Aruba Wi-Fi 6 Networks Deployment Guide

aruba

a Hewlett Packard Enterprise company

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
6280 America Center Drive
San Jose, CA 95002
USA

Revision History

The following table lists the revisions of this document.

Table 1: *Revision History*

Revision	Change Description
Revision 01	Initial release.

Chapter 1
About this Guide

This document is a quick reference guide to explain the enhancements developed in Wi-Fi 6 standards and provides the guidance for migrating to Wi-Fi 6 with respect to design, deployment, and configuration. Aruba Deployment Guides are best practice recommendation documents specifically designed to outline how the Aruba technology works and to enable customers who deploy Aruba solutions to achieve optimal results. This document is not only intended to serve as a deployment guide but also to provide descriptions of Aruba technology, network design decisions, configuration procedures, and best practices. This is a brief deployment guide for campus environments such as offices, university campuses, and dorm environments.

Intended Audience and Scope

This guide is intended for those who want to learn about the Wi-Fi 6 standards and understand the best practices in deploying a high-efficiency WLAN network by using wireless LAN controllers and Access Points (APs) from Aruba Networks, Inc.

Related Documents

The following documents may be helpful as supplemental reference material to this guide:

ArubaOS 8 Fundamentals Guide

Aruba Instant VRD

Aruba APs comparison

802.11ax, which is now familiar as "Wi-Fi 6", is the new IEEE standard from the 802.11 standards family. This standard is also referred to as "High Efficiency Wireless" as it warrants a fourfold increase in average throughput per user. Unlike its predecessors' technologies which were all about higher peak throughput, Wi-Fi 6 focuses on higher efficiency and solving problems for high-density environment.

Wi-Fi 6 promises higher throughput, greater capacity, improved reliability, and many more features. This latest generation of 802.11 WLAN applies to both 2.4GHz and 5GHz, and is fully backwards compatible with the previous generations.

Need for Wi-Fi 6

Wi-Fi 6 enhances the 802.11ac technology by focusing on **Network Efficiency** beyond **Higher Data Rates**. This standard builds on the strengths of 802.11ac by adding efficiency, flexibility, and scalability, which ensures increased speed and capacity to the ever-increasing demands of existing networks. IEEE proposed the 802.11ax standard so that it can combine the freedom of high-speed Gigabit Ethernet wireless with the reliability and predictability found in the licensed radio spectrum.

Although 802.11ac was able to break the gigabit per second barrier for Wi-Fi traffic, many organizations still find limitations around the number of channels, devices, and the capacity supported by the current standard. This is mainly because these throughput gains have not been enough to keep pace with the ever-increasing demand.

Wi-Fi 6 aims to solve the congestion issue by redesigning how Wi-Fi works and implementing the Orthogonal Frequency-Division Multiple Access (OFDMA) technology. With OFDMA, multiple clients can simultaneously share a Wi-Fi channel instead of having to take turns. It enables a 20 MHz channel to transmit to up to nine clients at once, versus four as in 802.11ac. As a result, supported client devices can make better usage of available bandwidth within the network.

Wi-Fi 6 also introduces some enhancements for the 2.4 GHz band. These are long-awaited enhancements beneficial to meet the exponentially growing demands. Also, these improvements will help the IoT market, where superior propagation characteristics of this band can be exploited.

Wi-Fi 6 also adopts power-saving features like TWT, 20 MHz-only support and so on, which will contribute to extending battery life far enough to make inroads into the emerging IoT market.

On the whole, 802.11ax offers increased aggregate network throughput, reduced overhead, lower latency, increased efficiency in dense networks, increased robustness of outdoor networks, and improved power efficiency, which will be explained in further sections.

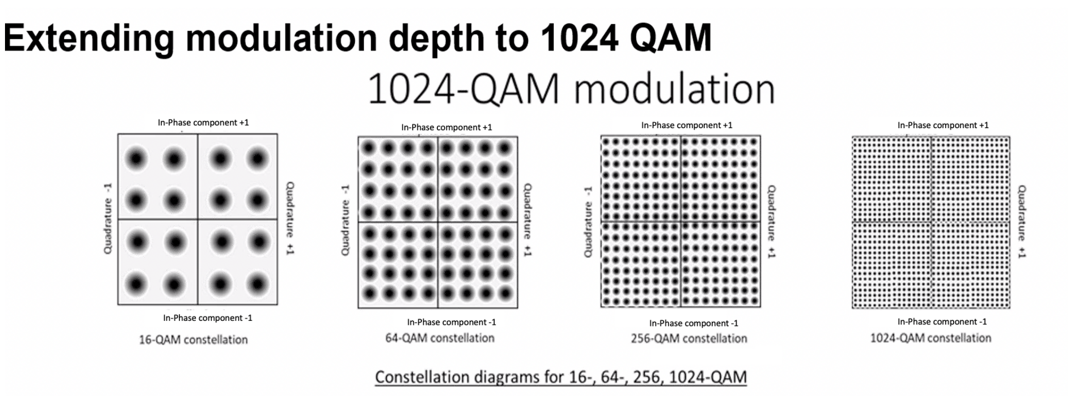
Chapter 3
Wi-Fi 6 Features and Benefits

The following section discusses the features and benefits of deploying Aruba's Wi-Fi 6 network.

Modulation Rates

The 802.11ax amendment continues to extend the sophistication of its modulation techniques. Building on the rates of up to 256 Quadrature Amplitude Modulation (QAM) of 802.11ac, it now extends to 1024-QAM. This means that each RF symbol represents one of the 1024 possible combinations of amplitude and phase as illustrated in Figure 1. The move from 256-QAM to 1024-QAM increases the number of bits carried per OFDM symbol from 8 to 10. This leads to 25% increase in PHY data rates and comes into play in clean environments with high signal to noise ratio (SNR).

Figure 1 *1024-QAM Modulation*



The key determinants of PHY data rate are:

- **Channel width**: Available channel widths are 20 MHz, 40 MHz, 80 MHz, 80 + 80 MHz and 160 MHz. Wider bandwidths permit the use of more subcarriers, for example there are 242 subcarriers in a 20 MHz channel and 996 subcarriers in an 80 MHz channel (hence the OFDMA terms RU242 and RU996).
- **Modulation and coding**: 802.11ax extends the modulation and coding scheme to add 1024-QAM options with coding rates of 3/4 and 5/6. All the earlier options are still available, and are used if SNR is too low to sustain the highest achievable rate.
- FFT size was enhanced from 64 in 802.11ac to 256 in 802.11ax for 20 MHz. This lead to decrease in subcarrier spacing and increase in number of data subcarriers. These factors contribute to 10% increase in efficiency.
- Symbol duration was increased to 13.6, 14.4 and 16 micro seconds. Extended symbol durations result in increased efficiency due to availability of more data tones compared to the older standards.
- **Guard interval**: Guard Intervals are necessary to avoid multipath reflections of one symbol from arriving late and interfering with the next symbol. Extended guard interval durations of, 1600 and 3200 nanoseconds have been introduced in addition to 800 nanoseconds from the 802.11ac. Longer guard

intervals allow for better protection against signal delay spread as it occurs in outdoor environments. These could also potentially increase the effective range of wireless outdoors.

All the above factors contribute to the increased PHY data rate and efficiency. The following table provides 802.11ax data rates for a single spatial stream full-bandwidth user.

Table 2: *Modulation and coding schemes for single spatial stream for a full-bandwidth user (i.e. not OFDMA)*

MCS index	Modulation type	Coding rate	Data rate (in Mb/s)[a]							
			20 MHz channels		40 MHz channels		80 MHz channels		160 MHz channels	
			1600 ns GI[b]	800 ns GI	1600 ns GI	800 ns GI	1600 ns GI	800 ns GI	1600 ns GI	800 ns GI
0	BPSK	1/2	8	8.6	16	17.2	34	36.0	68	72
1	QPSK	1/2	16	17.2	33	34.4	68	72.1	136	144
2	QPSK	3/4	24	25.8	49	51.6	102	108.1	204	216
3	16-QAM	1/2	33	34.4	65	68.8	136	144.1	272	282
4	16-QAM	3/4	49	51.6	98	103.2	204	216.2	408	432
5	64-QAM	2/3	65	68.8	130	137.6	272	288.2	544	576
6	64-QAM	3/4	73	77.4	146	154.9	306	324.4	613	649
7	64-QAM	5/6	81	86.0	163	172.1	340	360.3	681	721
8	256-QAM	3/4	98	103.2	195	206.5	408	432.4	817	865
9	256-QAM	5/6	108	114.7	217	229.4	453	480.4	907	961
10	1024-QAM	3/4	122	129.0	244	258.1	510	540.4	1021	1081
11	1024-QAM	5/6	135	143.4	271	286.8	567	600.5	1134	1201

a. A second stream doubles the theoretical data rate, a third one triples it, and so on.
b. GI stands for the guard interval.

