RF and Roaming Optimization for Aruba 802.11ac Networks

aruba

a Hewlett Packard Enterprise company

Copyright Information

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett-Packard Enterprise Company
Attn: General Counsel
6280 America Center Drive
San Jose, CA 95002
USA

Please specify the product and version for which you are requesting source code.

Chapter 1
Introduction

In the recent years, Wi-Fi has become a critical part of enterprise and campus networks. With the introduction of 802.11ac, which provides gigabit speed, many companies are moving towards all wireless offices. Moving to an all wireless office is cost-effective and provides a flexible work environment to employees, which enables them to work from anywhere. In an all wireless enterprise or campus network, where users are not restricted to working from their desks, roaming becomes an essential part of a wireless network design, people move to various parts of a building while on a Lync call using their smart phone and/or uploading/downloading files from the shared server.

To support this functionality, seamless roaming between access points is provided to ensure best quality of service and user experience. This document provides best practices and guidelines to optimize RF and improve roaming in the Aruba WLAN architecture that supports thousands of mobile devices such as laptops, smart phone, tablets, hand-held scanning terminals, and voice badges. The following areas are significantly impacted when a wireless network supports many roaming devices:

- AP Selection and Placement Recommendation
- RF Consideration
- Roaming Optimization
- Device Configuration

This guide discusses the design principles and configuration guidelines in each of the above areas.

AP Selection and Placement Recommendation

In most enterprises and campuses wireless has become the primary medium to access the network. Applications that run on WLAN require high throughput and/or less latency, jitter, and packet drops. Therefore, selection and placement of APs is the first step to ensure the network is ready to support all these requirements and support thousands of mobile devices. This section provides guidelines about AP selection and placement for different types of WLAN deployments.

RF Consideration

Roaming devices are extremely sensitive to RF congestion and inefficiencies. Device performance can be substantially improved by:

- Adjusting the AP’s power and channels using Aruba’s Adaptive Radio Management™ (ARM) technology.
- Ensuring proper load balancing and band steering clients across APs and channels using Aruba’s ClientMatch technology.
- Eliminating unnecessary chatty broadcast-multicast traffic from RF.
- Providing equal airtime to each client.

Roaming Optimization

This section provides guidelines to optimize RF for roaming devices.

Client's roam decision can be influenced by tuning data rates, beacon rates and AP's tx power.

In addition to influencing the roam decision, time taken for roaming between access points can also be reduced using techniques such as **Opportunistic Key Caching** and **802.11r/k/v**. The way devices behave based on the value set for these parameters may differ.

NOTE

It may take several trial and error iterations to come up with the right value that works for a specific WLAN environment.

Experienced engineers may have different views about the optimal settings that extract maximum benefits and the nominal values for these settings. This document provides guidelines about settings that can be adjusted and their suggested value to improve client roaming behavior on Aruba infrastructure.

Device Configuration

Mobile devices display different roaming behavior, depending on the wireless chipset and firmware. To ensure proper roaming on the WLAN infrastructure, ensure the best firmware version and configuration is available on the mobile device. This section provides guidelines to ensure the device is optimized to provide best roaming performance on WLAN.

Scope

This guide is designed for Aruba Mobility controllers running versions ArubaOS 6.3.x and later. It does not cover the fundamental wireless concepts. This guide assumes that the reader has a working knowledge of Aruba WLAN architecture and has already deployed it in an enterprise or campus environment.

- This design guide is best applicable in office and university campus/dorm environments.
- For information on Aruba Mobility Controllers and deployment models, see the Aruba Mobility Controllers and Deployment Validate Reference Design, available at www.arubanetworks.com/vrd.
- For information on Aruba controller campus deployment models, see the Campus Deployment Validate Reference Design, available on the Aruba website at www.arubanetworks.com/vrd.
- The complete suite of Aruba technical documentation is available for download from the Aruba support site at support.arubanetworks.com.
- For detailed instruction on configuring these parameters, refer to ArubaOS 6.4.x User Guide and ArubaOS 6.4.x Command-Line Interface Reference Guide.

NOTE

This solution guide does not apply to Aruba Instant architecture.

Summary of Recommendations

The following tables summarize the recommendations made in this guide, it is not a replacement for the material, but a quick reference that can be looked up later.

NOTE

Values that work in one environment, may not work in a different environment. A network administrator should adjust one parameter at a time and test it before using it in a production environment.

AP Placement

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

ARM Recommendations

To efficiently control the RF characteristics of each band and implement the recommendations included in this guide, create separate ARM profiles and assign them to their individual Radio profiles.

NOTE

The following ARM recommendations apply only to 6.x deployments. For ArubaOS 8.x deployments using Mobility Master, the AirMatch feature assigns radio channel and power. For recommendations on AirMatch, please refer to the latest ArubaOS 8.x User Guide.

Table 1: *ARM Recommendations*

Feature	Default Value	Recommended Value	Comments
Transmit Power (dBm)	**802.11a and 802.11g radio**: Min 9 / Max 127	**Open Office**: 5 GHz: Min 12/Max 15 2.4 GHz: Min 6/Max 9 **Walled office or Classroom**: 5 GHz: Min 15/Max 18 2.4 GHz: Min 6 /Max 9	• The difference between minimum and maximum transmission power on the same radio should not be more than 6 decibels (dB). • Transmit power of a 5 GHz radio should be 6 decibels higher than the 2.4 GHz radio.
Channels	• 80 MHz channels enabled. • ISM, U-NII-1, and U-NII-3.	• 80 MHz channels can be used in green field deployments. • U-NII-2A and U-NII-2C (DFS) channels must be used when operating on 80 MHz channels. • Remove channel 144 from list. • Consider using 40 MHz or 20 Mhz channels for better channel separation.	• Enable DFS channels if you are not close to an airport or military installation. • Enabling DFS channels could create coverage holes for clients who do not support it. • Most of the clients do not scan DFS channels initially, this makes roaming more inconsistent when using these channels. • Very few clients support channel 144. • 20 Mhz or 40 MHz channel width will help in reducing channel utilization in high density open air environment.
Ideal Coverage Index	10	6	In high density environments, prevents APs from settling on high Tx power.
Free Channel Index	25	40 (only for 2.4 GHz)	Moves APs to a new channel if the new channel has free channel index 40 or better.
Back Off Timer (sec)	240 sec	1800 sec	Reduces the chances of frequent changes in channel and Tx power of an AP.
Error rate threshold%	50	70	Reduces frequent channel changes in noisy environments.
Error rate wait time (sec)	30	90	Reduces frequent channel changes in noisy environments.

ClientMatch Recommendations

Table 2: *ClientMatch Recommendations*

Feature	Default Value	Recommended Value	Comments
Sticky Client SNR (db)	Up to ArubaOS 6.4.2.2: 25 dB ArubaOS 6.4.2.3 onwards: 18 db	18 db	18 dB SNR is ideal to initiate sticky move for most of the clients.
Load Balancing Client Threshold	Up to ArubaOS 6.4.2.2: 10 clients ArubaOS 6.4.2.3 onwards: 30 clients	30 clients	Avoids excessive load balancing events in HD environment.
Band steering g-max-signal (dBm)	-45 dBm	-10 dBm	Prevents users from getting stuck on 2.4 GHz in HD environment.
ClientMatch Restriction Timeout (sec)	10 sec	3 sec	In a production environment, reducing restriction timer to 3 seconds ensures that even during a failed steering event, the client can quickly reconnect to the network.

Recommendations to Optimize Broadcast and Multicast Traffic

Table 3: *Recommendations to Optimize Broadcast and Multicast Traffic*

Feature	Default Value	Recommended Value	Comments
Convert Broadcast ARP Requests to Unicast	Enabled	Enabled	Helps convert broadcast ARP and DHCP packets to unicast.
Drop Broadcast and Multicast	Disabled	Enabled	Prevents all broadcast and multicast traffic from flooding into AP tunnels. "Convert broadcast ARP to unicast” must be enabled.
AirGroup	Disabled	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.

Table 3: *Recommendations to Optimize Broadcast and Multicast Traffic*

Feature	Default Value	Recommended Value	Comments
Multicast Streaming: • Dynamic Multicast Optimization (DMO)	Disabled	• Enable if multicast streaming is needed. • Set DMO client threshold to 80. • Prioritize multicast stream using controller uplink ACL.	• Converts multicast frames to unicast to deliver at higher rates. • IGMP snooping or proxy needs to be enabled for DMO to work.
• Multicast Rate Optimization Disable	Disabled	Enabled	• Sends multicast frames at highest possible common rate. • Enable even if DMO is enabled.

Airtime Fairness Recommendations

Table 4: *Airtime Fairness Recommendations*

Feature	Default Value	Recommended Value	Comments
Airtime Fairness	Default Access	Fair Access	Provides equal airtime to all the clients.

Roaming Optimization Recommendations

CAUTION

Adjust these parameters only if you notice roaming issues in the existing design.

