Minimizing Cost, Maximizing Value:
WLAN Management Moves to the Cloud

A Farpoint Group White Paper

Document FPG 2011-288.1
June 2011

While wireless and mobile topics have been central to any discussion regarding IT strategy for some time, an element that goes hand-in-hand with mobility is the provisioning of a broad range of services in the cloud. *Cloud*, for our purposes here, refers to any capability that is made available via a network connection, this so as to encompass both public (typically, Web-based) as well as local or private-cloud services. The concept of cloud services, often referred to as Software as a Service, or SaaS, is of course very much in keeping with that other key contemporary trend in IT, *virtualization* (in this context, of services) which today forms the cornerstone of numerous IT strategies. But one of the most interesting possibilities in cloud-based services today is to offload or even outsource capabilities that would otherwise need to be provisioned and managed locally – in other words, converting the capital expense (CapEx) involved in implementing a needed IT service into an operating expense (OpEx) – the opposite of the advice we normally offer with respect to overall IT financial strategy. But, as we'll explore in the Farpoint Group White Paper, the flexibility inherent in provisioning the service in question here, WLAN management, in the cloud, along with the potential for bottom-line cost savings, is enormous. These two factors – flexibility and economics – after all, drive today's steadily-increasing interest in the cloud for everything in IT, from processing to storage to Web-based publishing and interaction to – wireless LAN management.

OK – we'll admit that, at first glance, the idea of an *essential, mission-critical* capability like WLAN management in the cloud might seem somewhere between counterintuitive and just plain crazy. After all, network management of any form includes such a broad range of vital services that any thought of an alternative to local residence might be easily dismissed without further consideration. On the contrary, though, and again as we'll discuss in detail in this document, the provisioning of WLAN (and even wired network) management services in the cloud has enormous potential for addressing evolving requirements as networks grow and change, enhancing reliability, minimizing time-to-solution, provisioning no-compromise "big system" services even in entry-level installations, providing unprecedented convenience and location-independent operations, and creating the possibility of enormous cost savings even though CapEx is being converted to OpEx. We believe that cloud-based WLAN management will in fact become obvious and natural, just as has become the case for such services as salesforce.com and dropbox.com.

In short, the cloud is now about *all* aspects of IT, with, assuming no compromise in function or reliability, the key decision point as to which alternative is optimal based largely on cost. But it can be argued that network management requires a more detailed consideration here; after all, network management is most certainly *not* a commodity and the huge range of function inherent in such a system will have an enormous impact not just on the productivity of its primary users, network operations staff, but also on the productivity of network users across the enterprise – essentially, then, *everyone*. So the selection of a WLAN management system and a deployment strategy for that solution can have far-reaching impacts that are not always obvious. We would of course encourage anyone specifying a network management solution to carefully consider the overall WLAN functionality required (and we'll review the key broad subcategories of

services within WLAN management systems below), and *then* decide on a deployment strategy. From our experience with cloud-based management systems so far, however, we believe that cloud-based deployments will become a very popular if not *dominant* direction over the next few years – yes, depending upon the specific implementation, of course, the cloud really is that good.

Exploring WLAN Management – Requirements and Strategies

Network management, wired or wireless (or, ideally, both together in a *unified* implementation) does not have anywhere near the visibility of most other IT functions, even within IT organizations. Long the province of a few specialized individuals within network operations departments, network management has historically been sited in specialized facilities, especially in larger organizations, commonly called Network Operations Centers, or NOCs. NOCs often have very much of a "Mission Control" look and feel because that is precisely the level of function which they support. The key objective of the NOC is to provide both high-level and detailed views into precisely what is happening within the network at any given moment in time and enable trained operations staff to take whatever actions might be appropriate to ensure optimal performance and overall security and integrity for what amounts to the circulatory system of the organization it serves.

Over time, however, and as has been emphasized especially during the recent economic recession, the overall expense associated with running a NOC has been questioned as IT budgets are reallocated and often cut. The current approach to NOCs in all but the largest organizations, then, is to consolidate functions, minimize staffing requirements, and automate wherever possible. But as wireless LANs with quite literally thousands of access points and tens to hundreds of thousands of users become more common, the demands placed on management systems only grow. We thus have two trends working against one another, visualized as the need for cost-effective solutions maximizing function while simultaneously minimizing cost, with cost often a function of the skilled labor required within network operations.

