aruba

a Hewlett Packard Enterprise company

MIDSIZE BUSINESS SELECTION GUIDE

CHOOSING THE RIGHT ACCESS POINT

As your business continues to grow, the need to hire more staff, support more customers, and expand into new ways of working grows along with it. This means more demand from devices, connections, and data sources on your network infrastructure.

But is your wireless network ready to handle the extra load?

While choosing the right access point for your network can be a challenge, knowing where to look and what variables to be aware of can make it easier to manage. Here are some helpful considerations to guide you along the way.

WHAT TYPE OF ACCESS POINT DO YOU NEED?

An access point (AP) connects to your access switching infrastructure to offer wireless local area network (WLAN) connectivity for devices of all kinds. Selecting the right access point starts with understanding the environment in which it's intended to operate.

Indoor access points

As the most common kind of AP, indoor access points are typically mounted on a wall or ceiling in a building or an otherwise enclosed space. They often play the heaviest role in any wireless network infrastructure, connecting everything from laptops to printers and other APs for wall-to-wall Wi-Fi coverage.

Remote access points

While they can usually mount on a wall or ceiling, a remote AP is often placed on a desk. They connect nearby devices with wired Ethernet in addition to providing Wi-Fi coverage. Remote access points are sometimes called hospitality APs due to their popularity in hotels and hospitality settings. Other places where they tend to be popular include small office/home offices, medical clinics, finance businesses, and remote working environments that need to enforce security policies outside the main building.

Outdoor access points

Outdoor access points are designed to endure everything from heavy winds to torrential downpours and extreme temperatures. They provide reliable connectivity in parking lots, open-air malls, and other outdoor locations. Be sure to identify IP water and dust resistance ratings, shock and vibration resistance, salt tolerance, and other conditions the outdoor AP can weather. The best place to find this information is in data sheets and certification records.

Ruggedized access points

Access points with ruggedized housing are built to withstand hazardous locations that contain flammable gases and chemicals. Ruggedized APs can double as outdoor APs, but some are indoor only.

If you're working in a chemical lab, industrial plant, or manufacturing facility, you may need a ruggedized access point. Be sure to check for any ratings and certifications that validate claims around where the AP will or will not function.

HOW MUCH PERFORMANCE IS ENOUGH?

After determining the types of access points you need for your growing business, the next step is to think about performance, including coverage, traffic volume, and technology for each part of your wireless network.

Wireless coverage

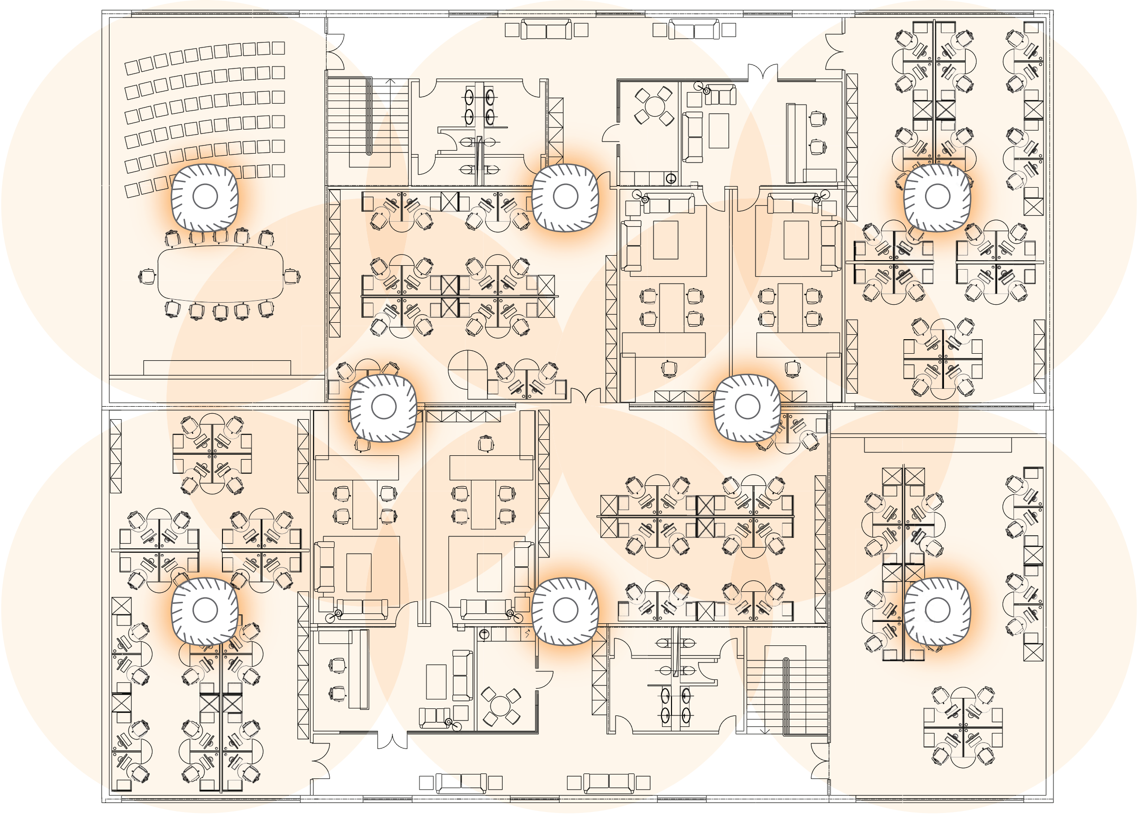
Wi-Fi works best and travels farthest when unimpeded by excessive noise or physical objects. While wireless access points have varied radio propagation characteristics, most have embedded omnidirectional antennas to distribute even wireless coverage.

