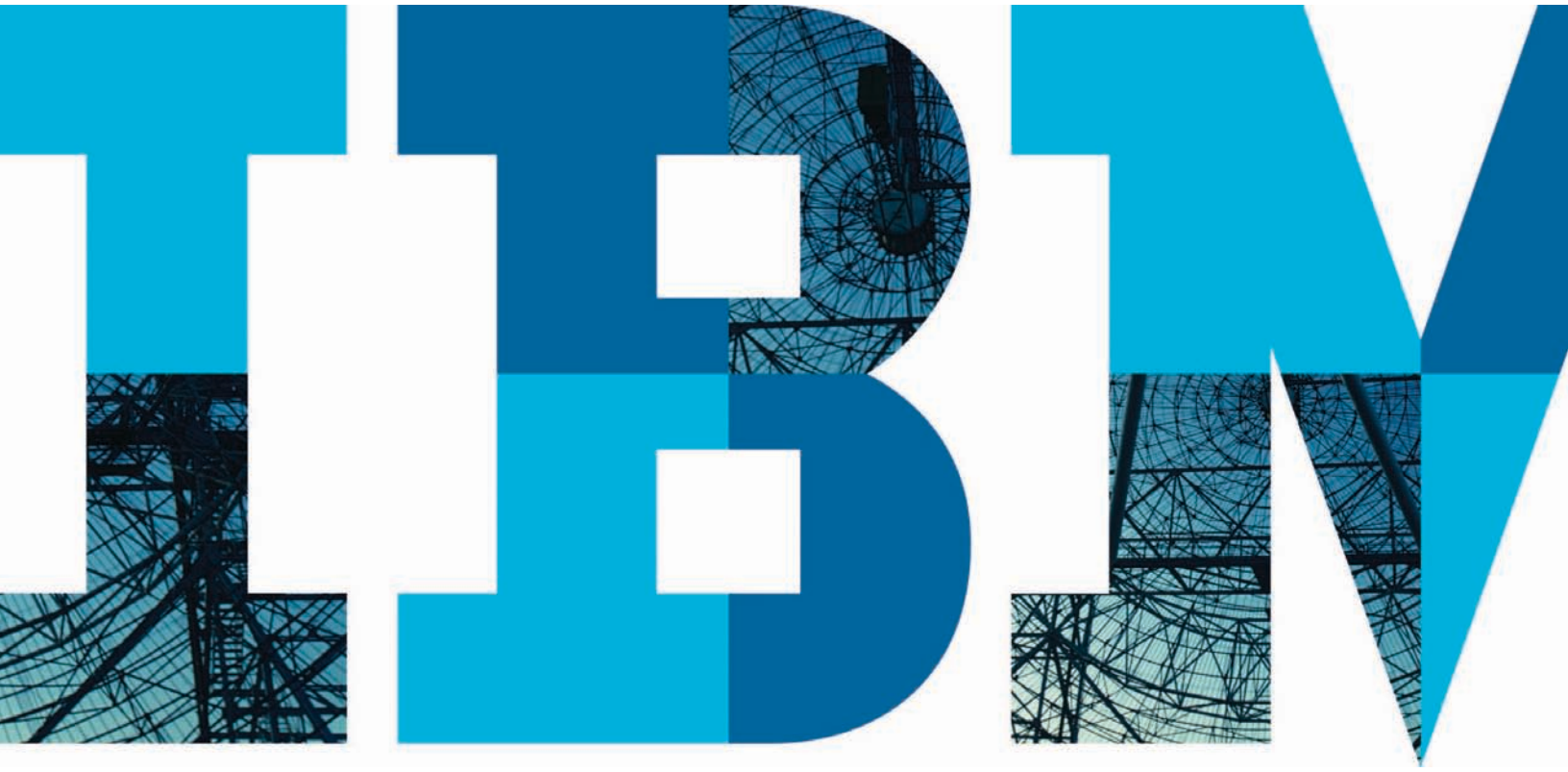
IBM Global Technology Services
Thought Leadership White Paper

Preparing your network for the mobile onslaught

How networks can overcome the security, delivery challenges posed by mobile devices



