SOLUTION OVERVIEW

# NETWORK RIGHTSIZING BLUEPRINT FOR THE ALL-WIRELESS WORKPLACE

The all-wireless workplace is all about mobility. It has to be. Today there are more Internet-connected mobile devices than people.

Workplaces should be architected so that every class of user – employees, contractors, customers and guests – gets seamless connectivity appropriate to their role and type of device.

Instead of company-owned computers, desk phones, and smart clients, many enterprises have already adopted a bring-your-own-device (BYOD) policy that frees IT from asset management to focus on mobile applications and services delivery.

Similarly, wired devices such as desktop phones, PBXs, projectors and audio-video conferencing systems are giving way to softphones and unified communications (UC) applications, such as Microsoft Lync, coupled with streaming devices such as Apple TV.

Financially, the all-wireless workplace affords IT an opportunity to reduce costs by as much as 76% by rightsizing the mix of wired and wireless infrastructure in their network.

Some enterprises are able to eliminate nearly all wired connectivity in the access infrastructure by replacing physical Ethernet ports with affordable and pervasive Wi-Fi coverage for data and voice. Others are maintaining wired infrastructure to accommodate shared resources such as printers and other exceptions.

Networking for the all-wireless workplace must ensure that each device and business application has reliable service tailored to its performance needs. And that the network is rightsized for mobility. Key characteristics of the network for the next-gen workplace include:

- **Wireless, everywhere:** Wireless LANs (WLANs) are the enabling technology for a flexible workplace where the workforce is not required to sit behind a desk. The same wireless experience needs to be securely extended to any office, any desk, even at home. And business critical applications must be reliably delivered every time.
- **Support BYO-everything:** Networks need to accommodate a wide choice of user-owned computing devices and smartphones. IT can no longer restrict support to company-owned devices and desk phones. Perhaps for the first time, IT can eliminate the need for company-issued computing devices and desk phones.
- **Automation of routine IT tasks:** Network and security systems need to be programmable so that IT intervention is not required for every addition, move or change. Likewise, device onboarding must be automated. This way, IT personnel can shift their focus to enabling users to onboard their own devices.
- **Unify operations:** Network rightsizing goes beyond physical infrastructure savings; it must simplify management – including policy and security management – of the wired, Wi-Fi and VPN environments with a single interface. Access policies must be unified so users have a common experience and security is consistently applied, regardless of where or how they login.

## BLUEPRINT FOR THE ALL-WIRELESS WORKPLACE

Creating the all-wireless workplace requires planning and an intelligent access solution from a vendor that understands what it takes to rightsize for mobility.

Enterprises that continue with status quo architectures and vendors will end up with more unused wired ports at cubicles, more telecom infrastructure and desktop phones collecting dust, and dedicated videoconferencing/ teleconferencing systems that are seldom used.

Understanding the drivers behind the all-wireless workplace is key to migrating away from hard-wired gear and toward a vision of full mobility. In addition, IT must address several technical considerations in transitioning to a fully mobile workplace. Here are four key considerations and how Aruba Networks addresses each.

## WIRELESS EVERYWHERE

In the all-wireless workplace, client devices are obviously Wi-Fi-enabled while shared devices such as printers and projectors may remain wired. Ethernet cabling will no longer be run to individual workstations, offices, and conference rooms, reducing the need for access switches in wiring closets and the network's aggregation layer.

Pervasive wireless access and seamless mobility require a high-capacity WLAN – based on technologies such as 802.11ac – that can accommodate dense user populations as well as high-bandwidth applications and devices.

Users often have several mobile devices that are always on, most of which, like iPads, only have Wi-Fi connectivity. A WLAN must dynamically manage its capacity to accommodate changing loads, roaming, and other aspects of a fully mobile workplace.

Congestion is common on WLANs because devices share the same channel. Therefore, the WLAN must ensure that users get the services they need to do their jobs and applications like latency-sensitive voice and video traffic get the bandwidth and quality of service (QoS) they need for a trusted mobility experience.

Likewise, the WLAN must ensure good performance for encrypted applications, such as Microsoft Lync, or users will complain to IT and/or be unwilling to use those applications, even if they are critical to the business.

Users will be frustrated If WLAN service is difficult to use or spotty. Employee productivity can suffer and helpdesk complaints spike, while customers may direct their business elsewhere. The WLAN for the all-wireless workplace must be easy to use and provide consistently good performance.