Run a wireless spectrum analysis using the many free and paid tools available through your current networking equipment or online. You'll want to map out your floorplan and find weak or oversaturated signal areas to better optimize Wi-Fi coverage. By spreading out your APs or making power level adjustments, you can help reduce user complaints related to spotty service.

As you plan your layout, consider placing APs close enough to each other to create overlapping coverage for roaming and redundancy in cluster configurations. If you have internet of things (IoT) devices, you may need to place additional access points in specific locations, like along the perimeter of a building to support sensors and keyless door locks. In general, your floorplan and how far you spread out each AP from the next will determine how many you'll need to blanket your business with corner-to-corner Wi-Fi.

Traffic volume

Consider the types of software running on each device on your network and the function of its user — for example, an employee within the creative department may need to transfer larger files more frequently than a front desk associate or a salesperson. Once you have that outlined, the next step is to calculate the average volume of traffic each device will generate. You may already have these numbers with the help of your current networking equipment or a network analyzer tool.



Sample office access point layout.

Look at how the path of travel may impact your review of traffic volume. East-west traffic defines data movement from one device to another within your local area network (LAN). In deployments where this kind of traffic is heavy you may need faster wireless throughput or to review your switching port and uplink speeds.

North-south traffic defines data movement from a device within your LAN to the outside world through the internet. When running into north-south slowdowns, consider adjusting network quality of service policies and identifying whether you need an upgraded internet plan.

The maximum throughput requirements to support your average traffic volume will determine how fast the AP needs to be for a given location. Meeting rooms, collaboration stations, and other areas that use video conferencing may require more powerful access points. Be sure to account for signal degradation, overhead, and extra capacity to support network traffic changes due to business and operational growth.

Technology

Growing businesses depend on the speed and quality of their network to stay a cut ahead of the competition. Every few years, Wi-Fi technology evolves, releasing a new Wi-Fi standard to meet the ever-increasing demand for wireless access. The latest standards available today are Wi-Fi 6 and Wi-Fi 6E.

Unlike legacy standards, Wi-Fi 6 and 6E represent a significant speed and efficiency upgrade for all the ways we connect. They increase data modulation rates, add OFDMA for enhanced capacity, improve battery life for IoT devices, and enable MU-MIMO for downstream and upstream traffic.

Wi-Fi 6E represents the largest increase of unlicensed spectrum in history. It opens up the 6 GHz frequency and expands available bandwidth by 1200 MHz, providing more 80 MHz and 160 MHz channels to support high-definition video, AR/VR, and other use cases.

Access points with the latest standard perform better and have a longer lifespan, providing you with lasting value. As you purchase devices for employees or offer new business services, take a look at your wireless infrastructure and consider your expected growth over the next three to five years.

