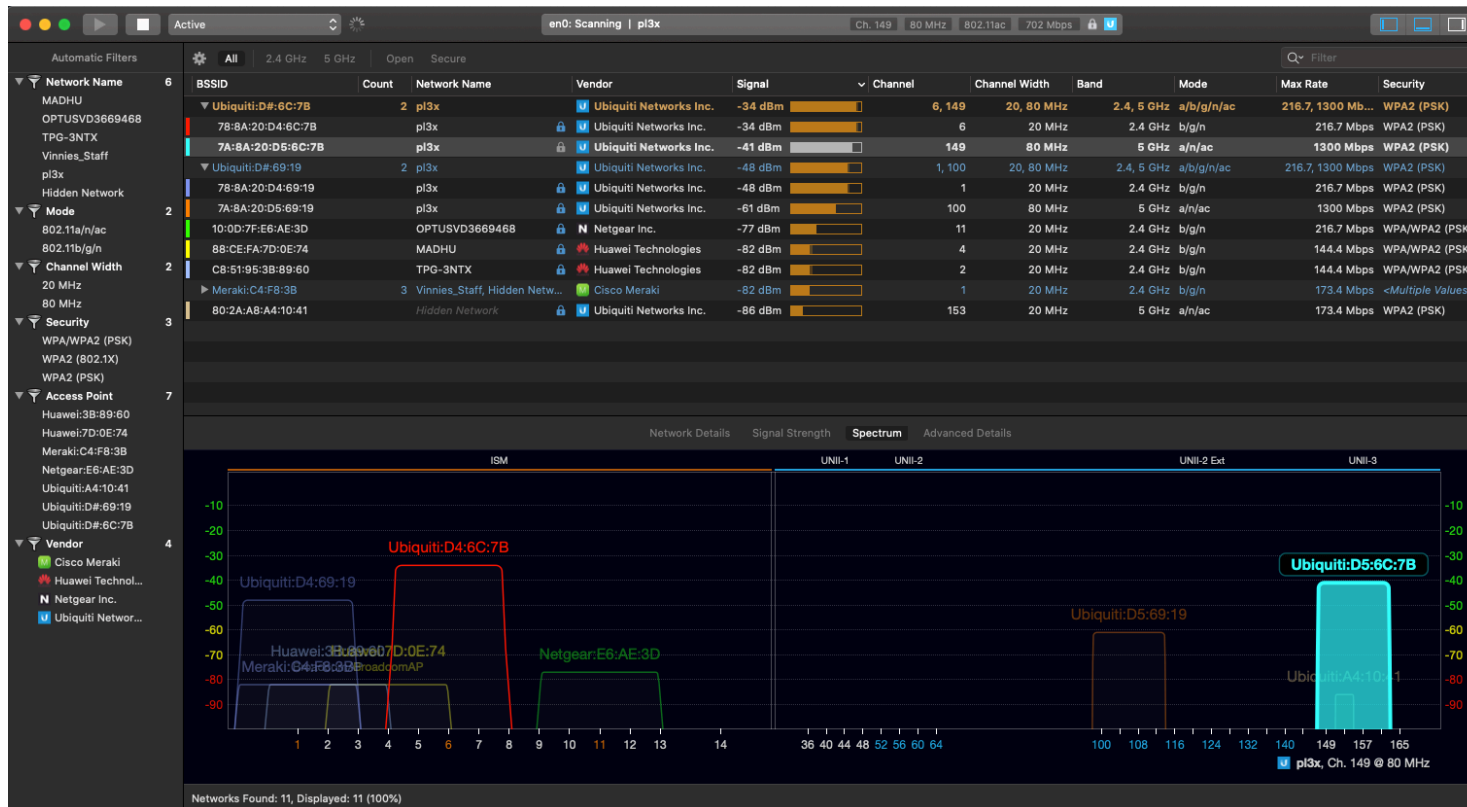
* We hate this phrase so much our PlexNet Tech Blog is called 'Single *Pain* of Glass'



