

AOS/Instant 8.4 Overview

John Schaap
john.schaap@hpe.com

11 April 2019

AOS 8.4: Agenda

- New Access Points
 - 11ax (AP-51x) + Green AP
 - 11ad (AP-387)
 - AP-303P
- WPA3 and Enhanced Open
- Multi-PSK
- IoT Enhancements
- Dynamic Segmentation Enhancements
- IPv6 Enhancements

Hardware Update

510 Series Campus Access Points

Mid-range 802.11ax Platform, 4x4 + 2x2 Dual Radio



- AP-515 (integrated antennas), AP-514 (antenna interfaces, 4x RP-SMA)
- Unified AP- same device supports controller-based and Instant deployments
- Operating modes: Campus Access Point, Remote AP, Air Monitor, Spectrum Analysis*, Mesh*
- 802.11ax: UL&DL OFDMA (up to 16 Resource Units)*, DL MU-MIMO*, BSS coloring*, 1024-QAM modulation
 - Supporting all mandatory features for Wi-Fi Alliance 802.11ax wave 1 certification program*, fully backwards compatible with 11abg, 11n, 11ac
 - Peak data rates: 4.8Gbps (5GHz, HE160/4SS), 575Mbps (2.4GHz, HE40/2SS)
 - Up to 512* associated clients per radio (hard limit; 150 max recommended)
- Dual Ethernet: E0 is 100/1000/2500 (Smart Rate, IEEE802.3bz), E1 is 100/1000
- Integrated BLE5.0 & 802.15.4 (ZigBee) radio, USB 2.0 host interface (5W max), Console port
- Power: 12Vdc or POE (on E0), max power consumption (excluding USB): 20.8W (POE) / 16W (DC)
- Deep-sleep mode support for Green AP system feature
- Environmental: 0C to +50C, 5% to 93% relative humidity (non-condensing), plenum rated
- Physical: 200mm x 200mm x 46mm, 810g. Reliability: MTBF 560khrs / 64yrs (+25C)

AP-5xx Green AP

- Enable AP power savings in a wide range of deployment settings
 - AP in sleep mode draws 3-4W of power
 - AP-5xx CAP only
 - MM required (no standalone)
- Netinsight to provide MM deep-sleep/wakeup requests and move APs to corresponding state
 - NetInsight collects WLAN data and provides prescriptive recommendations to the MM
 - AOS 8.4 provides APIs for NetInsight to complete a feedback loop into the AOS services.
- MM will forward the request to individual APs via managed device (controller)
- AP decides whether it is ready to go into power save state and responds back with the status. Will not enter sleep if:
 - It is rebooting, writing to flash or preloading image.
 - It has clients associated.
 - It is operating in mesh portal, multizone, RAP mode or IAP mode.
 - It has wired port or daisy chain enabled.
 - It has secure jack deployment

