6 Strategies to Modernize Your Wireless Network

How to refresh your Wi-Fi to support new workplace requirements

aruba
a Hewlett Packard Enterprise company

CONTENTS

INTRODUCTION

While investments in IT infrastructure either stagnated or decreased during 2020 and into 2021, new demands on networks—especially Wi-Fi networks—surged. Today, IT is tasked with modernizing Wi-Fi to support new workplace initiatives while also streamlining operations. This eBook outlines 6 strategies that help IT redefine the wireless experience in the workplace, while at the same time gaining greater operational efficiency and agility.

THE NEW WORKPLACE EXPERIENCE

AROUND THE WORLD, organizations are dealing with a changing workplace.

Consider **Maya**, based in the US, who now spends 2-3 days a week in the office and the remainder working from home.

- Maya is running late so she logs into her meeting using outdoor Wi-Fi directly from the parking garage.
- Once in the building, she seamlessly connects to indoor Wi-Fi and badges in, activating a concierge application that helps her locate the meeting room via wayfinding to continue her meeting in person.
- Between meetings, she works from a hot desk connecting to business-critical software-as-a-service (SaaS) applications over Wi-Fi.
- Later she joins a brainstorming session in a designated collaboration area and briefly responds to a call from home using Wi-Fi calling.
- At the end of the day, Maya heads out, ready to work from home the next day.

Amir, a doctor in Asia, needs immediate access to high-resolution images before discharging his patient.

- A newly installed wireless network provides multi-gigabit speeds to support high-bandwidth, advanced medical imaging systems.
- Throughout the hyper-aware healthcare facility, thousands of Internet of Things (IoT) devices monitor air quality and safety, connecting over Wi-Fi to analyze and identify any issues.
- Later at home, Amir uses a secure remote access point connection to update medical records and protect patient privacy.

Jules and Julie, grocery warehouse supervisors in separate EU countries, must determine the impact of the latest supply chain disruption.

- As they visit facilities, they receive daily and interim reports from ports and partners about what's on schedule and what's not.
- They keep team members up to date across vast campuses that include refrigerated sections and loading docks.
- Both receive real-time alerts from the warehouse about inventory shortages and shipping delays.

THE EVOLVING NETWORK

WHAT DO ALL THESE SCENARIOS have in common? The wireless network, serving as the on-ramp of the digital workplace. As described in the scenarios above, modern Wi-Fi:

- Establishes **secure connections** to corporate data from any location — at work, on a remote site, at home, indoors, and outdoors.
- Ensures **high-capacity, low-latency connectivity** to support rich data sources and real-time interaction.
- Equips organizations with **seamless coverage** over wide physical areas.
- Enables **location-aware** applications such as wayfinding and asset tracking.
- Supports many different types of sensors and can make **intelligent inferences** from large volumes of telemetry data.

As the workplace evolves, the network must also evolve to support the new definition of where and how work gets done. "The hybrid network is here to stay," says Zeus Kerravala, founder and principal analyst of ZK Research. "There are more devices, more bandwidth, and an overall expansion of the network."

As new endpoint/IoT devices are added and wireless networks expand to new spaces such as cafeterias and outdoor spaces, aging Wi-Fi networks are overburdened. The increased use of video and collaborative technologies has increased the volume of data passing through existing infrastructure, causing bandwidth issues. "I think many companies don't really have a wireless network that is suitable for the new workplace," says Kerravala.

Post pandemic, many organizations face two years of stagnating technical debt tied to increased security risks and user complaints of poor Wi-Fi performance. Some still rely on wired connections, limiting the flexibility to work anywhere.

A poor network experience that impacts business innovation and user satisfaction is something organizations can no longer afford. The good news? Here are six recommendations that can help IT leaders address the most pressing challenges around network modernization.

> *"I THINK MANY COMPANIES DON'T REALLY HAVE A WIRELESS NETWORK THAT IS SUITABLE FOR THE NEW WORKPLACE."*
>
> *— Zeus Kerravala, ZK Research*

MEETING NEW WORKPLACE REQUIREMENTS

CHALLENGE #1: WORK IS NO LONGER DEFINED BY WHERE EMPLOYEES SIT, PLACING NEW DEMANDS ON NETWORKS.

STRATEGY 1

Rearchitect the WLAN to improve the workplace experience

IN MANY WORKPLACES, employees spend less time at desks and more time in collaboration areas or even outdoors, necessitating a reassessment of coverage models. Employees are less likely to be assigned to specific desks (known as hoteling). "This is where companies need to do the homework and proper planning to make sure what they're putting in now works today, but also in the foreseeable future," says Kerravala.