Network engineers have long labored to make static switch architectures and VLANs – along with ACLs, filters, routes and QoS tags – accommodate mobility.

However, mobile environments are dynamic and IT needs an application-aware network that has visibility into individual application flows and automatically optimizes each flow, end to end, based on policies set by IT.

With programmable flow-based controls, IT can specify traffic handling policies based on who the user is, the specific client and application, and conditions on the network—and the network does the rest, whether the application resides locally or in the cloud.

## MAKING WIRELESS-EVERYWHERE A REALITY

Aruba Mobility-Defined Networks™ make it easy to provide ubiquitous, reliable Wi-Fi.

Mobility-Defined Networks empower a new generation of tech-savvy users who rely on their mobile devices for every aspect of work and personal communication. Known as #GenMobile, they demand to stay connected to everything all the time, no matter where they are.

To create a mobility experience that #GenMobile and IT can rely upon and trust, Aruba Mobility-Defined Networks automate infrastructure-wide performance optimization and trigger security actions that used to require manual IT intervention.

Mobility-Defined Networks control the dynamic mobility environment by correlating real-time data about users, devices, apps and location. Self-healing and self-optimization functions dramatically reduce helpdesk tickets and protect enterprise data.

Aruba employs a software approach that extends mobility intelligence across wired and wireless networks all the way to users, devices and apps. This makes Aruba Mobility-Defined Networks amazingly easy to deploy without any changes to the existing infrastructure.

As a result, customers can rightsize their fixed network infrastructure, which saves IT time, slashes capital costs and accelerates the delivery of network services. They can even engage guests and employees with personalized push notifications based on their indoor location.

### 802.11ac with ARM and ClientMatch

Aruba AP-220 series access points (APs) with 802.11ac, coupled with patented RF management technologies, ensure that the WLAN has both speed and the smarts to optimize that capacity for every client.

Aruba APs support 802.11ac devices in the 5-GHz and 2.4-GHz bands, at speeds up to 1.3 Gbps, enabling the WLAN to easily accommodate very dense client environments and high-bandwidth applications.

Aruba Adaptive Radio Management™ (ARM) and ClientMatch™ dynamically manage RF spectrum in order to optimize client, application, and overall network performance.

These RF management technologies leverage the intelligence embedded in the Aruba infrastructure to learn about the network, clients and applications and to apply infrastructure-based controls.

ARM optimizes WLAN performance by dynamically adapting to changes in the RF environment; for example, shifting radios between channels, adjusting transmit power, mitigating co-channel interference, modifying scanning intervals, enforcing airtime fairness, and other actions – all in direct response to network conditions.

ARM works in conjunction with ClientMatch to maximize client performance by putting the WLAN in control of client connectivity and roaming decisions, not clients.

ClientMatch monitors each client's capabilities and Wi-Fi connection and matches every client to the right radio on the right AP. This ensures WLAN capacity is used efficiently.

To ensure that overall network capacity and performance remain consistent, ClientMatch continuously optimizes client connections – key for mobility. ClientMatch is client agnostic, standards based, and requires no new client software, making it ideal for #GenMobile.

### AppRF for application-aware Wi-Fi

The Next-Generation Mobility Firewall with AppRF technology, which is inherent in Aruba Mobility Controllers, provide application visibility, even for encrypted apps and web-based traffic.

AppRF leverages this visibility at the RF layer to apply the appropriate QoS tags and auto-tune classes of service to ensure good performance for all applications, including toll-quality voice and video. This lets users depend on the WLAN to meet the most demanding application needs.

The Aruba application-layer gateway (ALG) for Microsoft Lync automatically provides QoS and priority handling for encrypted Lync sessions, including VoIP, video conferencing, desktop sharing and chat flows.

IT can even identify different Lync applications from the same device and assign different policies to the voice, video and desktop-sharing.

For example, prioritizing voice and video flows over data traffic. In addition, the Microsoft Lync ALG includes diagnostics that give IT end-to-end visibility into session statistics, such as call quality and air quality, so IT can monitor all aspects of a Lync session.

## SUPPORT BYO-EVERYTHING

#GenMobile users already own multiple mobile devices and that trend is accelerating. Unified communication vendors are also making it both technically and economically feasible to displace desk phones with smartphones using UC client software to support voice over the WLAN.

As a result, BYOD devices are increasingly being used for voice and video as well as data-driven business applications. As a starting point for eliminating desk phones, Gartner recommends that enterprises encourage employees with company-owned mobile devices to use mobile applications in place of desk phones.

