aruba
a Hewlett Packard
Enterprise company

Modernizing Mobility in Federal

SEAMLESS MOBILITY WITH WI-FI 6, WI-FI 6E, AND 5G TO SUPPORT MISSION OUTCOMES

TABLE OF CONTENTS

Selecting mobile communication technologies used to be simpler: Use wireless LANs to connect laptops, phones, and other devices in offices and campuses and use cellular to connect devices over long distances. But as wireless LAN and cellular technology evolved to meet the requirements of a digital-first world, U.S. federal IT leaders gained a slew of new choices: Wi-Fi 6, Wi-Fi 6E, and 5G.

As Wi-Fi and cellular have overlapping some capabilities, there has been contention in the industry that Wi-Fi 6/6E and 5G are either/or propositions. The reality is that no one mobility technology can do it all.

At Aruba, we believe Wi-Fi and cellular technologies are complementary. Most federal organizations will deploy Wi-Fi networks for indoor, campus, and home office connectivity, especially as agencies upgrade from legacy Wi-Fi technologies to the faster, more secure Wi-Fi 6 and Wi-Fi 6E. Wi-Fi is a smooth on-ramp to 4G/5G cellular networks or an agency's WAN.

Adding to nuances of decision-making are new deployment models, including cloud-managed networks and Network-as-a-Service (NaaS), which present alternatives to on-premises controller architectures.

Let's take a closer look at how Wi-Fi 6, Wi-Fi 6E, and 5G fit together, their use cases, and deployment choices for federal.

A WI-FI 6 REFRESHER

Most new wireless LAN deployments today are Wi-Fi 6. In fact, the Wi-Fi 6 segment accounted for 74% of the overall wireless LAN market share in 2022, according to Grandview Research. Designed for high-density campus wireless deployments, Wi-Fi 6 (802.11ax) delivers a step-change in performance with up to 4X more throughput capacity than legacy Wi-Fi 5 (802.11ac). It also delivers optimized use of the 2.5 GHz and 5 GHz bands, delivering a better experience for staff, whether they have older mobile or new ones, whether they are calling, texting, or using their apps.

As agencies modernize their campus networks, Wi-Fi 6 is the logical choice for campus environments with high mobility needs or heavy usage of voice and video. Wi-Fi 6 brings the advantage of secure connectivity, as it supports WPA3, the strongest available security for Wi-Fi, making it the default choice for security-conscious deployments and work from home. Enhanced Open simplifies and secures guest Wi-Fi as well. Wi-Fi 6 also introduced a capability to extend the battery life of IoT devices by allowing APs to ping IoT devices, such as cameras, locks, or sensors, at longer intervals.

WHAT IS WI-FI 6E?

Wi-Fi 6 has been the logical upgrade path for legacy wireless LANs. But recently, IT decision-makers have another choice for campus connectivity: Wi-Fi 6E.

Wi-Fi 6E operates in the 6 GHz spectrum, whereas Wi-Fi networks have traditionally operated in the 2.4GHz and 5 GHz bands. In 2021, the Federal Communications Commission (FCC) opened up the use of the 6 GHz band, which nearly tripled the spectrum available for Wi-Fi. In just two years, some 60 countries have announced or enacted 6 GHz regulations, leading to massive increases in unlicensed spectrum available for Wi-Fi and the prospect of global harmonization.

The "E" in Wi-Fi 6E stands for "Extended" since Wi-Fi 6E extends the capabilities of Wi-Fi 6 to the 6 GHz band for more capacity, wider channels, and less interference. Only 6-GHz-capable devices can use the band, so there's no interference from microwaves, cordless phones, and legacy 2.4-GHz devices. Wi-Fi 6E also mandates the use of WPA3, the strongest Wi-Fi security, making it the default choice for the most security-conscious deployments.

Three Types of Wi-Fi 6E Access Points

Point-to-point microwave for public safety and mobile backhaul, satellite services, and television broadcasters currently use the 6 GHz band, and interference with these incumbent (and licensed) users must be avoided. As a result, there are three types of Wi-Fi 6E access points.

- **Standard power (SP)** APs support outdoor and indoor operations, which are coordinated through an Automated Frequency Coordination (AFC) service that mitigates possible interference with the incumbent users' 6 GHz services.
- **Low Power Indoor (LPI)** APs are used in indoor campus deployments. As the name suggests, LPI APs use lower power and thus can operate without an AFC. Coverage is similar to Wi-Fi 6 APs.
- **Very Low Power (VLP)** APs are designed to support both mobile indoor and outdoor uses. It is most applicable to in-vehicle use cases or for a personal area network to connect AV/VR headsets to computers or consoles.