Corporate real estate teams are becoming "workplace experience" teams, partnering with IT to meet the new requirements for collaboration, hoteling, and AV. Hybrid workplaces need to support a mix of in-person and remote workers over video conferencing applications, requiring high bandwidth, low latency connectivity.

To deliver the highest-quality experience, teams must refresh the campus network to better address provisioning challenges, support remote workers, ensure network and application performance, and proactively troubleshoot issues that impact workers. In addition, organizations that have not already done so should move to a wireless-first model, removing wired connections that leave employees tethered to their desks.

HERE'S HOW TO SUPPORT THE FUTURE OF WORK:

- **Revisit the WLAN coverage model** to account for higher-density collaboration areas and video conferencing demands. With previous generations of Wi-Fi, dense deployments needed to use 40 MHz channels to avoid interference. By taking advantage of additional spectrum in the 6 GHz band, Wi-Fi 6E access points (APs) provide more 80/160 MHz channels for high-bandwidth, low-latency applications like high-definition video.
- **Enforce application service levels** by assigning necessary application priority and bandwidth. For example, business-critical video collaboration tools can be assigned high priority while streaming sports on YouTube is deprioritized. Prior to Wi-Fi 6, the network infrastructure was unable to control scheduling or to segregate traffic to guarantee that resources would be allocated to match quality of service requirements. Wi-Fi 6E builds upon Wi-Fi 6 by offering additional spectrum and scheduling capabilities.
- **Add wayfinding and other location-based services** to help employees navigate to hot desks and meeting rooms using a wide variety of client devices. Select Wi-Fi 6 and Wi-Fi 6E APs that include indoor location-ranging capabilities based on fine time measurement and built-in GPS receivers to allow APs to automatically locate themselves. This equips IT to develop highly accurate wayfinding applications and other indoor location services, including location-based analytics using universal reference coordinates (latitude and longitude).

SUPPORTING THE FUTURE OF WORK

- Revisit the WLAN coverage model
- Enforce application service levels
- Add wayfinding and other location-based services

CHALLENGE #2: LEGACY TECHNOLOGY CAN'T COMPETE WITH AT-HOME NETWORKS.

STRATEGY 2

Address workplace technical debt with new Wi-Fi advances

AFTER SEVERAL YEARS OF DELAYS, it is critical to modernize, centralize, and simplify the network. Older generations of Wi-Fi like Wi-Fi 4 and 5 are challenged by lower data rates and less secure password/guest encryption. They also lack newer technologies like multi-user, multiple-input, multiple-output technology (MU-MIMO) and orthogonal frequency-division multiple access (OFDMA) that provide multi-user efficiencies and increase performance.

Wi-Fi 6 and 6E APs enable enterprises both large and small to deliver seamless and secure connectivity. Both are based on the 802.11ax standard, offering greater efficiency and traffic flow as well as backward client and device compatibility.

The difference: Wi-Fi 6E extends the benefits to the 6 GHz band to deliver up to 1200 MHz of clean spectrum and true multi-gigabit connectivity. This solves connection and congestion issues, offers wider channels (up to 160 MHz), which are ideal for high-definition video and virtual reality, and less interference.

HERE'S HOW TO PREPARE:

- **Determine whether Wi-Fi 6 or 6E** best supports your needs while considering supply chain constraints.
- **Wherever possible, deploy Wi-Fi 6E APs** to extend refresh cycles by 2+ years; these support greater device density, more ultrawide channels (ideal for high-bandwidth applications), and true multi-gigabit speeds. Ensure that your solution takes advantage of the 6 GHz band via fine-grained, dynamic filtering that eliminates channel interference between the 5 GHz and 6 GHz bands.
- **Don't wait for Wi-Fi 7.** Wi-Fi 6E brings the benefits of up to 1200 MHz of clean spectrum and wider channels to organizations and individuals right now. According to Chris Depuy, Technology Analyst with the 650 Group, "Leading Enterprise WLAN companies began placing orders for Wi-Fi 6E chips over a year ago and they are taking shipments of those chips today. Today, there are no Wi-Fi 7 chips available. We anticipate that by the time Wi-Fi 7 access points shipments become meaningful, Wi-Fi 6E will represent significantly over a quarter of all access points shipped."
- **Select Wi-Fi Alliance tested and certified technology** and look for a lifetime warranty.

