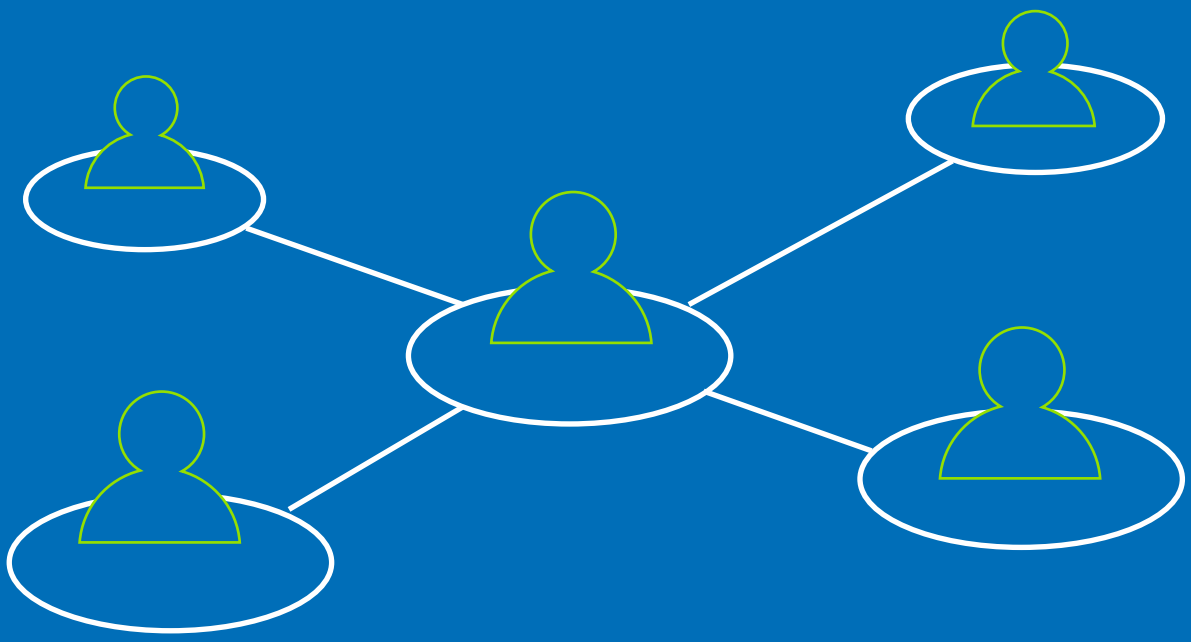
Going Mobile-First with a Digital Workplace

Key Network Success Factors



BASED ON ACTUAL USER EXPERIENCES AND OPINIONS

IT Central Station: Reviews of Networking Solutions and Other IT Products From Real Users

Contents

Abstract

Information workers today want and expect to have mobility at work. Work is not just happening in the office. It's taking place at home, on the road, in public places and pretty much anywhere people want to get things done on extended corporate campuses.

Drivers of this trend include changes in workplace norms, the pervasive nature of wireless connectivity, the proliferation of smart devices and the simultaneous rise of Bring Your Own Device (BYOD) policies. Almost every organization has the rudiments of a digital workplace, but most are far from optimizing the environment from the perspectives of user experience and IT department efficiency. Realizing the true digital workplace is about technical excellence: a combination of network hardware, best practices and policies. This paper looks at the mobile-first path to the digital workplace and key network success factor that make it a reality.

Introduction

The world of work is undergoing a major shift. People are more engaged, but not tied to their desks anymore. They may not even be in the office – but they're still hard at work. You've probably noticed it, or participated but perhaps didn't realize just how significant the change has been. It should make sense, though. The ubiquitous presence of advanced mobile devices at work and the parallel deployment of nearly universal wireless networks have resulted in what some analyst are calling Generation Mobile. Or, #GenMobile, if you're part of it.

#GenMobile works in the new digital workplace. A digital workplace enables people to work anywhere, from any device. Industry data shows it be a driver of increased productivity. Making a work environment into a truly effective digital workplace takes effort, however. Network functionality and performance are essential to success. This paper explores what it takes to realize a digital workplace. It examines the impact of the change on the IT department and reviews best practices for deploying the kind of wireless network that ensures true workplace mobility.

