IDC TECHNOLOGY SPOTLIGHT

Rethinking Traditional Architectures for Enterprise Wireless Networks

July 2014

Adapted from *Cloud-Managed WiFi: An Emerging Network Architecture for Enterprise IT* by Nolan Greene and Rohit Mehra, IDC #249172

Sponsored by Aerohive

Today's corporate networks are becoming increasingly complex. With increased mobility and Internet usage, virtualized applications, cloud services, data backup from distributed sites, and security and application updates, the network handles more tasks than ever before. The growing number of network endpoints with the emerging Internet of Things (IoT) phenomenon adds to the challenge of effectively deploying and managing a wireless network in today's enterprise. Moreover, lean budgets, geographically distributed deployments and, in some cases, a lack of onsite RF expertise pose additional potential obstacles for network managers. This Technology Spotlight addresses how newer cloud-managed distributed control network architectures, such as those offered by Aerohive, address these challenges as enterprise WLAN use cases become more diverse.

Introduction

Enterprise WiFi has come a long way since the era of the 802.11g standard, when WiFi began its ascent into the mainstream of the home and the workplace. At the time, WiFi came about to meet the needs of workers using laptops wirelessly. It was seen as a "nice to have" for a subset of employees rather than a critical business enabler. WiFi of that era was also largely deployed through autonomous access points (APs) without a controller to provide centralized visibility to the control, management, and data planes. However, these dynamics were bound to change.

Today, enterprises see new challenges on their networks because of the proliferation of smart mobile devices with BYOD that are running more bandwidth-intensive applications (including voice and video) than ever before. In many cases, BYOD is too entrenched and invaluable to be cast aside, yet it still presents a number of security and policy concerns for the enterprise. Adding to this is the fact that many "BYO" devices are accessing mission-critical applications (and their data).

The emerging Internet of Things phenomenon is also contributing to the exponential increase in the number of network endpoints. These challenges have served as an impetus for multiple changing dynamics in the enterprise wireless networking market — perhaps most noticeably the emergence and swift mainstreaming of the 802.11ac (Gigabit WiFi) standard and the growing adoption of cloud-managed distributed WiFi architectures. These cloud-based architectures are creating new wireless network possibilities for enterprises — particularly those that are distributed (geographically dispersed) or in the small and medium-sized enterprise (SME) and midmarket spaces.

Enterprise networks today commonly find the following challenges to capacity, density, and aggregate throughput:

- **BYOD and mobility.** BYOD was once a buzzword coined to describe the proliferation of end user–owned devices accessing corporate networks and, in many cases, corporate applications. However, BYOD has entered the mainstream of enterprise IT. IDC forecasts that by 2017, 79% of

mobile devices in the enterprise will be "employee liable." The bandwidth and security challenges of BYOD are here to stay, and the network must be able to accommodate.

- **Increased number of endpoints.** As BYOD has become more common and new mobile device forms (e.g., tablets, 2-in-1s) have emerged, network managers have found themselves supporting a seemingly ever-increasing number of endpoints. Many enterprise network managers will soon find themselves needing to support an impending onslaught of IoT devices. IDC defines IoT as a network of uniquely identifiable endpoints (or "things") that communicate without human interaction using IP connectivity, whether "locally" or globally. IDC forecasts that the number of connected "things" will grow from 11.4 billion in 2014 to 28.1 billion in 2020. Many of these endpoints will be connected via WiFi, meaning there will be substantial impact on enterprise WiFi networks.

- **Demand for greater "speeds and feeds.**" Many enterprises today find themselves conducting increasing amounts of business activities over wireless networks. In turn, networks must be pervasive, redundant, and responsive in real time, even in the face of applications that are data intensive and bandwidth hungry. The emerging 802.11ac standard was born out of this need for speed and bandwidth and will see incrementally ramping adoption over the next few years, likely exceeding 802.11n in new deployments by 2016.

- **Management by context and application levels**. From entry-level employees to senior management, there are more internal users on enterprise networks. Many enterprises choose to allocate and restrict network and application access based on employee credentials. Additionally, many network applications (Facebook, YouTube, etc.) are made completely off-limits. Given this fact, and that many enterprises — particularly in retail, hospitality, healthcare, and education — have opened up WiFi access for customers, network administrators need to set different policies for different types of users and be able to consistently monitor and enforce those policies.