ADDRESSING TECHNICAL DEBT

- Select Wi-Fi 6 or 6E to support needs
- Wherever possible, deploy Wi-Fi 6E APs
- Don't wait for Wi-Fi 7
- Select Wi-Fi Alliance tested and certified technology

CHALLENGE #3: IT'S A STRUGGLE TO MANAGE TODAY'S COMPLEX HYBRID ENVIRONMENTS WITH EXISTING IT STAFF, MANUAL PROCESSES, AND ON-PREM SILOED MANAGEMENT CONSOLES.

STRATEGY 3

Drive greater agility with cloud-based management advances

A CLOUD-BASED NETWORK MANAGEMENT MODEL can simplify IT operations, improve agility, and reduce costs by unifying management of all network infrastructure, allowing IT teams to meet greater demands with constrained resources. It also enables network as a service (NaaS). In fact, technology market research firm IDC predicts that 50% of new wireless implementations will be cloud managed.

In a cloud network management model, a centralized interface for managing wireless, WAN, and wired networks in distributed environments simplifies network deployment, maintenance, and management. This enables Zero Touch Provisioning and GUI-driven workflows to speed up implementation.

Simply put, cloud-based microservices architectures better support continuous innovation at scale as organizations evolve network services and roll out new applications.

Despite the advantages, not all organizations are ready to move to the cloud. "A cloud-first foundation enables the automation enhancements that will help organizations implement self-driving networks, and many of our customers are taking that path," says Chuck Lukaszewski, wireless CTO at Aruba, a Hewlett Packard Enterprise company. "Those not yet ready can take advantage of on-premises network management that will allow them to move to a cloud-first model when they are ready."

HERE'S HOW TO PLAN YOUR CLOUD JOURNEY:

- **Determine your organization's cloud readiness.** Select a flexible solution that can be used either on-prem, in the cloud, with unified APs that support both deployment modes.
- **Identify an area to prototype**. Select a lab, new building, or remote work infrastructure to test cloud management.
- **Avoid "swivel chair management."** Focus on unifying views across devices and users; wireless and wired; and campus, branch, and remote environments.
- **Partner with your security team**. Factor in integrated capabilities to support Zero Trust network access, AI-powered endpoint profiling, and secure access service edge (SASE).

PLANNING YOUR CLOUD JOURNEY

- Determine your organization's cloud readiness
- Identify an area to prototype
- Avoid "swivel chair management"
- Partner with your security team

CHALLENGE #4: TODAY'S HYBRID WORKPLACES ARE TOO COMPLEX FOR MANUAL CORRELATION DUE TO INCREASED NETWORK SIZE, VOLUME OF TRAFFIC, AND DIVERSITY OF DEVICES AND APPLICATIONS.

STRATEGY 4 Leverage AIOps and automation to resolve issues and optimize IT resources

TO IMPROVE THE WORKPLACE EXPERIENCE and reduce demands on networking teams, 30% of enterprises will adopt AI-enabled tools to augment traditional monitoring approaches by 2023, according to Gartner.[1]

AI capabilities enable analysis of massive amounts of metadata in the cloud. Machine learning translates raw telemetry into clear insights and recommendations that identify issues and increase performance benefits – often without new infrastructure.

Key benefits of artificial intelligence for IT operations (AIOps) include optimized user experience, accelerated delivery of network services, increased network reliability, consistency across environments, and accelerated mean time to resolution.

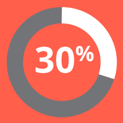
However, an AI solution is only as good as the data used to create the models. "When assessing AIOps, it's essential to work with a company that has a good data foundation and domain-specific data to develop suitable models," says Maribel Lopez, founder of Lopez Research. "Typically, this leads to more established providers with a large corpus of network data and insights to analyze."

HERE'S HOW TO GET STARTED:

- **Look for dynamic baseline capabilities** that automatically account for changing conditions (versus manually setting thresholds); this eliminates false positives that can cause alert fatigue and drain resources.
- **Select a solution that offers proactive insights** to optimize your configuration (versus purely surfacing anomalies). Flagged issues should include the probable root cause, severity or impact, and how to fix it.
- **Identify performance benchmarks** (or peer comparisons) to improve the overall workplace experience.
- **Ensure that AIOps solutions** address wired, wireless, and WAN networks, as well as security concerns. Correlate performance metrics across networks to address the root cause of connectivity issues more succinctly. Remember, the network itself is not the cause of every issue.
- **Incorporate location services** to make network analytics location aware. Leverage Open Locate is an industry initiative to standardize how APs share their reference locations with the ecosystem, over-the-air and via cloud-based APIs. Such standards enable mobile devices to locate themselves and to support location and analytics applications such as workplace utilization, space analytics, geofencing, and wayfinding services.
- **Don't assume that AIOps and automation will eliminate** the need for trained IT professionals. The goal is to surface insights and leverage automation where appropriate, allowing the network team to apply expertise where needed most.

