AVAYA
The Power of We™

A Unified Network for the Mobile Era

Establishing a scalable, high-performance, and intelligent network

Table of Contents

Introduction

The appetite for mobility has never been greater. Driven in large part by the Bring Your Own Device (BYOD) phenomenon and user devotion to smartphones and tablets, this trend is motivating IT departments to increase their investment in wireless LAN (WLAN) technology. In doing so, enterprises seek to ensure that the user experience of their mobile workforce is seamless and that business applications are available anytime, anywhere, on any device.

As the enterprise WLAN becomes the network of choice for employees and associates, networks are expected to support an increasing number of real-time applications, such as voice and video communications. Yet WLANs were not designed to meet business demands for performance, scalability, consolidated management, improved Total Cost of Ownership (TCO) and, more importantly, security. In addition to the pressure that real-time applications place on WLANs, the influx of personal devices is forcing enterprises to be much more vigilant in protecting assets, intellectual property and sensitive information.

So how should an enterprise address the expectations of their increasingly mobile workforce in this BYOD-driven era? The answer is an intelligent, easily managed network that is truly unified and smart enough to deliver services rapidly and seamlessly.

Bottom line, the answer is Avaya Virtual Enterprise Network Architecture (VENA) Unified Access.

Section 1: A New Era In Enterprise WLANS

Ubiquitous enterprise mobility and accommodating the BYOD traffic explosion require a thorough rethinking of current WLAN architectures.

For many enterprises, the upgrade to 802.11n and 802.11ac* will mark a new era in the use of WLANs because, prior to the 802.11n standard, WLANs were seen

*802.11ac is a WLAN standard under development and is expected to be finalized late 2012. It will enable WLAN throughput of at least 1Gbps.

as secondary and complementary to the wired infrastructure and, in general practice, were implemented on an ad hoc basis in support of highly targeted mobility, productivity or cost-saving objectives.

The 802.11n standard has helped usher in a new era in WLANs in which they are no longer just a "network of convenience" but an integrated dimension of the corporate IT infrastructure providing employees with high-performance, ubiquitous wireless access to critical tools and applications. And vital to enterprises, this includes support for bandwidth-hungry, real-time voice and video applications.

Delivering these types of applications to users wherever they need to roam will require a thorough rethinking of current approaches to WLAN architectures on the key issues of:

- Scalability: traditional WLAN architectures offer limited scalability
- Reliability: WLAN reliability must be on par with that of wired LANs
- Quality of Service: WLANs must ensure optimal QoS on mobile devices by prioritizing network flow
- CAPEX and OPEX: expenses associated with WLAN hardware and management resources must decrease

Section 2: Inadequacies of Current WLAN Architectures

Current WLAN architectures, whether centralized, distributed or somewhere in between, come up short in a number of areas including:

Lack of performance: Many existing WLAN architectures were built as an overlay, never optimized for performance, and never intended as the primary network access methodology. Therefore, existing WLAN architectures:

- Offer limited scaleability
- Have built-in traffic management inefficiencies
- Use LAN hardware as dumb plumbing which fails to optimize the hardware
- Are not designed for real-time applications

Extra hardware costs: All current architectural approaches to WLANs require a significant investment in additional hardware such as extra:

- Devices to control APs
- Servers to manage the WLAN separately from the LAN

- Devices to maintain WLAN security (with some having an overlay sensor network on top of the overlay AP network)
- Quality of service (QoS) features
- Wiring closet hardware to power APs in many cases
- Network administrators to keep it all running

Reliability: All current approaches suffer from inherent reliability issues and have multiple points of failure:

- Controller failure impacts both control and data plane functionality
- Failures typically take minutes to recover from, with APs generally having to reboot and locate a new Controller
- More components in a system mean more spares to maintain and a greater likelihood that some component will fail

WLAN management: All require additional management resources:

- Separate standalone management application that has very limited integration into a holistic management application framework
- Standalone management applications for add-on solutions, such as RFID tags, advanced WIDS security , or guest account provisioning

Security: All require a separate focus on security:

- Functions such as policy enforcement and intrusion detection and prevention (IDS/IPS) are handled in separate silos
- WLAN products rarely leverage previously deployed and maintained security appliances and applications such as firewalls, wired IDS/IPS, or endpoint inspection and tend to have their own built-in (and scaled down) versions of these features, making security management even more complicated and prone to breakdowns in policy enforcement

What is needed is a different approach, a next generation architecture than can address the issues discussed above and deliver seamless, ubiquitous and scalable Wi-Fi. The answer is Avaya VENA* Unified Access.