WHAT TYPES OF DEVICES DO YOU NEED TO CONNECT?

Network devices come in many shapes and styles, from laptops and mobile phones to sensors and medical equipment. It's not always possible or practical to connect everything using wired Ethernet. Striking a balance between resilience and flexibility here means looking at the different kinds of devices on your network and considering their needs and characteristics.

End-user devices

From desks to meeting rooms to collaboration stations, employees move around their workspace in the pursuit of productivity. When they do, their laptops, smartphones, and tablets tend to go along with them. These kinds of end-user devices depend on strong Wi-Fi connectivity to remain mobile.

Creating a seamless wireless network for mobility requires access points that can support roaming, often in a mesh or cluster topology where each AP can be connected and aware of other APs within the same segment. Another capability to look for is intelligent load balancing, which helps prevent slow connections and overburdened APs by adjusting where and how each device is connected.

Guest Devices

Whether it's to support business meetings, local ordering, or other standard services, many businesses offer wireless connectivity to customers, partners and visitors. However, letting outside devices connect to your business network can be a big threat to your security.

To minimize risk, IT professionals prefer to isolate guest devices to APs that broadcast a separate guest network. Security can be further enhanced through common practices like using a captive portal to serve a branded webpage with terms-of-service details. Like end-user devices, guest devices often tend to move around and can also benefit from the same AP capabilities.

Internet of Things (IoT) devices

While some IoT devices can connect directly to wired or Wi-Fi infrastructure, others require a separate hub as an intermediary for connectivity and analytics. With low bandwidth demands and wide applications for process improvement, automation, and data collection, many growing businesses plan to adopt IoT devices to enhance and complement services. A considerable drawback, however, is that they tend to be more vulnerable to cyberattacks due to the absence of embedded endpoint security.

Access points that offer Zigbee and Bluetooth radios give businesses the option to skip the hub while adding individual device visibility for granular IoT monitoring. To reduce risk and enhance security posture, look for APs that can pass IoT traffic through a role-based policy enforcement firewall for inspection and segmentation, limiting access to only the parts of the network it needs to function.

Other access point devices

Access points can be used to connect other APs in a point-to-point fashion, wirelessly delivering network and internet access from one building to the next. To effectively bridge connectivity over a large space, look for APs that have directional antennas or RP-SMA connectors and antenna accessories to ensure wireless signal quality stays strong. You may also need to look at gateways to ensure seamless building-to-building wireless connectivity.

HOW IMPORTANT IS NETWORK SECURITY?

As companies adopt technology to address business needs, they continuously face new security challenges. From employee-owned phones to guest devices and autonomous IoT equipment, every new device on the network can increase the attack surface, requiring IT professionals to re-think risk mitigation plans.

When combined with malicious intent, common network threats like unauthorized access to data and leaks of privileged information can be not only damaging but catastrophic to business operations. Despite the significant degree of human error involved in security breaches, your access points can support risk mitigation efforts.

It starts with wireless encryption, the latest of which is WPA3-Enterprise, introduced alongside Wi-Fi 6 and 6E. This version solved several issues that WPA-2 had, enhancing encryption strength to 192-bit and applying a different algorithm for each session. In addition to WPA3-Enterprise, Enhanced Open authentication has replaced the legacy open unencrypted wireless.

As your business grows, so too does your attack surface and your risk of being targeted. If it's not already in place, this is when you should seriously consider a multi-layered security strategy. Embracing adjacent hardware and services like gateways and policy enforcement firewalls can be a big help, using deep packet inspection to isolate, segment, and enforce role-based access policies.

The right access point for your deployment should support company security stances, deliver the latest in wireless encryption, give the right degree of control over network privileges and policies, and deliver the right amount of access for your people to be productive.

HOW DO YOU PLAN TO MANAGE THE NETWORK?

No matter the access point, its management interface is where most IT staff will spend their time. They perform tasks like deploying and configuring new hardware, onboarding and assigning segment policies to new employee devices, and implementing changes as a result of complaints, data-informed insights, and troubleshooting.

For many, management can be a question of preference. Older access points offered command line interface (CLI) configuration or depended on external hardware for management and control, adding cost for the benefit of scale.

