

ARUBA OS – ARUBA CONTROLLER FEATURES USED TO OPTIMIZE PERFORMANCE

Technical Climb Webinar

10:00 GMT | 11:00 CET | 13:00 GST
Oct 26th, 2016

Presenter: Barath Srinivasan

barath.srinivasan@hpe.com

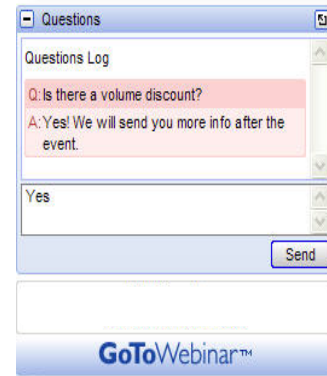


Welcome to the Technical Climb Webinar

Listen to this webinar using the **computer audio broadcasting** or dial in by phone.

The dial in number can be found in the audio panel, click **additional numbers** to view local dial in numbers.

If you experience any difficulties accessing the webinar contact us using the **questions panel**.



Housekeeping



This webinar will be recorded



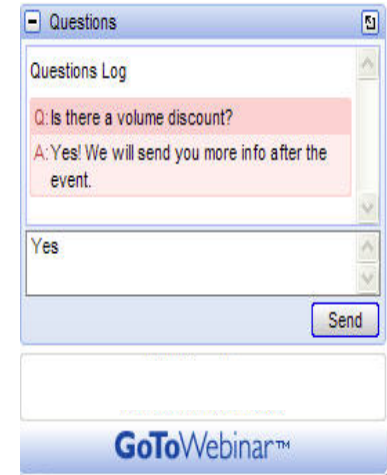
All lines will be muted during the webinar



How can you ask questions?
Use the question panel on your screen



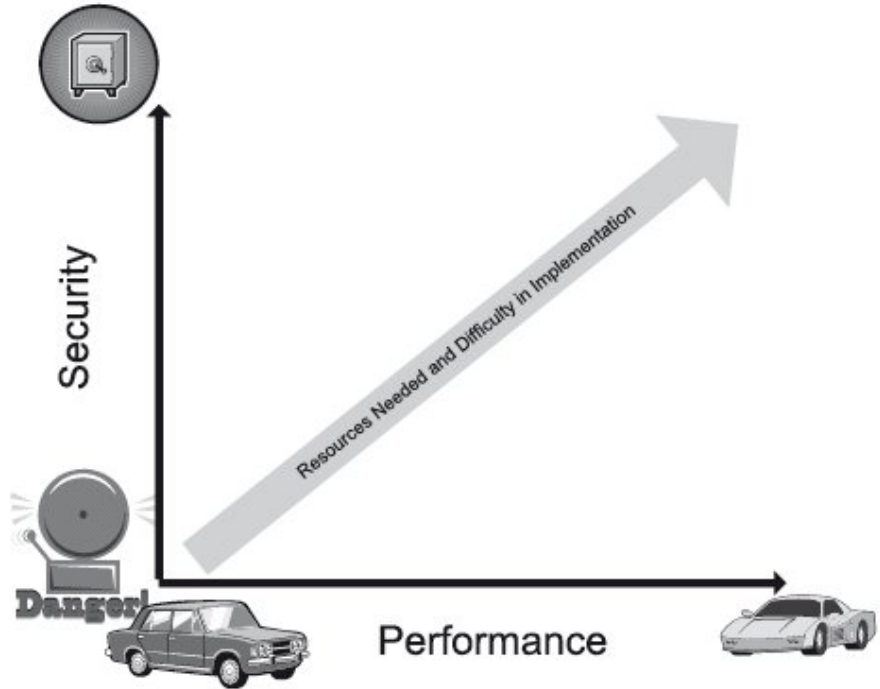
The recorded presentation will be posted on Arubapedia for Partners (<https://arubapedia.arubanetworks.com/afp/>)