LEVERAGING AIOPS AND AUTOMATION

- Look for dynamic baseline capabilities
- Select a solution that offers proactive insights
- Identify performance benchmarks
- Ensure that AIOps solutions address wired, wireless, and WAN networks
- Incorporate location services
- Don't assume that AIOps and automation will eliminate the need for IT



OF ENTERPRISES WILL ADOPT AI-ENABLED TOOLS TO AUGMENT TRADITIONAL MONITORING APPROACHES BY 2023[2]

[1] Gartner, "Use AIOps for a Data-Driven Approach to Improve Insights from IT Operations Monitoring Tools," May 2020

[2] Gartner, "Use AIOps for a Data-Driven Approach to Improve Insights from IT Operations Monitoring Tools," May 2020

CHALLENGE #5: GROWTH IN IOT AND SMART BUILDING INITIATIVES ARE FURTHER STRAINING IT TEAMS, WHICH LACK KNOWLEDGE OF IOT, DATA TRANSPORT, DATA SECURITY, AND BUSINESS APPLICATIONS.

STRATEGY 5

Integrate and secure IoT connectivity

ENTERPRISES AND OTHER ORGANIZATIONS will expect new building facilities to be "hyper aware" with built-in sensing and smart management capabilities. To support this, analyst firm IoT Analytics predicts that active IoT connections will grow to 14.4 billion in 2022, then almost double to approximately 27 billion connected IoT devices in 2025.

IoT growth places increased demands on constrained IT departments. IT is expected to provision very large numbers of IoT devices with network credentials and to support new IoT-driven applications for telemetry and context, data security and privacy, locating people and things, and deciding where to compute workloads. Rather than deploying and managing a new overlay network, APs can act as a secure IoT platform to provide connectivity.

"Wi-Fi 6 and 6E are much more accommodating for power-challenged and low-bandwidth devices," says Aruba's Lukaszewski. "With previous Wi-Fi generations, each device had to wake up every few seconds to see if any information was queued up for it. Now we can personalize schedules for each device to wake up every 10 minutes or every day. The device can safely go to sleep for that entire time and not miss any traffic along the way."

Importantly, with the clean spectrum available in the 6 GHz band, organizations can segment Wi-Fi 6E networks to dedicate the 2.4 GHz band to IoT while reserving the 5 GHz band for existing client devices and the 6 GHz band for new Wi-Fi 6E-enabled clients.

HERE'S HOW TO GET ROLLING:

- **Adapt and respond** to the physical and technical needs by leveraging APs to communicate directly with IoT devices and bidirectionally tunnel the data to target applications. Using APs as an IoT platform minimizes the need for overlay gateways, reduces system complexity and cost, increases reliability, and removes a vulnerable attack surface. Cloud-managed Wi-Fi simplifies the provisioning of large numbers of IoT devices with network credentials.
- **Replace aging APs** with Wi-Fi 6 or 6E APs to extend the battery life of IoT devices. Wi-Fi 6 and 6E APs include support for target wake time (TWT) to maximize sleep time and extend battery life by up to 10x that of previous technologies. They also include 20 MHz operation for lower-power operation.
- **Secure IoT connectivity** by funneling IoT traffic through APs and switches to fingerprint devices; this way, policies can be automatically assigned and any IoT devices quarantined if necessary.

NTEGRATING AND SECURING IOT CONNECTIVITY

- Adapt and respond to physical and technical needs
- Replace aging APs to extend IoT battery life
- Secure IoT connectivity by funneling IoT traffic through APs and switches

CHALLENGE #6: ORGANIZATIONS ARE TOO RESOURCE- AND BUDGET-CONSTRAINED TO EMBARK ON NETWORK MODERNIZATION.

STRATEGY 6

Build in flexible acquisition, deployment, and management

BUDGET AND RESOURCE CHALLENGES can delay critical projects, and in turn, delay deployment. In many cases, the pressures of daily operations simply trump any efforts to transform the workplace experience. But a flexible, agile NaaS model provides new options for acquiring, deploying, and managing networking solutions.