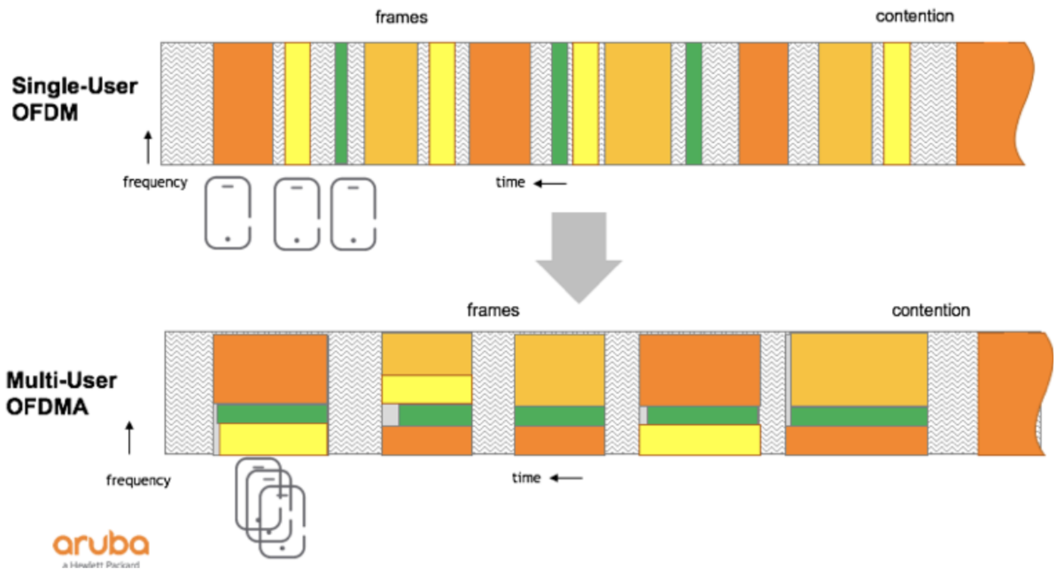
Orthogonal frequency division multiple-access

OFDMA is a transmission technique, which enables multiple devices to share the same Wi-Fi channel at the same time. Wi-Fi was the first major consumer technology to adopt OFDMA over 20 years ago, and it was subsequently used by 3GPP community when designing LTE and now 5G New Radio. In turn, Wi-Fi 6 adopted OFDMA technology from other wireless technologies like WiMAX and LTE.

With OFDMA, multiple clients can simultaneously share a Wi-Fi channel instead of having to take turns. It enables a 20 MHz channel to transmit to up to nine clients at once, versus four as in 802.11ac. This scales linearly as the channel width increases i.e. 18 clients for 40 MHz and 37 clients for 80 MHz channels. And when needed, a single client can also use the entire channel making sure that better client density doesn't come at a cost of peak performance. Importantly, OFDMA is bi-directional, bringing uplink multi-user capability to Wi-Fi for the first time.

Take into consideration a scenario where AP has to send data to 3 clients. In 802.11ac Single User operation (SU), the AP would contend for the medium and then send three packets consecutively as shown in the figure below. Whereas in 802.11ax with OFDMA, transmissions for these 3 client devices are assigned a fractional channel and then sent to all 3 clients simultaneously.

Figure 2 *OFDMA Operation*



To summarize, OFDMA allows the access point to bundle several frames together with a single preamble, in different sub-channels in a single transmit opportunity. Clients can then tune their radios to the respective sub-channels to receive their transmissions.

Benefits of OFDMA

- It helps in reducing latency between Wi-Fi clients and APs.
- It helps in reducing contention overhead which means that there is very little deterioration in capacity as the number of clients increases. This is extremely helpful in HD environments as it improves network capacity.
- It helps to increase overall network efficiency.
- 802.11ax also improves performance for legacy generations. As more Wi-Fi 6 devices enter the market and use OFDMA to reduce airtime consumption, there is more usable airtime leftover for earlier Wi-Fi generations.

Applications

The following section discusses key OFDMA applications:

Voice over Wi-Fi

One of the most important applications of OFDMA is Voice over Wi-Fi (VoWi-Fi). In High Density environments, where a lot of users are contending for the medium; could result in increased latency and jitter. These factors can cause gaps in the re-creation and playback of the voice signal leading to an undesirable user experience. OFDMA also enables strong QoS mechanism by enabling the AP to control medium access for both DL and UL. This eliminates the need for medium contention and allows AP to schedule transmissions. That is how OFDMA allows the access point to control latency and jitter. With 802.11ax, the access point can assign frequent, short transmission opportunities so it can transmit and receive packets without the need to buffer them. This can be extremely helpful in low-bandwidth streams of VoWi-Fi by reducing latency and jitter thus improving the call quality.

In addition to this, Aruba offers Air Slice, a key Aruba Wi-Fi 6 differentiator, designed to optimize user and application experience. Existing wireless multimedia (WMM QoS) standard prioritizes traffic according to four access categories:

- Voice (AC_VO)
- Video (AC_VI)
- Best-effort (AC_BE)
- Background (AC_BK)

Hence it lacks the granularity to prioritize the applications in the same access category. A growing number of enterprises are using latency-sensitive, bandwidth-demanding applications like AR/VR, or other collaborative applications such as Zoom, Skype for Business, Slack and so on. These new applications have stringent quality of service requirements in terms of latency, bandwidth, and throughput, hence there is a need to enhance the quality of service for these newer applications and IoT devices.

By combining Aruba's Policy Enforcement Firewall (PEF) and Layer-7 Deep Packet Inspection (DPI) to identify user roles and applications, APs will dynamically allocate the bandwidth and other RF resources that are required to meet the performance metrics for business-critical applications to ensure better user experience. Using Air Slice, IT can further orchestrate radio resources to work with ClientMatch to go beyond the traditional capabilities of Airtime Fairness.

This capability of going beyond traditional Wireless Multimedia quality of service requirements to achieve application performance SLAs over the air, differentiates HPE-Aruba products from competitors that use the same chipsets and base radio software.

IoT

The important metrics for an IoT device are data rate, device density, range, power consumption, security, and ease of configuration. OFDMA addresses the first three of these requirements. First, OFDMA divides transmissions across frequency domain and the smallest unit of allocated bandwidth can be as small as 2 MHz. This in turn allows more individual devices to be reliably supported on an AP and thus fulfills the second critical IoT requirement, scaling to support higher device densities. Unlike most of the mainstream Wi-Fi applications, IoT devices usually use lower-speed connections, often in sub-megabit range. Finally, the narrower sub-channels used by OFDMA inherently helps in improving the uplink range of IoT devices because they are permitted to use higher Power Spectral Density (PSD) towards the AP.

In addition to this, Wi-Fi 6 also offers various power-save features like TWT, Receive Operating Mode Indication, Transmit Operating Mode Indication, and so on along with '20 MHz-only clients' to addresses most of basic requirements for encroaching into IoT Markets.

Video and Factory Automation Applications

OFDMA is ideal for latency sensitive applications like video and factory automation applications. It enables many low-bandwidth streams to be transmitted in parallel, which aids in reducing latency and jitter thus extremely useful in video streaming and factory automation applications.

MU-MIMO Improvements in Wi-Fi 6

Multi-user Multiple-Input, Multiple-Output (MU MIMO) is a multi-user capability, originally introduced in 802.11ac for downlink traffic. MU-MIMO technology improves the network capacity by allowing multiple devices to transmit simultaneously, making use of multipath spatial channels. The use of MU-MIMO in today's Wi-Fi devices has increased multifold and it is a commonly adopted technology in the Wi-Fi space.

The first wave of Wi-Fi 6 introduces some new enhancements to the existing 802.11ac DL MU-MIMO. The number of users in a group were expanded to eight users for MU-MIMO operation. Due to this advancement, now even with devices in single stream mode, MU-MIMO throughput can be doubled or tripled over single user operation. This improvement of increasing the size of downlink multi-user MIMO groups results in more efficient operation.

In addition to this, Wi-Fi 6 uses UL OFDMA as part of the sounding protocol, which is more efficient than using single user transmission of the feedback used for the sounding protocol in 802.11ac.

All these factors lead increased capacity and efficiency and is particularly useful in high-bandwidth applications like mission-critical voice calls and video streaming.

The second wave of Wi-Fi 6 will introduce MU-MIMO in the uplink direction (UL-MU-MIMO), enabling both multi-user techniques to be fully bidirectional.

Power-Save Enhancements

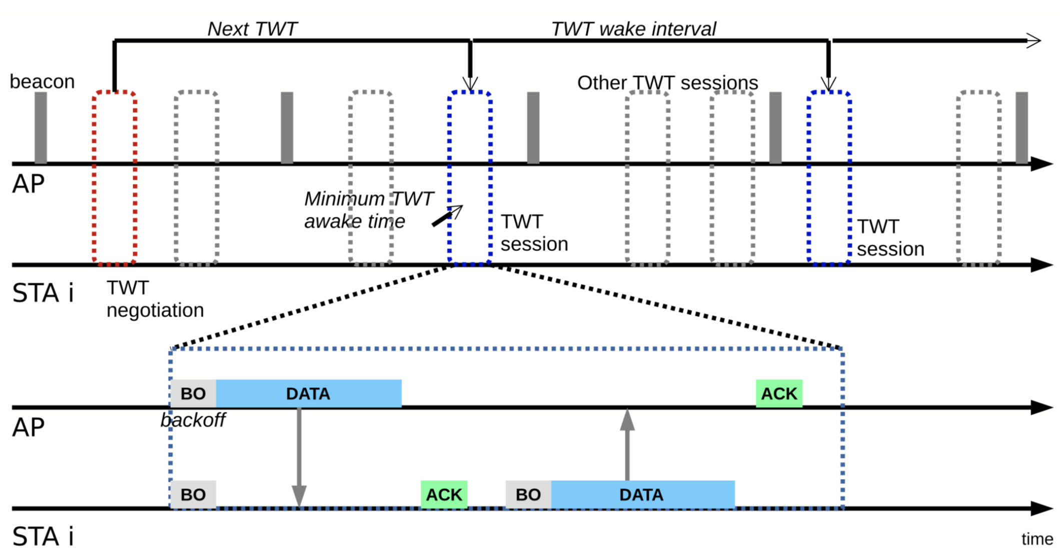
Wi-Fi 6 introduces various enhancements to the already existing power-save modes. These new and improved power-save mechanisms allow longer sleep intervals and scheduled wake times for the client devices. These enhancements were adopted to address the power consumption issue mainly for handheld and battery powered devices and are targeted towards the emerging IoT markets.