*See Avaya VENA sidebar

Section 3: A New Approach: Avaya VENA Unified Access

The Avaya VENA Unified Access solution delivers performance, scalability and flexibility

The attempt to balance cost, performance, and accessibility in today's WLANS results in a series of perpetual tradeoffs. None of the current architectural approaches offer a satisfactory resolution. What is needed is a solution that leverages the power of the centralized Controller without sacrificing performance and yet allows for distribution. That is exactly what Avaya VENA Unified Access does.

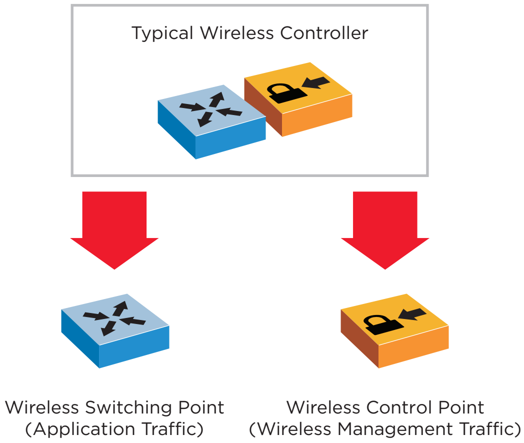

Figure 1: Wireless Controller

What is Unified Access?

Separation of the data plane (the actual packet forwarding path) from the management or control plane (where all other decisions are made including authentication) has been around since the first controller-based architectures. Many fat AP solutions implemented Controllers as control-only or security/ firewall appliances and left the data plane local to the AP.

Avaya proposes a new approach that lowers costs by doing away with the need for WLAN switching hardware. Instead of focusing on whether the data plane is best handled in the AP or in the Controller, the Avaya approach, called Unified Access, integrates the wireless data plane directly into the wired networking, splitting it off from classic WLAN components altogether.

Avaya’s Unified Access approach works as follows:

Traditional Ethernet Switches already have most of the capabilities, including processing power, needed to handle WLAN traffic natively. What traditional Ethernet Switches lack is knowledge of the mobility context for roaming sessions because, when a mobile device has moved around the campus, it carries an IP Address from a foreign subnet. Using a lightweight mobility agent added to the Switch to program switching tables in real-time as sessions move, and with a little assistance from the control plane, the Avaya Unified Access approach incorporates IP address information from foreign subnets. And, because it does not hamstring the WLAN by inserting software switching points throughout or by backhauling packets to another location just to make switching decisions, the Avaya Unified Access approach is more efficient, elegant and effective than other approaches.

Scalability and Performance: No longer burdened by data plane operations, existing Controllers can scale their control plane capacity several fold by reusing resources once reserved for data plane switching or attempts to become unified. Additional benefits include increased Controller capacity and reduced data plane tromboning, hardware tunnel processing, and overlay traffic forwarding hardware.

Reliability: As the data plane takes on the reliability characteristics of the underlying Ethernet Switching network, WLAN reliability makes a giant leap forward. Now that the WLAN Controller is out-of-band, single points of failure can be removed from the WLAN data plane and data forwarding responsibilities can be offloaded from the traditional Controller. This means that the 5x9s reliability profile enjoyed by best-in-class core network deployments can be inherited automatically by the WLAN solution. Furthermore, the control plane becomes more robust because failure of a control point has no direct impact on switching point functionality. Sessions continue to work as before even if a single control point should fail which, for the most part, negates the requirement for complex, expensive active/standby or active/active failover capabilities.

Lower Costs and Virtualization of the Control Plane: Cost is minimized by elimination of the need for expensive Controllers to handle tens of Gbps of traffic switching and, without the need for specialized switching hardware and certain port layouts, the control plane is reduced to a series of software functions that are easily quantified in terms of scaling requirements per AP. Quantifiable software scaling requirements can leverage powerful trends in the virtualization of services on commercial off-the-shelf (COTS) platforms. This way, Controller

Benefits of a Unified Wired/Wireless Architecture

Scalability: Control and data planes scale independently and at rates determined by their relative requirements

Lower Costs (CAPEX and OPEX): Unification of the data plane onto the Switching hardware—or virtualization of the wireless control point—results in fewer boxes and less to administer and maintain.