Table 5: *Roaming Optimization Recommendations (High Density Corporate and Education deployments)*

Feature	Default Value	Recommended Value	Comments
Data rates (Mbps)	**802.11a**: Basic rates: 6,12,24 Transmit Rates: 6,9,12,18,24,36,48,54 **802.11g**: Basic rates: 1,2 Transmit Rates: 1,2,5,6,9,11,12,18,24, 36,48,54	802.11a/ g: Basic rates: 6,12,24 802.11a/ g transmit rates: 6, 12,24,36,48,54	If you have IoT devices and gaming consoles operating in 2.4GHz frequency, connecting to the network then add back data rates 5, 6, 9 and 11 Mbps to the G radio Basic and Transmit rates Note: Older gaming consoles (namely the Xbox 360) were known to have issues connecting to the WLAN when lower basic rates are disabled.
Beacon Rate (Mbps)	By default lowest configured basic rate.	For both 802.11a and 802.11g radio use 12 or 18.	Sends out beacons at the configured rate rather than lowest configured basic rate.
Local Prob Req Threshold (db)	0	0-15dB	AP stops responding to client probe request if SNR is less than 15 db. **NOTE: Do not exceed 15dB.**

NOTE

Trimming some of the lower basic rates is a common practice to enhance roaming experience in high density environments such as corporate enterprise campuses and school campuses. For warehouses, retail and hospital environments, please operate with default values for data rates and beacon rate.

Table 6: *Roaming Optimization Recommendations (Warehouses, Retail and Hospital deployments)*

Feature	Default Value	Recommended Value
Data rates (Mbps)	802.11a: Basic rates: 6,12,24 Transmit Rates: 6,9,12,18,24,36,48,54 802.11g: Basic rates: 1,2 Transmit Rates: 1,2,5,6,9,11,12,18,24,36,48,54	Use default values
Beacon Rate (Mbps)	By default - lowest configured basic rate.	Use default values
Local Prob Req Threshold (db)	0	Use default values

Fast Roaming Recommendations

Table 7: *Fast Roaming Recommendations*

Feature	Default Value	Recommended Value	Comments
Opportunistic Key Caching (OKC)	Enabled	Enabled	Avoids full dot1x key exchange during roaming by caching theopportunistic key. **NOTE**: macOS and iOS devices do not support OKC. Apple devices support 802.11k,v and r.
Validate PMKID	Enabled	Enabled	Matches PMKID sent by client with the PMKID stored in the Aruba controller before using OKC.
EAPOL Rate Optimization	Enabled	Enabled	Sends EAP packets at lowest configured transmit rate.

Table 7: *Fast Roaming Recommendations*

Feature	Default Value	Recommended Value	Comments
802.11r Fast BSS Transition	Disabled	Enabled	802.11r enables supporting clients to roam faster. macOS, iOS, most Android, and Win10 devices support 802.11r. For a list of devices tested for interoperability please visit https://www.arubanetworks.com/support-services/interoperability/. **NOTE:** Some older 802.11n devices, handheld scanners and printers may have connectivity issues with 802.11r enabled on WLAN.
802.11k	Disabled	Enable 11k with these additional changes: - Beacon report set to **Active Channel Report.** - Disable **Quiet Information Element** parameter from the Radio Resource Management profile.	Helps clients make a quicker decision to roam.
802.11v BSS Transition Management	Disabled	Enabled	Helps clients to roam faster.

NOTE

802.11r (recommended to be enabled) and 802.11v (enabled by default) help improve roaming experience on Apple devices such as macOS and iOS devices.

Voice Devices Recommendations

Table 8: *Voice Devices Recommendations*

Feature	Default Value	Recommended Value	Comments
Channels	- U-NII-2A and U-NII-2C disabled. - Channel 165 enabled.	- Disabled - Disable this channel if the VOIP client doesn't support it.	- Voice devices do not scan many channels. - Some VOIP handsets do not support channel 165. Check the device manual for support details.
WMM	Disabled	- Enable this feature if the device is WMM-capable. - Set required DSCP values for different types of traffic.	Helps to prioritize voice traffic.

This section discusses AP placement recommendations for office and campus environments. These guidelines can also be used for open offices, walled offices, classrooms, and dorm environments, where there is a high density of users (40 to 60 clients on a radio). AP placement is important to ensure there is 100% pervasive coverage and special care has to be taken in high density deployments.

Capacity-Based RF Coverage

In terms of AP density, a WLAN network can be designed in two ways:

- Coverage based
- Capacity based

In a coverage-based network, fewer APs are deployed and spaced significantly apart from each other. The APs operate at a higher TX power and therefore cover larger areas. Whereas, in a capacity-based network more APs are deployed, which operate at a lower TX power to keep the cell size smaller. In this deployment, devices within these cells associate at higher PHY rates and therefore experience better performance.

Most devices use wireless as the primary medium to access the network. Applications such as Netflix, FaceTime, Lync, Skype, and so on running on these devices require higher bandwidth to provide better quality of service. Hence, capacity-based AP deployment is recommended for any new deployment that uses wireless as a primary medium to access the network.

In a high density deployment, the distance between centers of two neighboring APs is around 50 ft, with client count on a radio between 40 to 60 APs. This type of deployment is generally seen in class rooms, dorms, and enterprise office environments.

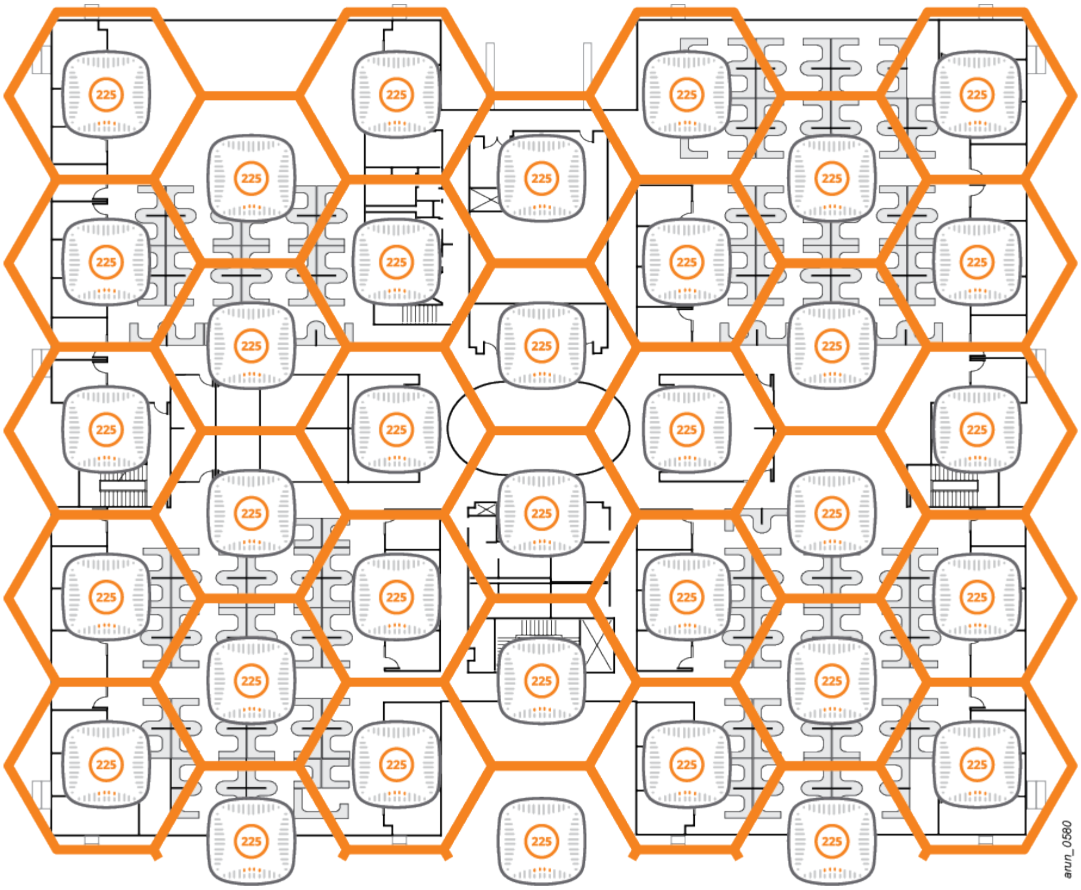
In an ultra-high density deployment, the distance between the center of two neighboring APs is approximately 30 to 35 ft with client count on a radio between 40 to 60 APs. This type of deployment is seen in large conference halls, auditoriums, and public venues.

In a normal or sparse deployment, the distance between the center of two neighboring APs is 70 ft or higher. This type of deployment is seen in warehouses and manufacturing facilities.

Carpeted Office Space

In a carpeted office space the recommended distance from the center of one AP to the center of neighboring AP is 50 ft. In such scenarios, a honeycomb pattern of deployment is recommended. The following illustration is an example of the honeycomb pattern with 36 APs. This pattern ensures that distance is normalized along all directions for the best coverage.

Figure 1 *- Honeycomb Pattern AP Deployment*



AP Selection Recommendations

11ac AP Considerations

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

- AP-224 or AP-225 for indoor deployments
- AP-274 or AP-275 for outdoor deployments
- AP-109 or AP-155 for RAP deployments

Chapter 4
RF Considerations

802.11 WLAN uses the unlicensed Industrial Scientific and Medical (ISM) RF spectrum in 2.4 GHz band and Unlicensed National Information Infrastructure (U-NII) RF spectrum in 5 GHz band. There are multiple Wi-Fi and non-Wi-Fi devices that share the same RF spectrum. Also, there are multiple wireless devices available today and the behavior of each is different when connected to WLAN. To improve the performance of wireless clients and reduce the roam time form one access point to another, RF is optimized based on the WLAN deployment.