And such is the case irrespective of the size of the organization - indeed, Farpoint Group has found that, while it's popular to think that smaller organizations can get by with less network management functionality, the opposite is instead the reality: the only difference between network management deployments in larger and smaller settings is in *scale*, not function. All of the services and capabilities detailed below are required in *every* network installation.

This being said, consider the broad range of functionality required in just the wireless end of a contemporary network management system today (see Figure 1):

- *Planning* – Management tools can often be very useful even *before* the network is deployed. Some have the ability to simulate RF performance, and just using the system to visualize the placement of access points can be valuable in gauging

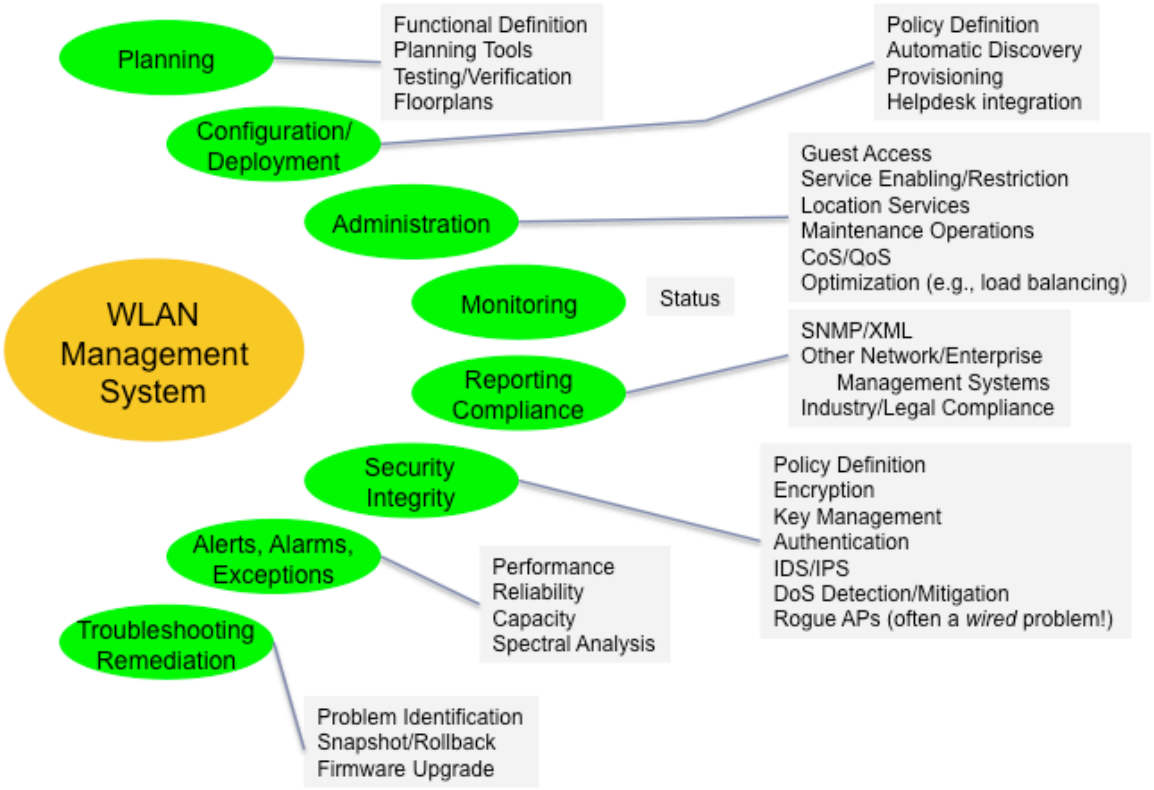

Figure 1 – An overview of WLAN system management functions. The range of functionality here can involve reach hundreds of specific settings, monitored variables, and reporting options. *Source:* Farpoint Group.

overall requirements. Existing network management logs provide a wealth of information as to demand by application, location, and time of day, making it much easier to decide on which infrastructure elements to deploy or upgrade - whether these involve a rip-and-replace strategy or perhaps just a few more APs. Some management systems also perform inventory management for both functional units and spares.