Consequently, the all-wireless workplace – and the WLAN underpinning it – must be able to securely support an ever-increasing number of mobile clients and the applications used by those clients.

Today's wired infrastructure provides strong security. The WLAN must provide even more robust, scalable security, including authentication, access controls, endpoint health checks, and other mechanisms that operate consistently across the wired and wireless infrastructure and can accommodate growing numbers of endpoints and mobile applications seamlessly.

## MAKING BYO-EVERYTHING A REALITY

Aruba makes it easy to embrace BYO-everything by giving IT the ability to manage role-based access policies, onboard and profile devices, and admit guest users — all from a single pane of glass.

### ClearPass for integrated policy management

The Aruba ClearPass Access Management System™ integrates every critical aspect of BYOD – network access control, mobile device management and mobile application management – into a single platform.

With ClearPass, IT can define personalized access policies, onboard and profile devices, assess device health, and admit guest users. ClearPass monitors, audits and protects what's on user devices, and controls how devices are configured.

ClearPass policy management capabilities can secure tens of thousands of mobile users and devices from one integrated platform. Offering strong network access security and compliance, ClearPass streamlines operations across wired, wireless and VPN infrastructure.

Unique device credentials are distributed automatically for stronger and more resilient BYOD security. Consequently, IT can easily revoke network access for lost or stolen devices, with no impact on other devices that belong to the user.

ClearPass performs automated endpoint health checks and posture assessments to ensure that devices are compliant before they connect to wired and wireless networks. This enterprise-class NAC framework delivers exceptional protection against vulnerabilities.

## AUTOMATE ROUTINE IT TASKS

Today, IT spends considerable time onboarding and managing desktop computers, phones, and other company-owned assets, as well as provisioning and managing the wired data and voice infrastructure.

With the all-wireless workplace, IT's focus will shift to enabling users to onboard their own devices and to provisioning applications for business productivity.

### Flow-based networking

Mobility is all about flexibility, so the network must be capable of dynamically adjusting to the application mix, client density, and other factors to ensure a consistently positive #GenMobile experience.

Flow-based networks can monitor and control connections in real time, automatically optimizing traffic around people, devices, and applications without requiring any IT intervention.

### Self-service tools

Enterprise support for BYOD continues to rise. Many businesses today offer employees a stipend to purchase a computing device, even smartphones, rather than purchase and manage those assets themselves.

IT can't afford the time or risks involved in configuring each BYOD device separately. IT needs tools for rapid onboarding, including self-provisioning, personalized access controls, and guest access.

## MAKING AUTOMATION OF IT TASKS A REALITY

Aruba brings intelligent, flow-based traffic management to the network with its Mobility Controllers, and empowers mobile users while streamlining IT operations.

### Flow-based traffic management

Aruba Mobility Controllers provide flow-based traffic management to the network using an integrated context-based mobility firewall that recognizes which users are on the network, what devices and applications are being used, and in what location, and automatically adjusts the way traffic flows across a network to maximize performance and user experience.

Working with ClearPass, controllers steer traffic based on visibility into a user's role, devices, and apps; track and prioritize flows even when the traffic is encrypted; restrict bandwidth usage by time of day, location or other parameters; and optimize bandwidth for video across the WLAN.

Aruba even simplifies support for DLNA-, AirPlay- and AirPrint-capable mobile devices in enterprise networks. For example, the Aruba AirGroup™ registration portal within ClearPass lets users self-register their Apple devices and allows IT to define per user-group and location-based usage policies.

In addition, with application visibility available from AppRF, Aruba AirGroup dynamically stitches forwarding paths on-demand for applications such as AirPlay and AirPrint.

### ClearPass for easy BYOD support

To reduce help desk tickets and simplify management of the influx of mobile devices, ClearPass offloads routine tasks to users through guest self-registration portals.

ClearPass also automates the most formidable tasks associated with BYOD, freeing IT time and resources for more important jobs.

ClearPass visitor management provides secure wireless and wired network access for hundreds of thousands of guests and their mobile devices. Ideal for streamlining workflow processes, ClearPass makes it easy for non-IT staff to create temporary guest accounts for network access.

## UNIFIED NETWORK MANAGEMENT

IT needs global visibility into everything that affects service quality – Wi-Fi coverage, APs, controllers and the wired network. IT also needs a common set of tools to improve operations and manage RF security, including user location and mapping, real-time monitoring, proactive alerts, historical reporting, and efficient troubleshooting.