IBM

Contents

Introduction

The smart phone. The laptop. The tablet computer and the e-reader. These are some of the mobile devices consumers use in their daily lives. Increasingly, they expect to use these same devices at work. Many employers want to fulfill these expectations. Businesses recognize that, in allowing employees to work from anywhere, at any time, with anyone, mobile devices can help improve productivity and enhance an organization's ability to compete. No wonder then that in a recent survey by Cisco Systems, 95 percent of the more than 600 IT professionals responding said their organizations permit some use of employee-owned devices in the workplace.[1]

But determining how to meet mobile expectations is a struggle for many organizations. The "consumerization" of information technology requires a fundamental shift in the thinking of CIOs, IT directors and networking directors. Until the current age of mobile collaboration and bring-your-own-device capabilities, IT only had to worry about desktops and laptops—and tailoring IT operations to support those devices. Now, as employees choose or bring their own equipment, IT is left scrambling to determine how to accommodate a broad range of mobile devices and operating systems. This introduces a number of IT challenges, including managing these devices and developing mobile applications.

The "consumerization" of information technology requires a fundamental shift in the thinking of CIOs, IT directors and networking directors.

Three key elements of any intelligent mobile collaboration or BYOD solution are the mobile devices themselves, mobile applications, and the network that underpins them both. With so much emphasis placed on mobile devices and applications, IBM has found that the role of the network and its capabilities often becomes a secondary or tertiary concern. In IBM's view, this can be a mistake. IBM believes that the fundamental goal of any mobile collaboration or BYOD policy should be to provide employees with the best end user experience possible—allowing them to easily and reliably access the information, applications and mobile collaboration tools they need to excel in their jobs. Only by providing a consistent, high quality end user experience can the organization fulfill mobility's potential to bring value to the business by improving productivity and competitiveness. The network has a critical role to play in meeting this goal. Networks will need to deliver new levels of security while easing onboarding and access for legitimate users. They will have to deliver a higher level of performance. They will need specialized tools to improve device manageability and control management costs.

While network point solutions are available to address immediate needs, IBM believes that the best way to provide a quality end user experience is by taking a comprehensive approach to modernizing the network so that it better supports mobile devices and applications. This approach entails assessing the current network and planning a network architecture and migration strategy that addresses new requirements for network security, device manageability and service delivery.

The challenges

The organizational IT infrastructure houses copious amounts of confidential corporate information: work products, employee information and client data. No one is going to sacrifice the security of that information at the altar of mobility. Therefore, today's IT leaders recognize that one of the most important challenges in implementing an intelligent mobile or BYOD strategy is **securing the network**—and organizational assets—from unauthorized users while concurrently providing easy, consistent access for approved personnel. In this new era of mobile collaboration, it is critically important for the network to determine what users and devices are accessing what information and applications, and from where. This can be tricky, especially as users roam between corporate WLANs, cellular networks and WiFi hotspots.

Mobile devices inherently represent a threat to IT. Therefore, IT needs to tackle the complex task of **managing the devices**. As mobile devices have grown more prevalent, so have instances of malware attacks. There is no "safe" mobile device: malware attacks cross device types and operating systems and can threaten corporate networks as mobile devices connect to them. In addition, mobile devices are easy to lose, easy to steal. When this happens, organizations risk breach of the corporate information stored on these machines. While mobile device management tools can assist in this task—improving enforcement of access policies by allowing employees access to only certain applications and data sets—proper network security is the first line of defense against these security risks.

There is no "safe" mobile device: malware attacks cross device types and operating systems and can threaten corporate networks as mobile devices connect to them.

Another task—onboarding—spans the challenges of manageability and **service delivery**. The onboarding process can overwhelm IT and stymie end users if the process is too complex or cumbersome. IT must develop and implement a strategy to determine how to automatically onboard a large number of disparate devices—offered by a range of manufacturers and employing a range of operating systems—each of which may require a slightly different process for accessing corporate networks. Further, IT must make the onboarding process consistent across organizational campuses and buildings—no easy task when different locations can have different types of IT infrastructures. But make no mistake: an easy, consistent, onboarding process is essential if employees are to enthusiastically take part in a BYOD program and not overwhelm IT with help requests.