- *Configuration and Deployment* – Apart from the site survey, which we continue to suggest isn't always necessary, management consoles can perform all of the initial configuration with respect to SSIDs, VLANs (if used), class of service, user permissions, connections to external directory, security, and other management databases, and performing initial functional verification. Fault-tolerance, as required, can also be configured at this time. In short, all functions necessary before users are allowed on the system must be provisioned in the management system.

- *Administration* – Every functional network has requirements for changes and additions, and these are also handled via the management system. These can include enabling guest access on a per-user (and/or per-use) basis, enabling or

restricting mobility based on specific device, location, time, or user profile, changes to user profiles, and more.

- *Monitoring* – While the "Big Board" approach to network operations may be on the decline, if for no other reason than recession-driven restrictions in the operational budgets involved, knowing what's happening in the network at any given moment in time can be both reassuring and a valuable aid to resolving problems – or even becoming aware of potential impacts before they begin to affect user productivity. Most network management systems include numerous functions that provide a display of raw data as well as instant analysis and visualization of complex, often multi-variate and multi-dimensional data. And note that such analysis must be mobile as well, available on an anytime/anywhere basis.

- *Alerts, Alarms, Exception Handling, Troubleshooting, and Remediation* – And, of course, it's vital to be able to define error conditions and produce alerts when these occur, and to provide alarm limits which might be related to throughput ceilings being reached, numbers of connections reaching a given threshold, or other capacity-related conditions that may ultimately dictate adding more APs or other equipment to deal with the problem. As networks always grow over time, driven by growth in number of users, devices, application demands, and more complex traffic types, most notably voice and video, alerts and alarms provide a convenient mechanism to proactively address eventualities – or to know that action is required for unusual conditions, such as the failure of an AP (most often due to power inadvertently being cut, but other possibilities do exist here) or other conditions requiring the attention of a network technician. Ideally, though, automation inherent in the management system will address a broad range of conditions with minimal operator involvement.

- *Security and Integrity* – Network management of necessity involves many functions related to security, from the definition of 802.11 security settings to privileges by class of user to monitoring for intrusion and subsequent (and even automated) remediation. A number of databases can be involved in this process, and links to external functions, like RADIUS and directory services, are becoming more common if not required.

- *Reporting and Compliance* – As both local policies (including security, acceptable use, social networking, mobility, and others) and industry-wide regulations (such as PCI, HIPAA, and Sarbanes-Oxley) become much more important to IT operations, network management systems often include both monitoring and reporting functions with compliance in mind. Interfacing with external systems via SNMP or XML can also be important.

- *Assurance* – And, finally, it is not unusual today to find entirely separate systems, often with their own hardware sensors, deployed to handle IDS/IPS, spectral assurance (monitoring the physical layer of the network for interference),

inventory, compliance, and many other functions. Farpoint Group believes that, over time, and with only rare exceptions due to the requirements of auditors in certain industries, assurance functionality will be rolled entirely into network management system proper, enhancing once again the value of the management console.

It is important to note here that we are only talking about the *Management Plane* (see Figure 2) of a WLAN system, and not the Data or Control Planes which define how data moves within the WLAN system and where system control functions reside, respectively. Farpoint Group believes that while a fully-distributed data plane, what we call a *direct-forwarding architecture*, and a distributed control plane eliminating bottlenecks and maximizing redundancy and fault-tolerance, are both rapidly coming to dominate successful and scalable WLAN systems architecture, the management plane must *always* and regardless be implemented as a *centralized* resource. It must, in other words, allow dominion over the entire network from a single (if mobile or relocateable, in many cases) location. But note this says nothing about how or where the management plane is implemented – and, as we will discuss below, leaves the door wide open (and, in fact, puts out the welcome mat) for a cloud-based implementation.

