**SOLUTION OVERVIEW**

# THE NETWORK SWITCH IN A MOBILE FIRST WORLD

Its new role goes beyond performance to intelligence

## THE IMPACT OF MOBILE, CLOUD, AND IOT DISRUPTION

The digital workplace is placing crushing demands on enterprise networks. The Mobile-Cloud era is upon us with dramatic Wi-Fi growth as users move to primarily wireless and SaaS applications. Business growth and success has become dependent upon a smooth adoption of mobile technologies, from airport baggage handling to retail shopper engagement to employee collaboration.

Cloud is changing both the types and delivery of applications, creating new pressures on IT from remote branches to large campuses. The Internet-of-Things has moved from buzzword to reality with the surge of connected things in both Enterprise and Industrial contexts. These mega-trends are making waves and, in what many in IT have overlooked, is that these trends fundamentally expand the role of the enterprise network switch.

While the number of wired ports may decline in this Mobile First world, the importance and intelligence of the switch is emerging as an opportunity to bring new business value to the network.

## THE EMERGING ROLE OF THE SWITCH

Traditionally a network switch (i.e. closet switch, Ethernet switch, IDF) had one job to do: provide wired access. Users connected their desktop computers to Ethernet ports with cable runs back to a centralized closet. A few printers and local servers might be connected as well. The profile of these devices was IT-controlled, with typically low bandwidth utilization and minimal power requirements.

The shift to digital has changed this and disrupted every part of the network from the edge to the core. In the Mobile First world, the network switch now has three distinct jobs:

1. Traditional wired connectivity
2. Wireless aggregation
3. Wired IoT connectivity
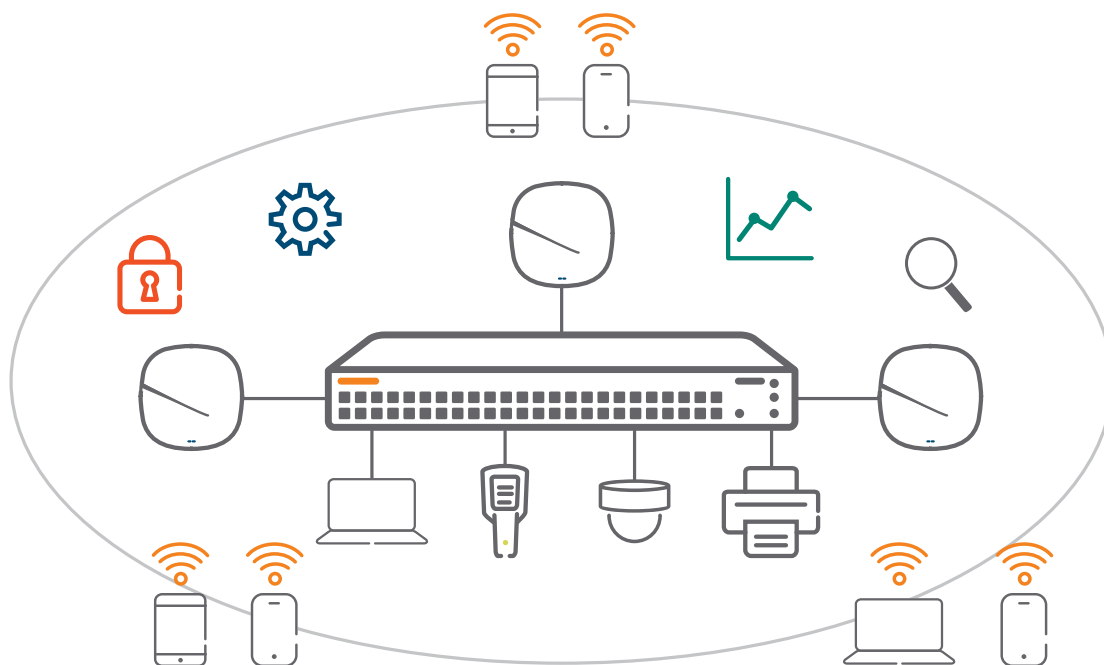
In the past a 48 port switch would have typically connected a few dozen desktops, a handful of printers and had several ports unused. Today, this same switch takes on the critical role of a gateway for a dozen wireless access points that support hundreds of users, provide connectivity and Power Over Ethernet (PoE) for IoT devices such door locks, badge readers, video cameras, printers, and for power users requiring wired Ethernet connections.