Greater Resiliency: The Avaya Unified Access solution enables wireless control plane clustering and the ability to leverage established high-availability solutions for the wired network, for example, Avaya VENA Switch Clustering.

Common Policy: Avaya Identity Engines centralized access policy offers consistent policy enforcement, security, and guest management. In conjunction with Avaya VENA Unified Access, it offers a complete solution for a unified access layer.

Improved Performance: Implementing the Avaya Unified Access solution results in a platform that is optimized for specific functions that must be performed, lowers forwarding latency, and reduces energy consumption.

Simplification: In addition to the ability to run the data plane as a unified service on common Switching hardware, the Avaya Unified Access approach enables a common network management system for both wireless functions and the data infrastructure.

costs are reduced even further as the control plane is unified within modern Data Center application delivery platforms. Hardware costs are reduced greatly and are replaced by a less expensive software licensing structure.

Unified Network Management: With the Avaya Unified Access approach, WLAN management becomes a plug-in application that leverages the full framework of other Unified Management applications and, through unification, both OPEX and CAPEX costs are reduced.

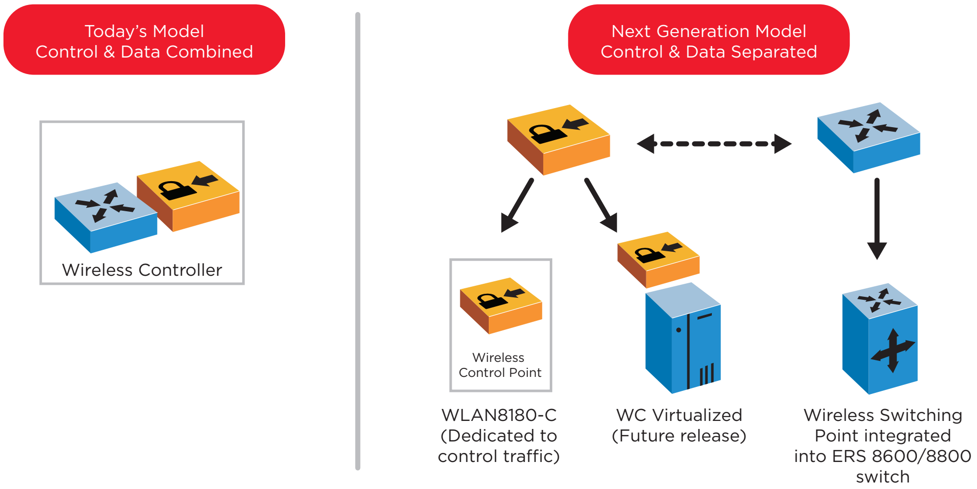

Figure 2: Legacy model versus the Avaya VENA Unified Access next-generation model

Section 4: Unified Identity and Network Access Control

It is important to create an intelligent, policy-enabled network edge that authenticates every device, every user, and application being accessed. By doing so, network administrators have no need to provision users or devices manually nor do they need to worry about whether devices are corporate or personally owned. The network will profile (fingerprint) a BYOD device and, based on policies in place, will provision appropriate network connectivity automatically.

Avaya Identity Engines assigns network access rights and permissions based on a user's role, the user's location (local or remote), and how the user connects (wired or wireless). Depending on IT policies for devices, BYOD device access can be limited to select resources, granted secure corporate access, or be treated as a guest device. The centralized nature of the access control solution unifies the user access experience across wired and wireless networks and, without placing additional burden on stretched IT staff resources, grants system administrators full visibility into who has accessed and who is on the network.