To optimize RF, following areas should be considered:

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

Selecting Optimal 802.11 Channel and Transmit Power

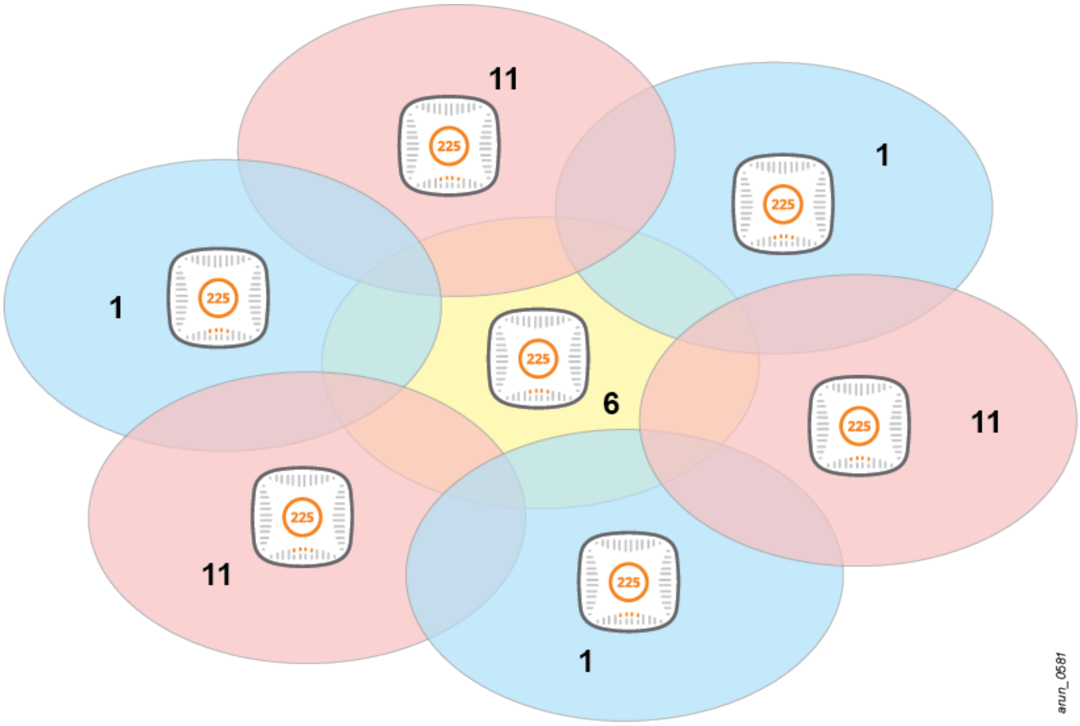
Selecting the right AP transmit power and channel helps improve the overall performance of the WLAN and provides better user experience. For example, if APs are operating on high power, then their coverage cells are large, resulting in co-channel and adjacent channel interference. Similar issues are observed if neighboring APs are operating on the same channel or an overlapping channel.

Earlier, network administrators had to perform a static site survey at each location to identify areas of RF coverage and interference, and then manually configure each AP according to the results of the site survey. Static site survey helps in choosing channel and power assignments for APs, but these surveys are often time consuming, expensive, and only reflect the state of the network at a single point in time. Also, RF conditions change as more new Wi-Fi and non-Wi-Fi devices come into the building.

Aruba's Adaptive Radio Management™ (ARM) technology solves these challenges by dynamically choosing the best 802.11 channel and transmit power for each AP in the current RF environment. With ARM scanning enabled:

- Aruba APs dynamically scan all 802.11 channels in its regulatory domain at regular intervals and reports them back to the controller. This includes, but is not limited to neighboring APs' transmission 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 APs' transmission power, ARM also calculates coverage index.
- APs decide to change or remain on the same channel depending on the information received from ARM. In scenarios like a broken antenna or blocked signal from neighboring APs, each AP can effectively increase or decrease transmission power to provide sufficient coverage.
- For VOIP protocols such as SIP, SCCP, and H323, APs will not change the channel until voice call is over. This is because ARM is voice aware.

Figure 2 *Sample Channel and Power Selection by Adaptive Radio Management*



Channel

Though ARM takes care of selecting the appropriate channel for the APs, the following points should be considered as well:

- Since 802.11ac standard supports 80MHz channel boding, it can be used in Greenfield deployment (all 802.11ac access points). However, if 80MHz channel bonding needs to be used then U-NII-2A and U-NII-2C channels should be enabled to reduce adjacent channel and co-channel interference.
- Remove channel 144 from the list, as it is not supported by many devices.
- In high density open air environment, 20 or 40 MHz 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 such instances, do not use U-NII-2A and U-NII-2C channels.
- If VOIP devices are connecting to the networks, check if channel 165 is supported.
- Do not use DFS channels if you are operating close to an airport, military base station, ports, or active water ways, due to radar detection.
- Before enabling DFS channels ensure that all the devices on the WLAN support DFS channels, else it can create coverage holes.
- Although some clients support DFS channels, while roaming they try not to pick APs 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.

Transmit Power

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

- A difference of not more than 6 dB should be maintained between minimum and maximum transmit power within each ARM profile.
- A difference of 6 dB 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 radio due to stronger signal strength.
- For 802.11ac APs that are deployed approximately 50 feet apart, the following minimum and maximum transmission power values are applicable :

Table 9: *Transmission Power Values*

	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

NOTE

VoIP phones and badges have a restriction on the maximum transmission power they can support. Refer to the user manual or check the vendor's site and adjust APs transmit power accordingly.

NOTE

When there is no active user on the network, check the value of **channel busy** on Airwave or any other management tool**.** If the value is more than 30%, it indicates the presence of multiple beacons on the channel and co-channel interference could occur due to the AP's high transmit power.

NOTE

To efficiently control the RF characteristics of each band and implement the recommendations included in this guide, create separate ARM profiles and assign them to their individual Radio profiles.

Addition of ARM Parameters

Frequent changes in the RF conditions could cause changes to the AP's channel and transmit power, and impact client connectivity. The following parameters should be modified to avoid such instances:

Ideal coverage index - In dense deployments this parameter helps in avoiding APs from transmitting on high power. ARM considers SNR of neighboring APs and uses this value to calculate Ideal Coverage Index. APs with a high coverage index can hear neighboring APs clearly. In case they are unable to hear them, the AP increases its power to reach a close to ideal coverage index of 10. In high density open office environment, if APs transmit on high power it will create a co-channel interference. To avoid APs transmitting on high power, the value of this parameter should be reduced to 6.

Free channel index - Value of this parameter helps ARM to select a new channel for an AP, which has been less utilized and has better quality. After scanning all channels, the AP calculates the **Interference Index** on its current channel and all other channels available on the same radio. If the AP traces another channel with the **Interference Index** value lesser than AP's current channel, it will move the AP to a new channel. The difference of total **Interference Index** between an AP's current channel and new channel should be equal to or more than the value defined by **Free Channel Index** (default value is 25).

The last column in the output of **show ap arm rf-summary ap-name <ap-name>** shows the total interference index. For example, if an AP's current channel has interference index of 100 and if another channel is available on the same radio with interference index of 70, the default **Free Channel Index** is 25. Since the difference between the AP's current channel and the other channel on the radio is more than 25, ARM will move the AP to a new channel.

NOTE

The ARM algorithm considers many other parameters before moving an AP to a new channel, but free channel index is one of them.

Back off time - Once an AP changes to another channel or transmit power, ARM does not try again to change the channel or power till the **back off time** expires. To avoid frequent changes in the channel and transmission power, the value of this parameter should be increased.

Error-rate-threshold - The reason for an AP to move to a new channel is due to the MAC and PHY errors on the current channel. If the percentage of errors on an AP's current channel is higher than the value configured, for more than the default value set, then ARM moves AP to a new channel with less errors. In noisy environments, the value of this parameter should be increased for both a and g radios.

Error-rate-wait-time - This parameter defines the amount of time ARM waits and monitors errors on an AP's current channel before moving to a new channel. The default the value of this parameter is 30 seconds. If the errors on an AP's current channel remains higher than the value configured under **Error-rate-threshold** for 30 seconds, then ARM will move the AP to a new channel with less errors, if the channel is available.

Aruba Recommendations

- Ideal coverage index should be reduced from 10 to 6.
- Only for 2.4 GHz, free channel index should be increased from 25 to 40.
- Back off time should be increased from 240 second to 1800 seconds.
- Error-rate-threshold should be increased from 50% to 70% for both 2.4 GHz and 5 GHz.
- Error-rate-wait time should be increased to 90 seconds.