Target Wake Time

Target Wake Time (TWT) is a power saving mechanism that was introduced in 802.11ah. A schedule is negotiated between each station (client) and its AP, which allows the station to sleep for extremely long periods of time, potentially several days or even weeks, and wake up in pre-scheduled (target) times to exchange information with its AP. TWT also significantly reduces small and inefficient control frame traffic that stations are required to use regularly to poll the AP for buffered frames.

In addition to reducing the contention between stations, the use of TWT may also contribute to taking full advantage of other novel mechanisms in the IEEE 802.11 universe, such as mult-iuser transmissions, multi-AP co-operation, spatial reuse, and coexistence in high-density WLAN scenarios. This operation is ideal for IoT devices that do not communicate frequently and it improves client power savings and reduces airtime contention with other clients.

Figure 3 *Example of Individual TWT agreement*



20 MHz-only Operation

'20 MHz-only operation' feature was specifically introduced for IoT markets. This feature reduces complexity, leading to low-power, lower-cost chips. Such devices are capable of operating in both 2.4 & 5 GHz spectrums and also support nearly all Wi-Fi 6 mandatory features.

Receive Operating Mode Indication

This enables both the AP and its associated stations to adapt to the number of active receive chains and channel width for reception of subsequent PPDU's by using a field in the MAC header of a data frame. This mechanism has reduced overheads compared to 802.11ac as there is no additional 'Operating Mode Notification' management frame exchange as in 802.11ac.

Transmit Operating Mode Indication

This allows both the AP and its associated client devices to dynamically adapt their transmit capabilities like channel width and maximum number of spatial streams.

Uplink/Downlink (UL/DL) flag

UL/DL flag in every preamble allows to identify the frames as transmitted by an AP or client device. This helps the client devices to switch off their radio circuitry as soon as they see an 'uplink' bit in the preamble.

Backward Compatibility

As always with Wi-Fi, 802.11ax radios are backward compatible and fully support legacy 802.11a/b/g/n/ac client radios. While this new standard includes new, higher-efficiency techniques, and frame formats that can only be decoded by other 802.11ax devices, continued support of VHT, HT, and older 802.11 equipment is an integral part of the standard. 802.11ax radios will communicate with other 802.11ax radios using HE OFDMA symbols and Physical Protocol Data Unit (PPDU) formats. As far as compatibility with clients is concerned, they can communicate with 802.11a/g, 802.11n (HT) and 802.11ac (VHT) clients using 802.11a/g/n/ac formatted PPDUs. When 802.11ax-only OFDMA conversations are occurring, the RTS/CTS mechanism may be used to protect legacy receivers during the period when HE transmissions are underway.

This ensures that an 802.11ax AP is a good neighbor to the adjacent to older APs while fully embracing all of the generations of client devices that exist in the environment. 802.11ax has a number of features for co-existence, but the main one is the extension of an 802.11n/ac technique. The first 20 microseconds of 802.11ax preamble uses the 802.11a preamble. Non-802.11ax equipment can read the first 20 microseconds and identify that the channel will be occupied for a given time, and therefore can avoid transmitting simultaneously with the high efficiency frame. In conclusion, 802.11ax is backward compatible with legacy 802.11 standards and can be deployed in mixed environment with legacy APs.

Protection, Dynamic Bandwidth, and Channelization

802.11ax inherits the dynamic bandwidth operation and protection mechanisms from 802.11ac standard. There have not been any new modifications to the these mechanisms in this new standard. Also, the available RF channels in most countries have not changed very much since 802.11ac was introduced. Please refer to the *'Protection, Dynamic Bandwidth, and Channelization'* section of Aruba 802.11ac Networks Validated Reference Design.

Chapter 4
Wi-Fi 6 Planning and Deployment Guidelines

The following section provides the guidelines for planning and deploying Wi-Fi 6.

AP PoE Requirements

An important consideration while choosing the wired access switch for powering the 802.11ax APs is the PoE capability. It is recommended to use 802.3bt capable switches at the access layer to supply power to the APs. Although Aruba APs support full 802.11ax functionality with 802.3at (PoE+) power source, the high-end 11ax APs operate with some reduced capabilities. If 802.3bt is not available, then these reduced capabilities may be overcome by enabling Intelligent Power Monitoring (IPM) or using dual-ethernet to enable APs to combine power and utilize necessary power for full functionality.

The following table gives a brief overview of AP power requirements and configuration options for full functionality:

Table 3: *AP power requirements for full functionality*

802.11ax Capable AP Model	802.3bt	2 x 802.3at (PoE+) (Shared)	802.3at (PoE+)	2 x 802.3af	802.3af
AP-550 Series	No Restrictions	No Restrictions	No Restrictions* (IPM Enabled)	Not Supported	Not Supported
AP-530 Series	No Restrictions	No Restrictions	No Restrictions* (IPM Enabled)	Not Supported	Not Supported
AP-510 Series	No Restrictions	Not Supported	No Restrictions	-	No Restrictions (IPM Enabled)
AP-500 Series	No Restrictions	Not Supported	No Restrictions	-	No Restrictions (IPM Enabled)

***IPM may apply additional restrictions as required, depending on PSE delivered power. IPM is admin configurable**

For more details regarding restrictions applied without IPM, please refer to Intelligent Power Monitoring on page 10.

Power over Ethernet (PoE) Options

With the release of Aruba's Wi-Fi 6 Indoor Access Points, new POE requirements were introduced with 802.11bt (Class 5/6 up to 60W). Because wired switching and POE infrastructure are often on longer refresh cycles than the WLAN infrastructure, Aruba worked to ensure that we provided a platform that was as flexible and accommodating as possible. In addition to the regular 802.11af/at/bt options, we also include support for aggregating power to the APs with dual ethernet cables to accommodate deployments that may not be able to upgrade to the latest POE options required for these higher-powered APs. Aruba has also provided configuration options in software to help conserve power that will allow for the Wi-Fi 6 APs to operate with full features enabled in situations where sub-optimal power solutions are available.

The following sections will serve as a primer to the POE options available today, what the Wi-Fi 6 APs require, and what configuration options will work, both in hardware connectivity and in software to help ensure operability.

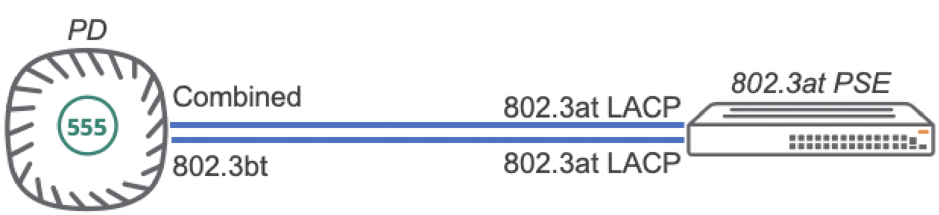
Dual Ethernet Options

Recognizing that not every customer will have 802.3bt capable switches across their enterprise, Aruba designed the higher performing APs to be able to use dual ethernet connections that can take power from both cables and combine them together to power the AP. This way, if customers have run dual ethernet cables to their 802.11ax access points, or if they ran two cables for redundancy purposes, both cables can be plugged in into the AP, ensuring that there is a PSE on the end of each cable, and the AP will intelligently combine the power from both cables. The two Aruba Wi-Fi 6 APs that support this capability are the Aruba AP-530 series and the AP-555 access points. Note that while the AP is sharing power over the two links, the actual power draw may not always be 50/50. There could be variances of power draw between the two ethernet interfaces.

For the AP-53x and AP-55x access points, when dual ethernet links are used, the APs have the capability to combine power from both lower-powered uplinks to the Power Sourcing Equipment (PSE) to equal a combined higher power. For ArubaOS, the APs can be configured to either share power or to use prioritized power under **ap system-profile <profile name>**. With the AP set to 'share POE power', which is the default setting, the AP will request equal power from each interface to balance the power request and combine them at the AP. When using shared mode, each interface will draw approximately 65% of the power required, resulting in the AP in 'Shared POE' mode drawing slightly more power (approx. 30% more) than a single uplink would draw. In this case, the total power draw does not increase, but since we cannot ensure a 50/50 split, we have to reserve more than half from each power source.

The most straight-forward and effective way to use two ethernet uplinks is to use Link Aggregation Control Protocol (LACP) on the switches (if supported) and allow the AP to negotiate LACP and use both links at the same time. The LACP link is configured as a single interface on the switch and AP, which not only allows for power combining across both links, but also doubles the wired bandwidth available for the AP to use. No special configuration should be required to enable LACP support on the AP-530 series or AP-555. In the following illustration, a PSE is configured for LACP providing dual 802.3at power, which the AP combines for 802.3bt power on the AP-555 or AP-530.

Figure 4 *AP using dual ethernet for full functionality when LACP is configured*



Intelligent Power Monitoring

In addition to the hardware options within the AP platforms, there are several software technologies both within the AP itself, as well as within the software, that can be leveraged to provide more flexibility with power solutions management. When dealing with access points, there are number of factors that are involved in how much power the AP draws (CPU utilization, temperature, user counts, AP power, and so on), and the AP has to ensure that it has asked for enough power from the PSE that should any one of those factors go up suddenly, that there is enough overhead to allow the AP to continue to operate. As such, while in most cases when the AP has its ideal power allocation from the PSE, the software can be modified to allow the AP to more dynamically manage its power consumption to help save some power.

The most critical feature that should be enabled is IPM, which allows the AP to enable or disable features, and dynamically manage the radio settings and restrictions to maximize and optimize power consumption. While this can help minimize the total power draw to maximize electrical power costs, it can also help allow the AP to run fully enabled, even if it's connected to a PSE that provides less than the ideal power class. IPM works in real time and can adjust on the fly as needed. IPM can be enabled under **ap system-profile <profile name>**.