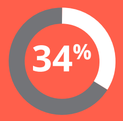
The fundamental definition of NaaS is the delivery of network services inclusive of the hardware, software, and services. This subscription model enables organizations to shift from CapEx to OpEx, in turn driving greater predictability. Although NaaS is often thought of as a cloud-based managed service, it can be delivered on prem or in the cloud and run by the organization's in-house IT team or managed by the vendor or managed service provider (MSP). The objective is to equip organizations with a wide range of options so they have the right blend of offerings, consumption, and operations to meet their needs.

HERE'S HOW TO OVERCOME BUDGET AND RESOURCE IMPEDIMENTS:

- **Opt for a subscription model** that doesn't require significant capital investments; this alleviates network lifecycle planning and budgeting by combining hardware, software, and services in one place. NaaS can also alleviate delays due to supply chain constraints — allowing organizations to act sooner on network modernization and digital initiatives.
- **Right-size your investment** with subscription models that let you "flex up" as needed or "flex down" to more closely align spend with usage.
- **Determine your NaaS operating model** and whether to run NaaS internally or augment your corporate IT team to take advantage of third-party support and services.
- **Achieve corporate environmental goals** through sustainable reuse and retirement of assets provided by the NaaS vendor.

OVERCOMING BUDGET CONSTRAINTS

- Opt for a subscription model
- Right-size your investment
- Determine your NaaS operating model
- Achieve environmental goals via NaaS



OF ORGANIZATIONS SAY THEY HAVE DEPLOYED NAAS[3]

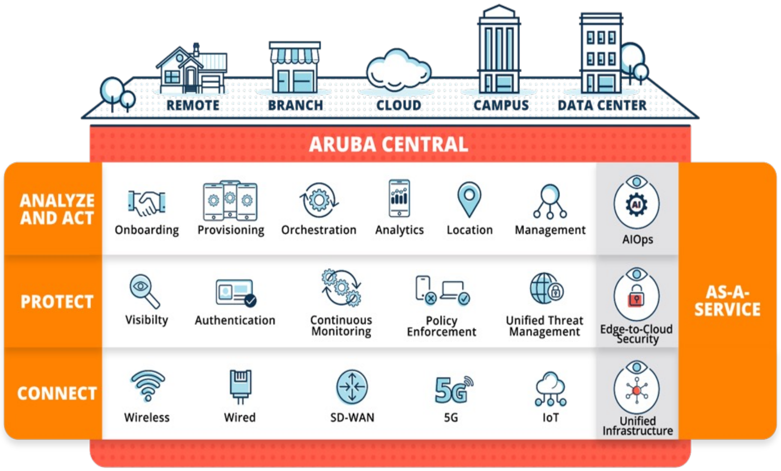
[3] IDC Aruba NaaS Study, sponsored by Aruba, a HPE company, December 2021

WHY NOW? WHY ARUBA?

ORGANIZATIONS MUST RESPOND to new, largely unanticipated demands on the network due to how and where employees work and the resulting increased technical complexity and performance requirements of the workplace environment.

With Aruba's cloud-based management, market-leading Wi-Fi and switching, and consumption and operational flexibility, organizations big and small are transforming the workplace experience with:

- **Greater agility and streamlined operations** via cloud-based Aruba Central's unified approach to network management that spans wired and wireless as well as campus, branch, and remote work environments.
- **Industry-leading Wi-Fi 6 and Wi-Fi 6E APs** and optional gateways designed for indoor, outdoor, hazardous locations, and remote work with support for application-level quality of service, all types of IoT devices, and indoor location services at 1-meter accuracy.
- **Industry-leading switches** that create a high-performance foundation for the modern wireless experience by supporting unified operations and management, secure unified role-based access, increased demand for power over Ethernet (PoE), and upgraded conference rooms – with always-on availability.
- **Performance optimization** and faster problem resolution leveraging AIOps and automation within Aruba Central that spans wired and wireless, with self-healing workflows and built-in recommendations, to accurately identify and resolve issues rapidly — based on the largest data set available.
- **Zero Trust Security and SASE frameworks** with unified policy enforcement across wired, wireless, and WAN users, applications, and devices.
- **Options to deploy management** in the cloud or on-premises, depending on what's needed, using a simple, subscription-based model.



LEARN MORE.
VISIT ARUBA UNIFIED INFRASTRUCTURE.

Aruba helps modernize the network with cloud-based management and market-leading Wi-Fi and switching offerings combined with the most flexible consumption and operations options, so you can reduce operating costs by up to 25% *(TechValidate, 2021)*.

aruba

a Hewlett Packard
Enterprise company