## MAKING UNIFIED NETWORK MANAGEMENT A REALITY

Aruba AirWave™ provides unified, vendor independent wired and wireless management, giving IT the end-to-end visibility and control to manage #GenMobile users on multivendor, multisite networks.

Instead of managing ports and devices, AirWave employs a user-centric approach, identifying who is on the network, where they are accessing the network, the mobile devices they're using, and how much bandwidth is being consumed by specific devices.

AirWave lets IT see everything that affects service quality – Wi-Fi coverage, APs, controllers, and the wired network. It also offers tools to improve operations and manage RF security, including user location and mapping, real-time monitoring, proactive alerts, historical reporting, and efficient troubleshooting.

## RIGHTSIZING THE INFRASTRUCTURE

Rightsizing the mix of wired and wireless infrastructure in the network is key to supporting the all-wireless workplace. Together, WLANs and #GenMobile clients yield productivity gains for by delivering anytime, anywhere access to business-critical applications, services and people.

Imagine the flexibility of your CEO, for instance, being able to spontaneously use his tablet to invite his geographically far-flung staff to impromptu video conferences when critical business issues arise.

In many industries, including retail, hospitality, and health care, providing WLAN access for customers can add to the bottom line by increasing customer satisfaction and loyalty.

Beyond these soft benefits, rightsizing provides an opportunity to reduce IT costs, freeing up resources for mobility and other projects. A rightsized access infrastructure can cut network capital and operations costs significantly, a full 76% according to analysis done by Aruba.

Today, many enterprises maintain both a wired and wireless access network. This duplicate infrastructure is costly and increasingly unnecessary as WLANs, softphones, and other technologies have matured.

In addition, wired infrastructures are static, making them unsuitable for today's highly dynamic mobile business environment and cost prohibitive for adds, moves and changes.

In evaluating customer data and other sources, Aruba has identified key capital and operation savings, along with green benefits, that enterprises can realize by rightsizing their access network. These include:

### Capital savings

- **Wired infrastructure:** Fewer access and aggregation switches are required. There's no need to pull cabling for network expansion or greenfield deployments.
- **Data:** Eliminate IT-issued desktops and laptops with stipends for BYOD laptops and tablets.
- **Voice:** Eliminate desktop phones and PBX, replace with softphones and/or BYOD smartphones coupled with UC applications for voice over WLANs.
- **Video:** Eliminate videoconferencing/telepresence systems, projectors, LCD TV or other screens and replace with UC applications such as Microsoft Lync running on smart clients coupled with display alternatives such as Apple TV.
- **Management**: Reduce or eliminate individual management platforms for the wired and Wi-Fi access infrastructure, PBX, videoconferencing system, as well as separate solutions for network access control and policy management.

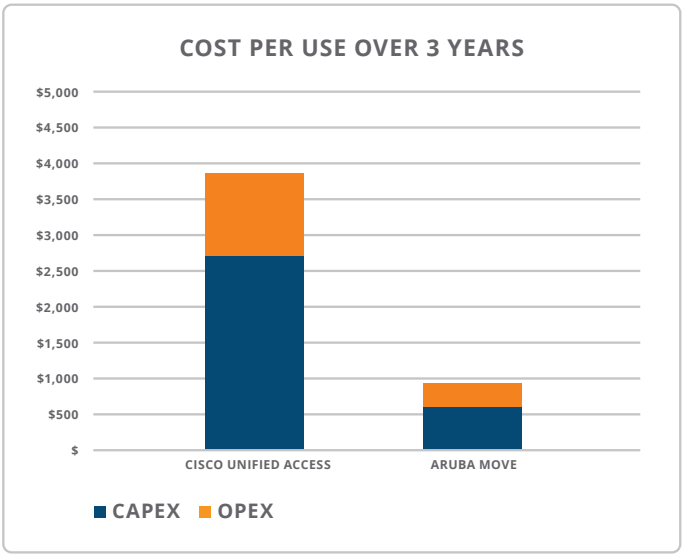
This can be achieved through a single management platform that provides unified network, device and policy management, encompassing wireless, wired and VPNs, BYOD clients, voice and video.