Once IPM is enabled, there are two behaviors available. The AP will disable elements of the AP to conserve power. Usually that involves disabling the USB port (since that is not often in use) and the second ethernet interface (when a single uplink is present, there's not much need to spend power to keep the second ethernet link available). From there, the AP will dynamically disable features as needed on the AP, such as radio power, number of chains, and so. Secondly, IPM includes a user-defined list of capabilities to disable, in order of priority as part of the power saving algorithm. This could be to disable an entire radio first, or maybe drop the number of chains to 2x2, or even decrease the CPU resource utilization. They key though is that IPM allows the administrator to define how the APs conserve power, instead of the AP doing it on its own, giving the most flexibility and control to the administrator.

In addition to IPM, there is also an option within ArubaOS to provision the APs with **ap-poe-power-optimization** configured. This option can be configured under **ap provisioning-profile <profile name>**. Enabling optimization minimizes the POE draw of the AP. This forces the APs provisioned with that setting enabled to disable the USB port and disable any PSE functionality within the AP (if present). Note, this should not be used if the intent is to use the AP's USB port or PSE functionality to power a Powered Device (PD) on the downlink.

The following table provides a high-level overview of how APs behave under different powered states:

Table 4: *AP-500 Series IPM Operation with Class 5 POE Device and Dual gigabit POE interface or DC power*

	802.3bt	2 x 802.3at (Shared)	802.3at	2 x 802.3af	802.3af
Maximum PoE Draw (Without / with a USB attached)	■ AP55X - 38.2W/ 43.2W ■ AP-53X - 26.4W/ 32.1W ■ AP-51X - 20.8W/ 26.5W ■ AP-50X - 11W/ 16.5W	■ AP55X - 38.2W/ 43.2W ■ AP-53X - 26.4W/ 32.1W ■ AP-51X/50X - Not Supported	■ AP55X - 25.1W/ 30.1W ■ AP-53X - 23.3W/ 29W ■ AP-51X - 20.8W/ 26.5W ■ AP-50X - 11W/ 16.5W	Not Supported	■ AP55X/53X - Not Supported ■ AP-51X - 13.5W/ 19.2W ■ AP-50X - 11W/ 13.5W
IPM Enabled	No restrictions	No restrictions	No restrictions*	Not Supported	■ AP-55X/53X - Not Supported ■ AP-51X/50X – No restrictions*
IPM Disabled	No restrictions	No restrictions	■ AP-555: Disable split-5GHz mode	Not Supported	■ AP-55X/53X - Not Supported

	802.3bt	2 x 802.3at (Shared)	802.3at	2 x 802.3af	802.3af
			4x4 @ 5GHz Only ■ AP-55x/53X: Disable USB Disable 2nd Eth ■ AP-51X/50X – No restrictions**		■ AP-51X – No restrictions ■ AP-50X – USB port disabled

* IPM may apply additional restrictions as required, depending on PSE delivered power, IPM is admin configurable

** In an extremely unlikely and worst case scenario, we may hit the 25.5W PoE budget limit when exceeding 4W. We won't be able to source the full 5W for an attached USB device.

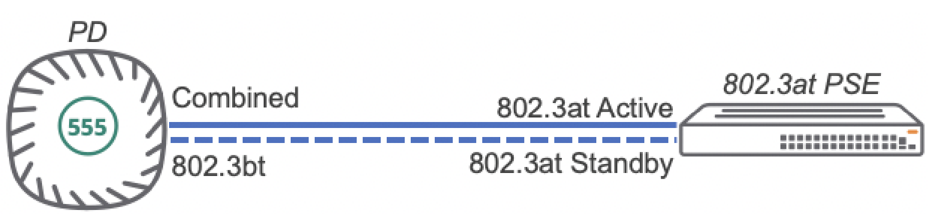
PoE Redundancy

For the AP-53x and AP-55x, dual ethernet links can be used to provide PoE redundancy. For ArubaOS, the APs can be configured to either share power or to use prioritized power. With 'failover POE power' configured under **ap system-profile <profile name>**, the AP will prioritize its full power from one interface, and if that one fails, the AP will seamlessly request and draw power from the other interface. While 'shared POE power' is the most flexible, it will draw a total amount of power higher than a 'failover POE power' when configured for 'failover'. As a result, on switches with lots of APs where the POE budget is tight, using 'failover' mode for POE may help reduce the total POE power drawn against the switch's POE budget.

For Aruba InstantOS, the AP can only support 'shared POE power'.

If LACP is not configured, the dual interface AP can be connected to the switch with both ports, where the AP will work with an 'Active/Standby' configuration (this is enabled without any explicit configuration on the AP or controller). The AP will elect to make Eth0 the 'Active' interface and the Eth1 interface as the 'Standby' as shown in the following illustration. All traffic will go over the Active link, and power will be drawn from both. If Eth0 goes down, the AP will move its uplink connection to Eth1 and will change the power to source fully from Eth1. When the connection to Eth1 is re-established, the AP will move back to Eth0 after approximately 15 seconds. Note, there will be 1-3 pings lost as the AP's uplink changes. This allows for a lower level of redundancy compared to LACP and results in a single interface of throughput (instead of combining the overall throughput of both links).

Figure 5 *AP in 'Active/Standby' configuration when LACP is not configured*

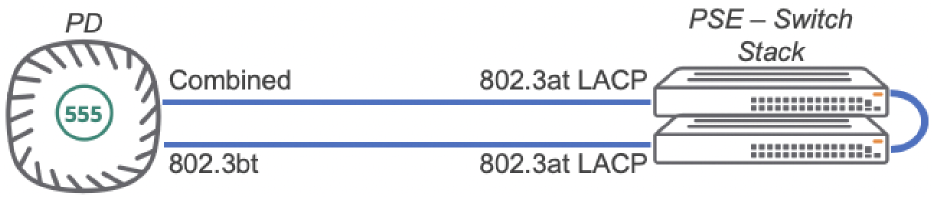


Additionally, to build redundancy between the AP and switches, should there be a need for both cable and switch redundancy, a stack of switches can be used, building LACP between the two ports used within the stack, so that if one of the switches fails on one link, the AP can still get data and power from the other link, as shown in the following illustration.

NOTE

For AP-555, the switches in the stack would have to be 802.3bt enabled so that the AP-555 still operates on a single uplink.

Figure 6 *Building redundancy between APs and switches by using dual ethernet when LACP is configured*



AP Wired Uplink Considerations

First generation 802.11ax radios supports 1024-QAM modulation, which means that 802.11ax APs are capable of achieving very high data rates with the higher MCS values. Each radio may be transmitting concurrently, increasing the overall instantaneous bandwidth. To ensure that these APs can achieve best possible performance based on their environment during periods of high client demand, it is essential to provide them with Smart Rate uplink especially for higher-end APs from 530 and 550 series.

RF Planning

Wi-Fi has become a necessity and it falls at the center of mobility. With the explosion of Internet connected devices, Wi-Fi is not only a must have, but also expected to sustain the growing number of Wi-Fi devices. Every individual, whether in a corporate environment, schools, or hospitals carries an average of two Wi-Fi capable devices. This requires careful planning and design of WLAN deployment. This Deployment Guide provides guidelines for High Density Campus deployments.

In the following sections we look at each of our decision-making points in more detail.

Supported Applications

Voice and Video applications such as Facetime,Skype for Business, and Wi-Fi Calling are very common in a campus deployments such as education, enterprise, or hospitals. This demands WLAN to be optimized for real time applications (how far apart the APs are placed, ensure good AP density, good Wi-Fi client SNR, and seamless roaming).

As a first step towards that, APs must be placed approximately 40-60 feet apart, in a honeycomb structure. Good Wi-Fi deployment should ensure Wi-Fi client signal to noise ratio (SNR) of 35dB or higher. This ensures good density of APs for clients to roam without affecting real-time application performance.

Exceptions may exist within a campus, such as an indoor large meeting area or conference center. In that case, those sections of the campus must be treated as VHD arenas and VHD deployment guidelines must be used.

In addition to AP Placement, there are other features and/or parameters that we need to enable or tweak in order to ensure good quality air and reduce RF Channel utilization by using various optimization configurations.

WLAN should be optimized for RF performance using various features such as Airmatch, Client Match, and WLAN Rate Optimization.

RF Optimization

RF optimization enables or disables load balancing based on a user-defined number of clients or degree of AP utilization on an AP. This profile can be used to detect coverage holes, radio interference and STA association failures, and configure RSSI metrics.

- Airmatch will help APs arrive at an optimum channel and power.
- Client match helps steer dual-band capable clients to 5 GHz. In addition, it forces sticky-clients to move to a better AP.

WLAN Rate Optimization

Broadcast or Multicast Rate (BC/MC) Optimization dynamically selects the rate for sending broadcast or multicast frames on any BSS. This feature determines the optimal rate for sending broadcast and multicast frames based on the lowest of the unicast rates across all associated clients.

- Mcast Rate optimization.
- Drop Unknown BC/MC from going out on Wireless, thus saving valuable airtime.
- Elect to use Dynamic multicast optimization to enhance multicast video quality and multicast traffic performance over wireless in general.

Recommended Wi-Fi Device Mix (1SS, 2SS, 3, or 4SS and/or MU-MIMO)

AP53x/AP55x 802.11ax APs are the baseline recommendations for HD deployments. Since these APs can support devices all the way up to 4x4:4 capable wireless clients as well.

We recommend visiting the below link for AP comparison. The AP comparison tool is an effective way to compare AP capabilities side-by-side for up to 3 APs:

https://www.arubanetworks.com/products/networking/access-points/compare/#132904,150581,150598

Recommended Wired Access Switches

POE capability, Smart Rate support, and Jumbo Frame support are a few key considerations when choosing the right wired access switch. For Wi-Fi 6 deployments, consider the following recommendations:

- 802.3bt or 802.3at (POE+) capable switches.
- High-performance APs like AP53x/AP55x, with 802.3bt power supply so that the APs can operate without any restrictions.