- **Increasing leanness of IT.** A lingering side effect of the economic uncertainties of the past several years is that many enterprises continue to be austere in terms of IT investments. While IDC projects enterprise IT spending to rise modestly in the near term, key decision makers still look to optimize total cost of ownership (TCO), shift spending from capex to opex, and minimize associated labor costs. At the same time, many CIOs are finding that their network operations do not possess the RF expertise necessary to accommodate the challenges brought about by so many new devices on the network. As a result of "lean IT," these CIOs do not believe they will receive the resources needed to add additional RF talent and resources. In some cases, lean IT and its challenges are being met through third-party managed service providers (MSPs).

Alternative Architectures for Network Control

Recognizing the need to improve visibility into and control of wireless network traffic, centralized WiFi controllers entered the mainstream in the 2000s. Controllers led to great improvements in terms of network efficiency, management, and security. However, with advances in WiFi capacity, controllers represent a substantial capital investment and can serve as a chokepoint to expanding the network as more controllers (and redundant controllers) must be deployed if the number of APs increases significantly. In recent years, alternative architectures have emerged. Among those alternative architectures are delivery models where control can reside in the cloud or be distributed throughout deployed APs.

For many enterprises, these alternative architectures have proven beneficial. Eliminating controllers reduces the possibility of a "single point of failure." In the example of distributed control, network intelligence is shared among APs, which provides failover if one or more APs stop working. In addition to redundancy, many enterprises find that not having to route wireless traffic through the controller may increase speed. Furthermore, regarding scalability, traditional controllers have upper

limits as to the number of APs that can be managed. At times, the expense of a controller (plus redundancy) can be prohibitive to enterprises needing to add new APs. Non-controller-based architectures provide scalability benefits from a financial perspective as enterprises will not need to purchase additional controllers (and redundant controllers) as the network scales up.

Moving WiFi Management to the Cloud

In recent years, the concept of cloud computing has moved from the abstract to the mainstream. IT managers and line-of-business (LOB) personnel have increasingly migrated core functions such as document storage and sharing (Box, SharePoint), CRM (salesforce.com), email service (Outlook 365), and other custom apps to cloud-based applications that can be accessed from any device. At one time, the idea of paying for such services via a subscription model, while bypassing physical hardware and software, seemed to be a radical concept. However, these types of mobile cloud applications are ascending into the mainstream and must be supported with a strong wireless network. At the same time, these applications have lent legitimacy to other flavors of cloud IT, including cloud-based network management.

Recent trends in IT buying have looked favorably upon opex-oriented investments and "everything as a service." This also holds true for enterprise networking. In terms of WiFi, management can now be hosted in the cloud. Fully capable management suites (including network design, deployment, analysis, and support capabilities) can be purchased on a per-license subscription basis, meeting many enterprises' desire to move IT purchases to opex. Moving network management into the cloud is also highly beneficial for distributed enterprises, where enterprise IT must centrally manage geographically dispersed APs.

It is also worth noting that there are multiple delivery models within the realm of cloud-managed enterprise WiFi. Potential users of cloud-managed WiFi should know that they can employ either a public cloud (multi-tenant datacenter owned by WLAN vendor or service provider) or a private cloud (an enterprise's proprietary datacenter) to host their cloud networking solutions, according to what fits better with the enterprise's preexisting IT paradigm. Many cloud-managed WiFi vendors support both means of providing cloud-based networking.

Cloud-Managed WiFi: Optimized for Distributed Large Enterprises, Midmarket Enterprises, and SMEs

Enterprise-grade network deployments are no longer just for carpeted enterprises, manufacturing plants, and large healthcare and educational facilities. Recent trends in mobility, consumerization, industry regulation, and vertical-specific use cases have led to a sharp growth in enterprise networking deployments in distributed settings within retail, hospitality, healthcare, and K–12 education. Large enterprises within these verticals often are distributed anywhere, from multiple neighborhoods within a city to multiple continents.

At the same time, these enterprises tend to have one centrally located staff team (or even one team member!) managing the entire network, with little ability to personally touch all the branch locations. Additionally, these enterprises often need to scale quickly, with little preexisting infrastructure and space for equipment. Similarly, SME and midmarket enterprises may not have distributed locations in every case but may have similar concerns around infrastructure, staffing, and capital investment.

The following benefits of cloud-managed WiFi can add value to these types of enterprises:

- **Automated provisioning and configuration:** One of the most noted ease-of-use benefits of cloud-managed WiFi is the ability to offer automated provisioning and configuration across multiple remote sites. In the cloud WiFi space, certain vendors are able to ship "preconfigured" APs to remote branch locations; all that staff at these locations have to do is plug in the AP. From

there, the AP downloads the information it needs, discovers its network, and is fully self-configured. Generally, this happens in a matter of minutes. Having the control plane situated in the cloud allows for these and similar innovations when it comes to automated provisioning and configuration.