Though ARM takes care of selecting appropriate channel for APs, following points should be considered as well:

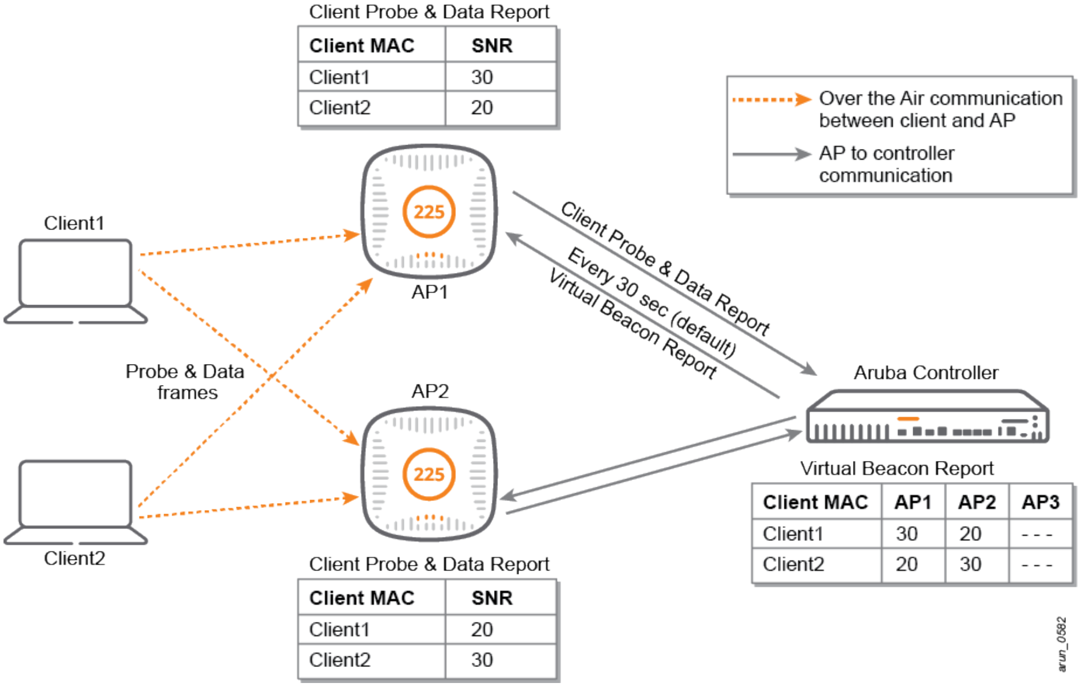
- As 802.11ac standard supports 80 MHz channel bonding, it can be used in greenfield deployment. However, to use 80 MHz channel bonding, U-NII-2A and U-NII-2C channels must be enabled to reduce adjacent channel and co-channel interference.
- Remove channel 144 from the list as it is no longer supported by many devices.
- At times in high density open air environment, 20 or 40 MHz channel width will help reduce channel utilization and improve overall network performance by providing more clear channels.
- Majority of voice specific devices do not scan many channels before roaming as they have active voice calls. For such devices, do not use U-NII-2A and U-NII-2C channels.
- One of the reasons behind VOIP devices not connecting to the network could be because some of these devices do not support channel 165.
- Due to the risk of radar detection do not use DFS channels if you are operating close to the airport or military base station.
- Most of the clients do not scan DFS channels initially, this will make roaming inconsistent when using DFS channels.
- Roaming test should be performed using different types of clients expected on the WLAN, to see their behavior on DFS channels.

Selecting Optimal ClientMatch Settings

After optimal channel and power are selected for the APs, check if clients are connected to the appropriate radio. The current 802.11 standard leaves most of the decision making to the client, which lacks both the network wide prospective and intelligence to connect to right radio and AP.

In ArubaOS 6.3, the ClientMatch technology was introduced as a part of ARM 3.0. Aruba's ClientMatch technology eliminates sticky clients and improves overall system throughput by continuously monitoring mobile devices session performance metrics and using this information to steer each client to the closest AP and the best radio on WLAN. Before a device is steered to a new AP, the system waits for the latency sensitive voice and video application to end. ClientMatch uses standard based 802.11 messages supported by 802.11a/b/g/n/ac, but there is no special client device requirement.

Figure 3 *ClientMatch Functionality*



Client Probe & Data Report

Client MAC	SNR
Client1	30
Client2	20

Client Probe & Data Report

Client MAC	SNR
Client1	20
Client2	30

Virtual Beacon Report

Client MAC	AP1	AP2	AP3
Client1	30	20	- - -
Client2	20	30	- - -

The ClientMatch figure shows how ClientMatch monitors each client's capabilities and connection on a WLAN using probe requests and data frames sent by the client.

- Each AP forms a client probe and data report, which includes a list of all the clients that an AP can hear, including the SNR.
- By default every 30 seconds APs send out this information to the controller, based on which a Virtual Beacon Report (VBR) is created, this maps each client to all the radios that can hear the client. Aruba controller sends out virtual beacon report of each client to the AP it is associated with.
- Based on the information received in the Virtual Beacon Report, an AP may decide to initiate band steering or sticky move for the clients associated to it. The decision to dynamically load balance the clients is however taken by the controller and not the APs.
- When a ClientMatch is initiated to move a client to the desired radio, all the radios in the RF vicinity except the one selected, blacklist the client for a short duration (default: 10 sec). This ensures that the client moves to the desired radio.

ClientMatch Capabilities

ClientMatch features a number of capabilities that enable it to pair clients to the desired APs and radios. In general, the following client/AP mismatch conditions are managed by client match:

Band Steering

Dual band clients scan all the channels on both 2.4 GHz and 5 GHz radio and try to connect to the BSSID with the strongest signal or the BSSID that responds first to the client's probe request. This may result in a client connecting to a SSID in 2.4 GHz at lower PHY rates, where as it could have connected to the same SSID in a clear 5 GHz channel with better PHY rates. In such scenarios, the ClientMatch band steers clients to the appropriate band.

The band steering logic of client match continuously monitors a client's association and band steers it to the desired band when appropriate. A clientmatch enabled Aruba AP monitors the clients associated to its 802.11b/g radio and band steers the clients if the following conditions are met:

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

Dynamic Load Balancing

Dynamic Load Balancing enables APs and controllers to dynamically load balance Wi-Fi clients to the APs within the same RF neighborhood on underutilized channels. This technique helps stationary and roaming clients in dense office environments, conference rooms, lecture halls, and environments that have high bandwidth applications as client density to dynamically balance among APs in the same vicinity.

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 (default: 10)
- The client SNR on a radio with lesser load is higher than the load balancing SNR threshold (default: 30 db).

Sticky Client Steering

Once attached to an AP, many clients tend to stay attached even when users begin to move away from the AP and WLAN signal weakens. As a result of this stickiness, performance for mobile users and clients often degrades, and the overall network throughput deteriorates. ClientMatch steers such sticky clients to a better AP and improves user experience and overall network performance.

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 (default: 18 db)
- Based on a virtual beacon report, there is a better radio to steer clients to if the following conditions are met:
  - SNR of the target radio is higher than the SNR threshold (default 10 db) and
  - Signal strength of the target radio is equal or higher than Sticky Min Signal (default: -70 dBm)

NOTE

802.11v and 802.11k capable clients will usually have a smoother, non-disruptive ClientMatch Steering experience.

Aruba Recommendations

As ClientMatch is an advanced configuration, all the parameters are accessible through CLI only, the Web UI is used only to enable or disable ClientMatch.

Aruba 2xx Series (.11 ac) APs supports band steering, load balancing, and sticky client steer only through ClientMatch. Unlike 1xx series APs, legacy ArubaOS parameters like **band steering**, **spectrum load balancing** and **client hand off assist** does not work with 2xx series APs when ClientMatch is disabled.

Table 10: *ClientMatch Configurations*

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.

Restricting Unnecessary Broadcast and Multicast Traffic

Right from when a client is associated to the network, it transmits broadcast-multicast packets. When initially associated to the network, it could be DHCP and ARP packets or it could be background applications running on clients, that used multicast traffic. Each broadcast or multicast packet gets multiplied by the total number of APs and communicates with all the APs that have clients in the same subnet.

Flooding of broadcast-multicast traffic consumes air time, as it goes at the lowest configured basic rate for SSID, which has a default value of 1 Mbps for g radio to 6 Mbps for a radio. In a large university campus and enterprise where large subnets are used to accommodate thousands of users, broadcast-multicast traffic can slow down WLAN performance significantly and consume unnecessary bandwidth on wired and wireless side.

Aruba WLAN has parameters to restrict unnecessary broadcast-multicast traffic and at the same time allows multicast traffic for required applications like Airplay, Chromecast. In the following sections we will first discuss the parameters used to restrict and optimize the broadcast and multicast traffic and later discuss the parameters used to allow multicast traffic required for the applications like Airplay, Chromecast and multicast streaming.

Broadcast Filter ARP

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

Drop Broadcast and Multicast Traffic

After ARP and DHCP packets are converted to unicast, the next step is to restrict broadcast and multicast that might be generated as a part of some applications running on the client devices. Most common applications uses either NetBIOS, mDNS, or DLNA based services, which are multicast based. To restrict such applications from consuming airtime, ArubaOS has introduced Drop Broadcast and Multicast parameter in the Virtual-AP profile. When this parameter is enabled, all the broadcast and multicast traffic on the WLAN is dropped.

NOTE

Drop Broadcast Multicast parameter will drop broadcast ARP and DHCP packets as well if Convert broadcast ARP to unicast parameter is not enabled.

Even if multicast based application is required to work on WLAN, it is advisable to enable Drop Broadcast Multicast parameter.