Growing Wi-Fi 6E Momentum

While Wi-Fi 6 has the biggest market share today, Wi-Fi 6E sales will grow steadily as more Wi-Fi-6E-capable devices come to market. Grandview Research estimates that more than 7 billion Wi-Fi 6E devices will be sold by 2030.

Wi-Fi 6E is ideal for greenfield deployments or applications that need multiple gigabits of speed or low-latency requirements, such as augmented/ virtual reality used for training exercises, telepresence, or secure, ultra-reliable voice calls. Intelligence, surveillance, and reconnaissance can be supported with high-def video streamed from Wi-Fi 6E devices. Wi-Fi 6E will typically be deployed in one area of the network, and in conjunction with Wi-Fi 6 for broader use.

Wi-Fi 6E can be leveraged for sensors and other IoT devices that used for smart building or smart base services, such as environmental controls or physical safety and security. Healthcare facilities that have dense deployments of clinical and biomedical devices are likely to be early adopters of Wi-Fi 6E to ensure that clinicians and staff have highly responsive application access as they move around the campus.

Wi-Fi 6E is also well suited for large campuses with high device densities, universities as well as large public venues like airports, stadiums, and convention centers.

There is a cost consideration to deploying Wi-Fi 6E, although the performance increase may make it worthwhile. Beyond the APs, the decision must include practical considerations, such as the use of high-spec cable, such as Cat 6 or 6A. Edge switches should support Smart Rate gigabit Ethernet ports with PoE++ to accommodate the higher power consumption of Wi-Fi 6E access points.

SHOULD YOU WAIT FOR WI-FI 7?

Wi-Fi 6, Wi-Fi 6E, and now people are talking about Wi-Fi 7? Wi-Fi 7 (802.11be) is the next-generation, emerging standard from the Wi-Fi Alliance. It builds on Wi-Fi 6E and increases data rates through the use of 320 MHz channels. We expect that Wi-Fi 7 products will be available in 2024 or 2025. If your agency waits, you'll miss out on the immediate security and performance enhancements that Wi-Fi 6/6E can bring to agency staff and constituents.

WI-FI 6 VS. WI-FI 6E

BAND	2.4 and 5.0 GHz spectrum	2.4, 5, and 6 GHz spectrum (Devices must be 6 GHz enabled.)
FEATURES	• Multi-user efficiencies, multi-user input/output (MU-MIMO) to remove bottlenecks • OFDMA to create "carpool lanes" to piggyback smaller packets like voice • Target Wake Time (TWT) to allow APs to ping IoT devices at longer intervals and reduce traffic and extend battery life • WPA3 and Enhanced Open to enhance guest access security	• Includes all features in Wi-Fi 6 plus: • More capacity in the 6 GHz band • Wider channels, up to 160 MHz, which are ideal for HD video and virtual reality • No interference from microwaves, etc. because only 6E-capable devices can use the band
BENEFITS	Increased efficiencies to provide greater throughput with the same number of APs, ideal for dense environments and large numbers of IoT devices	Greater capacity and wider channels to support multigigabit traffic, ideal for HD video and AR/VR

WI-FI 6/6E IS AN ONRAMP TO 5G

The 5G transformation has been underway with promises to deliver faster download speeds with lower latency and better suited to edge computing and IoT device connectivity. But service providers' rollout of global 5G has been slower than expected, given the radical architecture change from 4G/LTE.

Getting a reliable cell signal inside a building is often challenging, and spotty indoor coverage is expected to continue, given the nature of 5G and more efficient building construction. For that reason, 5G is unlikely to become the network technology of choice for campus networks. However, people will still expect their calls and applications to stay connected as they move from a cellular network to an indoor private network. The Wi-Fi Alliance Passpoint® solution makes this transition even more seamless, as it streamlines Wi-Fi access and eliminates the need for users to find and authenticate to a network each time they visit.

5G is ideal for security mobility across long distances, such as to support voice, video, and training. 5G can help improve situational awareness for first responders and support tactical operations. 5G-enabled medical centers can have far-reaching impacts for veterans and their families, improving clinical training, patient diagnoses and clinical training, leading to better care for veterans and their families.

SEAMLESS MOBILITY REQUIRES BOTH WI-FI AND CELLULAR

Federal IT leaders can choose the best combination of mobile communications technologies to meet their use cases. In many cases, it will be a combination of fit-for-purpose Wi-Fi 6/6E and cellular technologies.

Hybrid work is a continued reality across agencies both large and small. Modernizing the office Wi-Fi to the newer Wi-Fi 6/6E is ideal to support the tools of the hybrid workplace: videoconferencing, virtual desktop environments, and access to cloud-based apps.