The Avaya Identity Engines Ignition Server performs user and context-based authentication and authorization for clients attempting to access the network. It supports:

- AAA identity-based network access control
- An easy-to-use, standards-based policy engine
- RADIUS integration with all enterprise network equipment
- Quick and deep integration with major directories

Avaya VENA Unified Access – Integrating Avaya WLAN 8100 and Avaya Ethernet Routing Switch 8800

Avaya WLAN 8100

A next-generation WLAN solution from Avaya, the Avaya WLAN 8100 is designed to deliver a scalable, high performance foundation that enables enterprises to fully leverage their mobility investment. The Avaya WLAN 8100 Series is comprised of three primary components:

- **WLAN Access Points,** which provide wireless access to mobile devices and perform encryption/decryption for wireless traffic, priority queuing and radio frequency (RF) monitoring, including rogue AP identification and containment.
- **WLAN Controllers,** that control access points and perform key centralized functions such as security, networking, quality of service (QoS) and roaming for mobile users. Controllers can be deployed as either standalone Wireless Controllers (control & data traffic) or as a dedicated control point where the data plane is integrated into the Ethernet Routing Switch (ERS)8600/8800 Switches as part of the VENA Unified Access Architecture.
- **WLAN Management Software** is a comprehensive design and management tool that identifies ideal access point locations on detailed floor plans, configures all devices with a single click and provides granular monitoring and reporting for complete visibility and control over the entire system.

Avaya ERS 8800

The Ethernet Routing Switch 8800 is a collection of modular Ethernet Switching systems that deliver always-on networking and high-density connectivity. Supporting hot-swappable modules, redundant fans, and power supplies, each of these individual platforms is highly resilient and, when deployed in Switch Cluster configurations, delivers true end-to-end reliability and always-on application access. Available in a wide range of models, these systems are specifically designed to address the critical enterprise need for reliability, efficiency, and scalability.

The Ethernet Routing Switch 8800 is a key component of the Avaya Virtual Enterprise Network Architecture, supporting full-featured network virtualization capabilities for campus cores and data center applications.

Avaya Virtual Enterprise Network Architecture (VENA)

Avaya Virtual Enterprise Network Architecture (VENA) is an enterprise-wide virtualization framework that simplifies the network, streamlines the deployment of cloud-based services and improves the delivery of always-on content. It enables enterprises to successfully build and operate next-generation architectures, such as the Private Cloud.

Avaya VENA groups together a number of complementary capabilities – some well established and some new and emerging – under an umbrella that clearly identifies them as being strategic, fit-for-purpose, business-centric solutions. So whether it's the decade-old Avaya VENA Switch Clustering or the new Avaya VENA Unified Access, the most important thing to know is that if it's part of the Avaya VENA strategy then it is specifically engineered to promote availability, performance, and simplicity.

Avaya VENA solutions are designed to meet the needs of mainstream enterprises. Matching the business goals and aspirations of a typical enterprise with a typical corporate network, VENA solutions are engineered to deliver more IT performance for every IT dollar invested through lower levels of complexity and higher levels of uptime and throughput.

The Identity Engines Ignition Access Portal grants access to users with devices that do not support the 802.1x protocol and users with un-managed devices. In addition, the Access Portal can host the Identity Engines Ignition CASE Client, a dissolvable client that enables auto-configuration of managed and un-managed devices for wired and wireless secure access.

Avaya Identity Engines also supports Unified Guest Access Management and, with Avaya Identity Engines Guest Manager, front desk personnel can generate unique user IDs and passwords for each visitor, providing secure, convenient network connectivity for guests and temporary users. Employees or even guests themselves can self-provision access.

A key value of Avaya Identity Engines guest access solution is that it is a unified solution; a user is provisioned once and, whether they connect using a wired or wireless connection, will be associated with the same security profile.

Conclusion: A Scalable, High Performance Unified Network

Avaya is delivering a unified access solution that addresses key challenges in today's enterprise.

The Avaya Unified Access Solution delivers ubiquitous access to enterprise applications and unified communications tools which can have a dramatic impact on productivity and performance. By integrating the wireless data plane with the wired data network through a Unified Access approach, this solution overcomes the disadvantages of current centralized and distributed WLAN approaches and creates a scalable, reliable, high-performance architecture for the mobile era.

Available today, Avaya Unified Access and Identity Engines network authentication services to create an intelligent edge that reduces costs through a smart efficient network that authenticates, auto-provisions and provides security without the constant intervention of a network administrator.

About Avaya

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

08/12 • DN7118