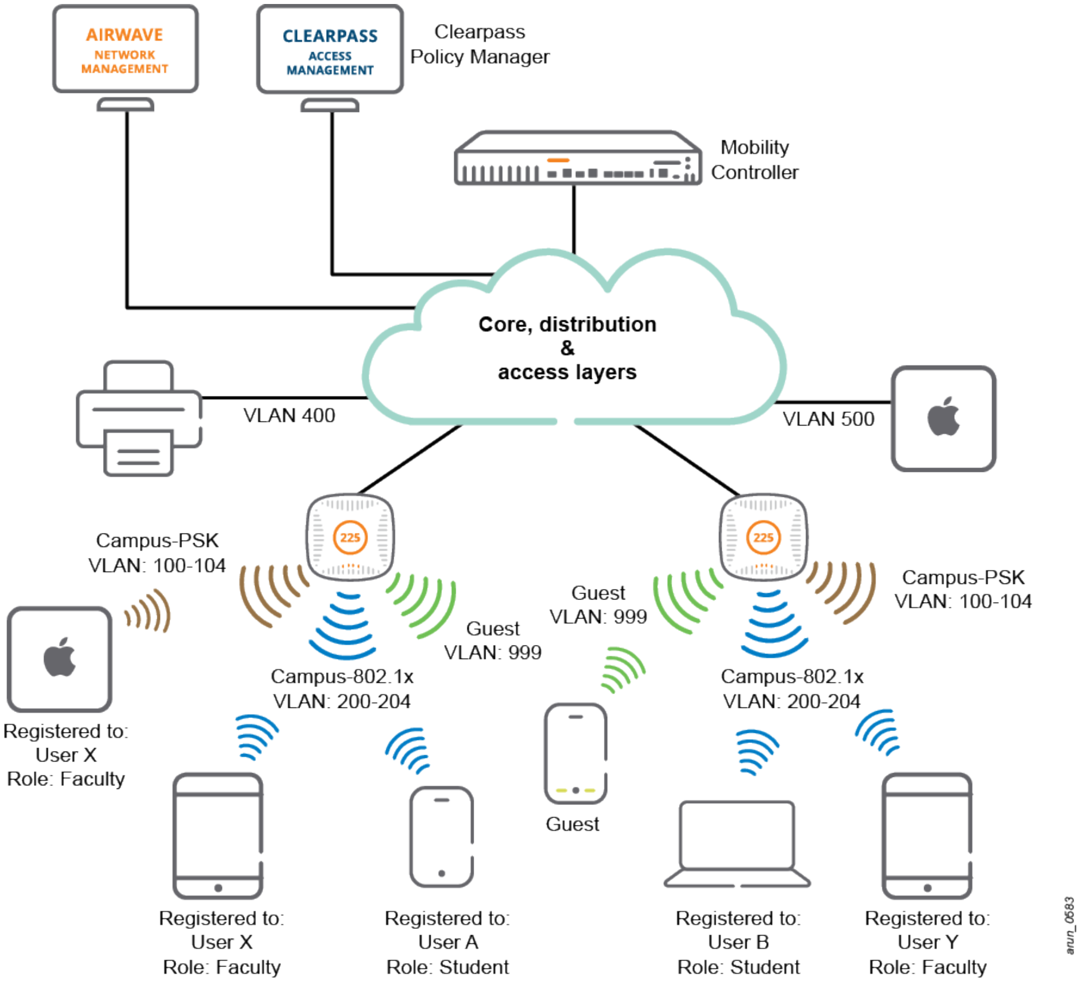
Allow Multicast Based Services Using AirGroup Feature

If the broadcast–multicast traffic is dropped in the air, in enterprise or campus deployments DLNA, mDNS, and other zero-configuration services are essential. To enable these services for applications like airplay and chromecast, Aruba WLAN with AirGroup technology enables context aware access to DLNA, Apple Bonjour®, and other shared devices without affecting WLAN performance.

The following figure illustrates an AirGroup enabled network. When AirGroup is enabled, controller maintains the list of the servers and clients that use one of the multicast services. It also distributes the list across multiple controllers and subnets. Each time a new client tries to access a service, or the server broadcasts the service, the controller stores this information and proxies it on behalf of the client or server. This is ideal when there are a large number of users in the campus environment and hundreds of servers, it saves significant bandwidth on the wired and wireless side.

Refer to the technical briefs provided by Aruba to gather additional details about the Arigroup feature.

Figure 4 *WLAN running Aruba's AirGroup Technology*


AIRWAVE
NETWORK MANAGEMENT
CLEARPASS
ACCESS MANAGEMENT
Clearpass Policy Manager
Mobility Controller
Core, distribution & access layers
VLAN 400
VLAN 500
Campus-PSK VLAN: 100-104
Guest VLAN: 999
Guest VLAN: 999
Campus-PSK VLAN: 100-104
Campus-802.1x VLAN: 200-204
Campus-802.1x VLAN: 200-204
Registered to: User X Role: Faculty
Guest
Registered to: User X Role: Faculty
Registered to: User A Role: Student
Registered to: User B Role: Student
Registered to: User Y Role: Faculty
arun_0583

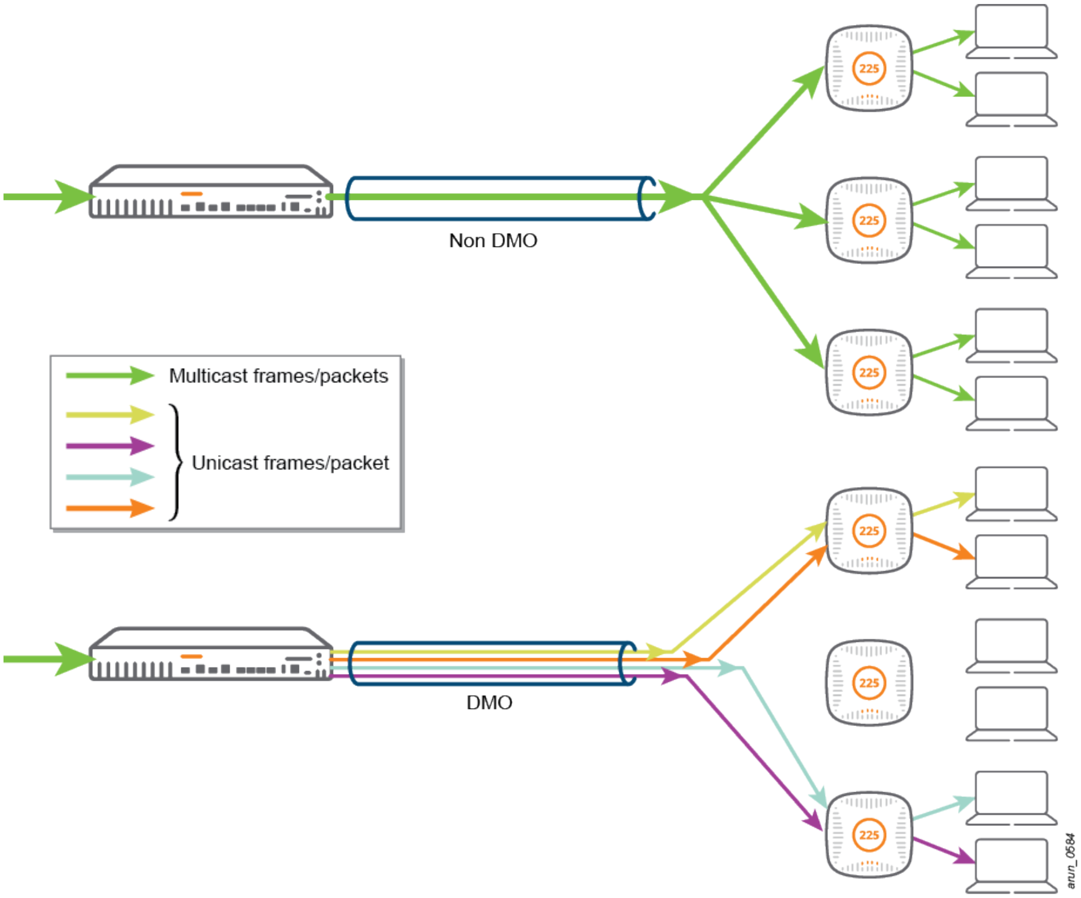
Allow Known Multicast Traffic

AirGroup optimizes multicast based services like Airplay and Chromecast, but in a large enterprise or campus network, there could be other types of multicast traffic that needs to be permitted. Many companies or universities have multicast video streams running in their network for business and educational purpose. There might also be other custom applications, which run on multicast. To meet these requirements, Aruba controller provides parameters like to Dynamic Multicast Optimization and Multicast Rate Optimization to optimize multicast traffic over the Air. The functionality of these parameters is described in the following sections:

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 a few clients have subscribed to a multicast stream.

Figure 5 *Multicast Traffic Flow in a WLAN with and without Optimization*



The above figure illustrates how Dynamic Multicast Optimization (DMO) parameter converts multicast packets to unicast and transmits it at a higher unicast rate over the air. In case of tunnel mode, the conversion is executed in the Aruba controller while in D-Tunnel mode, it is executed at the AP level. In D-tunnel mode, as conversion of multicast traffic to unicast is distributed across multiple APs, it is known as Distributed Dynamic Multicast Optimization (D-DMO). By default DMO threshold has a default value of six clients. Once threshold is reached, multicast traffic will be sent as is to other clients. The value of the DMO threshold should be high enough to match the expected number of clients on an AP.

NOTE

IGMP snooping or IGMP proxy needs to be enabled for DMO to work. Multicast stream should be prioritized by configuring uplink ACL and correct WMM parameter to match DSCP values.

Multicast Rate Optimization

Multicast rate optimization 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 VAP are transmitting at a data rate of 24 Mbps or higher, multicast frames are transmitted at 24 Mbps, rather than the lowest basic rate, which ranges between 1 or 6 Mbps.

NOTE

Multicast Rate Optimization should be enabled along with DMO to optimize the multicast traffic once DMO client threshold is hit.

Aruba Recommendations

- Enable Convert broadcast ARP packet to unicast parameter.
- Enable Drop broadcast and multicast traffic parameter.
  - Ensure that Convert broadcast ARP packets 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 to be enabled for DMO.
  - Prioritize multicast stream by configuring uplink ACL and WMM parameters.