## Traditional Wired Connnectivity

In a world where more and more users are 'cutting the cord', who remains a wired user? Most organizations, including those who adopt all wireless offices, retain some residual wired connectivity. Power users such as graphic designers, movie animators or engineering workstations, require high and consistent bandwidth for data-intensive applications yet don't need physical mobility. These remaining wired users demand a high performance wired network and have network performance expectations that are much higher than the typical use in the legacy all-wired workplace.

## Wireless Aggregation

The network switch is in fact no longer a pure access switch, it now also serves as an important aggregator of wireless access points. As wireless becomes the primary connectivity method for users, the failure domain of the humble closet switch can increase ten-fold. It now must support dozens to hundreds of users, as well as wireless IoT devices. If wireless is mission critical, then reliable, resilient and high performance aggregation of that wireless traffic must occur to ensure network availability for the best mobile user experience.
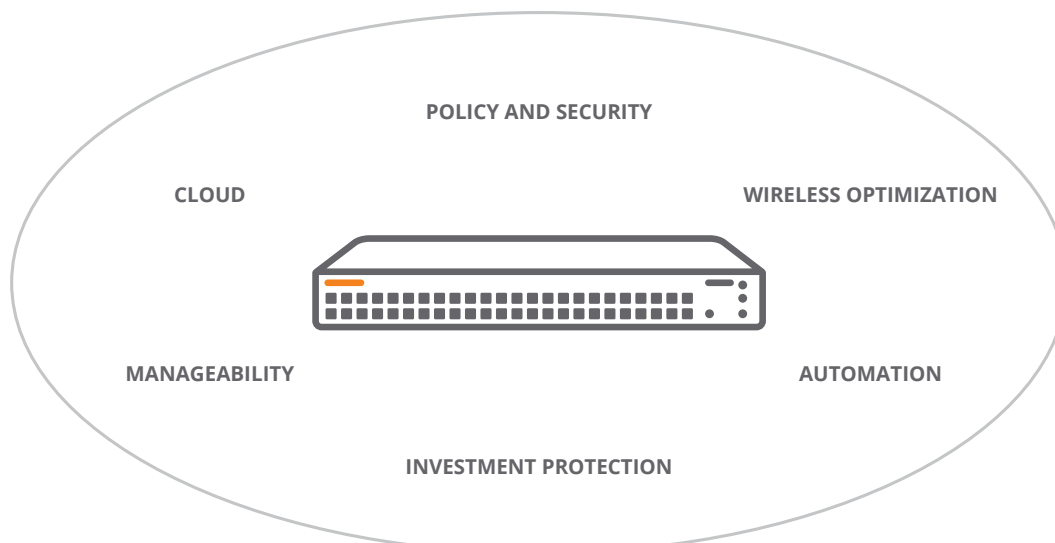
## Wired IoT Connectivity

A significant portion of IoT in the indoor carpeted space is wired. Typical wired IoT devices include surveillance cameras, building management systems (BMS), and heating ventilation & air conditioning (HVAC) systems. Many customers still use Voice-over-IP (VoIP) phones with PoE which may or may not be tied to a particular vendor's unified communication system.

Organizations also continue to add new wired IoT devices, like connected sprinkler systems on school campuses to connected heart monitors in healthcare. The profile of many—but not all—of these devices is the opposite of traditional wired user access: minimal bandwidth, unmanaged by IT, inability to securely authenticate, and a high requirement for PoE power.