PERFORMANCE VS SECURITY AN OVERVIEW

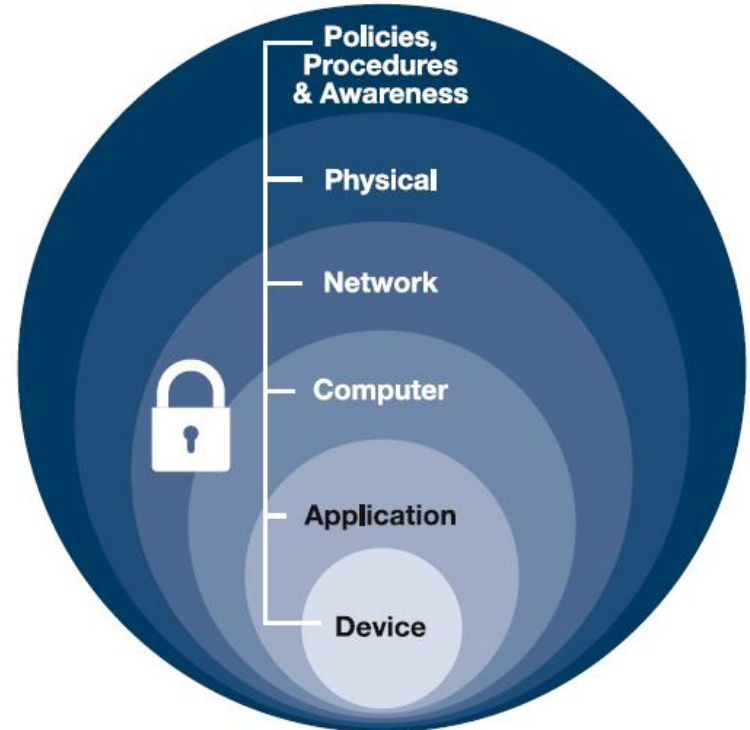
Performance Vs Security

- Network Attacks are evolving to become more sophisticated
- Performance vs security is always a trade-off unless high amount of resources are committed to the task
- Performance wants to rapidly move packets and security's job is to stop packets infecting the next host
- New threats, Compliance, Perimeter safety, Cost are factors largely influencing network security
- Scalability, Stability, Interoperability, Throughput, Connectivity and coverage are factors influencing network performance



Network Security Layers

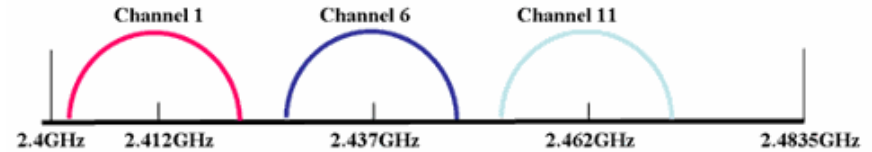
- Network security must be applied in layers, in order to be most effective
- Layered approach provides safety at multiple levels, even if one of the layer is hacked/compromised, the threat can be detected before any vital data breach occurs
- An effective perimeter security or deterrent is a better cost vs benefit value
- An example would be, Mac/802.1x authentication and then performing CP/VPN authentication against AD resources



Factors influencing Performance

- Density of user devices vs Density of active Access points
- Cleanliness of the WLAN environment (i.e., Coverage Area – Fig.1)
- Reliability of the LAN network to transport packets from AP to Controller and vice versa
- Stability of the Access and Distribution network (Switching network)
- Effective and quick centralized packet processing solution (Mobility Controller) and core network
- High performance AAA solution and AD integration, preferably with the lowest latency

DSSS First Set: 3 non-overlapping channels:



DSSS Second Set: 6 half-overlapping channels

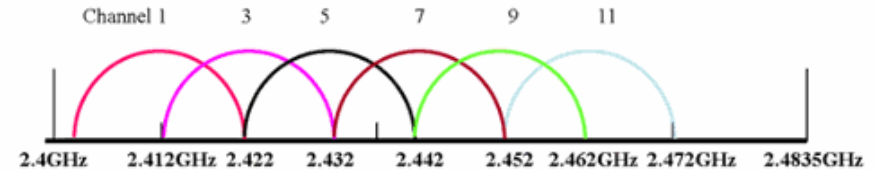


Figure 1. Wi-Fi Channelization

NETWORK OPTIMIZATION

How to optimize your existing Aruba WiFi

It is generally ideal to assess network optimization prior to committing resources.
Let us begin with design, then Deployment, Config, Coverage, Performance & Security

