AVAYA
The Power of We™

BYOD and the Wireless Revolution

Smartphones. Touch screen tablets. Handheld video conferencing tools. Wireless devices are invading every aspect of enterprise operations, causing IT managers to reexamine their WLAN deployments.

Table of Contents

On average, a new wireless device, complete with its own quirks and running on an increasingly sophisticated array of operating systems, reaches the market every 45 days. Once simply a means of maintaining communications, these devices are now capable of running powerful business applications, processing high definition video and consuming ever more bandwidth.

As these devices become more powerful and plentiful, more people will bring them to work. Wireless smart devices will replace cumbersome equipment once thought indispensable to business, enabling employees to choose the tools they are most comfortable with to perform their duties.

For IT departments whose networks are ready to support the surge in wireless traffic, the "bring your own device" (BYOD) revolution promises huge gains in productivity, mobility and cost savings, all on devices purchased by the employees.

Are you ready for the revolution?

Giving employees the ability to perform critical business functions at any time and any place can provide huge gains in productivity.

The virtualization of business applications to the cloud means almost unlimited computing power can be pushed to almost any device, no matter where that device is, enabling real-time collaboration, instant access and a truly mobile workforce. The devices running these applications have no Ethernet ports and rely instead on a fast and capable wireless environment.

Enterprises that are not prepared for the tidal wave of wireless devices massing in the market will not only fail to realize the benefits of the BYOD revolution; their networks will be crippled.

Meeting the needs of a truly wireless enterprise

Wireless networks are becoming more and more dominant and the following considerations are crucial to building a wireless network that can withstand the BYOD invasion

• Access and authentication control: Enterprise users have, on average, three wireless devices that need provisioning and monitoring. Any solution that fails to allow IT managers to quickly and easily add, remove and change devices on the network will end up costing much more than it's worth.

• Security: Open by nature, wireless networks must be secure enough to protect the enterprise from malicious attacks, viruses and rogue devices.

• Scalability: Because devices and users can jump on and off at any point, any wireless network trying to compete in the market must be instantly scalable.

• Guest Management: Solution must provide for both active and passive guest management, allowing IT managers to take a direct interest in an individual guest's level of access, or let that access level be predetermined by guest location and other factors.

• QoS Assurance: A wireless network that cannot assure Quality of Service is not worth having.

BYOD doesn't have to mean Bring Your Own Difficulties

Wireless doesn't mean defenseless

Every new wireless device brings with it the possibility of malware, viruses and other programs that could damage or disrupt the corporate network. In addition, because WiFi guest networks are open by nature, they are susceptible to piracy by users outside the enterprise, which can lead to performance degradation, security breaches and other problems.

But having an open network doesn't have to mean leaving that network open to attack. When considering a wireless solution, security must be a prime concern.

(Virtual) power to the people

The days of an equal number of employees and wireless connections are over. Today, every person in an organization brings multiple WiFi-enabled devices to work. Monitoring these devices while ensuring an appropriate level of access can be a significant expense and can cause IT departments regular headaches.

Allowing managers to quickly and efficiently add devices to the network and control the access level for those devices is critical to keeping the network running smoothly. Every network needs strict network access control (NAC) and an ability to scale the breadth of that control. Otherwise, the network will quickly become clogged with devices and sunk by bandwidth leakages.

Extending network hospitality

Providing guests wireless Internet access is an expected courtesy in today's enterprise environment. Business partners also need to be able to access resources through the corporate network.

Similar challenges exist for IT administrators whether they're trying to add new devices or temporary users to the network. In both cases, network administrators must ensure that devices coming onto the network have the freedom to access outside websites, corporate directories and other information while protecting sensitive enterprise data. Since guest devices are not accessible to or managed by network administrators, here more than anywhere, security is of prime concern.

Also, provisioning temporary users on the network, such as hospital guests or students in a classroom, can be excessively time consuming for IT staff and can distract from other tasks.

Get the bandwidth, or fall off the bandwagon

Today's devices have the processing power of laptops from just a few years ago, and every new generation is faster and more bandwidth-hungry than the last.