More recent access points maintain CLI capabilities and additionally embed an operating system with a web GUI that enables intelligence and management with added cluster control, configuration, and redundancy.

When a network is smaller, IT generalists can manage a handful of access point clusters and switches through a web GUI. It's even possible to use VPN capabilities to manage remote worksites this way. As a growing business expands its networking infrastructure, however, the manual effort required by this method can become too extensive to manage.

That's why modern networking equipment offers on-premise and cloud-based management solutions. Simplicity and usability are often improved with the transition from web UI to software, paving the way for centralized network management. The ability to have every business site and networking device accessible and configurable from behind a single, secure log-in provides unparalleled business scale.

When reviewing management solution options for a selected access point, you may want to consider whether it offers any time-saving capabilities. A small or one-person IT team, for example, may be interested in workflow templates and automation to streamline repetitive tasks and reduce workload. They may also benefit from artificial intelligence, machine learning, and real-time reporting systems that are designed to proactively uncover challenges and help implement solutions before they might become an internal email or a ticketed issue.

ARUBA ACCESS POINTS FOR MIDSIZE BUSINESSES

With Aruba, you can put your network to work for you, using smart, scalable, and secure access points that keep your business in the fast lane.

Aruba wireless solutions include a variety of indoor, outdoor, remote, and ruggedized APs that deliver seamless, corner-to-corner coverage to every employee, guest, and device on your network. Deploy Aruba APs with a gateway, Aruba Central management, or in Instant Mode for cluster configuration, Wi-Fi optimization, and best-in-class security.

They're easy to set up, scale, and manage, helping you resolve issues faster and freeing up IT resources to support business growth of any kind — all while keeping your people, data, and customers safe.

Whether you're expanding your Wi-Fi network inside or out, Aruba has you covered with expertly engineered equipment backed by global support services and an industry-leading limited lifetime warranty on all indoor and outdoor APs.

ADDITIONAL RESOURCES

- Learn more about indoor APs, outdoor APs, and remote APs on the Aruba website.
- Looking for a tailored recommendation? Try the Product Finder.
- Contact us if you're ready to get started.

COMPARISON CHART

Aruba Access Points	500H Series	500 Series	510 Series	530 Series	550 Series	630 Series
Access point type	Remote/Hospitality	Indoor	Indoor	Indoor	Indoor	Indoor
Wi-Fi generation	Wi-Fi 6	Wi-Fi 6	Wi-Fi 6	Wi-Fi 6	Wi-Fi 6	Wi-Fi 6E
Combined peak wireless data rate	1.49 Gbps	1.49 Gbps	2.69 Gbps	2.97 Gbps	5.37 Gbps	3.9 Gbps
Client count per radio — practical (maximum)	75 (256)	75 (256)	100 (512)	150 (1024)	150 (1024)	100 (512)
Supported radios	2.4GHz 5Ghz	2.4GHz 5Ghz	2.4GHz 5GHz	2.4GHz 5GHz	2.4GHz 5GHz	2.4GHz 5GHz 6GHz
Radio MIMO type spatial streams	2x2:2	2x2:2	2x2:2 (2.4GHz) 4x4:4 (5GHz)	4x4:4	4x4:4 for 2.4GHz 8x8:8 for 5GHz (dual 4x4:4 for 5GHz)	2x2:2
HE160 bandwidth support[1]			●	●	●	● (6 GHz Only)
OFDMA (RUs)	● (8)	● (8)	● (16)	● (37)	● (37)	● (8/8/37)
Multigig ethernet	● (1x 2.5, 4x 1Gbps)[2]	1x 1Gbps	● (1x 2.5, 1x 1Gbps)	● (2x 5Gbps)	● (2x 5Gbps)	● (2x 2.5Gbps)
Physical size (mm)	86 x 150 x 47	160 x 161 x 37	200 x 200 x 46	240 x 240 x 57	260 x 260 x 61	220 x 220 x 51
Weight (g)	360	500	810	1270	1570	1300