11ad Multi-Gigabit Wireless System at 60Ghz

60GHz Current Market State

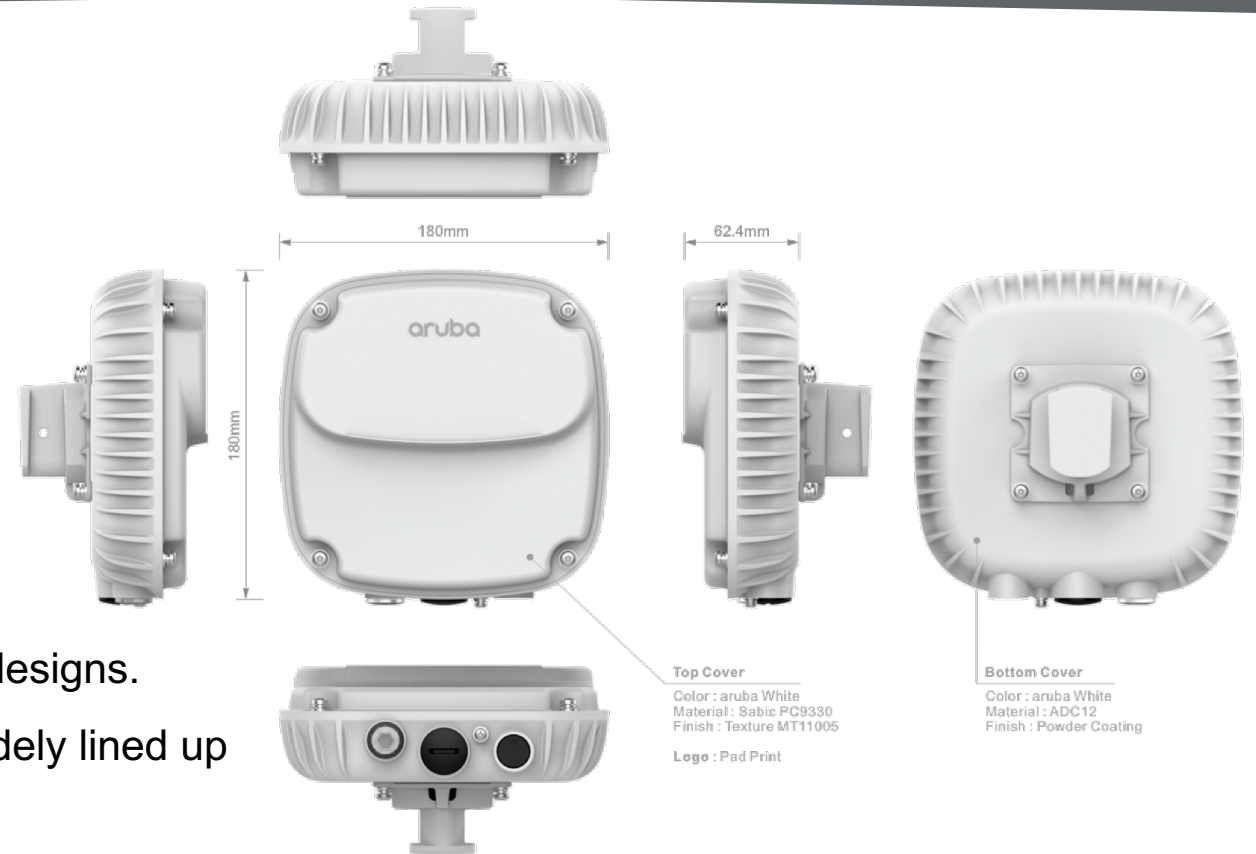
- Links can be expensive
- Antennas are highly directional and require precise alignment by experts
- Long links have issues with rain induced fades

Old school in a big way

- Exploits significant chunks of spectrum at 60 GHz
- 2 to 8 GHz of spectrum is available around the world
- Oxygen Absorption spectrum adds challenges and benefits
- Uses simpler modulation techniques but on a massive scale
 - Single Carrier 1.76 GSps
 - BPSK/QPSK/16 QAM
 - Up to 4.5 Gbps on air data rate

AP-387 Attributes

- Dual radio, 802.11ac 2x2 and 11ad
 - 5GHz: 867 Mbps max (with 2SS/VHT80)
 - 60 GHz: 2502 Mbps max
 - Integrated BLE radio: location, wireless console access
 - 100/1000 Gb Ethernet network interface
 - MU-MIMO, TxBF, console, reset
 - 802.3at POE 14W max
 - Reduced operation mode on 802.3af
- Outdoor hardened HW leveraging successful outdoor designs.
- Link is self acquiring so long as the radios are only crudely lined up
 - Eliminates the need for precision deployment
- 60 GHz radio leverages the scanning antenna capability built into the chipset solution
 - Scans a narrow beam +/- 40 horizontal and +/-10 degrees vertical
- Will reuse Aruba outdoor AP-270-MNT-H1/H2 mount solutions
- Aggregate throughput of the 5 and 60 GHz radio
 - Allows for graceful degradation of the two links
 - 5 GHz is not impacted by weather



AP-303P Campus Access Point (Arranta program)