RF Consideration & Roaming

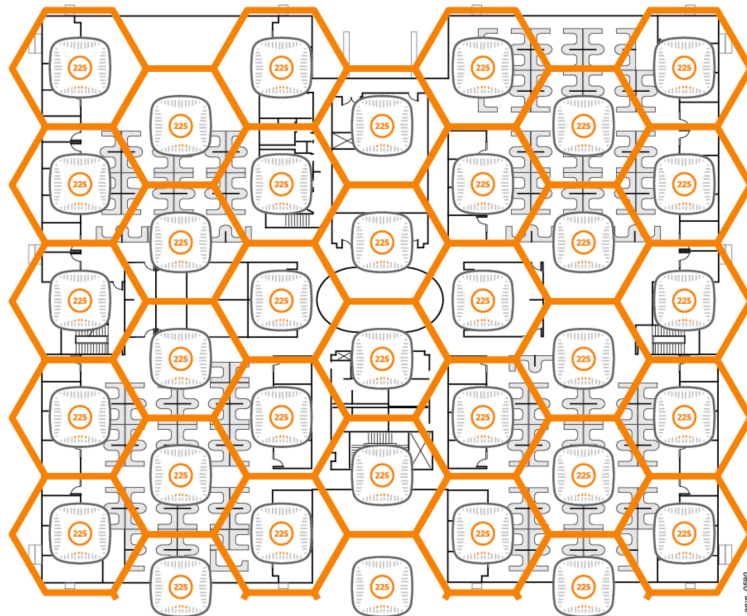
- Adjusting the AP's power and channels using Aruba's Adaptive Radio Management (ARM) technology.
- Ensuring Proper load balancing and band steering clients across AP's and channels using Aruba's Client Match technology
- Eliminating unnecessary chatty broadcast-multicast traffic from RF
- Client's roam decision can be influenced by tuning data rates, beacon rates and AP's tx power
- Time taken for roaming between clients can also be influenced by means of using opportunistic key caching (trial and error process)

Optimization

AP Placement

In the 802.11 ac capacity based design, Aruba recommends distance between centers of two AP's should be approximately 50ft. AP placement also depends on client density. In an all wireless office where AP's are deployed every 50ft, the expected client count on an AP's radio is approximately 40 to 60 clients.

If the client density is higher than these values, then the AP's should be deployed closer.



Optimization

AP Selection Recommendations

There is a substantial increase in the number of applications and high definition multimedia streaming used by the devices that connect to WiFi. 11ac addresses these high bandwidth requirements by providing data rates in excess of 1 Gbps. Aruba recommends the use of 11ac AP's to achieve high network performance.

AP-224 or AP-225 for indoor deployments

AP-274 or AP-275 for outdoor deployments

AP-109 or AP-155 for RAP deployments

Optimizing RF

- Choose the most optimal 802.11 channel and transmit power
- Choose the most optimal RF band and AP type
- Restrict unnecessary broadcast-multicast traffic in the air
- Apply a proper traffic shaping policy