Defining the Digital Workplace

A digital workplace enables employees to work anywhere on any approved device. This is already possible, at least in theory, at many workplaces. However, execution is typically uneven. A truly digital workplace will ensure a consistently high level of user experience that is not commonly available. The best digital workplaces have the following qualities:

- Totally pervasive high-speed wireless connectivity in every part of the workplace. This goes beyond the office to exterior areas, employee cafeterias, and lounge areas.
- Seamless login for workers and guests.
- Ability to work on smart phones, tablets and laptops.
- 24/7 ability to connect to the workplace from home or other off-site locations without serious depracation of user experience.

One of the main differences today, also, is the level of employee expectation. A few years ago, information workers might have thought that working wirelessly in the lounge was "cool." Today, it's considered almost an inalienable right. The up and coming generation at work is digitally native. They have deep, personal connections with their devices. No longer just a phone, the smart mobile device is the source of entertainment, social connections, news, information and more. The workplace is just one more extension of this device relationship.

Figure 1 - Highlights of the digital workplace.

Universal collaboration defines another critical dimension of the digital workplace. The level of access and high quality wireless network are simply the enabling factors

[1] Source: *IDC: The Tipping Point Is Here — All-Wireless Workplaces Show Benefit over Traditional Wired Technology, October 2014*

for a new way of working together. This is largely a software phenomenon, but it's quite network dependent. And, the results are striking. According to the research firm IDC, the all-wireless-workplace contributes to productivity gains of over $9 million per year for organizations with more than 5,000 users. Onboarding time drops by 72% and infrastructure cost declines by 32% when the organization deploys an all-wireless-workplace.[1]

The Role of the Wireless Network in the Digital Workplace

You already have Wi-Fi almost everywhere. That's a given. However, supporting a large mobile workforce means rethinking the wireless network. The new "mobile-first" worker has different connectivity needs from its predecessor, the sometimes-mobile, semi-wired workforce of recent times. Think about it like this: Providing Wi-Fi for mobile users, 90% of whom prefer to work in hard-wired Ethernet work stations is completely different from supporting multi-device mobility for nearly 100% of the workforce.

Consider the office depicted in Figure 2. There are 30 people working in this collaborative, open table environment. Until recently, the wireless network might have to support about 20% of those people doing a relatively light mix of work. Table 1 offers a simple breakdown of wireless network usage by use cause under the status quo of recent years compared to the all-wireless workplace. (Usage metrics are approximate and intended only for informational purposes.) Today, there are many more users on the wireless network,

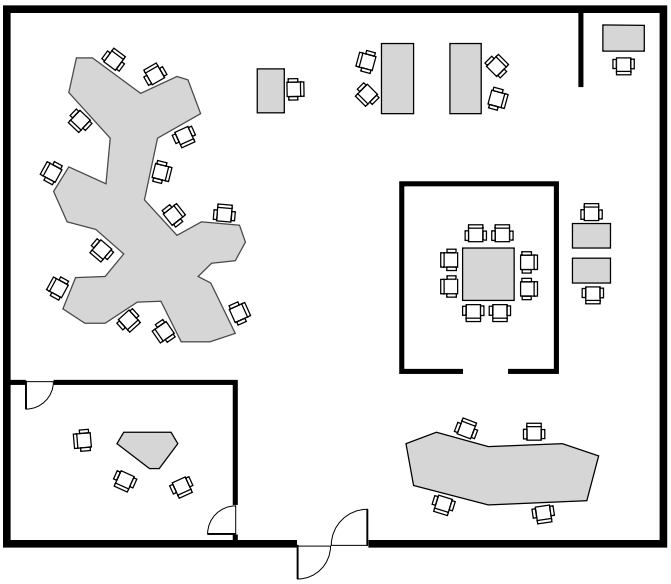


Figure 2 – The layout of a modern, collaborative 30-person office reveals the potential need for a new approach to wireless networking. It's no longer people working alone in wired cubicles.

but they are also doing more bandwidth intensive work, such as viewing video. As the table shows, the bandwidth usage is nearly 5X higher under the all-wireless approach. And, there will be inevitable clustering of even more intense wireless usage in certain locations such as the conference room and lounge areas.