Low cost Campus 802.11ac Wave 2 AP platform with daisy-chain support

- Basic platform specs and capabilities identical to AP-303 (11ac dual)
 - Almost identical mechanical design. Share mounts, covers, etc.
- **Added:** second Ethernet port (E1) with **POE PSE power sourcing** capability
 - Attached device(s) share(s) same wired connectivity, switch port
 - POE: with 802.3at from the switch (30W, class 4, AP-303P can supply 802.3af POE to attached device
 - Also: with 802.3bt from the switch (45W, class 5), AP-303P can supply 802.3at POE to attached device
 - And: using 48Vdc as the power source, AP-303P can supply 802.3at POE to attached device
 - But: when AP-303P is powered by an 802.3af POE source, the PSE capability is disabled
- Use-cases:
 - Daisy chain another AP (or even two) from first AP-303P. Reduced cost, simplified install
 - Connect and power an Ethernet camera or IOT gateway
- Also added: 802.15.4 support (added to BLE radio)
 - Enables use-cases requiring Zigbee radio (2.4GHz only)



WPA3 and Enhanced Open

Wi-Fi Security Challenges

WPA2 is past retirement (first introduced in 2004)

- WPA2-personal was 'broken on arrival'
 - Every couple of years someone "rediscovers" off-line dictionary attacks
- WPA2-enterprise is still secure, but
 - can be used in ways that lessen its overall security
 - makes it more complicated to provision

For example, use cases with ill-suited security:

- Stadiums, Airports, Guest Captive Portals, BYOD Onboarding use Open SSIDs
- Coffee shops use WPA2-PSK with a shared and public PSK
- Enterprises, banks, schools , hospitals use WPA2-PSK for IoT (or people!)
- Hotspots have no way of offering server-side (infrastructure) only authentication

Solution: WPA3

"WPA3 closes these gaps and evolves Wi-Fi security for the next decade!" Dan Harkins

What is WPA3? Two New WFA Certifications

1. Enhanced Open - OWE (Opportunistic Wireless Encryption) replaces Open

- Problem: all wireless traffic is passed in the clear
- Solution: all wireless traffic gets encrypted
- Not part of WiFi Alliance WPA3 Cert

2a. SAE (Simultaneous Authentication of Equals) replaces WPA2-PSK

- Problem: passive attack results in off-line dictionary attack to discover session key
- Solution: protocol is resistant to active, passive, and dictionary attack

2b. Suite B/Commercial National Security Algorithms ciphers

- Problem: mix-and-match nature of WPA2-Enterprise can result in less-than-optimal security
- Solution: create a cipher suite and a set of rules to ensure consistent primitive security
- WFA requires basic (similar to WPA2 with enforced Protected Mgmt Frame settings)
- Optional Mode for 256-bit + security protocols

Aruba Support for OWE and WPA3

- Supported from ArubaOS 8.4 and beyond
- Supported on the following AP models:
 - AP-303, AP-305, AP-315, AP-318, AP-325, AP-335, AP-345, AP-387, AP-36x, AP-37x, AP-515
 - AP-34x uses SW encrypt
- NOT Supported on other AP models:
 - AP-1xx, AP-2xx
 - An error is logged when configured
`<3761> <WARN> [stm] Virtual AP "ap225-5" rejected for AP "demo-sae-vap"; reason: AP doesn't support WPA3/OWE`
- OWE/WPA3 + PMF supported in Tunnel mode ONLY for CAP, RAP

WPA3 Client Devices

- Very few WPA3 certified chipsets / clients today, increasing numbers expected from 2019
- **Broadcom claims support for 11ax and WPA3 with their BCM4375 chipset powering Samsung S10**
- **Qualcomm with Snapdragon 855 chipset claims support for 11ax and WPA3**
- **Windows 10 19H1 update with tentative release in Spring 2019 might support WPA3, as observed in build 18272 of Win 10 SDK!!**
- Linux supplicant code today (version 2.6) includes WPA3 support
- Apple IOS ?? No info, TBD, could be new phones next year
- Transition time of ~2 years expected for critical mass of WPA3 certified clients within Enterprises

WHAT DOES WPA3 MEAN TO YOU?

- **100% Encryption by default**
 - Privacy before identity credentials
 - Encrypted walled gardens, coffee shops/bars
- **New opportunities and longer lifespan for PSK**
 - Combine with strong profiling
 - Basic IoT, Guest, BYOD, home
- **Quantum-resistant enterprise SSID**
 - Leverage strong SuiteB ciphers
 - If modern devices support it, leverage it
- **Protected Management Frames**
- **Better security with no added complexity!**
- **Leverage WPA3 as a differentiator today!**

MultiPSK

Problem Statement

An increasing number of "headless" devices which are unable to support 802.1X joining the network using a single WPA2-PSK passphrase that is shared among all devices which are connected to the same SSID present an ever-growing security risk.