Additional service delivery challenges focus on bandwidth and ease of roaming from network to network. Lack of bandwidth will become a significant issue. IBM expects that, in the near future, users may bring anywhere from three to five mobile devices into the workplace, causing a 26-fold traffic increase on wireless local area networks (WLANs) by 2015.[2] This potential demand will overwhelm current WLANs, which were installed as conveniences—not as business-critical networks. Therefore, by design, the performance, security and management capabilities of these WLANs will typically prove unable to meet the demands of a surge in mobile devices that come with built-in, always-on WLAN-access capabilities. While not all devices will be in use at any one time, many will default to trying to access the nearest WLAN, a process that in and of itself eats up bandwidth. In addition, machine-to-machine communications, rich media applications and the need to access information and programs stored on corporate clouds will further strain WLANs—propelling the need for larger infrastructures, improved availability and more sophisticated network management.

It is too optimistic to believe that there will be enough bandwidth to support every user and every activity equally. Therefore, the need for bandwidth prioritization will grow. Organizations must consider how to give the most bandwidth to those applications deemed most important to organizational goals. Put simply, organizations must decide, for example, if real-time collaboration applications should get more bandwidth than email.

The need for bandwidth prioritization increases in the mobile arena. Organizations must determine how to give the most bandwidth to those applications that bring the most value to the business.

Of course, mobile devices will connect to many networks, not just a single "home" WLAN. Therefore, the organizational network must be configured in such a way that employees can access corporate information and applications seamlessly as they transition from campus WLAN to campus WLAN, to cellular data networks, to WiFi hotspots. Only in this way can mobility's promise of improved productivity be fulfilled.

Network considerations for mobile collaboration and BYOD

Development of a comprehensive, holistic networking strategy is essential to the implementation of an intelligent mobile collaboration or BYOD solution. Such a solution must provide for wired, wireless, cellular and WiFi network access. The access must be secure and seamless. It must also provide network support for the most prevalent device types and brands, and be able to grow to support new devices as they hit the market.

A sound mobile/BYOD collaboration solution must also allow users to onboard easily. It must provide the bandwidth levels and prioritization capabilities necessary for employees to access the tools they need to do their jobs. In short, the solution must meet the security, device management and service delivery challenges discussed earlier in this paper. IT must architect the organization's network to meet these challenges.

Security is a key aspect of any mobile solution. Many companies will deploy automated network access control (NAC) tools to help in this area. These tools help IT place rules on mobile devices, determining who can access which organizational data and applications, and from where. Automated NAC tools can also allow organizations to capture and push information from and onto mobile devices. For example, these tools can determine whether a device has up-to-date antivirus software before allowing the device access to the organizational network, and send updates to the device if necessary. They can deny network access to non-compliant devices. If a device is lost or stolen, these tools can remotely lock it, and, using the device's global satellite positioning system, find it.

Virtual private networks together with virtual desktop infrastructures also prove crucial to securing the organization's network. Virtual private networks provide an extra layer of protection—beyond standard credentialing—when an employee is attempting to access corporate networks from cellular networks or WiFi hotspots. Virtual desktop infrastructures, meanwhile, can allow employees access to sensitive applications and data without having to store that data on the mobile device. Encryption technologies are available to protect data in transmission.

To implement an intelligent BYOD solution that will bring value to the business, organizations need to develop a comprehensive, holistic networking strategy.

Service delivery considerations begin with onboarding. Organizations may want to deploy specialized tools to automate this work. These tools provide a "zero touch" process, making it easier for end users to onboard devices quickly and saving IT from an onslaught of help requests. The best of these tools support a broad array of devices, readying them for onboarding with a simple software download. These tools can link the user to the device (or multiple devices), then allow approved users network access. They can also configure devices so that they work seamlessly across network types. Complementary technologies provide an additional layer of network security for devices to be onboarded. Posturing technologies can be deployed before devices access the network in order to ensure that they comply with network access policies. For example, these technologies may scan mobile devices to see if they have the appropriate antivirus software and firewall software. Policy management applications forward information received from the posturing technologies to the server and evaluate it, determining whether the device and user can safely access the network. Additional programs make it possible to automate policy management, taking information obtained from posturing and policy management activities, and assigning the user to a certain access class (for example, management, staff, guest), thus determining the information and applications the user should be allowed to access.