### Operational savings

- **Support contracts:** Save on support contracts for switches, PBX, and other hard-wired devices.
- **Additions, moves and changes:** Eliminate the cost of adds, moves and changes that require port reconfiguration on switches and the PBX; these average $500 per incident according to Gartner.
- **Heating and cooling:** Cutting back on the wired infrastructure reduces heating and cooling costs for those devices.
- **Telecommuting:** Enabling employees to telecommute lets enterprises reduce overhead costs associated with maintaining large, centralized offices, including real estate costs, insurance, heating, cooling, lighting, and other facilities expenses; also cuts the carbon emissions associated with work commutes.

### 1,000-person workplace example

Applying the blueprint discussed earlier to a 1,000-employee company results in a 76% savings. The chart below shows that the Cisco unified access architecture has a higher cost-per-user of $3,878 while the Aruba MOVE solution costs only $933 over a three-year period.




This savings is realized due to the following rightsizing assumptions and optimizations:

- User devices are primarily wireless and employee-owned.
  - IT no longer provides computing devices to employees. All devices are employee-owned for BYOD. This frees up IT resources from having to manage and maintain devices.
  - Each user has at least two devices – a laptop and a smartphone – and at least 50% of them carry a tablet. These devices use Wi-Fi for connectivity.
  - Guest users, such as contractors and visitors, account for 10% of the all devices connected to the network.
  - The result is a total of 2,600 Wi-Fi devices on the network, excluding shared devices like printers and projectors.
- Only the shared devices are wired and dedicated video conferencing equipment is obsolete.
  - Printers and surveillance cameras are shared devices and hardwired into switch ports – 5% printers and surveillance cameras for a total of 50.
  - Telepresence gear is hardwired and includes TV screens, projectors and conference phones. There are 50 conference rooms in this 1000-employee company.
    - > Cisco recommends dedicated telepresence gear in every conference room like hardwired IP phones and network connected screens – 5% conference phones and 5% projectors for a total of 100.
    - > Aruba recommends hardwired telepresence gear in the larger conference rooms with rest of the conference rooms relying on soft phones and unified communications apps like Microsoft Lync – 2% conference phones and 2% projectors for a total of 40.
  - Apple TVs in lieu of projectors
    - > Cisco recommends dedicated projectors and screens in every conference room. Total Apple TVs – 0
    - > Aruba recommends an Apple TV in every conference room. Total Apple TVs – 50
- Total number of APs
  - Assuming a maximum of 25 devices per AP, a network of 2,600 devices will need 104 APs.
- Total wired ports
  - Cisco recommends two wired ports per user to the desk for a total of 2,000 ports. In addition, there are 150 wired devices and 104 APs for a total of 2,254 switch ports.
  - Aruba recommends an all-wireless workplace with no switch ports to user desks but 250 switch ports spread across 50 conference rooms. There are also 140 wired devices and 104 APs for a total of 494 switch ports.
  - Assuming 30% reserved capacity on each 24-port switch, a total of 151 switches are required in the Cisco environment compared to only 33 for Aruba.
- Voice
  - Cisco recommends dedicated VoIP phones for every user, with 20% of users opting for an additional soft phone license, for a total of 1,200 PBX licenses.
  - Aruba recommends eliminating the desk phone except where absolutely necessary (20%) and enabling every device with a soft phone, for a total of 2,700 PBX licenses.

## BUILD THE ALL-WIRELESS WORKPLACE WITH ARUBA

The all-wireless workplace is defined by mobility, which requires a network that provides ubiquitous wireless access and broad BYOD support for users, and simplifies IT's job by unifying management and automating routine tasks.

Aruba is the only company whose products and technologies address these requirements and enable enterprises to reduce capex and opex as they rightsize their networks to support the all-wireless workplace for #GenMobile.

The company's suite of unified access products provide the network capacity and automated tools that enterprises need to accommodate the influx of #GenMobile clients and media-rich applications.

Aruba technologies operate in concert to create an intelligent, rightsized WLAN that lets customers save up to 76% of the cost of dual wired-and-wireless solutions over a three year period. In fact, many customers fund WLAN deployments based on savings from their reduced wired footprint.

With Aruba, enterprises can deliver reliable Wi-Fi services that are tailored to the performance needs of each device and business application – crucial for mobility. With Aruba, the transition to the all-wireless workplace for #GenMobile starts today.

aruba NETWORKS

**1344 CROSSMAN AVE | SUNNYVALE, CA 94089**
**1.866.55.ARUBA | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM**

**www.arubanetworks.com**