The higher will necessitate a review of access points, controllers and switches. The wireless network needs to be able to handle peak loads, such as when 8 people are all watching separate videos on their personal devices in the conference room. Rethinking the network will likely lead to a rebuilding. The mobile-first workplace and its new approach to work require a rebuilt network.

Assumptions		Network Usage	Status Quo	All-Wireless
Total Users	30	% of throughput per user		
		Web browsing	50%	15%
Use Cases	Throughput (Mbps)	Audio	20%	20%
Web Browsing	0.5	Video	10%	40%
Audio	0.1	File sharing	20%	25%
Video	1	Total	100%	100%
File Sharing	2			
		Throughput per user (Mbps)		
		Web browsing	0.25	0.075
		Audio	0.02	0.02
		Video	0.1	0.4
		File sharing	0.4	0.5
		Total throughput per user	0.77	0.995
		% Users on wireless	20%	70%
		Users on wireless	6	21
		Total throughput (Mbps)	4.62	20.90

Table 1 – Wireless network throughput, comparing the status quo with the new, all-wireless workplace.

Mobile-First's Impact on the IT Department

Figure 3 - The IT department focus areas required to support the digital workplace.

In addition to changing the wireless network topology, the digital/mobile-first workplace has an effect on the IT department. With the increased importance of the wireless network in everyone's work, its reliability becomes more critical. Monitoring the network grows in significance. Outages and congestion are not forgiven easily. The support desk emerges as a nerve center, expected to resolve network issues that could be impeding the most important tasks. IT managers find themselves with an updated wireless mission. Wi-Fi is no longer a "nice to have" feature in the office. It defines the workplace.

Key Network Success Factors for Digital Workplaces

In addition to changing the wireless network topology, the digital/mobile-first workplace has an effect on the IT department. With the increased importance of the wireless network in everyone's work, its reliability becomes more critical. Monitoring the network grows in significance. Outages and congestion are not forgiven easily. The support desk emerges as a nerve center, expected to resolve network issues that could be impeding the most important tasks. IT managers find themselves with an updated wireless mission. Wi-Fi is no longer a "nice to have" feature in the office. It defines the workplace.

Efficient Management of Multiple Network Components Across Locations

Network managers cite efficient management of multiple network components as an essential factor in expanding a wireless network's reach. IT resources are limited, so it's quite useful if the network management technology can help IT staff be efficient in managing multiple components across locations.

A new generation of network management tools makes this kind of efficiency possible. One IT Central Station member, a Security/Pre-Sales Consultant at a mid-sized tech services company, described how his new network management platform enabled him to reduce the number of components he had to manage. He said, "We phased out Microsoft Network Policy Server (NPS) and Cisco Access Control Server ACS." The new tool made the work more efficient. He added that the tool improved the network guest experience while lowering the load on the IT department.

An IT Support Engineer at an energy company with between 100 and 1000 employees described the efficiency potential of new network management tools this way: "The most valuable feature for us is the ability to manage each access point from a single application." The engineer noted that the tool, "made our work easier as we were connected to Wi-Fi on our laptop, meaning we weren't constrained to our desks." A Systems Engineer at a tech services company expressed a view that the digital workplace becomes more easily achieved when the IT department has, "The ability to control all devices connecting to their network and the ability to even form a database of all the endpoints in the network and their fingerprints as well."

Broad, Intuitive Monitoring and Analytics of both Wired and Wireless Networks

Network managers have to be aware of network availability and performance in real time. And, if there is an issue, they need to be able to diagnose the problem quickly so it can be resolved before it affects the business. Monitoring

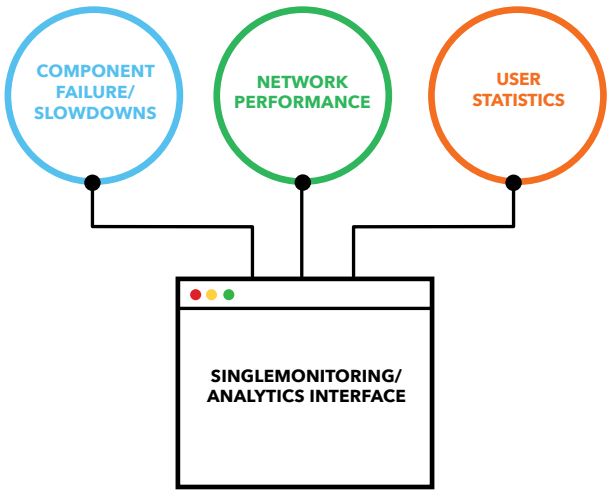


Figure 4 – The recommended practice is to arrange for all data related to network management to follow into a single monitoring and analytics interface.digital workplace.