Useful Tools

FREE OR LOW COST

Some cool low-cost tools - Mac



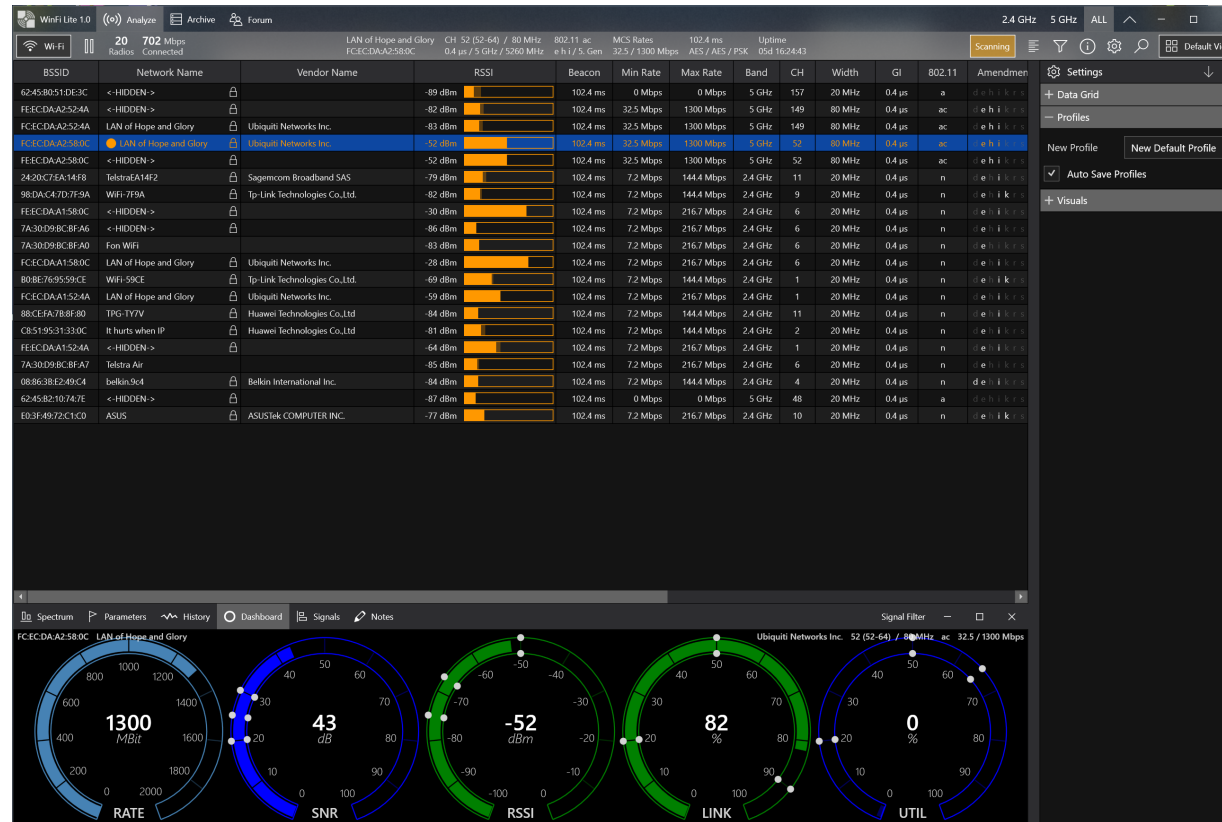
Wi-Fi Signal

Wi-Fi Explorer Pro

<https://www.adriangranados.com>



Some cool low-cost tools - Windows



WinFi - Lite

<https://www.helge-keck.com/download.html>

Some cool low cost tools



WLAN Pi

- iPerf 2 / 3 Server
- Kismet
- Speedtests

Great for Ekahau Throughput tests or any device that requires an iPerf 2 or 3 server

<https://www.wlanpi.com>

Screenshots brought to you by:



#WiFiDesignDay

by ekahau

Thankyou

Dom Fitzgibbon

@fit70z

dom.fitzgibbon@plexnet.com.au

www.plexnet.com.au