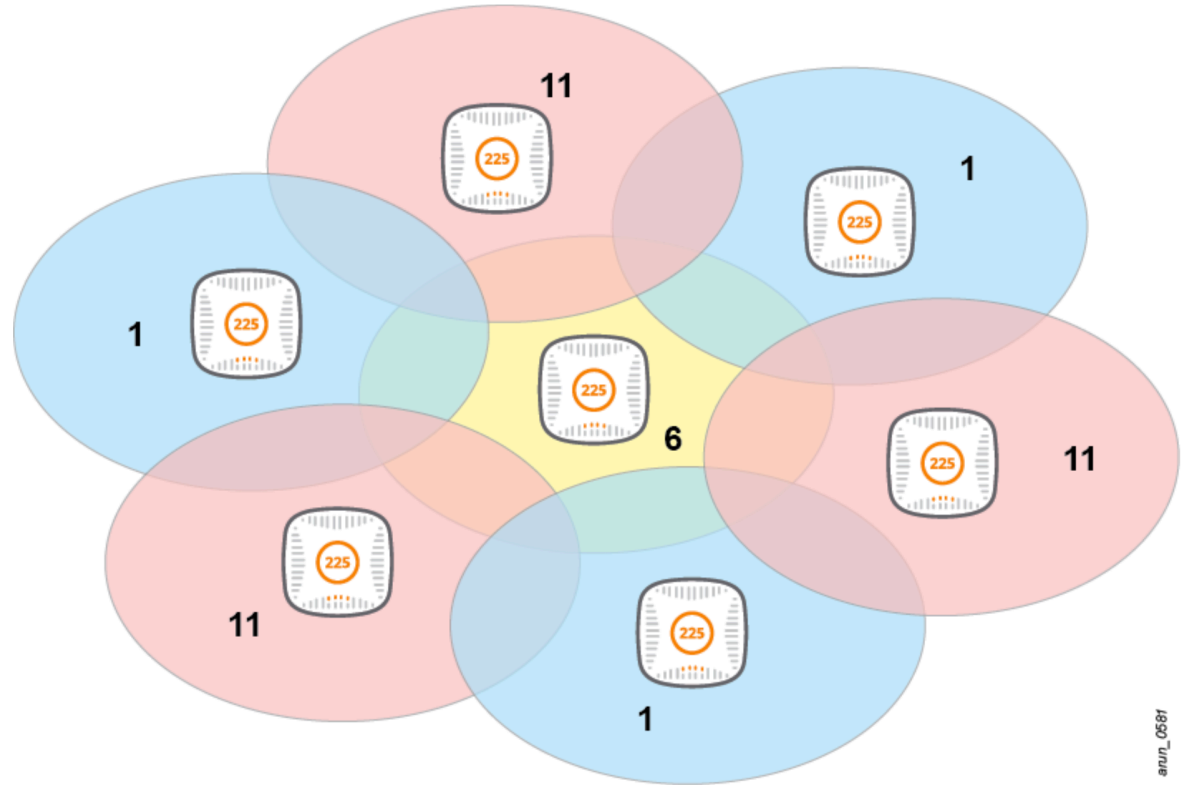
Optimization

Benefits of using ARM

- Aruba AP's dynamically scan all 802.11 channels in its regulatory domain at regular intervals and reports them back to the controller. This includes, but not limited to neighbor AP TX power and channel, data regarding WLAN coverage, interference and intrusion detection
- ARM uses the information collected and calculates the channel quality for each channel in the spectrum and reports it back to the AP. Based on neighboring AP's TX power, ARM also calculates coverage index.
- AP's decide to change or remain on the same channel depending on the information received from ARM. In scenarios like a broken antenna, blocked signal from neighbor AP's, each AP can effectively increase or decrease Tx power to provide sufficient coverage
- For VoIP protocols such as SIP, SCCP and H323, AP's will not change the channel until voice call is over. This is because ARM is voice aware.

Optimization

- A sample of the ideal Channel distribution which ARM tries to achieve.



Optimization

Tips & Tricks

- Remove channel 144 from the list, it is not supported by many devices
- In high density open air environment, 20 or 40Mhz channel width helps in reducing channel utilization and improves overall network performance by providing more clear channels
- Many voice specific devices do not like scanning multiple channels before roaming, as they have active voice calls, in these cases DO NOT use UNII-2 and UNII-2e channels
- Do not use DFS channels if you are operating close to an airport, military base, port or active water ways, due to radar detection
- Although some clients support DFS channels, while roaming they try not to pick AP's with DFS channels, as this may cause roaming issues
- Roaming test should be performed using different types of clients expected on the WLAN to check their behavior on DFS channels

Optimization

Transmit power

Although ARM alters AP's transmit power, there could still be instances when edge AP's operate on maximum tx power as they cannot hear neighboring AP's and center AP's could be operating on low transmission power due to the presence of too many neighbors.

- A difference of not more than 6dbm should be maintained between min and max tx power within each ARM profile
- A difference of 6 dbm should be maintained between 802.11a and 802.11g radios, so that both bands have equal coverage and clients do not switch to 802.11g due to stronger signal strength

- These Tx power values are applicable for AP's separated by a distance of approx. 50ft

	Open Office	Walled Office
A Radio Min Tx Power	12 dbm	15 dbm
A Radio Max Tx Power	15 dbm	18 dbm
G Radio Min Tx Power	6 dbm	6 dbm
G Radio Max Tx Power	9 dbm	9 dbm