## NEW RESPONSIBILITIES REQUIRE NEW CAPABILITIES

Now that switching is tasked with a three-part role a new approach is needed for this key Mobile First infrastructure component. For IT to deliver on business expectations for mobility with Wi-Fi aggregation, cloud-based application traffic, power users, and IoT devices, new software and hardware capabilities should be considered and planned for.

POLICY AND SECURITY

CLOUD

WIRELESS OPTIMIZATION

MANAGEABILITY

AUTOMATION

INVESTMENT PROTECTION

### Policy and Security

The network switch now plays a critical role in the authentication of devices and users on the network. IoT in particular creates new challenges, much like the Bring-Your-Own-Device (BYOD) trend nearly a decade ago. 'Things' are untrusted and unmanaged yet IT is required to support these devices. It is now more important and difficult to segment the wired network based on who, what, when, and how which is similar to how a wireless network operates.

The switch works together with a profiler and enforcer of policy, ideally leveraging the concept of 'roles' based on context (e.g. device, authentication information, location, time). Beyond security, to ensure optimal user experience, the switch also must dynamically assign the appropriate Quality of Service (QoS) and PoE priority as those are critically important for optimal wireless AP performance. The switch can serve as both a security sensor (by sharing granular security telemetry) and a security enforcer (by implementing role-based policies at the edge).

### Manageability

Networks have become much more complicated with IT resources stretched thin. Enterprise networks cannot be efficiently managed using a box-by-box model. Tracing the path of a user's traffic is critical, as is network-centric troubleshooting, monitoring of network elements, and seeing the entire wired and wireless topology in the same pane of glass. Soon network administrators will be expected to pinpoint users, not just IP addresses, on the wired network just as it is done today for wireless users.

### Cloud

Cloud-based applications and services are pervasive and expected to grow. Scalable remote management that helps IT teams scale is the main reason why cloud management is one of the biggest trends in enterprise networking. Critical in the Mobile-Cloud-IoT era is the flexibility to move from on premise to Cloud, or adopt a hybrid strategy with Cloud-management in small distributed branch locations and an on premise option in large campus locations. The switch needs to be flexible enough to operate in either mode as business requirements frequently change within the 5+ years of the life of a switch.

### Automated Provisioning

As the switch becomes plays a bigger role in the Mobile First world, deployment and provisioning becomes more complex especially for remote branch offices such as retail shops, healthcare clinics, or enterprise sales offices. Zero Touch Provisioning (ZTP) becomes an essential automation method to both simplify operations. No on-site IT personnel needed and IT can create and deploy centralized configurations thus avoiding error prone local set-up.

The switch boots up, securely finds its configuration and reboots without any local intervention other than power and Ethernet cabling. REST API's that allows the infrastructure to be orchestrated end-to-end for service roll-out, rapid network changes, and easier remediation are also required.

### Wireless Optimization

Understanding how Mobile First context can be used reveals many opportunities for the switch to engage in intelligent conversations with the wireless infrastructure to optimize network operations. The switch should be intelligent enough to automatically assign PoE priority, QoS and VLAN settings when detecting a wireless access point.

This enhanced communication between switches and access points can be used in many situations including the detection of a rogue access point. After identifying an unauthorized access point, the wireless network can inform the switch which can trigger an automatic quarantine of the correct port based on MAC address mapping.

### Investment Protection

Despite these trends towards cloud-based solutions and virtualization of applications and network services, the quality and robustness of switch hardware matters more than ever in each of its roles. Considering the long lifecycle of a typical switch—anywhere from 5 to 10 years—the switch acting as a wireless aggregator requires the highest component quality and redundancy in power supplies to ensure high reliability over its entire life.

As wireless protocols such as IEEE 802.11ac Wave 2 and upcoming 802.11ax push traffic between access points and switches to above a gigabit. To meet this challenge switches with HPE Smart Rate multi-gigabit Ethernet can support speeds of 2.5Gbps, 5Gbps, or even 10Gbps over existing cabling.