- **Easier to manage and troubleshoot remotely:** As mentioned, cloud-managed WiFi provides immense advantages to centrally located IT managers who are responsible for networks that are widely dispersed geographically. With management centralized in the cloud, a network manager who is asked to troubleshoot a problem 2,000 miles away can do so from the network management interface instead of having to travel to fix the problem (which is impractical and expensive) or having to hire someone in that location to do it (which is more practical but still expensive). The ease of centralized management and troubleshooting makes it easier to standardize the network as concerns about local ability to work with certain vendors and products dissipate. In the case of WiFi, with intelligence residing in the cloud (or distributed among APs), there is no single point of failure, reducing downtime and the risk of a network outage.

- **Scalability:** In a networking environment with physical controllers and switches, the costs of network expansion are step variable (i.e., additional costs are incurred incrementally until the point where existing controller and switch architecture is exhausted). Then, there is a larger investment in a new controller with the potential for expensive, unused extra capacity. With cloud-managed WiFi, scaling costs remain linear — and can be staggered to accommodate immediate budget constraints. There are no additional large capital investments that serve as a bottleneck to scaling. In tight economic times, CIOs can breathe easy, knowing that the network can expand as business locations and/or network endpoints are added, and as more applications clamor for bandwidth. CFOs can also breathe easy, knowing the network can grow at the rate it needs to while largely avoiding additional substantial capital investments.

- **Redundancy:** Specifically referring to the distributed control delivery model of cloud-managed WiFi, redundancy is integrated into the architecture, which does not include a physical controller. In the traditional controller-based delivery model, if the controller goes down, the wireless network can fail. In a distributed control mode, the network can remain up and running, given that intelligence is shared among all the APs; there is less possibility of a single point of failure than in the controller-based model.

Challenges for Cloud-Managed WiFi

Any newer technology can shake up the status quo of enterprise IT and create challenges for administrators and end users. IDC expects the impact of these challenges to be minimal but advises enterprise IT to be aware of their possibilities:

- **Cloud datacenter (and connectivity) can be a single point of failure.** While a datacenter failure that causes a cloud network outage is very unlikely, given the redundancies cloud providers have put in place, it is a concern and sometimes a barrier to the adoption of cloud technologies for business-critical functions. Cloud connectivity failure can impact certain management and control functions in remote networks. IDC advises examining local survivability requirements to ensure failover capabilities.

- **Organizational barriers must be overcome.** Similar to any other paradigm shift in IT, cloud-managed WiFi requires a change in thinking about what IT infrastructure looks like. Key stakeholders may have "traditionalist" views about WiFi infrastructure and/or may have concerns with performance, security, redundancy, and other important factors. It is important not to overlook organizational concerns, cultural barriers, and any other potential internal barriers in determining rollout strategy and communication.

- **Cloud WiFi may be new to the channel and service partners.** As mentioned, cloud-managed WiFi is not entirely new but is now in a period of fast growth. Your value-added resellers (VARs), systems integrators (SIs), and/or managed service providers may also be coming up to speed on cloud WiFi. IDC believes that this transition will, for the most part, be smooth but advises IT managers to anticipate some bumpiness during this introductory period. Be sure to assess history and compare partners' track records in cloud technologies (especially newer ones) when evaluating cloud-managed WiFi.

Future Outlook and Considerations

IDC expects that as the WiFi needs of SMEs and midmarket and distributed enterprises continue to grow, the market for cloud-managed WiFi infrastructure and managed services will grow at a notable rate. From 2013 to 2018, this market will grow nearly 6x from $422.3 million to $2.5 billion, representing a CAGR of 42.5%.

The growing requirements of BYOD, mobility, IoT, and regulatory requirements (e.g., PCI DSS, HIPAA) are raising the need for enterprise-grade networks in businesses where the traditional architectures may not be the best fit. The most pronounced advantages of cloud-managed networking will continue to be for distributed enterprises, but cost efficiencies and a shift toward opex-only spending will give pause to more IT managers deploying traditional networking architectures to consider the cloud for wireless deployment and management.

Additionally, with the approaching ratification of the 802.11ac (Gigabit WiFi) standard, the time is right for enterprise IT to reconsider its wireless paradigm. Furthermore, where appropriate, enterprises should not miss out on the opportunity to leverage the network for improved customer experience and monetization (with applications such as location-based services). With these factors in motion, IDC expects swift adoption of cloud-managed WiFi in well-suited enterprises.