Problem Statement Cont'

Attempting to overcome the single WPA-PSK passphrase limitation by creating multiple SSID results in an inefficient RF utilization



Multi-PSK - Overcoming the limitations

With the use of MPSK customers will gain the following:

- The ability to support multiple PSK on the same SSID
- Improved RF bandwidth utilization by using a single SSID
- Reduction in Time/effort of IT department
- Ability to provide better security by providing multiple PSK



Supported Multi-PSK Use-Cases

Devices are associated to individual users (e.g. John, Jane or Jim)

–1:1 MPSK where there is a single device (i.e. MAC Address) registered and mapped to a single generated PSK visible and managed by a single user.

Enabled through ClearPass Self-Service Device Registration

Devices are associated to groups of users (e.g. Marketing, Sales, IoT)

–Many:1 MPSK where there are multiple devices (i.e. MAC Address) mapped to a single generated PSK.

Enabled through Enforcement Policy by ClearPass administrator

Multi-PSK Solution Elements



ClearPass

- ClearPass is required for MPSK support
- MPSK will require ClearPass 6.8

Mobility Controller

- MPSK is supported with ArubaOS 8.4
- MPSK supported in Tunnel-Mode only

Instant Access Points

- MPSK will be supported on Instant OS 8.4
- MPSK will require ClearPass 6.8


IoT Enhancements

IoT Solution Summary in Release 8.4

- Flexible, extensible and configurable transport framework for IoT data developed
- North-bound API from controllers augmented with IOT telemetry feed
 - Standardized endpoints named “aruba telemetry-https” and “aruba telemetry-websocket” defined
 - Generic format of streaming data established which vendors can parse as necessary
- Parsing new device types supported: Eddystone beacon, EnOcean switch/sensors
- IOT manager on MM or IAP offers global visibility of all IOT devices being managed or observed by AP’s IOT radio
- BLE beacons and tags support enhanced with config update and firmware upgrade
- Strategic partner integrations:
 - SES-imagotag
 - Assa-Abloy door locks
 - ZF OpenMatics (from 8.3)

Partner Integrations in 8.4 - ZigBee & Proprietary Protocols

- Solution works for AOS and Instant
- IoT radio operates in 2.4 GHz

Partner	Wireless Protocol	Use-Case	Radio	Supported AP Platforms
SES-imagotag	Proprietary	Electronic Shelf Labels	External Dongle from SES	AP-303H/304/305/314/315/324/325/334/335/AP344/345/514/515
Assa-Abloy	 ZigBee®	Smart Door Locks	External Dongle from Digi	AP2xx AP3xx

- Digi Zigbee dongle support on IAP/CAP (XU-Z11 Recommended)
- Enables single network for Wifi and Zigbee which in turn enables cost savings in terms of installation and infrastructure.
- The door lock solution to work seamlessly for Assa-abloy, Vingcard door locks , Elsafe

SES Imagotag Electronic Shelf Labels (ESL) Solutions

- ... integration with Aruba, to lower infrastructure costs



SES Imagotag is the market leader in Electronic shelf labels for retail.

Previously, it required an overlay of proprietary radio devices, to communicate with these labels.

With Aruba, this can now be done from the Access point.

Proprietary solution in 2.4 GHz connects ESL tags to ZigBee aggregator

Aruba AP transports the ESL payload data to ESL management server

This gives the following benefits:

- No extra cost of deploying additional technology (Cabling / switchport)
- No extra devices to maintain / patch / keep secure
- Less RF interference

Assa Abloy VingCard / Digi

– Integration to optimize / Simplify hospitality



Elsafe Safes



- Assa Abloy VingCard is a leading provider of access control primarily used in Hospitality.
- Manage keycard, In Room Safe, In Room Thermostats.
- Previously required a massive network of Zigbee access gateways in hallways / rooms to control these devices.
- With Aruba, this can be done directly from the Access point. This reduce the needed infrastructure (Cabling / Wired ethernet ports), devices installed in the ceiling.
- Traditionally Access control has been managed by security staff with limited IT knowledge. This enhancement will help optimize efficiency and improve guest experience.