1. HE160 only available for 5 GHz and 6 GHz
2. AP-505H Only. AP-503H has 1x 1, 2x 1 Gbps ports.

COMPARISON CHART

Aruba Access Points	560 Series	570 Series	518 Series	560EX Series	570EX Series
Access point type	Outdoor	Outdoor	Ruggedized Indoor	Ruggedized Outdoor	Ruggedized Outdoor
Wi-Fi generation	Wi-Fi 6	Wi-Fi 6	Wi-Fi 6	Wi-Fi 6E	Wi-Fi 6E
Combined peak wireless data rate	1.49 Gbps	3.00 Gbps	3.00 Gbps	1.49 Gbps	3.00 Gbps
Client count per radio — practical (maximum)	50 (256)	100 (512)	100 (512)	50 (256)	100 (512)
Supported radios	2.4GHz 5GHz	2.4GHz 5GHz	2.4GHz 5GHz	2.4GHz 5GHz	2.4GHz 5GHz
Radio MIMO type spatial streams	2x2:2	2x2:2 4x4:4 (5GHz)	2x2:2 4x4:4 (5GHz))	2x2:2	2x2:2 4x4:4 (5GHz)
HE160 bandwidth support[1]		●	●		●
OFDMA (RUs)	● (8)	● (16)	● (16)	● (8)	● (16)
Multigig ethernet	1x 1Gbps	● (1x 2.5, 1x 1Gbps)	● (1x 2.5, 1x 1Gbps)	1x 1Gbps	● (1x 2.5, 1x 1Gbps)
Physical size (mm)	160 x 160 x 121	240 x 240 x 270	211 x 211 x 70	160 x 160 x 121	240 x 240 x 270
Weight (g)	1030	2500	1500	1030	2500
Operating conditions	**Temperature:** -40° C to +55° C with full solar loading **Humidity:** 5% to 95% non-condensing internal **Operating Altitude:** 3,000 m **Water & Dust:** IP66/67 **Salt Tolerance:** Tested to ASTM B117-07A Salt Spray 200hrs **Wind Survival:** Up to 165 Mph **Shock & Vibration:** ETSI 300-19-2-4	**Temperature:** -40° C to +65° C with full solar loading **Humidity:** 5% to 93% non-condensing internal **Operating Altitude:** 3,000 m **Water & Dust:** IP66/67 **Salt Tolerance:** Tested to ASTM B117-07A Salt Spray 200hrs **Wind Survival:** Up to 165 Mph Shock & Vibration: ETSI 300-19-2-4	**Temperature:** -40° C to +65° C with full solar loading **Humidity:** 5% to 93% non-condensing internal **Operating Altitude:** 3,000 m **Water & Dust:** IP55 **Shock & Vibration:** ETSI 300-19-2-4	**Class 1 Division 2 certified** **ATEX Zone 2 certified** **Temperature:** -40° C to +55° C with full solar loading **Humidity:** 5% to 95% non-condensing internal **Operating Altitude:** 3,000 m **Water & Dust:** IP66 **Salt Tolerance:** Tested to ASTM B117-07A Salt Spray 200hrs **Wind Survival:** Up to 165 Mph **Shock & Vibration:** ETSI 300-19-2-4	**Class 1 Division 2 certified** **ATEX Zone 2 certified** **Temperature:** -40° C to +65° C with full solar loading **Humidity:** 5% to 95% non-condensing internal **Operating Altitude:** 3,000 m **Water & Dust:** IP66 **Salt Tolerance:** Tested to ASTM B117-07A Salt Spray 200hrs **Wind Survival:** Up to 165 Mph **Shock & Vibration:** ETSI 300-19-2-4

[1] HE160 only available for 5 GHz and 6 GHz

ALL ARUBA ACCESS POINTS SUPPORT THE FOLLOWING:

- AP clustering
- Load balancing (Client Match)[3]
- RF optimization (AirMatch)[3]
- SLA-grade application assurance (AirSlice)[3]
- WPA3 encryption and enhanced open
- Captive portal and guest network services
- Policy enforcement firewall
- Flexible management: Aruba Central (cloud and on-prem), Aruba Instant Mode, web UI, console port

3. Add-on License or Aruba Central Management required

a Hewlett Packard
Enterprise company

BSG_SMB_Choosing-Right-AP_031022 a00121491enw EM

Contact Us **Share**