Behavior Changes from ArubaOS 6.4.1

- Prior to ArubaOS 6.4.1 [ArubaOS 6.2 to 6.4.0], when Broadcast Filter ALL and DMO parameters were enabled, the controller allowed multicast packets to be converted to unicast and forwarded them to wireless clients ranging from wired side destination range 225.0.0.0 to 239.255.255.255.
- From ArubaOS 6.4.1 onwards, when Broadcast Filter ALL parameter is enabled, the controller allows multicast packets to be forwarded if:
  - Packets originated from wired side with destination range of 225.0.0.0 to 239.255.255.255, and
  - A station was subscribes to multicast group (IGMP Snooping or Proxy enabled)

Traffic Shaping

In a wireless network with a combination of 802.11a/b/g/n/ac clients, it is possible that a slower client consumes more airtime and brings down the performance of the complete wireless network. To solve this issue and ensure fair airtime to all the clients independent of their wireless capabilities, traffic shaping can be implemented on the Aruba APs.

The following are the types of traffic shaping policies that can be applied to an Aruba AP:

Default Access - Traffic shaping is disabled by default as client performance is dependent on MAC contention resolution.

Fair Access - Each client gets the same airtime, regardless of the client capability and capacity. This option is useful in an environment like a training facility or exam hall, where a mix of legacy, 11n, and 11ac clients need equal amount of network resources, regardless of their capabilities.

Preferred Access - High throughput (802.11ac) clients do not get penalized due to slower legacy or .11n transmission that take more airtime due to lower rates.

Aruba Recommendations

Use Fair-Access in a production network to provide equal amount of airtime to each device irrespective of its 802.11 capabilities (legacy vs 11n vs 11ac).

Chapter 5
Roaming Optimization

The primary purpose of WLAN deployments is to support multiple roaming devices. To improve client performance optimize the radio frequency and perform roaming optimization.

AP placement plays a very important role in roaming and is the first step in designing the network. However, even after deploying APs at the right locations, roaming may not work as expected. This occurs due to the wide range of clients with different Network Interface Cards (NICs) and roaming algorithms. Although the roaming decision is mainly taken by the client, multiple parameters in ArubaOS can influence a client's roaming decision. In high density deployments, it is acceptable if a client does not roam to every AP in the roaming path and just roams to every alternate AP, as far as roaming is seamless before the client's Received Signal Strength Indicator (RSSI) drops between 75 dbm to 80 dbm.

Aruba Recommendations

- Verify with Aruba TAC or local Aruba engineers before modifying the parameters discussed in this section.
- The parameters discussed in this section should not be enabled by default, but should be used only when roaming issues are observed.
- Values of parameters can vary based on the environment, so a trial and error method should be used for fine tuning.
- Enable one parameter at a time and perform a roaming test to check if it is effective. If there is no negative impact then keep it enabled and try another parameter. It is recommended to run a test with different types of clients who will access the WLAN, to ensure that changes made to a parameter does not impact another.

Listed below are the roaming optimization parameters:

- Optimizing Cell Size
  - AP Transmit Power
  - Data Rates
- Assisting Clients in Selecting a Closer AP
  - Beacon Rate
  - Local Probe Request Threshold
- Optimizing Roam Time
  - Opportunistic Key Caching (OKC)
  - Fast BSS Transition (OKC, 802.11r, 802.11k, and 802.11v)
    - If required, you can disable 802.11v in ARM profile.

Optimizing Cell Size

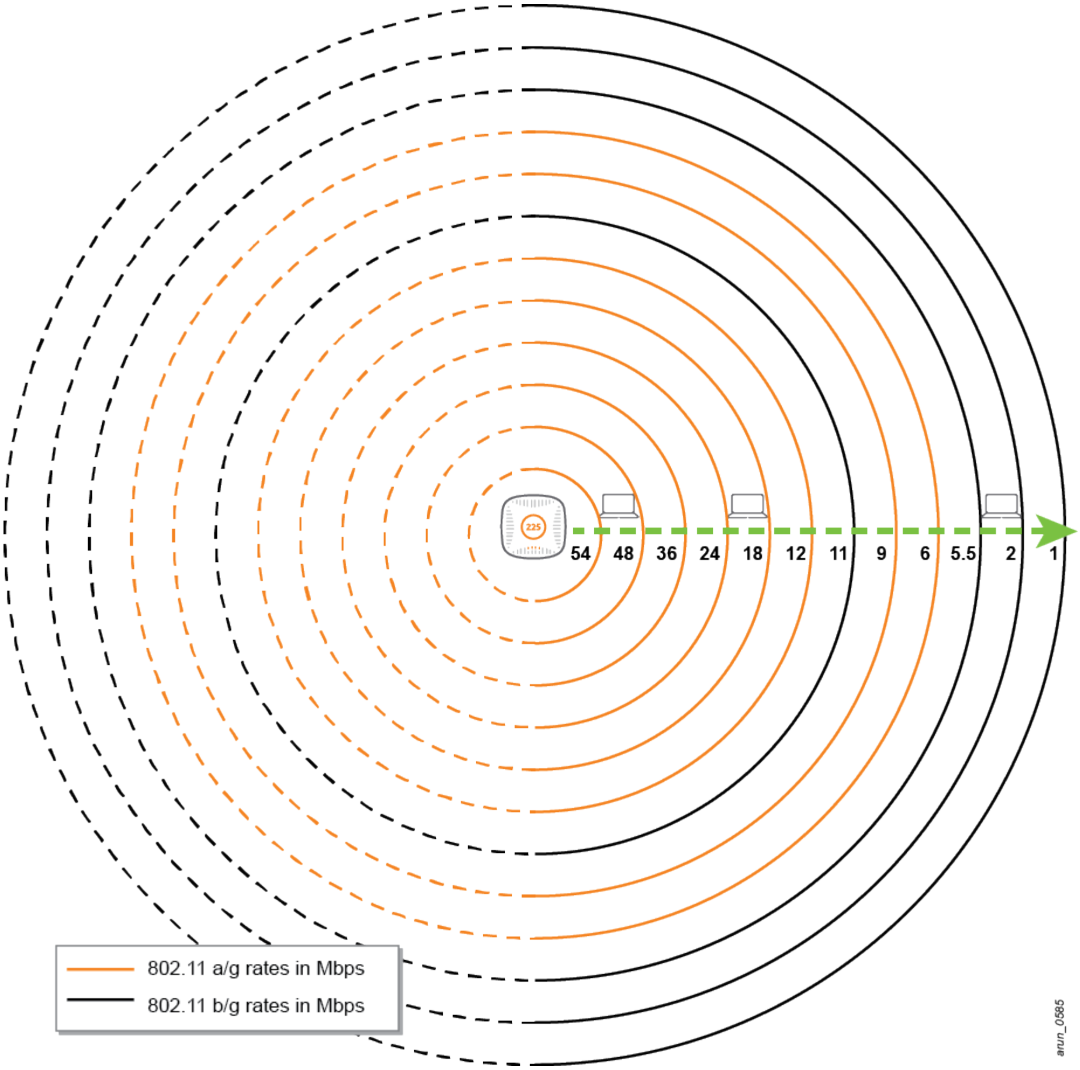
There is a drop in the data rate when a client starts moving towards the edge of the coverage cell. Clients at the edge of the coverage cell use very low data rates (1 Mbps or 6 Mbps), which impacts its performance and of the other clients connected to the same AP. In capacity-based deployments, when the coverage cell of neighboring APs 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.

Use the following options to optimize AP cell size:

- Reducing AP Transmit Power

- Cutting Down Lower Rates

Figure 6 *802.11a/b/g Coverage Cell*



Reducing AP Transmit 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 a very low value in capacity-based deployments can affect the network performance. It is recommended to follow the AP transmit power guidelines described in RF Considerations.

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 APs 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. Unlike basic rates, a station does not have to support all the transmit rates in order to be associated to an AP.

Management frames (beacons, probe request/response, association/disassociation, and authentication/deauthentication), control frames (RTS, CTS, PS-Pol, and acknowledge), broadcast frames, and multicast frames, transmit at the lowest supported rates so that all the clients can decode them. Data frames are transmitted at transmit rates depending on the client capability. An AP's cell size can be reduced by cutting down the lower rates from the SSID profile.

In a dense deployment, reducing an APs' cell size can influence clients to roam to another AP, as it cannot hear management 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 and transmit) from a SSID profile for A-radio, three outer most coverage cells are cut down as shown in the 802.11a/b/g Coverage Cell figure. Once the client's data rate drops below 18 Mbps, a client initiates roaming, which mainly impacts remote clients, as they use lower data rate.

Aruba Recommendations

The following are some recommendations from Aruba:

- Legacy clients (802.11b) require lower rates of 1 Mbps - 2 Mbps. Such clients may not even associate to the network if these rates are cut down.
- 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 in the network, remove the 802.11b rates for basic and transmit rates.
- For APs that are 50 feet apart, use the following rates for 802.11a and 802.11g radios:
  - Basic rates: 12, 24 Mbps
  - Transmit rates: 12, 18, 24, 36, 48, and 54 Mbps
- If you have gaming devices connected to the wireless network, add data rate 5, 6, 9, and 11 Mbps to the g radio basic and transmit rates.

Assisting Clients in Selecting a Closer AP

In deployments where the traffic is high, clients can hear multiple APs and radios broadcasting the same SSID. Based on the implementation of the client wireless NIC, a radio is automatically selected. In a high density enterprise or campus deployments, clients can hear multiple AP on the same floor as well as from the floor above and below. A lot of processing is required on the client side to go through the list of the APs it can hear and then decide on the AP that it could roam to. The following parameters helps clients listen only to APs that are closer:

- Beacon Rate
- Local Probe Request Threshold

Beacon Rate

By default beacons take the lowest configured basic rate of 1 Mbps on g radio and 6 Mbps on a radio. If these rates are used the cell size of the AP will increase and clients at the edge of the network can listen to the beacons and connect to the AP.