802.3at power supply will work but with reduced feature set as stated earlier in this document.

Smart Rate Capable HPE switches are recommended when using AP53x/AP55x, thus the AP uplink port can operate at a 2.5/5Gbps rate.

- The wired uplink from these access switches to the HPE Aruba Controller should be a minimum 10G pipe.
- Jumbo frame support should be supported end-to-end. Not having end-to-end Jumbo frame support will force intermediate devices to perform fragmentation reassembly.
- Either enable end-to-end Jumbo frames support to turn it off completely.

HPE-Aruba 6xxx AOS-CX switches are recommended for greenfield deployments. Also, any customer going through switch-refresh cycle should look at buying 802.3bt switches, as refreshing switches without upgrading PoE capability would be a mistake in terms of future-proofing.

Number of Devices Expected to be Supported

This section discusses the process of arriving at WLAN dimensioning and also deciding on a suitable controller + IAP/UAP model. This section also explains steps to arriving at the AP/User Count#.

AP/User count helps us arrive at a controller model to use; however, it is the controller redundancy that needs to define how many controllers are required in an environment. In a HD environment it is ideal to have between 40 to 60 simultaneously active (transmitting) clients per radio per AP. Associated but inactive (silent) clients may be several multiples of this.

It is key to arrive at the AP count based on how many clients you project your environment will have, by the end of the service life-cycle.

- 1User today typically carries at least = 3 Wi-Fi Devices, of which 1 may be considered active and 2 inactive at any given instant of time. Refer to the Very High-Density 802.11ac Networks VRD for more information

https://community.arubanetworks.com/t5/Validated-Reference-Design/Very-High-Density-802-11ac-Networks-Validated-Reference-Design/ta-p/230891

For example, if you do not expect to refresh your network before three years, plan to add APs in a way that can absorb the increased number of client devices before the next refresh.

Most clients are expected to join the 5 GHz radio (Aruba WLAN features ensure that). Hence, plan AP count based on per radio usage.

AP Count = 5 GHz Radio Count = Associated Device Capacity (5 GHz)/Max Associations Per Radio

Associated Device Capacity would be the best possible estimate of expected guest clients to be supported + employee client devices to be supported.

NOTE

This estimate should account for an increase in device count over years, for example, acquisitions and adding more employees.

WLAN Controller Model + WLAN Dimensioning

Once you have an AP and User count, this helps arrive at the controller model to be used as your AP termination controller. In HD campus deployments, the most common controller recommendation is the 72xx series (7280/7240XM being the highest capacity for very large campus, and 7205 being the small campus controller). For more information see, https://www.arubanetworks.com/assets/ds/DS_7200Series.pdf. In addition to AP/User, redundancy is the third factor in dimensioning WLAN.

For more information, refer to the controller comparison tool online at:
https://www.arubanetworks.com/products/networking/access-points/compare/ - 132904,150581,150598

Sessions and Effective Firewall Throughput.

'Platform Size >= Associated Device Capacity', if expected user capacity is less than 32,000.

WLAN Dimensioning - Number of Controllers Required

Follow the link below to use the controller comparison tool:
http://www.arubanetworks.com/products/networking/controllers/compare/#19997,19999,99240

For a detailed best practice recommendations of how to deploy controller based architectures, please refer to the following ArubaOS 8 Fundamentals Guide: https://community.arubanetworks.com/t5/Controller-Based-WLANs/ArubaOS-8-Fundamentals-Guide/ta-p/428914

RF Design

When you are planning to deploy a WLAN network, it is important to understand how and where your APs will be mounted to have a seamless Wi-Fi experience. You should identify the attenuation and interference sources in your environment, which can degrade your network performance. The following section provides RF planning guidelines to deploy an 802.11ax WLAN network.

AP Mounting Recommendations

Indoor APs are typically deployed in one of the following methods:

- Ceiling mount deployment
- Wall mount deployment

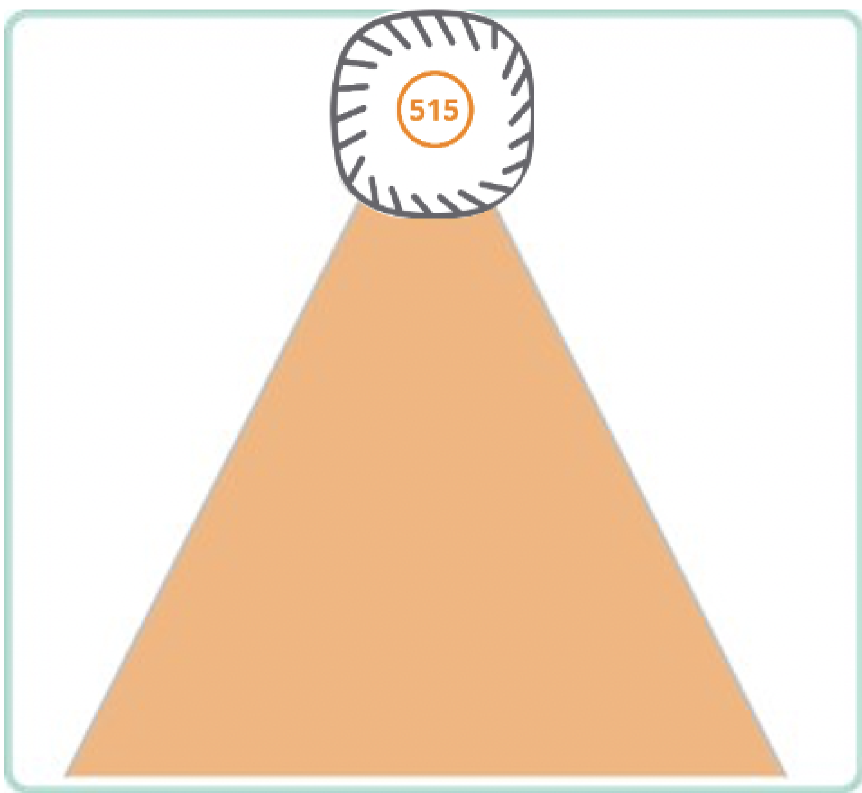
Aruba does not recommend desk or cubicle mounts. These locations typically do not allow for a clear line-of-sight throughout the coverage area, which in turn can reduce WLAN performance.

Ceiling Mount Deployment

The majority of modern WLAN deployments are at the ceiling level. A ceiling deployment can be done at or below the level of the ceiling material. In general, it is not recommended to mount APs above any type of ceiling material, especially suspended or "false" ceilings. There are two reasons for this:

- Most ceiling tiles contain materials or metallic backing that can greatly reduce signal quality.
- The space above the ceiling is full of fixtures, air conditioning ducts, pipes, conduits, and other normal mechanical items. These items directly obstruct signal and can harm the user experience.

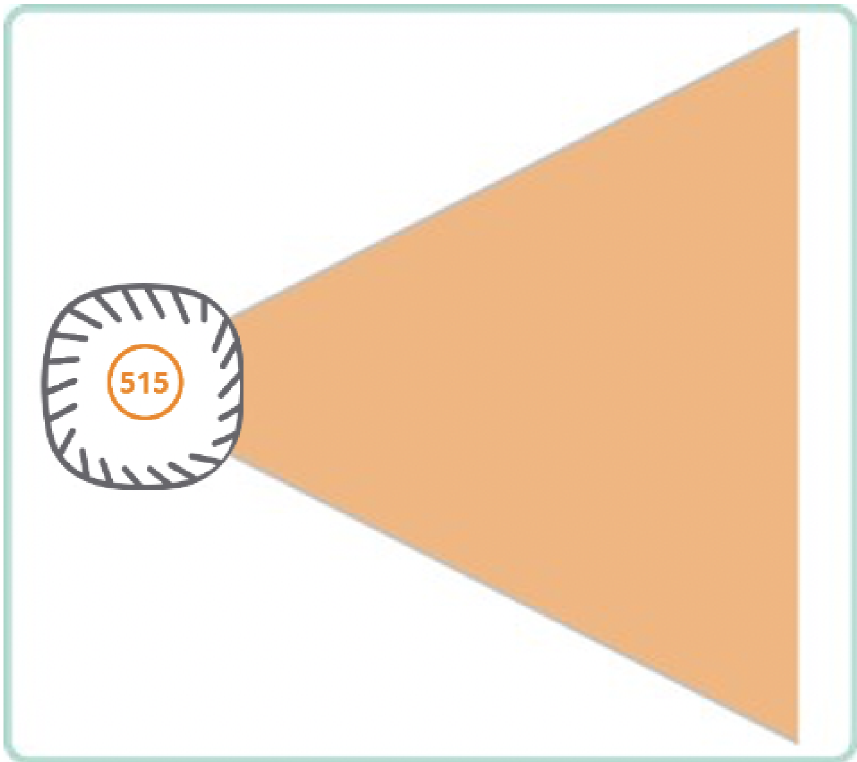
Figure 7 *Ceiling mounted Access Point*



Wall Deployment

Wall deployments are not as common as ceiling deployments, but are often found in hotels and dormitory rooms. Walls are a common deployment location for large spaces such as lecture halls because reaching the ceiling is difficult. Wall deployments may also be preferable in areas with a hard ceiling where cabling cannot be run. If you are not using the AP-503H, which was designed for wall mounting, consider the antenna pattern before you deploy wall-mounted APs.