Optimization

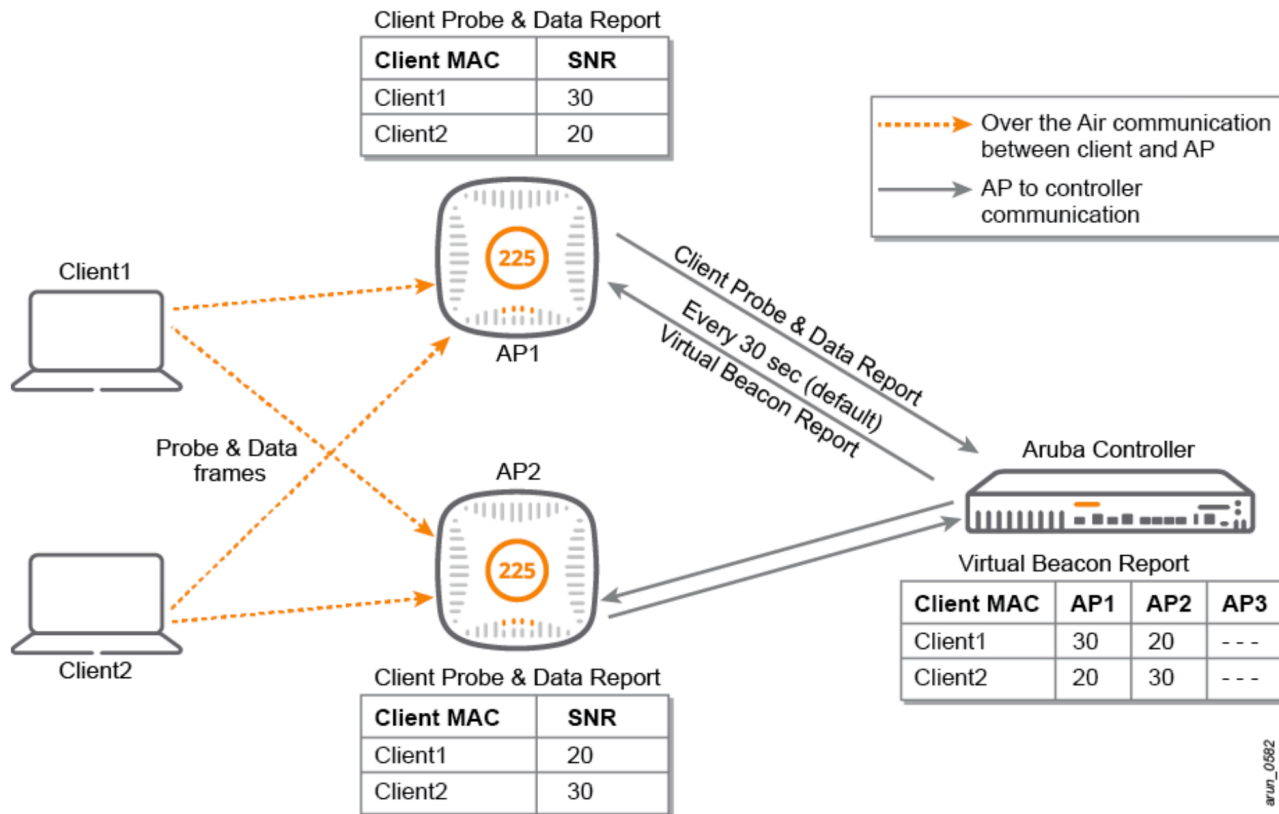
ClientMatch Tweaks

Client match was introduced in ArubaOS 6.3 as a part of ARM 3.0. This technology eliminates sticky clients and dramatically improves system throughput by constant monitoring of session performance metrics and using this data to steer each client to the closest AP and best WLAN radio.

ClientMatch Settings	Default Values	Recommended Values	Comments
ClientMatch Sticky Client Check SNR (db)	25	18	From internal testing and field experience, SNR value of 18 db has been identified as the best value before initiating sticky move for a wide variety of clients.
ClientMatch Load Balancing Client Threshold	18	30	Increasing the value of this parameter from 10 clients to 30 clients, avoids too many load balancing events in a production environment.
Bandsteering g-max signal (dbm)	-45	-10	By increasing the value of this parameter to -10 dbm, ensures that ClientMatch will try to band steer most of the clients from g-radio to a-radio.
ClientMatch restriction timeout (sec)	10	3	To steer client to the designated radio, all other radios except the designated one, blacklists the client for the time configured here. In a production environment, reducing restriction timer to 3 sec ensures that even during failed steering event client can quickly reconnect to the network.

Optimization

- Sampling done by ClientMatch technology to constantly assess WLAN client and RF performance



Optimization

Band Steering

Dual band clients scan all the channels on both 2.4Ghz and 5Ghz and try to connect to the BSSID with the strongest signal or the BSSID that responds first to the client probe request. If the client tries to connect at a lower PHY rate, ClientMatch band steers the clients to the appropriate band.