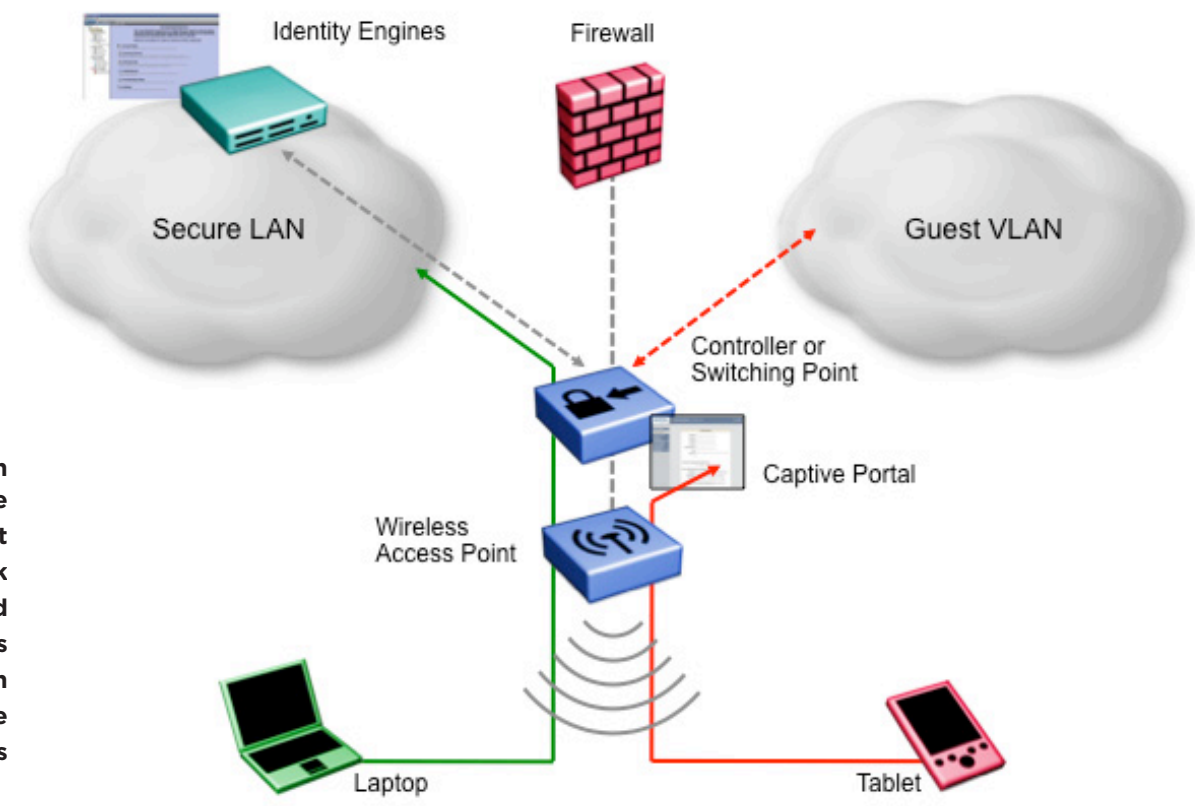
The number of wireless devices on enterprise networks is increasing at an amazing pace. The average enterprise network user carries three wireless devices, many of which are capable of processing high-quality, real-time applications such as high definition video. Most wireless networks were simply not designed to cope with this kind of demand.

According to a Gartner study, the explosion of wireless devices on the network will cause 80 percent of enterprise networks to be obsolete by 2015.[1]

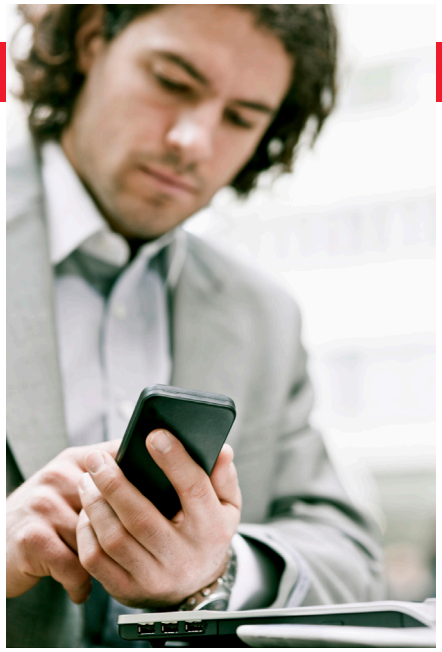
Wired speeds and service quality, without the wires

Guaranteeing Quality of Service (QoS) on WiFi devices is critical for businesses that want to realize the full benefits of the BYOD revolution.