Figure 8 *Wall Mounted Access Point*



Site Survey

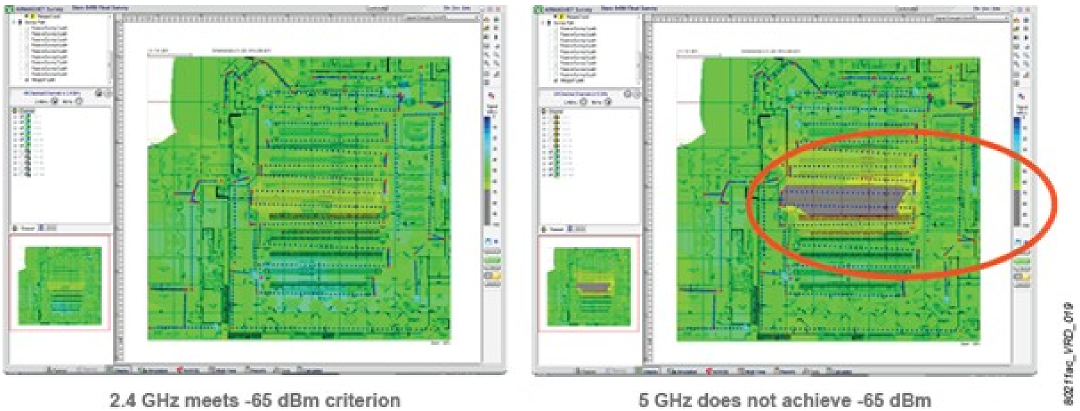
One of the important steps in RF planning is site survey analysis, which helps to identify AP placements to provide high-quality wireless experience throughout the facility. There are different types of site survey methods available such as virtual site survey, passive site survey, active site survey, and spectrum clearing site survey.

Although virtual site survey is a quick way to simulate AP placements and understand coverage patterns, it is recommended to conduct a physical site survey to validate the estimates of virtual site survey and verify the coverage and capacity of your network.

For more details regarding wireless site survey, refer to the indoor site survey and planning VRD available here.

When conducting site survey to plan for AP placements for a ubiquitous Wi-Fi coverage, it is important to remember that RF signals with higher frequency cover short distance compared to the low-frequency signals. You should plan your network in such a way that the 5 GHz band signals cover the area where you need to provide Wi-Fi to the users. If you plan the network based on 2.4 GHz band coverage, you might create a coverage hole as shown below.

Figure 9 *Comparison of 2.4 GHz and 5 GHz coverage pattern*



Aruba Recommendations for AP Placements

AP placement recommendations for an enterprise network, which needs to support high-performing 802.11ax network along with real-time voice and video applications, are as follows:

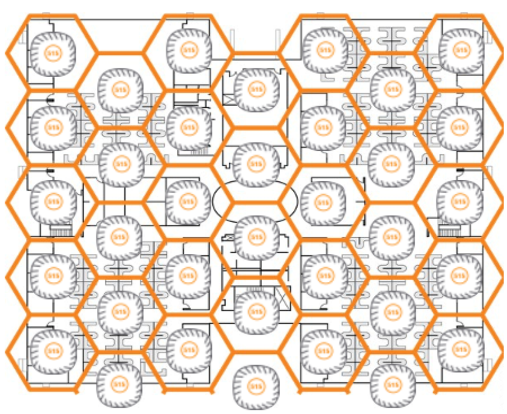
- Distance between two APs should be approximately 40 to 60 feet.
- Minimum RSSI should be -55 dBm throughout the coverage area.

The reason behind choosing RSSI to be -55 is that it could reliably provide MCS11 on 40 MHz for most high density deployments. The minimum receive sensitivity for HE MCS11rates are:

a. HE20: -60 dBm
b. HE40: -57 dBm
c. HE80: -54 dBm
d. HE160: -51 dBm

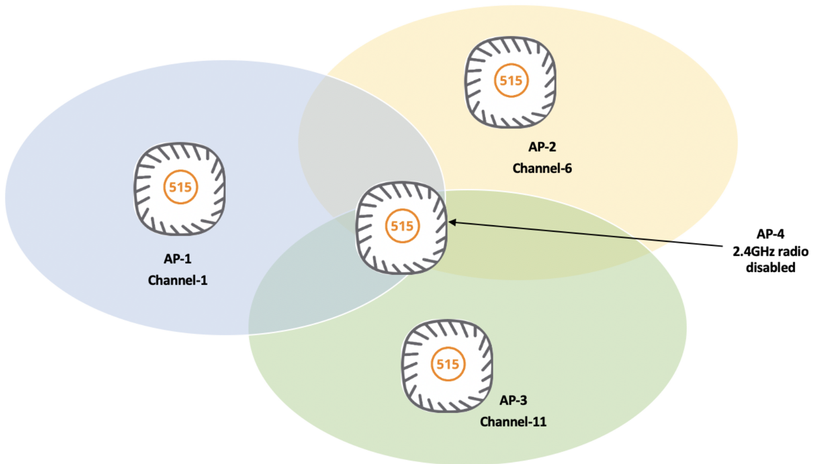
- SNR should be at least 35dB to achieve the highest 1024-QAM rates (MCS10 – 11).
- APs should be deployed in a honeycomb pattern as shown in the following diagram. This pattern ensures that distance is normalized along all directions to have the best coverage.

Figure 10 *Honeycomb Pattern AP Deployment*



When you design an 802.11ax network using dual band APs in such a way that 5 GHz band signal covers the entire facility, it might create co-channel interference in the 2.4 GHz band. This is because 2.4 GHz signals have greater coverage range compared to 5 GHz signals. To avoid this scenario, you can disable the 2.4 GHz radio on some of the APs on your network as show in the following illustration.

Figure 11 *Mitigating CCI in 2.4 GHz band*



In this illustration, as 3 APs are enough to have a 2.4 GHz coverage, you can disable the 2.4 GHz radio on the 4th AP to avoid co-channel interference. You can use the 2.4 GHz radio on the 4th AP either as a dedicated spectrum monitor to collect spectrum analysis data or as a dedicated air monitor to perform wireless intrusion detection and wireless intrusion protection.

Factors Attenuating Wireless Signals

It is important to understand the physical environment where we are planning to deploy 802.11ax WLAN because different materials have different attenuation characteristics which can impact the wireless performance. The following table compares the attenuation caused in 2.4 GHz and 5 GHz bands due to walls, glass window, or other such things.

Table 5: *Attenuation in 2.4 GHz and 5 GHz*

Indoor Environment	Attenuation in 2.4 GHz	Attenuation in 5 GHz
Fabric, blinds, ceiling tiles	Approximately 1 dB	Approximately 1.5 dB
Interior drywall	3–4 dB	3–5 dB
Cubicle wall	2–5 dB	4–9 dB
Wood door (Hollow –Solid)	3–4 dB	6–7 dB
Brick/concrete wall	6–18 dB	10–30 dB
Glass/window (not tinted)	2–3 dB	6–8 dB
Double-pane coated glass	13 dB	20 dB
Steel/fire exit door	13–19 dB	25–32 dB

Forwarding Mode Recommendations

For campus AP deployment, Aruba supports three different forwarding modes

- Tunnel Mode
- Decrypt-Tunnel mode
- Bridge mode.

NOTE

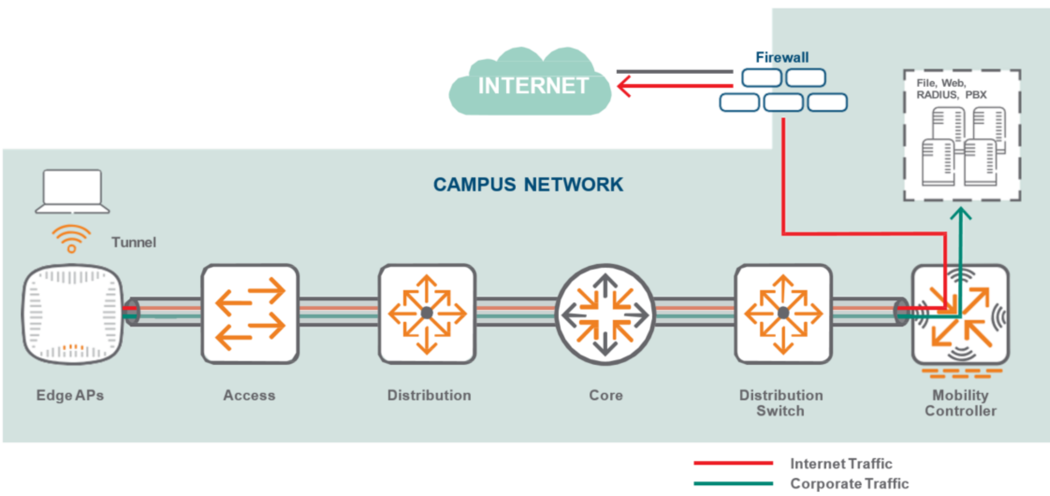
In general, bridge mode is not recommended to be used in campus environments.

This section provides information on the most common AP forwarding modes and the recommended mode for 802.11a deployments.

Tunnel Mode

The bulk of today's deployments utilize tunnel mode as the de-facto AP forwarding mode, where the AP sends the 802.11 traffic back to the controller without decrypting it first. One of the advantages of the tunnel mode is centralized encryption of control and data traffic. That is, in this mode, the control and data traffic between the AP and the mobility controller remains encrypted on the wire, which increases network security and can reduce latency under high loads due to the high-speed cryptography subsystem in the controller.

Figure 12 *Tunnel Mode*



Tunnel mode is our preferred mode of operation and has met the requirements of Aruba customers for nearly two decades. And since forwarding decisions are typically made on the controller (in L3 mode with default gateway) or by an upstream router (in L2 mode) there is no benefit to local decryption of raw wireless frames at the AP.

As discussed earlier, with frame aggregation techniques, 802.11ax frame is now a jumbo frame. Without jumbo frame support, Aruba controller and APs with service set identifiers (SSIDs) in tunnel mode do not participate in A-MSDU negotiations and hence there will be an impact on performance. To achieve high performance, it is always recommended to enable jumbo frames end-to-end, that is your switches and routers should also support jumbo frames. Not enabling jumbo frames in tunnel mode leads to a penalty of roughly 20-30%.