- The client signal strength on g-radio is lower than the band steer g-band min signal (def: -45dbm)
- The client signal strength on a radio on the same AP is higher than the band steer a-band min signal (def: -75dbm)

Dynamic Load Balancing

Aruba controller monitors the clients associated to each radio and load balances them if the following conditions are met,

- The client count on a radio is higher than the load balancing client threshold (def: 10)
- The client SNR on a radio with lesser load is higher than the load balancing SNR threshold (def: 30dbm)

Optimization

Sticky client steering

Aruba AP monitors the SNR of the clients associated to it and initiates a sticky move if the following conditions are met,

- The client SNR is lesser than the sticky client check SNR (def: 18db)
- Based on a virtual beacon report, there is a better radio to steer clients to if -
 - SNR of the target radio is higher than the SNR threshold (def: 10db)
 - Signal strength of the target radio is greater than or equal to Stick Min signal (def: -70dbm)

Optimization

Restrict unnecessary broadcast and multicast traffic to improve WLAN network performance

Broadcast Filter ARP

In a large enterprise or campus WLAN, broadcast DHCP and ARP packets can flood the WLAN network and also impact the performance of the other wireless users. Broadcast filter ARP parameter in Virtual AP profile addresses this problem by converting broadcast ARP requests destined for wireless clients to unicast request. It also converts broadcast DHCP offers/ACKs into unicast DHCP frames OTA.

Drop Broadcast and Multicast Traffic

After ARP and DHCP packets are converted to unicast, the next step is to restrict broadcast and multicast that is generated by client applications. Such as, NetBIOS, MDNS or DLNA based services which are Mcast based. To restrict such applications, use “Drop broadcast and multicast” parameter in the Virtual-AP profile.

Optimization

Broadcast & Multicast Optimization

Feature	Default Value	Recommended Value	Comments
Convert Broadcast ARP Requests to Unicast	Enable	Enable	Helps convert broadcast ARP and DHCP packets to unicast.
Drop Broadcast and Multicast	Disable	Enable	Prevents all broadcast and multicast traffic from flooding into AP tunnels. "Convert broadcast ARP to unicast" must be enabled.
AirGroup	Disable	Enable if MDNS, DLNA, or other zero-config services are needed.	Allows applications such as Airplay and ChromeCast even if "drop broadcast and multicast" is enabled.

Optimization

Allow multicast based services using Airgroup

While broadcast and multicast is being dropped in the air, some essential services like DLNA and MDNS might be required. To enable these services for applications like airplay and chromecast, Airgroup service can be enabled on the Aruba mobility controller. It uses context aware access to DLNA, Apple Bonjour and other shared services without affecting network performance.