In deployments with less traffic, if the data rates is low, client connectivity can be maintained. But when the traffic is high, clients that are roaming might connect to APs that are far even if APs are available closer. This results in a drop in the overall WLAN performance. By configuring the beacon rate to a higher value, the overall distance that the beacon can travel is reduced.

Aruba Recommendations

- Beacon rate can be configured as one of the supported basic rates. Higher the value, lesser the distance a beacon can travel.
- Before modifying the value of this parameter, ensure that there are no 802.11b clients on the WLAN.

Local Probe Request Threshold

Beacon is a passive method of discovering available wireless networks and access points, the active method is using probe requests. When a client sends broadcast probe requests, all APs that hear the request send a probe response with a list of the wireless networks that they broadcast. Probe requests are configured on the lowest basic rate (1 or 6 Mbps) so that APs that are far away can also listen and reply to the request.

The **Local Probe Request** threshold parameter in ArubaOS prevents clients from discovering and associating with an AP that is far away. The value set for this parameter is a SNR value. When the SNR of the client probe request is lesser than the local probe request threshold value, APs do not revert to the client with a probe response. As a result clients are unable to discover APs that are far away.

Aruba Recommendations

- For APs 50 ft apart the beacon rate for A and G radio should be configured as 12 or 24 Mbps, depending on the roaming results.
- The default value of Local Probe Request Threshold parameter is 0 and should be adjusted only by the engineer, after a careful analysis.If adjusted, the value of this parameter should be 3 db less than ClientMatch Sticky SNR. As recommended, the value for Sticky SNR is 18 db and the Local Probe Request Threshold should not be higher than 15 db.
- Setting a high beacon rate results in clients hearing the beacon and other management frames from APs, but their probe requests are ignored by the APs.

Optimizing Roam Time

In an enterprise network where most of the clients connect to 802.1X SSID, EAP authentication can be time consuming when a client roams from one AP to another. Increased roaming time can directly affect the voice quality or any other latency sensitive application. ArubaOS provides multiple options to optimize the time taken to complete 802.1X authentication while roaming.

Pairwise Master Key Caching

Pairwise Master Key (PMK) caching is defined by 802.11i and is a technique available for authentication between a single AP and a station. If a station authenticates an AP, roams away from that AP, and comes back, it does not have to perform a full authentication exchange. Only the 802.11i 4-way handshake is performed to establish transient encryption keys.

Clients who want to use PMK caching should send the PMKID in the association (or re-association) frame, as specified by 802.11i. If the PMKID matches the one cached by the controller for the station’s MAC address, the system skips the authentication step and proceeds directly to key exchange. If the PMKID is not sent, or does not match the one cached by the controller, a full authentication process is done.

NOTE

PMK caching is always enabled and cannot be disabled for WPA2 ESSIDs.

Opportunistic Key Caching

When WPA2 is used with 802.1X and Opportunistic Key Caching (OKC) is enabled on Aruba controller, there is an ideal balance of security and performance. Opportunistic key is already cached on the controller and sent to the target AP in an event of roaming. Consequently, the client does not have to go through a complete 802.1X authentication, but a four-way key exchange for WPA2 is sufficient.

During client roaming, OKC reduces the number of frames exchanged by one-fourth. OKC lowers the roaming time significantly, which reduces the impact on voice call quality and latency sensitive applications. There is no penalty for enabling OKC even if it is not supported by certain clients in the network. These clients will go through a complete 802.1X authentication.

NOTE

macOS and iOS devices do not support OKC. Please consider enabling 802.11r and 802.11k on the network if a significant number of macOS and iOS devices are expected on the network. 802.11v is enabled by default. For more information, seeTable 7.

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 (802.11r)

From ArubaOS version 6.3.0.0 onwards, Aruba supports Fast BSS Transition (IEEE 802.11r) to reduce the delay caused due to re-authentication, every time a client roams from one AP to another. In an 802.11r environment, the FT mechanism allows a client station to establish security and QoS state at the target AP prior to re-association. This reduces the delay that occurs when connecting to the distribution system after transition.

802.11k Support

The 802.11k protocol provides mechanisms for APs and clients to dynamically measure the available radio resources. In an 802.11k enabled network, APs and clients can send neighbor reports, beacon reports, and link measurement reports to each other. This allows clients to take the appropriate action when there is an issue with the connection.

Along with 802.11k, ArubaOS supports Radio Resource Management Information Elements (RRM IEs).

BSS Transition Management - 802.11v Support

As 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 BSS Transition Management is enabled by default if 802.11k is enabled.

Aruba Recommendations

- OKC and validate PMKID are enabled by default and should always be kept enabled.
- It is recommended to enable 802.11r on the network. However, It is recommended to test interoperability of most common devices expected in your environment with this feature enabled. Some older 802.11n devices, handheld scanners and printers may have connectivity issues with 802.11r enabled on WLAN. 802.11r supports faster client roaming.
- 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.

Chapter 6
Device Configuration

There are a wide range of devices that connect to WLAN in an enterprise or campus deployment. The roaming behavior of these devices depends on the wireless NIC and wireless capability (802.11a/b/g/n/ac).Some devices roam at higher Signal-to-Noise Ratio (SNR) where as other sticky devices connect to the access point from a distance. Some devices probe regularly to check for access points close to their locations, where as other devices might not start probing until the signal strength of the access point is lower than the threshold value. The configuration of a device is highly dependent on the way logic is implemented in the wireless chipset and it's driver version.

Follow the steps below when deploying WLAN involving multiple mobile devices:

1. Verify with the manufacturer if the device has the recommended version or update all the devices to the latest firmware tested by Aruba.

   The support site lists the driver versions of the devices tested by Aruba.
2. Prepare a list of all configurable settings and default values.
3. Contact the device vendor and Aruba system engineer for the latest best practice settings applicable to your deployment scenario.
4. Perform a pilot test to check the values shared by the device vendor, and other relevant checks.

NOTE

Some clients expose different configuration values to different tools. For example, voice handsets typically have a subset of values that can be configured directly on the phone, while a separate provisioning tool provides more control over the device.

Shared or Dedicated SSID

It is recommended that a wireless architect always use a shared Service Set Identifier (SSID). Each defined SSID uses system resources for:

- Applying policies.
- Allocating additional LAN bandwidth for additional tunnels.
- Managing spectrum for beacons and other overheads.

NOTE

Beacons and other management traffic goes at the lowest configured rate in the SSID, which means it slows downs the overall network speed. The SSID overhead calculator allows the network administrator to calculate the overhead based on the number of APs and VAPs.

Each device has a different type of RF and 802.11 security capability. Depending on the device capability and type of traffic that needs to be supported by the device, you can choose to add a new SSID or share the same one.

Listed below are the common criteria for using a dedicated SSID:

- **Security Capabilities**: Although most devices support the use of 802.1X authentication with WPA2-AES encryption, some scanning and voice specific devices still do not support it as they require Open or Pre-Shared-Key (PSK). For VoIP phones or badges, it is recommended to use PSK rather 802.1X to reduce time taken during roaming, especially if OKC or 802.11r is not supported.
- **RF Capabilities**: Since some older hand held devices like VoIP phones or badges are still only 802.11b capable, it is necessary to reduce the 802.11b rates and other parameters that impact such clients while

optimizing roaming on 11ac SSIDs. It is also recommended to have a separate SSID for legacy (802.11b) devices, rather than sharing it with 802.11n and 11 ac capable devices.

- **QoS Requirement**: Some voice devices require a dedicated VLAN and ACL for QoS to access an application server. It is recommended to use a dedicated SSID in some cases, but Aruba's role-based access policies help in achieving this using a shared SSID. Aruba recommends using role-based access rather than creating separate SSIDs. For additional information, refer to the *Campus Network Design version 8* available at support.arubanetworks.com.
- Parameters that are not enabled by default, should be enabled in the SSID profile or Virtual AP profile for certain devices. These devices may also require a dedicated SSID.

NOTE

If none of the above criteria matches, use the same SSIDs, encryption, and authentication methods to support roaming for all devices.

Recommendations for Voice Devices

- When voice calls are in progress, it is recommended not to use U-NII-2A and U-NII-2C channels for voice specific devices that do not encourage scanning through multiple channels before roaming.
- When you connect to VOIP devices on the network, some voice devices do not support channel 165. For more information about channel/frequency on which VOIP devices operate, refer to the Device manual.
- If a voice device is WMM capable, enable WMM in the SSID profile and configure the DSCP values for the different types of traffic.

For Skype for Business deployments, refer to Skype for Business over Aruba VRD on the Airheads Community page.

Wi-Fi Design for Apple Products

The Wireless LAN lifecycle provides a framework for network administrators to understand the iterative process of designing a network along with the importance of monitoring all aspects of the lifecycle for changes over time. The four components of the Wireless LAN Lifecycle are:

1. defining the purpose of the network,
2. designing the network to meet the definition,
3. deploying the hardware and software required to operate the network, and
4. validating that the network performance has met the design objectives.

A good design must take the Least Capable yet Most important (LCMI) device into consideration. This appendix provides an overview of the Apple device behaviors of which all designers should be aware.