NOTE

The forwarding mode does not affect the controllers' maximum AP limit and performance, for example a 7240 controller can handle 2048 campus APs operating in tunnel mode without any performance issues.

Decrypt-Tunnel Mode

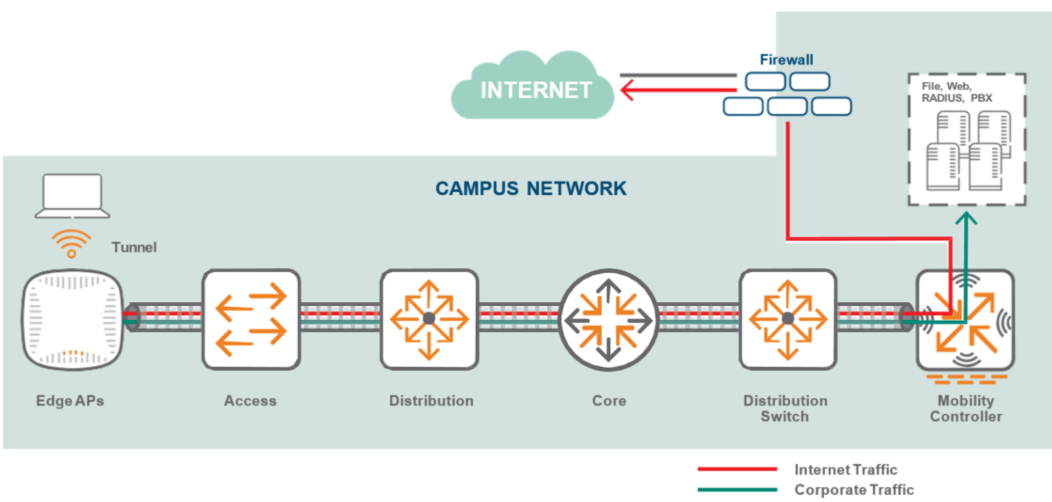
Decrypt-tunnel mode allows an AP-client pair to take full advantage of Aggregated-Media Access Control (MAC) Service Data Units (A-MSDUs) and Aggregated-MAC Packet Data Units (A-MPDUs) without the need for the wired network to transport Jumbo Frames. APs perform decryption and de-aggregation on themselves locally. It is mandatory to enable control plane security between APs and controllers when using decrypt-tunnel mode.

NOTE

Decrypt-tunnel mode does not provide end-to-end encryption. Only the control plane traffic between APs and Mobility Controllers is encrypted in the decrypt-tunnel mode.

In the decrypt-tunnel mode, an AP acts as a bridge between clients and the controller in addition to performing encryption and decryption. The controller still acts as the aggregation point for terminating data traffic. This allows the AP-client pair to take advantage of A-MSDU and A-MPDU on the WLAN radio side without requiring the wired network to transport the Jumbo Frames, since the AP performs all assembly aggregation and de-aggregation locally. The payload is then sent to the controller for firewall processing and L2/L3 forwarding. Decrypt-tunnel node is functionally equivalent to tunnel mode with jumbo frames enabled and is typically used for technology demonstrations. However, there is no centralized encryption because the user data traffic is decrypted by the AP and sent to the controller through a GRE tunnel.

Figure 13 *Decrypt-Tunnel Mode*



The performance of decrypt-tunnel mode is equivalent to tunnel mode with jumbo frames enabled. However, there is no centralized encryption because the user data traffic is decrypted by the AP and sent to the controller through a GRE tunnel.

Channel Width Selection

802.11ax products can be deployed to transmit in 20 MHz, 40 MHz, 80 MHz, and 160 MHz wide channels in 5 GHz band. To get the maximum performance results, it is recommended to allow 'Airmatch' to automatically determine the channel width whenever possible.

In general, the maximum channel width can be selected based on the number of available channels (20, 40 or 80 wide) and the number of APs that will share the same air space. Whenever the number of APs is less than the number of available channels, go as wide as possible. It is also true now that adding "interfering" APs (i.e. APs are spaced closer than one per channel) can improve performance, if the result is that by using wider channel widths the clients connect at faster data rates and utilize less airtime. As Airmatch takes care of all these factors, Aruba recommends to allow Airmatch to make all the channel width decisions.

Logically speaking, 802.11ax APs should be deployed to use 80 MHz or 160 MHz channel width. However, as discussed earlier, in the US there are only 6 available 80 MHz channels out of which 4 channels require DFS support to protect radar operation. We can design a network using the available six 80 MHz channels in 5 GHz band using DFS channels support; however, it might be a problem if there is radar interference near your environment, because when an AP operating in DFS channel detects a radar signal, it will disconnect the clients and move to a non-DFS channel. This will affect the users connected on that AP and might also create a co-channel interference with the neighboring AP, thereby degrading the network performance.

Selection of channel width depends on site environment and network requirements. . Aruba recommends that ultra-high-density networks with high activity factors should prefer deploying APs with 40 MHz or even 20 MHz channel widths so as to increase RF spatial reuse throughout the network without causing Wi-Fi interference.

Today, virtually all major consumer devices using Wi-Fi are capable of DFS operation. However, Aruba continues to see certain older or special-purpose devices that do not support DFS such as bar-code readers or legacy voice devices. You should also consider the clients' capabilities when planning for deploying APs with DFS channels to verify if all your clients support DFS channels. Even if some clients support DFS channel, they may not actively probe on those channels and only learn of them through passive scanning. This can lead to roaming issues. It is recommended to perform roaming test using different clients to analyze their roaming pattern with DFS channels.

Capacity planning

When planning for capacity, the most important things to consider are how many devices will access the network and what will be the type of client mix. Generally, people carry at least three devices such as a laptop, tablet, and a smart phone. The number of devices per user also has ramifications in the design of VLANs and subnets. Expected number of active devices trying to access the network will be one of the metrics to calculate the required AP density.

When calculating AP density for a capacity design, plan to have around 150 associate devices per radio for the high end APs from 550 and 530 series and 75 associated devices per radio for APs from 500 and 510 series. Assuming a 25-40% peak duty cycle, this will yield a simultaneously active user count of 40 – 60 devices per radio. Although APs can support even higher numbers of associated devices per radio, having more APs tp spread users will reduce congestion during demand spikes and provider high quality user experience. It is also important to select right devices to support your network requirements. Aruba Networks, Inc., have a wide portfolio of controllers and APs that allows you to select the best combination of devices to meet your network requirements.

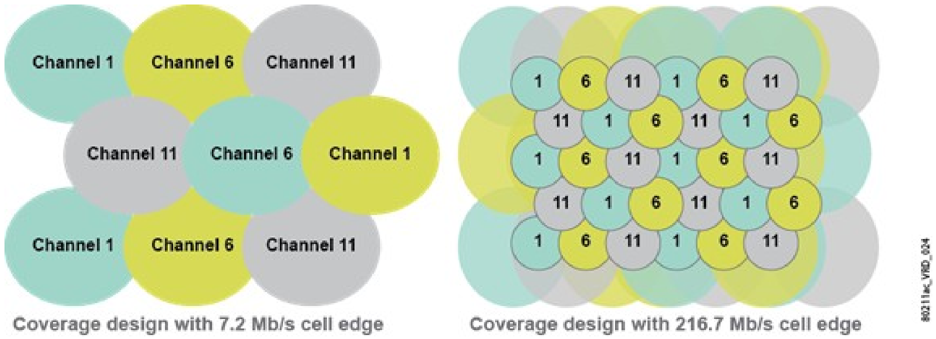
For detailed information about WLAN products, refer to http://www.arubanetworks.com/products/.

NOTE

Active devices are the clients which are associated to the AP and actively sending and receiving data on the wireless network. Associated devices are clients that are just associated to the AP and might not be involved in active data transfer activity.

As can be seen from the following illustration, typically in a capacity-based design, you will have to deploy more APs compared to coverage-based design. In a capacity design, users are generally associated with high data rates and get better wireless experience.

Figure 14 *Capacity Planning*



Transmit Beamforming (TxBF)

802.11ax employs an explicit beamforming procedure, similar to that of 802.11ac. Under this procedure, the beamformer (AP) initiates a channel sounding procedure with a Null Data Packet. The beamformee (client) measures the channel and responds with a beamforming feedback frame, containing a compressed feedback matrix. The beamformer uses this information to compute the antenna weights in order to focus the RF energy toward each user. It is recommended to keep this enabled to achieve optimal performance benefits.

TxBF can be configured using the High-efficiency SSID profile. To access this profile, go to managed network node hierarchy:

1. Navigate to the **Configuration > System > Profiles** tab.
2. Expand the **Wireless LAN** accordion.
3. Select High-Efficiency SSID and go to **Advanced**.

High Efficiency

All the 802.11ax specific features fall under High Efficiency profile. Enabling this parameter activates all the 802.11ax features on the radio and the user can utilize Wi-Fi 6 features like TxBF, HE supported higher MCS rates (10 and 11), HE OFDMA, MU-MIMO, TWT, and so on.

High Efficiency is enabled by default and it is recommended to keep it enabled to reap 802.11ax benefits. High Efficiency enable (radio) configuration can be found under RF Management profile.

To access this profile go to the Mobility Master node hierarchy:

1. Navigate to the **Configuration > System > Profiles** tab.
2. Expand the **RF Management profile** menu.
3. Select either the 2.4 GHz or the 5 GHz radio profile menu, then select the radio profile you wish to modify.

Ensure that High Efficiency is enabled.

NOTE

Having 'HE' enabled can cause connectivity issues with some legacy clients and those clients may need to have drivers updated to achieve optimal performance.

Please take a look at the Intel advisory. Following is the list of Intel adapters with the issue and the version of firmware required to correct it.
https://www.intel.com/content/www/us/en/support/articles/000054799/network-and-i-o/wireless-networking.html

If this is not possible, especially considering the BYOD kind of scenario, then set up a second SSID with HE disabled to support such legacy devices.