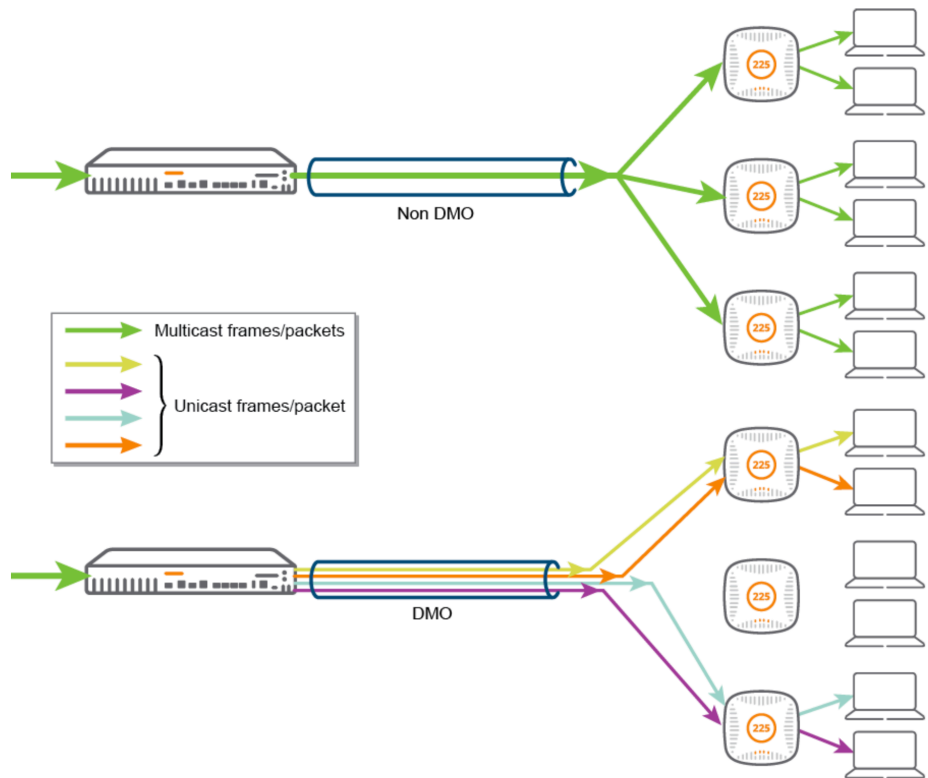
Dynamic multicast optimization

The 802.11 standard states that multicast over WLAN must be transmitted at the lowest basic rate so that all the clients are able to decode it. The low transmission rate results in increased airtime utilization, and decreased overall throughput. Due to decrease in speed, it is advisable to transform multicast traffic to unicast when only a few clients have subscribed to the multicast stream.

Optimization

Multicast rate optimization

It keeps track of the transmit rates sustainable for each associated client and uses the highest possible common rate for multicast transmission. For example, if all the clients connected to the VAP are transmitting at a data rate of 24Mbps or higher, multicast frames are transmitted at 24Mbps, rather than the lowest basic rate, which ranges between 1 or 6 Mbps



Optimization

Config Recommendations

- Enable Convert broadcast ARP packet to unicast parameter
- Enable Drop broadcast and multicast traffic parameter
 - (Ensure that convert broadcast ARP packet to unicast parameter is enabled before enabling this parameter)
- Enable Airgroup, if MDNS, DLNA or zero-config service based traffic is required.
- If any other type of multicast traffic is required, including multicast streaming, enable dynamic multicast optimization and multicast rate optimization. Set DMO client threshold to 80.
 - IGMP snooping or proxy should be enabled for DMO
 - Prioritize multicast stream by configuring uplink ACL and WMM parameters

Optimization

Feature	Default Value	Recommended Value	Comments
Multicast Streaming: <ul style="list-style-type: none">• Dynamic Multicast Optimization (DMO)	Disable	<ul style="list-style-type: none">• Enable if multicast streaming is needed.• Set DMO client threshold to 80.• Prioritize multicast stream using controller uplink ACL.	<ul style="list-style-type: none">• Converts multicast frames to unicast to deliver at higher rates.• IGMP snooping or proxy needs to be enabled for DMO to work.
<ul style="list-style-type: none">• Multicast Rate Optimization Disable	Disable	Enable	<ul style="list-style-type: none">• Sends multicast frames at highest possible common rate.• Enable even if DMO is enabled.

Optimization

Cell size optimization

There is a drop in data rate when a client starts moving towards the edge of the coverage cell. Clients at the edge of the coverage cell use very low data rates (1Mbps or 6Mbps), which impacts its performance and of the other clients connected to the same AP. In capacity-based deployments, when the coverage cell of neighboring AP's overlap, it is recommended to move clients to the next AP when client's data rate in the current AP's basic Service Set (BSS) drops below a certain value. By optimizing AP cell size, we can influence the client to roam to an AP that is closer with better signal strength and data rates.

Reducing AP Tx Power

In general, reducing the AP transmit power reduces the cell size, but as the transmit power reduces, the effective data rate at which a client can associate also reduces. Reducing the transmit power to very low value in capacity-based deployments can affect the network performance.