Government healthcare providers will likely use a combination of Wi-Fi 6/6E and 5G to deliver on connected health initiatives, as hospitals need pervasive Wi-Fi in their facilities to connect clinician, staff, and biomedical devices as well as 5G to support telehealth, robotic surgery, and remote patient monitoring.

Similarly, Wi-Fi 6/6E at agency bureaus or a military base and 5G for the WAN can support more responsive logistics and operations, including tracking of high-value assets and robots. 5G is ideal to provide smooth coverage to support AR/VR for immersive mission planning and connectivity for autonomous vehicles and drones in tactical operations.

ARUBA MOBILITY SOLUTIONS SUPPORT THE MISSION

At Aruba, we understand that network modernization is a journey for federal and we are committed to providing highly capable, secure, and resilient network solutions that meet the objectives of military and civilian agencies, whether large or small.

Aruba has consistently been a leader in delivering secure network connectivity and services to all parts of the federal government. Aruba products and solutions carry long list of government security certifications and compliance, including Common Criteria EAL-45, FIPS 140-2 Validation, DoD directives 8100.2 and 8420.01, and FedRAMP Authorized.

Aruba offers a portfolio of indoor, outdoor, and remote access points that support the latest Wi-Fi 6/6E as well as Wi-Fi 5, for use indoors, outdoors, in hazardous locations, and remote workers. Zero-touch provisioning makes it easy to roll temporary Wi-Fi to support emergency response.

With Aruba, federal IT leaders can choose the best-fit Wi-Fi technology for offices, hospitals, warehouses, temporary locations, or home offices, with superior network experiences for both older and the latest phones, tablets, laptops, and IoT devices.

For agencies ready to deploy Wi-Fi 6E to support their most demanding indoor environments and the newest devices, the Aruba 650 Series AP that is fully equipped to deliver faster performance, wider channels, and minimize interference. Our flagship campus Wi-Fi 6E APs deliver 7.8 Gbps maximum aggregate data rates and 4x4 MU-MIMO. Aruba 650 Series APs are IoT- and location-ready.

For mixed environments, the Aruba 630 Series is a tri-band AP that is also IoT- and location-ready. The 6 GHz band is used for the latest Wi-Fi-6E-capable devices; the 5 GHz band for mainstream, high-performance devices that are not 6 GHz-capable, and IoT or legacy devices in the 2.4 GHz band. The 630 Series delivers 3.9 Gbps maximum aggregate data rates.

Users and devices will seamlessly move between Aruba Wi-Fi and cellular networks. Aruba Air Pass, based on the foundations of Passpoint and Wi-Fi calling, creates a roaming network and enhances the user experience.

Deployment Your Way

With Aruba, IT decision-makers also have a choice of deployment options: traditional mobility controller and gateway architectures, cloud-managed networks, and the new Network-as-a-Service (NaaS) model.

Many agencies deploy their wireless and wired networks through the Aruba Mobility Controller, Aruba Access Points, Airwave Management System, and ClearPass Policy Management system, with network elements managed from on-premises. The Mobility Controller serves as the centralized control point for mobility, security, policy management, and remote access. Agencies can upgrade legacy Wi-Fi with Aruba Wi-Fi 6 and Wi-Fi 6E APs. Add on location services to track valuable assets or deliver new experiences like helping visitors and staff find their way around large facilities.

For those ready to consider a move to cloud-managed networks, Aruba Central is the only all-in-one cloud-native network management system to achieve FedRAMP Authorization. With Aruba Central, agencies can deliver secure, reliable wired and wireless connectivity to staff and guests in today's highly distributed world, while simplifying the management of wireless and wired networks, remote users, and SD-WAN. With Aruba Central, IT staff no longer need to update software on Mobility Controllers or firmware on APs.

Aruba Central brings the advantage of unified infrastructure, AIOps, and edge-to-cloud security, combined with certified cloud security, to Federal organizations. Advanced analytics and AIOps can automatically identify network, security, and performance issues, allowing IT to proactively solve issues before they can impact the user experience. A Zero Trust foundation is built in, giving IT the visibility, control, and enforcement needed to rising cybersecurity threats.

NaaS offers a flexible way to consume network services. HPE GreenLake for Aruba offers NaaS, which is ideal for cloud or edge use cases, which allows IT teams to stop building and operating wired and wireless networks and start consuming them.

LEARN MORE

Aruba solutions for U.S. federal overview

What is Wi-Fi 6 and Wi-Fi 6E

Common Criteria and other U.S. federal certifications for Aruba products and solutions

a Hewlett Packard
Enterprise company

www.arubanetworks.com | info@arubanetworks.com