Tools to set traffic rules and prioritize network flow are essential to ensure optimal QoS on mobile and smart devices. The ability to assign devices to specific service classes reduces the risk of service interruption and assures high-priority users receive high-quality service. The ability to regulate applications in a similar way can prevent secondary or tertiary applications from consuming undue amounts of bandwidth.



Avaya solutions are an open and secure network with support for 802.1X Network Access Control and advanced Wireless Intrusion Detection and RF Surveillance capabilities



Tomorrow's solutions, today

Avaya solutions have been built with the future in mind, providing maximum flexibility and access for users while keeping IT managers firmly in control of who is on the network and how that network is administered. Optimized for real-time applications, Avaya WLAN solutions deliver wired performance to wireless devices while providing the advanced management capabilities administrators need to ensure sensitive data is protected.

Open and Secure Networks

From user authentication and authorization to data encryption and advanced network surveillance, Avaya solutions provide IT managers comprehensive end-to-end wireless security.

Support for 802.1X Network Access Control and advanced Wireless Intrusion Detection and RF Surveillance capabilities help WLAN administrators secure communications for trusted computing assets and detect rogue network activity and malicious attacks. Administrators can also block known malicious websites or sites that are too resource-intensive.

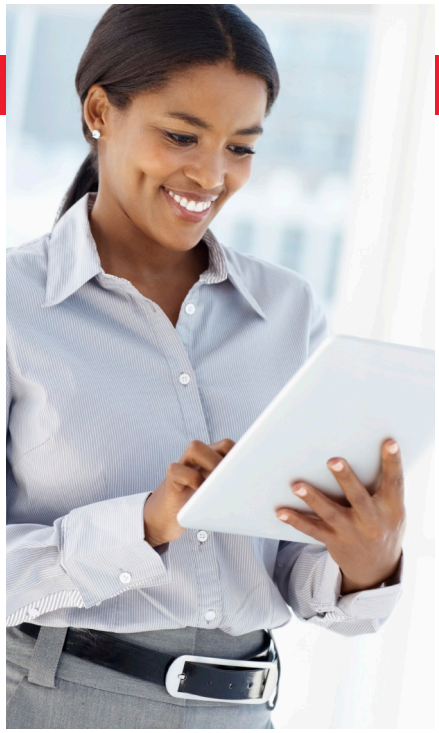
Avaya solutions provide Captive Portal and centralized user and device authentication and authorization. New devices connecting to the network through a wireless access point with either single or multiple SSIDs are validated by the Avaya Identity Engines solution using the RADIUS protocol. User credentials as well as device attributes are compared against federated corporate directories and are granted access to the network and applications accordingly. BYOD device access can be limited to select resources, can be granted secure corporate access or can be treated as a guest device depending on IT policies for devices. The centralized nature of the access control solution grants system administrators full visibility of who has accessed and who is on the network.

Ensure and secure network access for employees, contractors, guests and guest devices

Avaya solutions offer a centralized policy engine that controls user and device access based on a combination of user identity, device type and location. Administrators can instantly view and alter user account details and access privileges. Robust support for non-802.1X devices makes connecting equipment to the network such as printers, IP cameras and medical monitors simple and intuitive.

A standards-based, vendor agnostic policy server deployable over any underpinning network infrastructure allows administrators to quickly and easily add devices from a central hub and even assign multiple devices to a single user.

IT departments have many challenges to face, but monitoring and provisioning guests doesn't have to be one of them. The Avaya comprehensive Guest Management solution grants secure access to guests while offloading the task of



guest provisioning to front desk staff, other employees, security guards and even the guests themselves.