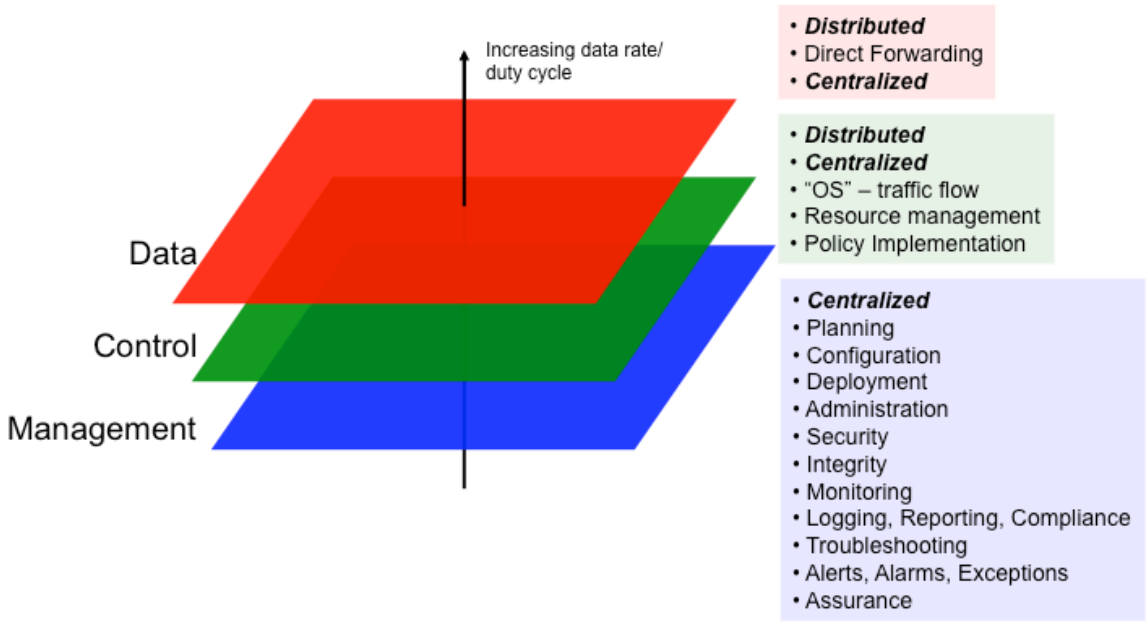

Figure 2 – Functional "planes" used to decribed a given WLAN system architecture. While a degree of variability remains in how data moves and where control functions reside, management functionality must be centralized, but available to authorized operations staff from any convenient location. Management is thus well-suited to residence in the cloud. *Source:* Farpoint Group.

Implementing WLAN Management in the Cloud

As we noted above, network management has historically been implemented internally to the enterprise, often within dedicated NOC facilities. This was partially out of necessity, as decentralized implementations simply did not exist, and as it made sense to group network operations and support experts around a single set of consoles and displays. The cost here could range from a few PCs or servers and management software to dedicated, custom-built facilities. But the economics of such strategies were called into question particularly during the recent recession, when IT organizations began to understand the new reality of having to dramatically improve productivity across the board. This ultimately meant that capital costs would need to decline, but without a corresponding increase in operational budgets – in short, getting more done with less became a universal mantra within IT.

At the same time, the requirements placed on management consoles continued to increase, as wireless augmented and then increasingly replaced wire at the edge for user access, and as the range of function required and desired by operations staff continued to expand. Smaller enterprises found themselves at a serious disadvantage, with the need for "big system" management functionality but without the budgets required to obtain such. And, of course, growth has remained a concern even during the recession as the number of users, their demand for a broader range of network services, and the increasing number of wireless devices and volume of traffic, including time-bounded services like voice and streaming video, all continued to expand. Scalability became a key concern in all network planning and operations, with management functionality no exception.

Cloud-based WLAN management, then, must involve no compromise in functionality – or reliability – if it is to be successful. Indeed, we would argue, especially now that we have some experience with the concept put into production, that cloud-based WLAN management can indeed be so effective that it may become the *preferred* model for all but a few of the largest organizations, and those in the government space where local facilities are required by mission, specification, and regulation. But there is one concern that repeatedly comes up when this topic is discussed among operations professionals – what happens if the WAN link to the management service goes down? Being without critical management capabilities might be little more than an inconvenience, especially if the outage is brief, but the situation could indeed be much worse.

