Business white paper

Re-architect your network for BYOD

Table of contents

Executive summary

If you've noticed more employees accessing the corporate network using their personally owned mobile devices, you're not alone. Many employees are boosting their productivity by using their smartphones and tablets at work.

Gone are the days of corporate IT departments dictating the types of mobile devices that could access the network. Bring your own device (BYOD) policies, while increasing employee satisfaction and productivity, are straining corporate networks.

Legacy networks, especially those common in campus locations and branch offices, are especially limited. They are inflexible and don't let employees personalize how they're using the network. They increase security risks as users connect mobile devices that the network designers never anticipated. They are complex and labor-intensive, requiring manual configuration changes to allow new devices to connect. And their old three-tier architecture can slow down modern applications, especially on wireless networks.

A re-architected corporate network will make BYOD easier to secure and manage. New generations of network equipment can help alleviate slowdowns. An updated network will be flexible and scalable. And superior network management applications can show administrators exactly what devices are on the network, what they are accessing and how secure they are—all from a single-pane-of-glass platform.

This white paper describes the limitations of legacy networks, especially for supporting BYOD. Understanding these limitations can pave the way for a successful BYOD management policy for campus and branch networks.

Is your legacy network holding you back?

It used to be that IT provided all the devices that plugged into the wired workplace network. Today, users likely have several devices, not necessarily provided or even approved by IT, and they expect to use them for complex applications such as streaming video or holding conversations over a wireless network.

As wireless networking demands become more complex and services change, your network needs to adapt. With an outdated network, this may be difficult. Legacy networks limit BYOD in four ways.

1. **Inflexibility:** They were designed for IT to manage users and location types. Employees can't personalize how they're using the network, thus stifling productivity. And IT staff members need to use—and learn—a different management platform for each technology on the network.
2. **Limited security:** They were built with well-defined boundaries but now present security risks as users connect with mobile devices that were not around when the network was originally designed.
3. **Complexity:** It takes time and manual labor to change the wireless network configuration, since it depends on scripting and making changes to the command line interface (CLI). Networks are more complex, requiring data, video, and voice to be transmitted smoothly, even over wireless.
4. **Slow three-tier network:** The traditional three-tier network was designed for times when the majority of employees used desktop computers, and wireless networking was the privilege of a few executives. Having three tiers instead of two makes the network slower because it requires an extra hop each time the network is used.

Let's examine these challenges and how to overcome them.

Inflexibility

Legacy networks were designed with a fixed configuration. Employees would be given computers by the IT department and the equipment would be plugged into the wired network. Each office had a network drop, and the setup didn't change. Because employees couldn't customize their network or the devices that were plugged into it, IT knew what devices were connected. Bandwidth and capacity were planned with the idea that each user would have one device on the network. To keep costs down, the network was not built with extra capacity.

Today, a single user may have a desktop computer, a laptop, a tablet, and a smartphone—all plugged into the network, possibly at the same time. Users expect the same performance whether they're watching a training video over Wi-Fi or conducting a Skype call from their desktop computer. The workplace model is changing, as well, with workers connecting to the network from conference rooms and other shared workspaces. Old network designs are not up to the task.

Limited security

Legacy networks allowed for tightly controlled security. Network administrators would determine what devices were allowed and what were not. Sophisticated firewalls kept unauthorized devices from accessing corporate data. And it was easy to tell whether a device was authorized, because IT provided every device that was allowed access: They bought it, they built it, and they provided remote support for it.

This is no longer the case. The best firewall can't provide complete protection against untrusted devices—but BYOD security policies essentially invite users to connect those devices. Security can no longer just protect the boundaries of the network; it has to apply wherever users are connecting to the network.

Today's network administrators need visibility into the devices connecting to the network: what type of device they are, what they are accessing, and how much bandwidth they are consuming. Solutions need to be flexible so that you can offer new services as they become available. The limitations of legacy networks make these types of changes and BYOD security a slow process.

Changing the legacy network has traditionally been done by hand, via CLI. But the volume of new devices—combined with the fact that users are not necessarily making the IT department aware of every new device they connect to the network—makes that impossible.

Guest users of the network present an additional challenge—and visitors to your office are more likely than most to show up with a tablet, laptop, or phone that they expect to connect to your network. You want to provide wireless LAN access to visitors at your campus or branch facilities, but you also want to be sure confidential corporate data is kept safe.

Finally, employees are demanding more wireless access, and they want it to be fast and reliable.

Complexity

With legacy networks, the number of devices on the network was relatively static—and IT administrators knew what those devices were.

The more functionality and features you add to the network, the more complicated management becomes. When a wireless network is added to the wired, there are suddenly two sets of networks, two sets of management applications, and two sets of security implementations.

Now the complexity is multiplied. With unknown devices getting on and off the network—and the same user accessing the network from a laptop one hour and a smartphone the next—it's important to have an integrated system that can manage all these interactions. Using CLI to define and enforce policies is no longer realistic.

Slow three-tier network

Legacy networks, with their three-tier architecture, were designed for wired access. Access switches connected to distribution switches, which in turn connected to the high-speed backbone. This made sense at the time the networks were designed because not all the access switches could connect directly to the core network. With a client/server architecture, network administrators physically segregated traffic into different subnets.