Wi-Fi Specs for Apple Products

Before you begin review the current Wi-Fi specifications for Apple devices that are capable of running current versions of the iOS and macOS operating systems. Consider requirements for older products, and as well as details for channel-width support, the number of spatial streams, and the supported physical layer (PHY) medium access specifications. For more information, refer to the following reference guides on the Apple website:

- macOS Deployment Reference
- iOS Deployment Reference

Network Discovery

When the Wi-Fi adapter is enabled on an iOS or Mac device, that device will look for a network to join. Part of this process involves probing for networks with broadcast and directed probe requests. The Apple iOS Security Guide reviews many of these features. Network discovery discussions should include the following considerations:

- **MAC Address Randomization**. iOS 8 and later protects iOS and Mac devices from tracking by randomizing the MAC address the device uses to probe for networks it can join, or when determining its location for geofenced applications.
  - MAC address randomization occurs when the device is not already associated to a network. When it is already associated, additional directed probe requests are not randomized.
  - Directed probe requests for a specific network are not random.
- **Probe Request Privacy**. To protect against leaking network names, iPhone 6S and later devices do not directly probe for non-broadcast or “hidden” networks.
- **iOS Auto-Join Behavior**. Devices running iOS 11.0 or later associate to auto-join enabled networks by first trying to associate with the most preferred network, then the most recently connected private network, followed by other private networks, and finally to open networks.
  - For networks broadcast on both 2.4 GHz and 5 GHz bands, the 5 GHz network is preferred when its received signal strength is -65 dBm.
  - Auto-join is enabled for a network the first time it is connected on iOS 11.0 and later.

NOTE

Refer to the Apple website for more information about how iOS devices roam in an enterprise Wi-Fi environment.

- **macOS Auto-Join Behavior**. macOS uses the preferred network list to establish network join priority. The preferred network list is found in the device's **Network Preferences**.
  - For networks that are broadcast on both 2.4 GHz and 5 GHz bands, the 5 GHz network is preferred when its received signal strength is -68 dBm
  - Auto-join is enabled on devices running macOS 10.13 or later when the device connects to a network for the first time.

NOTE

Refer to the Apple website for more information about macOS wireless roaming for enterprise customers.

- **Security Recommendations**. When an iOS device joins an insecure network, iOS will warn the user and provide a link to recommended settings for Wi-Fi routers and access points.
- **Unlock Required**. After an iOS device or Mac is restarted, the device must be unlocked before connecting to a network. This applies to all security types (including open networks), except for macOS 802.1X in system mode.
- **Password Sharing**. Users with devices running iOS 11.0 and later, or macOS 13.0 and later who wish to use a Wi-Fi network that is already known by another user can automatically request access to the network if they are in the contacts of the user who already has access. Password sharing has the following requirements
  - Pre-shared key for WPA/WPA2 network is shared.
  - Requestor Apple ID must be in contacts.
  - Wi-Fi and Bluetooth adapters must be enabled on both devices.
  - This does not apply if the network was provisioned with a profile or MDM.

Encryption and Authentication

Keeping data safe is a priority. Encryption of data at rest, in transit, and in iCloud are all part of the security and privacy requirements in Apple products.

- **Supported Encryption**. Apple devices support the Advanced Encryption Standard (AES) with 128-bit keys for both Enterprise and Personal Networks. The complete list of supported encryption types may be found in the latest version of Apple's **iOS Security Guide** and **macOS Security Overview**.
- **Authentication Protocols**. The following authentication protocols are supported on iOS and macOS.
  - EAP-TLS, EAP-TTLS (MSCHAPv2), EAP-FAST, EAP-AKA, EAP-SIM (iOS only), PEAPv0 (MSCHAPv2), PEAPv1 (EAP-GTC), and LEAP
  - The macOS Setup Assistant supports 802.1X EAP authentication using either TTLS or PEAP user name and password credentials.
- **Supported TLS Version**s. TLS versions 1.0, 1.1, and 1.2 are supported for 802.1X EAP exchanges. If the RADIUS server supports TLS 1.2, for example, you can control the minimum and maximum support version by configuring an MDM or configuration profile payload.
- **802.11w Protected Management Frames**. Encrypted management frames are supported on iPhone 6, iPad Air 2 and later iOS devices. Protected management frames help prevent unauthorized deauthentication by attackers who are not associated to the same Wi-Fi network.

Roaming Technologies

The decision to roam from one basic service set (BSS) to another lies within the client device. The roam trigger threshold informs an iOS device or Mac when to start looking for a better BSS for the device. For mobile clients, standards-based roaming technologies allow for a quicker roam.

- **Roam Trigger Threshold**. When the signal strength is reduced to a value below the roam trigger threshold, an iOS device or Mac will begin scanning for a new roam candidate.
  - The roam trigger threshold for iOS is -70 dBm. An iOS device will attempt to roam if the new BSS is 8 decibels better than the current BSS when the device is transmitting data. If device is not transmitting data the gaining BSS must be 12 decibels better for the roam to occur.
  - A Mac will roam if the gaining BSS signal is 12 decibels better, whether or not it is transmitting data.
- **Free Space Path Loss**. Free Space Path Loss describes the natural loss of a radio frequency signal as it travels through free space. Loss, or *attenuation*, is increased when signals travel through objects, and is measured in decibels. To calculate the Received Signal Strength Indicator (RSSI) at a given distance, calculate the loss in decibels (dB) from 0 dBm (1 milliwatt).

  $$\text{Loss in decibels (dB)} = 36.6 + 20\log10(f) + 20\log10(D)$$

  Where **f** is the frequency of the signal in Hertz, and **D** is the distance in miles. Convert distance to match the units, such as feet or kilometers, required for your environment.
- **802.11k Radio Measurement**. When 802.11k Radio Measurement is enabled on your enterprise Wi-Fi network, an iOS device will perform roam scans more quickly. The neighbor report provides a list of nearby Basic Service Set IDs (BSSIDs) and the channels that they are using. iOS roam scans are prioritized to scan the channels of the first six BSSIDs provided by the neighbor report. When 802.11k is not enabled on the network, iOS must scan all channels to find a suitable roam candidate, which may add several seconds to the discovery process. This feature is available on pre-shared key and 802.1X authentication networks on devices running iOS 6 or later.
- **802.11r Fast BSS Transition**. When an iOS device roams from one access point to another on the same network, 802.11r uses a feature called Fast Basic Service Set Transition (FT) to authenticate more quickly. This feature is available on pre-shared key and 802.1X authentication networks for devices running iOS 6 or later.

NOTE

Refer to the Apple website for more information about Wi-Fi network roaming with 802.11k, 802.11r, and 802.11v on iOS.

- **802.11v Wireless Network Management**. iOS supports the Basic Service Set (BSS) transition-management functionality of 802.11v on certain devices. BSS transition management allows the network's control layer to influence client-roaming behavior by providing load information of nearby access points. iOS takes this information into account when deciding upon possible roam candidates. This feature is available on pre-shared key and 802.1X authentication networks for devices running iOS 7 or later.

Mobile Device Management

Modern deployments leverage mobile device management to configure iOS and Mac devices at scale. To learn about the various Wi-Fi related configuration profile settings, download the Apple Developer Configuration Profile Reference Guide. For additional information, see also Mobile Device Management Settings.

- **iOS and iPadOS Functionality Restrictions**. You can set restrictions and modify features on iOS and iPadOS devices enrolled in a mobile device management solution. The following are examples of Wi-Fi related restrictions:
  - Force Wi-Fi on (Users can't turn off Wi-Fi)

  - Proximity AutoFill (Users' devices won't advertise themselves to nearby devices for Wi-Fi Password requests)
  - Share passwords over AirDrop
  - Modify Bluetooth settings
  - Join only Wi-Fi networks installed by a Wi-Fi payload

NOTE

Refer to the Apple website for more information about iOS and iPadOS restrictions.

- **macOS Functionality Restrictions**. You can set restrictions and modify features on macOS computers enrolled in a mobile device management solution. The following are examples of Wi-Fi related restrictions:
  - Proximity AutoFill (Users' devices won't advertise themselves to nearby devices for Wi-Fi Password requests)
  - Share passwords over AirDrop

NOTE

Refer to the Apple website or more information about macOS restrictions.

- **Network Payload Configuration**.Network mobile device management payload settings can configure network security, user authentication, Wi-Fi authentication, and VPN policy settings. The following sections of the Apple website describe network-related payload settings:
- Certificate payload settings
- SCEP payload settings
- Network payload
- VPN overview

Troubleshooting

If you are experiencing problems with connectivity, you can use the troubleshooting techniques and tools built in to macOS and iOS. First, use wireless diagnostics to analyze the network connection to the Internet. After the analysis is complete, it presents you with a list of detected issues and possible solutions, along with information about Wi-Fi best practices. The following sections of the Apple website describe these troubleshooting procedures:

- Use Wireless Diagnostics on your Mac
- If your Mac doesn't connect to the Internet over Wi-Fi
- **Diagnostic Logging Profiles**. Diagnostic profiles may be installed on iOS, macOS, tvOS, and watchOS to gather detailed log events to aid in troubleshooting. Click here to download profiles and instructions from the Apple website.
- **Remote Virtual Interface (RVI)**. Use your Mac to take a packet trace on an attached iOS device using the Remote Virtual Interface (RVI) mechanism. For more information, refer to the Set Up iOS Packet Tracing section of Apple Website.

  This technique requires the UUID of the connected iOS device to target. The UUID can be acquired by using the Apple Xcode **Devices and Simulators** tool. Additionally, you may script the setup of the interface to acquire the UUID automatically using the following system_profiler command:

```
UDID=$(system_profiler SPUSBDataType | awk '(length($NF) == 40) {print $NF}') rvictl -s $UDID
```