The answer here, though, might be surprising: with so much of overall enterprise operations now dependent upon access to the Internet and the Web, losing WLAN management for a period is likely to be the least of anyone's concerns. In short, availability and reliability here are addressed identically to any other network integrity requirement, via best practices with respect to geographic redundancy on the part of service providers, access redundancy with respect to ISPs and related services, and distributed staff trained in the operation of the console within the enterprise. Indeed, given the highly-distributed nature of modern enterprises, with staff spread quite literally around the globe but linked via network infrastructure from many different suppliers (including the enterprise itself with respect to the wireless LAN), there should be little

additional concern regarding the residence of WLAN management functionality in the cloud.

But, quite literally, an increased emphasis on system-wide continuity and contingency is the only cautionary note we can apply here. The benefits, on the other hand, are both extensive and valuable:

- *No compromise in function* – We would of course never suggest a compromise in capability unless absolutely necessary, but, as we noted above, none is required in moving WLAN management functions to the cloud (see Figure 3). There should be no difference in the level or range of service between the two delivery options, and, regardless, all of the facilities any given installation could require can, depending upon implementation, be present.

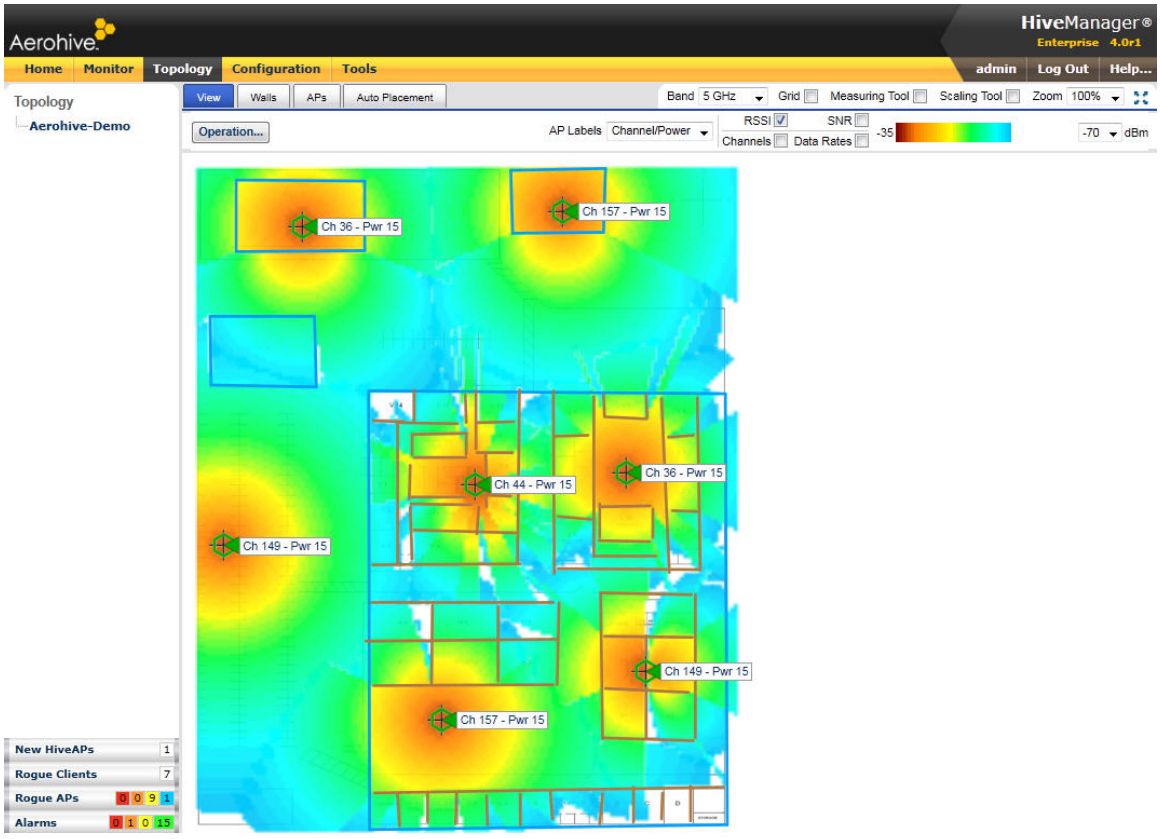

Figure 3 – An example of a cloud-based WLAN management console, in this case Aerohive's HiveManager Online (HMOL). All features, in this example a detailed look at RF performance, are identical in both the server-based and cloud-based versions. *Source:* Aerohive Networks.