Dynamic Segmentation Enhancements

8.4 Enhancement Background

- In the current Dynamic Segmentation (DS) 1.0 deployments
 - the VLAN is required to be configured on the switch and also on the controller.
 - This also means that the same VLAN must be configured across the network and used for the same purposes across the deployment.
 - In large enterprise deployments it's not possible to have all the VLANs across all the switches and controllers across all the buildings carrying the same subnets.
- In DS 2.0 (ArubaOS 8.4 and ArubaOS-Switch 16.08 release)
 - the requirement to have VLANs being configured on all the switches is removed.
 - The VLAN will be configured on the controllers and assigned to users through Role Based VLANs.
 - Switch is not aware of this user VLAN.
 - Controller will be replicating the broadcast / multicast packet for each individual user on that VLAN because switch is not aware of client VLAN

DS Requirements

- ArubaOS 8.4 controller will support both DS 1.0 and 2.0 deployment
 - DS 1.0 release is supported with switch releases 16.04.xx
 - DS 2.0 will be supported on switch release 16.08.xx
- It is mandatory to upgrade Cluster controllers to 8.4 version if switch is upgraded to 16.08.xx
- ClearPass Downloadable User Role (DUR) feature is supported for DS 1.0/2.0
- Role Based VLAN derivation is not supported for DS 1.0
- DS 1.0 does not require any additional licenses
 - But 8.4 will enforce licenses, whether it is 1.0 or 2.0
- DS 2.0 requires the same licenses as Access Points (AP's)
 - Access Point (AP), Policy Enforcement Firewall (PEF), RFProtect (RFP)
 - 8.4 will require and enforce license requirements regardless if the switch is 1.0 or 2.0
- Mobility Controller (MC) limits are also enforced with DS 2.0
 - Total number of switches and AP's cannot exceed the supported AP limit on the controller

Scale Information

- Switch DS– max 32 UBT's per port and 1024 UBT per switch are supported
 - 3 member Stack will only support a max of 1024 UBT's (same as a single switch)
- Controller scale is a max of GRE tunnel's supported by the controller
 - As an example – a 7240 can support a total of 32768 GRE tunnel's which also include;
 - AP and DS, you cannot exceed the total of 32768 GRE tunnels to the controller in this case a 7240
 - Cannot exceed the total number of APs on a MC

Controller Model	7005	7008	7010	7024	7030	7205	7210	7220	7240	7240xm	7280
MAX GRE Tunnels	256	256	512	512	1024	4096	8192	16384	32768	32768	32768

IPv6 Enhancements

ArubaOS 8.4 RAP IPv6 Split Tunneling

What's New in 8.4?

1

Enhances RAP functionality by supporting the Split-Tunnel forwarding mode

- 8.2 introduced IPv6 support for RAPs using Tunnel or D-Tunnel modes
- This 8.4 enhancement adds support for Split-Tunnel modes for Native IPv6 deployments
- Split-Tunneling can be enabled on WLANs and/or Wired AP Ports

Limitations

- Both RAPs and Users must be running Native IPv6
- The lc-rap-pool configuration on the MM currently only supports IPv4



ArubaOS 8.4 Web-CC Enhancements

What's New in 8.4?

1

Adds support for Web-CC classification and policy assignments for IPv6 traffic

- In previous releases, classification and policies only applied to IPv4 traffic
- Administrators can now configure and apply IPv6 policies that include Web-CC Categories and Reputations

2

Adds support to communicate to Webroot's BrightCloud servers using IPv6

- Connections can now use IPv6 to perform URL lookups and download the URL database
- Supports centralized (MM) or distributed (MD) modes
- Does not require a IPv6 connection to BrightCloud to classify IPv6 traffic!

3

Introduces associated CLI commands and show command enhancements



ArubaOS 8.4 RTLS Enhancements

What's New in 8.4?

1

Enhances existing AeroScout / RTLS functionality by enabling IPv6 support

- Enhancement allows Campus APs to communicate with Location Servers using IPv6
- CLI and Web-UI both allow a Global IPv6 address to be entered in the AP System Profile for either AeroScout RTLS Server or RTLS Server configurations
- This is a proactive enhancement only. At this time no RTLS servers implement IPv6!
- Assumes the Campus APs are using IPv6



airheads

TECH TALK *LIVE*

Thank You