Considering Aerohive's Solutions for Cloud-Managed WLAN

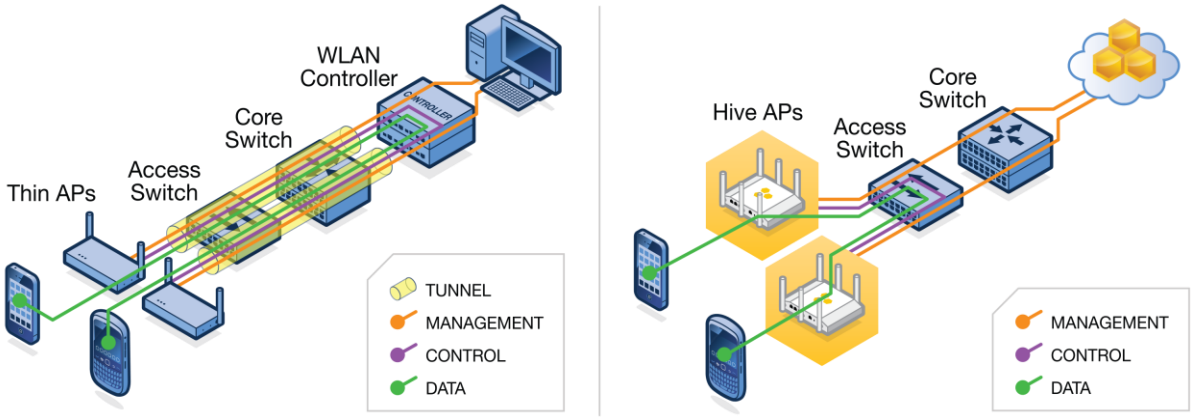
Aerohive offers a number of cloud-managed WLAN solutions to satisfy the requirements of midmarket and distributed enterprises. Aerohive provides a range of both 802.11ac and 802.11n access points to meet the needs of different enterprises through its Cooperative Control architecture, which provides the benefits of a controller-based WiFi solution without requiring a controller or overlay network. Aerohive's solution distributes all control functions, policy enforcement, and data forwarding to edge devices while maintaining a centralized management system for monitoring and configuration — similar to how routing and firewall systems function.

With Cooperative Control, APs are grouped together to share control functionality, allowing more linear scaling, and removal of data bottlenecks. With Aerohive, network survivability is built in, and interruptions to cloud connectivity do not impact ongoing network operations. This is because data does not go to the cloud to enable control or policy enforcement functions, such as authentication, roaming, or QoS. These functions are all handled at the edge by Cooperative Control architecture as shown in Figure 1.

Aerohive combines enterprise-class access points, branch routers, and switches with a suite of Cooperative Control protocols and functions to provide unified wired and wireless access that ensures consistent policy, permissions, and security based on identity and device type regardless of user location. HiveManager provides a centralized management console for the entire network that enables global policy, configuration, and monitoring with full application visibility of thousands of access points, routers, and switches. HiveManager lowers operating costs by speeding deployment, configuration, and monitoring of the entire network.

Figure 1

Legacy Controller-Based Solutions and Aerohive's Distributed Control Architecture



Source: Aerohive, 2014

Challenges

As mentioned, there are some challenges inherent to cloud-managed WiFi. Large enterprises, as well as WiFi "traditionalists," may want to stay with a tried and tested controller architecture. Given that vendors that offer both wired and wireless network infrastructure are increasingly rolling out highly capable unified networking management tools, there could be some resistance to a more pure-play wireless model such as the model offered by Aerohive.

Moreover, in any cloud-managed environment, there is the rare possibility of a cloud connectivity failure. However, Aerohive's Cooperative Control allows for short-term cloud outages not to impact network operations at the edge as user connectivity does not rely on the cloud. Finally, when Aerohive's solutions are evaluated for the first time, architectural differences may bring about resistance from WiFi traditionalists in an organization. Organizations should assess these challenges as part of a thorough evaluation of their enterprise WiFi options.

Conclusion

IDC has seen explosive growth of cloud-managed technologies for the enterprise, and that has started to manifest itself in network infrastructure investments. This interest has been driven in large part by the demands that mobility/BYOD, cloud applications, IoT, voice/video/collaboration, and other mission-critical functions have placed on the network. SMEs along with midmarket and distributed enterprises are more acutely feeling these demands.

The flexibility that cloud networking allows in terms of opex, staffing, and scalability, along with its ease of installation with automated configuration, makes cloud-managed WiFi a strong contender for these enterprises. Aerohive's solutions offer many of these capabilities. To the extent that the company addresses the challenges described in this Technology Spotlight, IDC believes that the solution set is well positioned for success.

ABOUT THIS PUBLICATION

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

For more information on IDC, visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserv/custom_solutions/index.jsp.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com