This automatically allows for the maximum wireless performance possible without costly upgrades of physical cabling infrastructure. To support IoT the switch and high PoE requirements intelligence is needed to sense granular information that informs profiling and analytics tools. And the switch supporting wired users must perform at the highest level of reliability and bandwidth delivery.

## MOBILE FIRST REQUIRES NETWORK SWITCH INTELLIGENCE

Considerations for the design, deployment, and management of a Mobile First network is best approached by looking at each component as an interlinking part of the solution. IT must plan now for new software and hardware capabilities needed over the next five years or more, with anticipation of the more complex and valuable role that switching must satisfy.

## ARUBA'S NETWORK SWITCH SOLUTION

Aruba's portfolio is designed to meet the challenges of the Mobile-Cloud and IoT era where visibility, automation, and security have become table stakes. Aruba's modern, programmable switches easily integrate with our industry leading network management solutions, either cloud-based Aruba Central or on premise Aruba AirWave.

They also come with built-in security features designed for mobile and IoT. Integration with Aruba ClearPass for advanced policy management delivers security and connectivity management. Customers have access to a complete portfolio ranging from entry level compact 8 port Layer 2 access switches to resilient and scalable campus core and aggregation switches that deliver 19.2Tbps switching capacity, carrier-class high availability. Automated visibility features reduce network complexity and enables faster response times when issues are encountered.
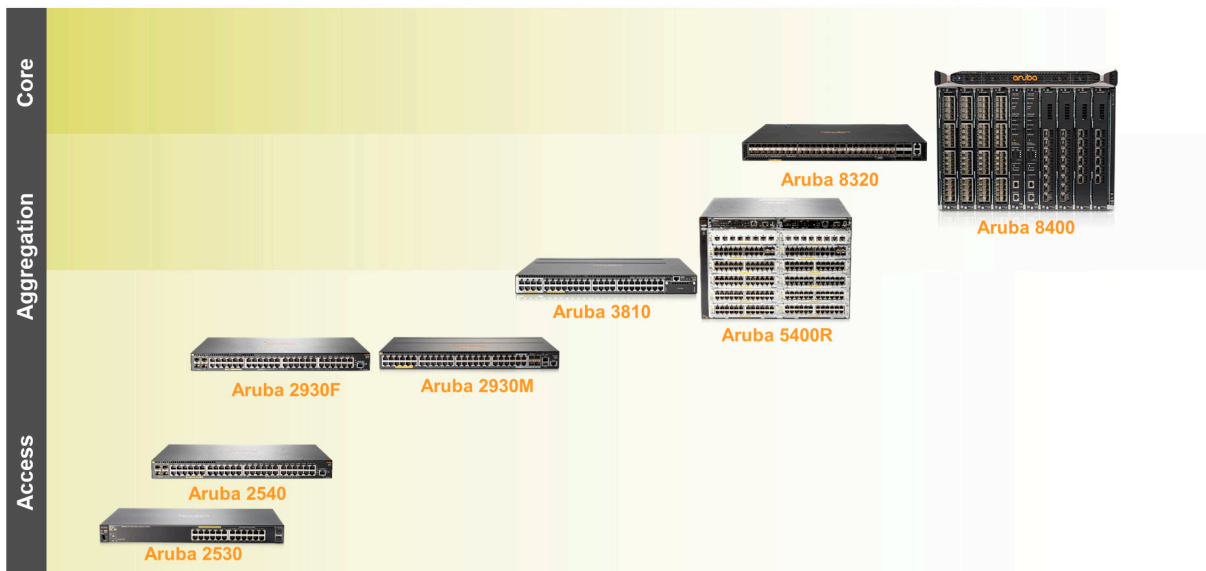


## TO LEARN MORE

Product datasheets and technical overview: Aruba Switches

Contact Us