and analytics of campus wired and wireless networks are therefore key success factors for the move to the digital workplace. Wired networks, while less prevalent for day-to-day knowledge workers, are still an integral part of most business operations. A Professional Services Engineer and Trainer at a tech services company noted in praising his network management tools, "It provides an easy way to track access point statistics and organization of access points."

A Network Professional at a communications service provider described the importance of monitoring by saying, "The feature that I use the most is the Access Tracker. It displays all relevant information of each authentication request and troubleshooting is a breeze on how the data is displayed." The Security/Pre-Sales Consultant at the tech services company, reflected that he values visibility reporting and the ability to see who accessed the network with which device.

Monitoring also helps keep the digital workplace secure. A Senior Information Security Specialist at a large utilities company explained that he, "Uses the Dynamic Host Configuration Protocol (DHCP) options for a long time to profile all types of devices communicating on a network." He then keeps his network management tool in monitoring mode so he can blocking profiled devices in batch mode.

Fast, Efficient New User Onboarding and Guest User Access

Efficient new user onboarding and guest user log-in are central to success with the digital workplace. Rapid provisioning of network access has not usually been a big issue for most companies, though it remains labor intensive for the IT department. In particular, with new Bring Your Own Device (BYOD) policies in place, the process can be more variable and error-prone. Now, with the new generation of network management tools, it's getting easier.

The Network Professional at the communications service provider commented on on-boarding, saying, "A major feature that I deploy and all my customers enjoy is the On-boarding function. Once properly set-up, it is very easy to configure and maintain all on boarded devices and users associated with those devices." The Co Founder of a tech services company concurred, noting that, "Aruba ClearPass Onboard reduces the IT admin burden as well." A Principal Network & Security Engineer at a large tech services company further described ClearPass onboarding, saying, "It has automated the bring-your-own-device process through the Onboard feature and posture health check validation through the OnGuard module, plus it has a robust and customized guest management experience."

The collaborative nature of today's work, which often

Figure 5 – Network management tooling needs to support access control for different classes of users without overtaxing IT department resources.

involves people from third party firms, means that guests are increasingly requesting wireless network access. Your organization is most likely engaging with contractors, freelancers and partner employees in numerous matrixed arrangements. Chances are that the guests on your wireless network are involved in important work for the business. Again, the quicker and more efficient the guest access process is, the more productive both the IT department and the company's workforce will be.

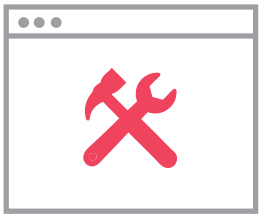
New network management tooling needs to address the need for efficient, flexible and secure guest access. An Assistant Manager of Solution Design at a tech services company affirmed the importance of guest access, describing the most valuable feature of his network management software as, "The guest on-boarding (BYOD provisioning, centralized access policies, posture assessment, etc.) It has improved Wi-Fi security and guest on-boarding to our networks." A member of the IT Division at another tech services company explained, "ClearPass Guest allows us to build a structured external captive portal with customized landing page for each customer."

Secure, Policy-Based Networks

Security has always been essential for networks, but today's new expectations of continual access by multiple device types across multiple location exposes networks to new risks. Once penetrated, the network offers malicious actors potential access to confidential data and systems of record. Network managers are under greater pressure than ever before to ensure both security and broad access at the same time. It has become a constant challenge to efficiently maintain access controls, logging, policy definition and enforcement.

The Network Professional at the communications service provider articulated an increasingly common perspective on the new realities of wireless network security, saying, "A lot of questions need to be answered before answering the real ROI question correctly. The biggest questions are how secure is your current network? Does it meet the industry security standards? Can you afford to have your network infiltrated or have loss of data? And can you afford to lose data? If not then pricing and licensing can be worked out."