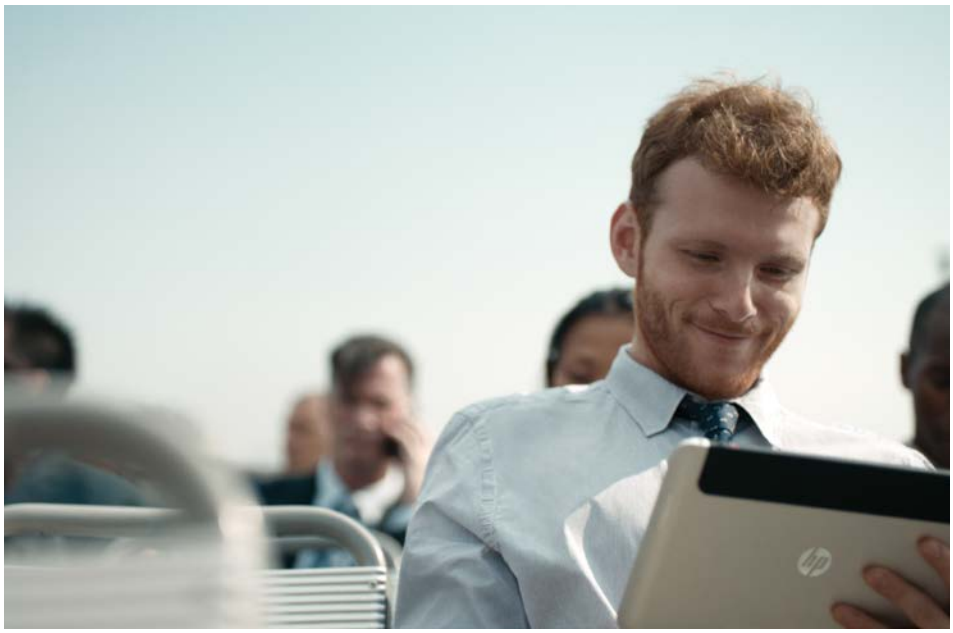
Today, however, workplace technology looks very different. Highly collaborative technologies like virtualization, video collaboration, voice over IP, and workgroup collaboration require a low latency network. In the case of desktop virtualization, for example, data and applications are stored in the cloud, which means the device has to connect to the cloud-based server each time the user needs the applications. The old three-tier architecture adds an extra hop on the network, slowing down this process.

The legacy wireless network is also not designed to support low-power mobile devices that need to be close to an access point for adequate connectivity. To properly support mobile devices, wireless networks have to be redesigned for higher density (more devices in a smaller area and closer to access points).

Re-architecting your network for BYOD

Best practices for BYOD wireless networks

Instead of being bogged down by the complexity that BYOD would add to your network, why not take this opportunity to simplify it? Consider re-architecting your network to a two-tier one for higher bandwidth and faster throughput. A software-defined network makes it easy to reconfigure the network to accommodate dynamic changes imposed by users.



A two-tier network will be faster and have lower latency, making videoconferences and similar uses work smoothly. It will be flexible enough to support new types of infrastructure—such as cloud services—even as it supports your existing investments and firewall, routing, and application delivery optimization policies. And with a single interface that shows everything from application usage to router latency, your IT staff will be more efficient and effective.

A network that's flexible and scalable allows employees to use multiple devices at work. It grows as new devices are added and new business demands are introduced. A flexible network also makes it easy to add access points where users are likely to congregate, such as in conference rooms, cafeterias, and other high-density spaces. New generations of WLAN controllers can be used to manage thousands of access points, many times more than older controllers, which is critical to successfully supporting BYOD.

Keeping the network secure

With a re-architected network, you can give your users more ways to be productive at work—and you can still keep your network secure. Here's how:

- Segment the network so the most sensitive parts aren't accessible to guests.
- Deploy a tool that can identify the type of device that is connecting to the network, the operating system it is running, and the browser it uses.
- Upgrade the network to support 802.1X authentication and network-access control (NAC). This will let your network administrator limit access to corporate resources based on the user, the device, or the location.

A unified wired and wireless network simplifies your network so that you give users a consistent experience, whether they're accessing business applications using their desktop PCs or their tablets. A simplified network can be automated to free you from manually making configuration changes to each of your management platforms and all of your networking equipment. It will easily integrate with your existing networking and security investments, so you can manage your multivendor infrastructure within a single platform.

Wireless simplified

Users increasingly demand wireless access that works as quickly and as smoothly as the wired network. One of the main applications driving BYOD is VoIP. This application requires better radio frequency (RF) coverage for superior voice quality and also needs high performance wireless LAN with assured quality of service.

Radio resource management (RRM) is one solution. RRM software helps ensure reliability, even with the growing number of mobile devices and the prevalence of performance-sapping sources of RF interference. Such interference could come from many devices commonly found in campus or branch sites, such as microwave ovens, cordless phones, wireless video cameras, and Bluetooth® headsets.

For example, users will experience very slow connectivity and access to applications if the current installation uses Wi-Fi standards older than IEEE 802.11n. Intelligent access points give priority to latency-sensitive applications such as IP telephony. They also manage airtime fairness, which ensures slower clients—older 802.11a/b/g clients—don't use up all of the airspace. Without airtime fairness, even the newer, faster 802.11n clients would experience a degraded WLAN performance.

Another solution is intelligent client load balancing, which ensures the number of devices managed by access points is adequately distributed to improve performance. For example, if one access point is supporting 25 devices and another has only two, intelligent load balancing would move some clients to the less crowded access point. This is especially helpful in conference rooms and other environments where many mobile devices are used at once.

Conclusion

The HP BYOD solution holds much potential for employee satisfaction and productivity. Don't let your legacy network get in the way. Read our technical white paper to learn how you can apply all the technologies we've outlined here to your network. And then contact your local business partner or HP sales office to discuss how you can create a BYOD-ready network for your campus or branch office.

Learn more at
hp.com/networking/byod

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document

4AA4-3882ENW, April 2014, Rev. 1