HE OFDMA

This feature is enabled by default and it is recommended to keep it enabled as it leads to increased efficiency and reduced latency. It is best for applications that require smaller packets (IoT, Voice applications, etc.) and is very suitable for low bandwidth applications. HE OFDMA can be configured using the High-efficiency SSID profile.

To access this profile, go to managed network node hierarchy:

1. Navigate to the **Configuration > System > Profiles tab**.
2. Expand the **Wireless LAN** accordion.
3. Select High-Efficiency SSID and go to **Advanced**.

Downlink MU-MIMO

This feature is enabled by default and it is recommended to keep it enabled in the configuration as it leads to increased capacity and enables higher speeds per user. It is best for applications that larger packets (Video, Streaming, etc.) and is very suitable for high bandwidth applications. HE MU-MIMO can be configured using the High-efficiency SSID profile.

To access this profile, go to managed network node hierarchy:

1. Navigate to the **Configuration > System > Profiles** tab.
2. Expand the **Wireless LAN** accordion.
3. Select High-Efficiency SSID and go to **Advanced**.

802.11ax Aware ClientMatch

ClientMatch continually monitors the RF neighborhood for each client to provide ongoing client bandsteering and load balancing, and enhanced AP reassignment for roaming mobile clients. Client Match is 802.11ax aware and there is no special knob for this feature. It will try to match 802.11ax clients to 802.11ax radios in a mixed AP deployment environment. Optimizes user experience by steering clients to the best AP.

NOTE

Legacy 802.11a/b/g devices do not support ClientMatch. When you enable ClientMatch on 802.11n-capable devices, ClientMatch overrides any settings configured for the legacy bandsteering or load balancing features. 802.11ac- capable devices do not support the legacy bandsteering, station hand off or load balancing settings, so these APs must be managed on using ClientMatch.

Target Wake Time

One of the main power saving features that 802.11ax offers is Target Wake Time (TWT), which will be very useful for IoT devices. The TWT has first proposed under 802.11h. TWT uses negotiated policies based on expected traffic activity between 802.11ax clients and an 802.11ax AP to specify a scheduled wake time for each client. 802.11ax IoT clients could potentially sleep for hours/days and conserve battery life.

This improves wake and sleep efficiency on smartphones and other mobile devices.

It is recommended to keep this feature enabled as it allows clients to request specific wake up time to AP, so that clients can go to sleep for longer time and save power.

This feature can be configured using the High-efficiency SSID profile.

To access this profile, go to managed network node hierarchy:

1. Navigate to the **Configuration > System > Profiles** tab.
2. Expand the **Wireless LAN** accordion.
3. Select High-Efficiency SSID and go to **Advanced**.

Wired Network Considerations

The following table summarizes Aruba's recommendation for wired networks to support 802.11ax WLAN deployments. For detailed description, please refer to 802.11ax Planning and Deployment Guidelines / Wired Network Considerations.

Table 6: *Wired Networks Consideration Recommendations*

Feature	Recommendation
PoE Requirements	■ It is preferred to use 802.3bt switches (Aruba 2930M Switch series, CX6200, CX6300, CX6400, etc.) to power AP-510, AP-530 and AP-555 series access points. ■ It is preferred to use 802.3at switches to power AP-500 series access points. ■ If 802.3bt capable switches are not available, then use dual ethernet connections that can take power from both cables and combine them together to power the AP, or leverage InteMP. **NOTE:** The feature is only available for Aruba AP-530 and AP-555 series. For details on Wi-Fi 6 and PoE options, please refer to the following section.
PoE redundancy	■ In a fresh deployment, it is recommended to plan for two Ethernet cables per AP for providing PoE fallback.
AP Uplink Consideration	■ Multi-Gigabit uplink is recommended for all 11ax APs (5xx series).
Ethernet Cable	■ Cat 6a Ethernet cables are recommended.
Access Network Uplink Consideration	■ Access switch terminating APs should have a 10 Gbps uplink.
Controller Uplink	■ It is recommended to at least have a 10 Gbps redundant uplink from the controller.
Jumbo Frame	■ It is recommended to have end-to-end Jumbo Frame support on your network to get maximum benefits of frame aggregation and improve 802.11ax performance.
VLAN Design	■ Design your network to have separate wired and wireless VLANs to avoid unnecessary broadcast and multicast traffic. ■ Configure a single flat VLAN for all the wireless clients. Take into consideration no. of clients per VLAN for your deployment. For further architectural considerations please refer to the Controller Reference Architectures topic in the AOS 8 Fundamentals Guide. ■ Configure Broadcast Multicast Optimization knobs.

RF Planning

The following table summarizes Aruba's recommendations for AP placement, AP mounting and channel width selection when planning for deploying 802.11ax WLAN. For detailed description, please refer to 802.11ax Planning and Deployment Guidelines / RF Planning

Table 7: *Recommendations for RF Planning*

Feature	Recommendation
AP Mounting Recommendation	■ Ceiling mount got for campus APs. ■ Wall mount for hospitality.
AP Placement	■ Place AP's approximately 40 to 60 feet (13 - 20 meters) apart. ■ Minimum Received Signal Strength Indicator (RSSI) should be -55 dB throughout your coverage area. ■ SNR should always be greater than 35dB to achieve highest 1024-QAM modulation and data rates. ■ APs should be deployed in honeycomb pattern.
AP Forwarding Mode	■ Tunnel Mode is preferred. ■ Decrypt-Tunnel mode can also be used on a case-by-case basis.
Channel Width Selection	Use 80 MHz channel with DFS channels only if no radar signal interference is detected near your facility. Also make sure that your legacy clients do not have wireless issues with 80 MHz channels and if they do, deploy 40 MHz channels. Consider 40 MHz or 20 MHz channel widths for better channel separation.
Client Density per AP	The higher-end 550 series APs and 530 series APs can support up to 1024 associated clients per radio. Whereas APs from 500 and 510 series support maximum of 512 associated clients per radio.

WLAN Optimizations

NOTE

The performance of a Wi-Fi 6 network is heavily dependent on the clients, client drivers and OS versions in play. The following is a summary of recommended WLAN Optimization knobs for Wi-Fi 6 design and deployment as tested with clients available early in the market. Baseline/requirements may vary case by case.

Table 8: *Recommendations for WLAN Optimizations*

Feature	Default Value	Recommended Value	Description
Transmit Power	■ 5 GHz: Min 15 / Max 21 ■ 2.4GHz: Min 6 / Max 12	Leave it at default values and let Airmatch take care of these values.	**NOTE:** The difference between minimum and maximum Tx power on the same radio should not be more than 6 dBm. Tx power of 5 GHz radio should be 6 dBm higher than that of 2.4 GHz radio.

Feature	Default Value	Recommended Value	Description
Transmit Beamforming (TxBF)	Enable	Enable	■ Enables an AP to achieve high throughput.
OFDMA	Enable	Enable	■ Enable multiple devices to transmit and receive simultaneously. ■ Helps in high density environments with small-pack applications like IoT, Voice, etc.
MU-MIMO	Enable	Enable	■ Enables multiple devices to transmit and receive simultaneously. ■ Helps in achieving higher throughput.
11ax aware Client Match	Enable	Enable	■ Optimizes user experience by steering clients to the best AP.
High Efficiency (HE)	Enable	Enable	■ Keep this enabled to reap 802.11ax benefits. For more details refer to HE section.
IPM (feature flexibility)	Disable	Enable	■ It is recommended to have this feature enabled at all time. ■ IPM helps minimize the total power draw to maximize electrical power costs. ■ It can also help the AP to run fully enabled, even if it's connected to a PSE that provides less than the ideal power class.
Convert Broadcast ARP Requests to Unicast	Enable	Enable	■ Helps to convert broadcast ARP and DHCP packets to unicast.
Drop Broadcast and Multicast	Disable	Enable	■ Restricts all the broadcast and multicast traffic flooding into AP tunnels. ■ **Convert Broadcast ARP Requests to Unicast** must be enabled.

Feature	Default Value	Recommended Value	Description
AirGroup	Disable	▪ Enable it if MDNS, DLNA or other zero-configuration services are needed.	Allows Airplay and ChromeCast type of applications even if "Drop Broadcast and Multicast" feature is enabled
Dynamic Multicast Optimization (DMO)	Disable Alert: Do not enable without viewing specific requirements.	▪ Enable it if multicast streaming is needed. ▪ Set DMO client threshold to 80. ▪ Prioritize multicast stream using controller uplink ACL.	Converts multicast frames to unicast frames to deliver them at higher rates **NOTE:** IGMP Snooping or Proxy feature needs to be enabled for DMO to work.
Multicast Rate Optimization	Disable	▪ Enable	▪ Sends multicast frames at the highest possible common rate. ▪ Enable it even if DMO is enabled.

Fast Roaming Recommendations

Table 9: *Fast Roaming Recommendations*

Feature	Default Value	Recommended Value	Comments
Opportunistic Key Caching (OKC)	Enabled	Enabled	Avoids full dot1x key exchange during roaming by caching the opportunistic 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.
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

Feature	Default Value	Recommended Value	Comments
			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.

Deployment Specific Roaming Optimization Recommendations - General Enterprise and K-12/Higher Education

Table 10: *Roaming Optimization Recommendations for 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: 12,24 802.11a/ g ■ Transmit rates: 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. ■ For Dense Deployments use 24	Sends out beacons at the configured rate rather than lowest configured basic rate.

Feature	Default Value	Recommended Value	Comments
		Mbps	
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.

Table 11: *Roaming Optimization Recommendations for 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

NOTE

All warehouse deployments are based on the client devices being supported. Baseline/requirements for each device first needs to be understood prior to configuration. Please perform configuration based on device requirements.