Network access control (NAC) is critical, said the Principal Network & Security Engineer at the tech services company. To him, the valuable features of his ClearPass network management tooling include a complete NAC solution with standard authentication, authorization, and accounting (AAA) functions. He also values its advanced policy enforcement



SECURITY TOOLING/ MANAGEMENT INTERFACE

FLEXIBLE POLICY DEFINITION AND ENFORCEMENT

ACCESS CONTROL

MONITORING AND ANOMALY REPORTING

features for multi-vendor wired and wireless networks. AAA describes a framework for access control, enforcing and auditing policies as well as measuring usage internal billing.

Upgrading network management tooling offers a chance to update security protocols. According to the Network Professional at the comms service provider, deploying ClearPass allows organizations to replace outdated and obsolete security protocols such as WEP and PSKs to MAC-based. The introduction of a new, single management platform also enables some organizations to get rid of multiple authentication and access solutions.

Management tooling should ideally automate certain security and compliance processes. For instance, the Information Security Assistant Manager at the large financial services firm praised the component of his network management tool that performs posture assessments. He said, "This product

helps the organization to perform the NAC concept and check the health of computers before granting them access to the network." A Professional Services Engineer and Trainer at a tech services company added, "Based on our implementations for many customers, it seems that they're most interested in the [ClearPass] OnGuard feature that checks the compliance of corporate laptops and which restricts network access for users who are not compliant with security policies."

IT department efficiency and end user productivity matter when it comes to security. The Security/Pre-Sales Consultant at the tech services company described the impact of his new network management tool by saying, "Security of wired and wireless network increased significantly without any complexity for our user community." Adaptability is also a useful quality for wireless security. The Principal Network & Security Engineer at the tech services company, favored his choice of NAC tool because it, "Was the best fit to address different client requirements and tailor the security access policy based on their needs."

Open Integration Potential with Other Platforms

Building the digital workplace often means integrating the network management toolset with other systems. Examples include identity management systems, privileged account management solutions, mobile device management platforms and so forth. No one solution can do all the work required to make a digital workplace. IT Central Station members express the importance of integration as a requirement for network management. The Security/Pre-Sales Consultant praised his choice of network management software for its "Excellent API/third party integration module."

Not all network management offerings are so open, however. As the Systems Engineer at the tech services company commented, "The greatest feature in Aruba ClearPass, in my opinion, is its modularity and its openness to all vendors. Unlike its competitor (Cisco ISE), Aruba ClearPass supports integration with almost all vendors."

Conclusion

The move to the digital workplace is happening in many organizations. If it hasn't begun in yours, it's probably coming soon. The rapidly changing business environment and new approaches to working are making it inevitable. The mandate for IT is to realize the digital workplace cost effectively and in a way that doesn't burden the IT staff. Success depends, to a great extent, on the network management tooling chosen for the task.

IT Central Station members who have implemented digital networks personally, recommend tooling that enables efficient – usually centralized/single pane of glass – management, monitoring and analytics of network performance. Rapid, intuitive onboarding of new users and simple access control for guests are key success factors to ensure a positive end user experience and low IT department workload. Security must be rigorous but flexible enough to accommodate changes in security policy without overloading network management staff. Integration with third party platforms is also essential, as the digital network management toolset invariably comprises part of a bigger mix of identity management and device management platforms.

About IT Central Station

User reviews, candid discussions, and more for enterprise technology professionals.

IT Central Station is a crowdsourced platform created to connect enterprise professionals with peers for researching and reviewing enterprise technologies.

IT Central Station is committed to offering user-contributed information that is valuable, objective and relevant. We validate all reviewers with a triple authentication process, and protect your privacy by providing an environment where you can post anonymously and freely express your views. As a result, the community becomes a valuable resource, ensuring you get access to the right information and connect to the right people, whenever you need it.

IT Central Station does not endorse or recommend any products or services. The views and opinions of reviewers quoted in this document, IT Central Station websites, and IT Central Station materials do not reflect the opinions of IT Central Station.

About Aruba Networks

A Hewlett Packard Enterprise Company

Aruba, a Hewlett Packard Enterprise company, is a networking vendor selling enterprise wireless LAN and edge access networking equipment. The company has over 1,800 employees and is headquartered in Sunnyvale, California.