Optimization

Cutting down lower rates

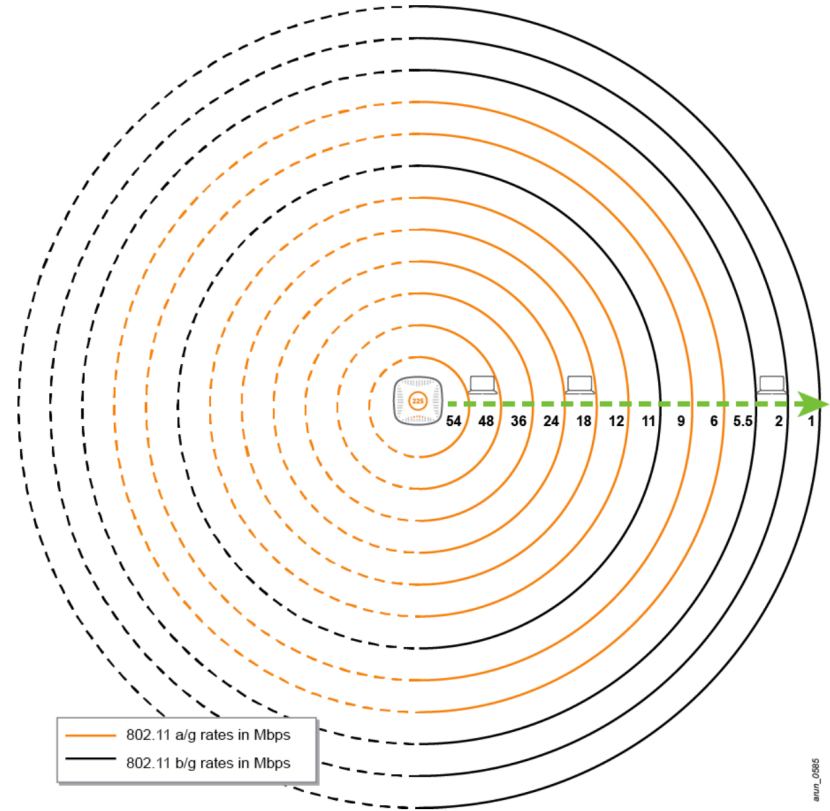
802.11 standard defines the basic and transmit rates for both 802.11a and 802.11g radios. An AP advertises basic and transmit rates in beacon and other management rates. These rates are used while communicating between AP's and stations in a WLAN.

Basic Rates

This is the rate at which a station communicates to successfully associate to the AP. Any station that is not capable of communicating with all the basic rates cannot associate with the AP

Transmit rates

These are supported rates that an AP advertises in addition to the basic rates. These additional rates can be used for AP/Client communication. A station does not have to support all of the transmit rates.



Optimization

In a dense deployment, reducing an AP's cell size can influence clients to roam to another AP, as it cannot hear mgmt frames after a certain distance, as lower rates are cut down. Roaming is initiated when clients start moving away from an AP and data rates drop. For example, when 6, 9, and 12 Mbps rates are cut down (Basic & Tx rates) from an SSID profile for A-Radio, three outer most coverage cells are cut down. Once a client's data rate drops below 18Mbps, a client initiates roaming, which mainly impacts remote clients, as they use lower data rate.

Recommendations

- Legacy clients (802.11b) require lower rates of 1Mbps – 2Mbps. Such clients may not even associate to the network if these rates are removed
- Cutting down lower rates may cause client connectivity issues. Before making changes on the production network, run a test in the lab environment with different types of clients that may access the WLAN.
- Broadcast and multicast frames also use one of the basic rates, cutting down the lower rate may impact delivery of such frames to clients at the edge of an AP's coverage cell.
- If there are no 802.11b devices on the network, remove the 802.11b rates for basic and transmit rates.
- If you have gaming devices connected to the WLAN, add data rate 5, 6, 9 and 11 to the g-radio basic and transmit rates.
- For AP's that are 5-ft apart, sue the following rates for 802.11 A and G radio
 - Basic rates – 12, 24 Mbps
 - Transmit rates – 12, 18, 24, 36, 48 and 54 Mbps

Optimization

Validate Pairwise Master Key (PMK) ID

This parameter instructs the controller to check the Pairwise Master Key (PMK) ID sent by the client and mainly helps when OKC is enabled. It ensures that the PMKID on the client and server matches before the controller uses the cached opportunistic key, if it does not match then the client will go through the complete 802.1X key exchange

Fast BSS Transition – 802.11v support

As a part of 802.11v implementation, ArubaOS supports BSS Transition Management. This support can improve throughput, effective data rates and QoS for voice clients in a network by transitioning individual clients to appropriate access points. 802.11v Fast BSS Transition is enabled by default if 802.11k is enabled. If needed you can disable 802.11v in the ARM profile.

- OKC and validate PMKID are enabled by default and should always be kept enabled
- 802.11k should be enabled with the measurement mode for beacon reports set to active channel report. As some of the clients cannot be interpreted, Quiet IE element from RRM IE profile should be disabled.
- 802.11r should be enabled only after testing it in the lab with different types of devices connecting to WLAN

QUESTIONS

Any Questions?

THANK YOU!