Providing adequate bandwidth is a second consideration for service delivery. Ultimately, organizations serious about their mobile collaboration and BYOD strategies will need robust unified communications capabilities featuring mobile clients; voice over Internet protocol; and chat, video chat and videoconferencing capabilities. These unified communications capabilities help integrate all forms of communication and foster interoperability between mobile endpoint devices. However, organizations can start smaller: improving performance and availability by making the most of the bandwidth they have and incrementally adding more. Virtualization, which can help secure the network, also has a role to play in the delivery of network services to end users: it can improve bandwidth utilization and availability. To further improve availability and reliability, new delivery tools

automatically prioritize network flow, assigning users and devices to specific service classes. Similarly, these tools can prioritize applications, preventing secondary programs from consuming too much bandwidth.

How to start developing a strategy for mobile collaboration and BYOD

The first task of any organization that wants to support mobile collaboration is determining what type of overall policy to implement. BYOD isn't right for every organization. Some—certain government agencies, certain financial institutions—will not allow any BYOD mobile access to their networks. At the other end of the spectrum, there may be some organizations that will fully embrace the mobile trend, allowing all of their employees mobile access to virtually all corporate applications and all data from any device and any place.

IBM posits that, in these early stages of mobile collaboration, most organizations will fall somewhere in the middle: providing some employees and devices access to some information and applications. This access will be staggered according to organizational role. Sales people will have access to certain corporate data and applications; accounting staff, access to a different set. Guests to a corporate campus may only be able to use its WLAN for secure Internet access. Therefore, before implementing a solution, business and IT leaders must understand user segments and their needs, determine their application and collaboration strategies and formulate their overall employee-device policies. Questions to be considered include:

- What information and applications does each employee set need access to?
- Which of our employees travel, including travel from campus to campus? What are these employees' specific access needs?
- What type of access should be granted to campus guests? To contractors?
- What types of collaboration applications do we need to extend to mobile employees in order for those employees to work most effectively?
- Do we envision broadening our mobile policy as time passes, to allow more users, access, and devices?

With answers to these questions in hand, an organization is better prepared to begin building a technological roadmap for its network, taking into account how the network supports the other key elements of a mobile collaboration solution—devices and applications. Questions to be considered include:

- Which type of mobile devices should we support?
- How do we plan to secure the network?
- How do we plan to manage and secure individual devices?
- What will we do to provide adequate bandwidth?
- How do we build the network and provision devices so employees can move seamlessly from network to network?

Why IBM?

Today, a number of vendors are offering solutions that they say address the security, management and delivery challenges presented in the mobile environment. However, most are point solutions, offering cures for specific problems. This piecemeal approach is often suboptimal: it is complex, costly to implement and requires IT to purchase and support multiple components that do not always operate well in the existing network infrastructure. IBM believes that to develop an optimal mobility solution, organizations need to take a planned, architectural approach to securing the network, managing devices and delivering the collaboration capabilities and service quality that make for a productive end user experience.

IBM helps design, implement and manage the type of networks that truly support mobile devices and applications, thereby establishing the foundation for broader, stronger mobile solutions.

The process starts with a network assessment. IBM assessments have been developed to give the client organization a clear view of its current network infrastructure (including its security, capacity, and manageability postures) while providing roadmaps for reaching the future state required by overall mobile collaboration/BYOD strategies and policies.

IBM assessments help organizations determine what planning, design, deployment, monitoring and management services an organization will likely need to secure information, applications and devices in a mobile environment while supporting optimal communication and collaboration opportunities among mobile employees.

If an organization should choose to work with IBM beyond the assessment stage, IBM can design, implement and manage a tailored networking solution to support the client's mobile collaboration and BYOD objectives. IBM helps develop the type of networks that truly support mobile devices and applications, thereby establishing the foundation for broader, stronger mobile solutions. As a systems integrator working with industry-leading communications service providers and network technology providers, IBM can offer a best-fit solution approach. This capability combined with our proven, world-class methodology and extensive networking expertise can help organizations implement the type of mobile collaboration and BYOD strategies that fuel employee productivity, hone competitive capabilities and deliver measurable value to the business.

For more information

To learn more how IBM can help your organization develop and implement an intelligent mobile collaboration strategy, please contact your IBM mobile collaboration/BYOD representative, or visit the following website:
ibm.com/services/integratedcommunications

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
September 2012

[1] Cisco IBSG Horizons Study, Cisco Systems, 2012.

[2] Cisco IBSG Horizons Study, Cisco Systems, 2012.

Please Recycle

GTW03038-USEN-00