Non-technical staff can enable guest access through a customizable Web-based interface. Granular control of policies allows administrators to determine exactly how long guests stay on the network and what kind of access they are granted.

For example, users with corporate directory-based credentials working from a corporate laptop can be granted full access while contractors with guest accounts using personal tablets can be granted long-term, limited corporate access.

For large events such as conferences or expos, enterprise staff can administer guest policies in bulk, eliminating the need to manually set guest preferences and rules. To ensure that guests don't outstay their welcome, these credentials automatically expire at a specified date and time.

Ensure an always-on, scalable network

The Avaya WLAN solution provides wireless networks that are as fast and reliable as wired LANs. Incorporating the latest 802.11n wireless standard, the Avaya WLAN solution features a unique "split plane" architecture that decouples wireless application and control traffic. Application traffic utilizes Ethernet switching infrastructure and is routed directly from its source to its destination. Wireless control traffic can be virtualized and run on servers, eliminating dedicated controller hardware. This enhances application performance as well as resiliency and allows application and control planes to be scaled independently to meet network requirements. Because application traffic scales more rapidly than control traffic, the Avaya WLAN solution can accommodate surges in traffic without degrading network performance.

Hitless failover without service interruption gives administrators the ability to add new switches with no network downtime, while access points that dynamically map to controllers enable optimized access point load balancing. The Avaya WLAN solution also enables many-to-many redundancy and access point / Controller clustering for additional network flexibility.

The future is not only bright; it's more affordable

Since the Avaya WLAN access solution simplifies the surveying, configuring, monitoring, deployment and reporting of enterprise wired and wireless infrastructures, businesses can embrace the BYOD revolution and benefit from a lower total cost of ownership as well. Split plane architecture makes it easy to scale enterprise networks to keep pace with an increasing reliance on wireless smart devices, and it makes adding, tracking and administering wireless devices and guests simple.

The Avaya WLAN solution provides a strong foundation while opening the door to enterprise application virtualization and a truly wireless environment, placing enterprises on the front lines of a truly transformative revolution of how businesses and people interact.

About Avaya

Avaya is a global provider of business collaboration and communications solutions, providing unified communications, contact centers, data solutions and related services to companies of all sizes around the world. For more information please visit **www.avaya.com**.

New clouds, old clouds and virtualization

The world is abuzz with the possibilities of the Cloud, but today's "Cloud" is not a new concept. What is new is the ability to virtualize and host applications and content on a massive scale while offering content to the public on demand in the manner of Netflix and other vendors. Private clouds have existed as long as networking has existed, albeit under different names, such as "server farms" and mainframes. A good example is corporate email, which is often stored on a central server (the "cloud") and not on each employee's individual computer.

For many enterprises, the ability to virtualize applications and services (such as access point control) rather than the ability to purchase hosted services from a public "Cloud" is what offers real and dramatic change.

Virtualization promises to revolutionize cost savings and enterprise access to critical programs within businesses. In order for that promise to be fulfilled, enterprise networks must be ready for an unprecedented increase in high-bandwidth wireless traffic from smart devices seeking to run these virtual applications. Avaya WLAN solutions have been designed to both enable cloud applications and to leverage cloud services. A split-plane architecture allows the control plane to move into the private cloud as a virtualized service while independently scaling the application plane to handle the explosion of traffic over wireless as users leverage private and/or public cloud-based applications. Splitting the two planes and leveraging the Cloud for both maximizes the effectiveness of each.

Offloading data forwarding to Ethernet switches gives Ethernet-quality performance and line-rate, non-blocking throughput based on current ASIC designs, regardless of packet tunneling. This ensures peak performance for the application traffic, maximizing throughput and reducing latency.

[1] Paul DeBeasi, Top Wireless Issues That May Derail Your Mobile Strategy (Gartner Symposium/ITxpo 2011 (October 16-20, 2011))

© 2011 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. and are registered in the United States and other countries. All trademarks identified by ®, ™, or SM are registered marks, trademarks, and service marks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. Avaya may also have trademark rights in other terms used herein. References to Avaya include the Nortel Enterprise business, which was acquired as of December 18, 2009.
12/11 • DN4849