- *Simple incremental growth* – A cloud-based management capability offers required "big system" functionality from the start, and allows an organization to grow without the need for major hardware and software upgrades or replacement of management systems - with the often-accompanying service disruptions and training expenses. Upgrades and both geographic and local-density expansion are simplified.

- *Improved reliability* – A cloud-based solution makes high availability (including 7/24/365) much easier and cost-effective to implement. It is also much easier and cost effective to provide the redundancy necessary for fault tolerance, although it is a good idea to include one's requirements here in any RFP.

- *Reduced facilities requirements* – There are of course no local space, power, HVAC, or other facilities requirements beyond a client, which, again, could be almost any browser-based device - even, in some cases, a smartphone.

- *Location-independence* – And, of course, network management staff has full access to all of the information and control mechanisms required to keep their network on the air from any location that has access to the Internet.

And there is one more – a significant cost benefit in many if not most cases. We noted above that our usual advice with respect to infrastructure has historically been to substitute capital expense for operating expense, this being the result of a simple analysis that shows that newer technologies always demonstrate improved price/performance, with corresponding productivity benefits for both operations staff and users, and that operating expense is labor-intensive, with precisely the opposite effect – higher costs. So our advocating the substitution of a service (operating) expense for the infrastructure required to build an equivalent management capability seems counterintuitive at best.

But it's not. While a given cost analysis will of course depend upon the specific needs of a given organization, customers applying the cloud strategy avoid needing to commit resources to both local infrastructure (servers, appliances, licenses, facilities, etc.), and to at least some operational staff otherwise required. All of this is instead amortized by the service provider across a potentially very large customer base, lowering costs and thus service prices – which, based on a recent study we performed, can be very inexpensive indeed. While it will still be important to verify the capabilities of any proposed supplier of management services, we believe that a competitive market will evolve here and that the usual benefits of such will accrue – improved quality and variety of services at falling prices. A cloud-services provider will regardless see economies of scale that competition will at least in part pass on to the customer as improved value. Expenses become predictable and otherwise increasing staff costs can be mitigated to a very great degree for both supplier and customer.

Finally, we alluded above to what we believe will become a trend: *the rise of the third-party management services industry*. While some WLAN system vendors will undoubtedly fill this role themselves, we believe that resellers will look upon this possible line extension here as the huge opportunity that it is. So we will shortly see a large variety of products, service providers, and business models practically assuring a workable if not optimal plan for essentially every WLAN customer. And, of course, with management services becoming an important differentiator, WLAN system vendors will be heavily motivated to continue the high rate of innovation we've seen in WLAN management systems to help their resellers (and thus their customers) be productive and successful.

Aerohive's HiveManager Online: Big-System Management in the Cloud

Wireless-LAN leader Aerohive Networks rose to prominence with a highly-distributed, controller-less system architecture, but, as we discovered in researching this White Paper, their HiveManager Online NMS (network management system) deserves an equal amount of attention. A full-featured management console with a very broad array of function, HiveManager Online (often called HMOL) was one of the first cloud-based WLAN management services to appear, duplicating the function of HiveManager as implemented on a server or appliance. We found HMOL very easy and straightforward to use, and its dual-mode operation seems ideal for organizations that want to get up to speed quickly but have all the functions a very large organization might eventually need. Express (or "Easy", as we call it) Mode allows new users to get up to speed and operational quickly, while Enterprise Mode exposes the details and extended capabilities where required or after users have some initial experience with the product.

"HiveManager Online is a very natural extension of our product line," said Stephen Philip, Vice President of Corporate and Product Marketing at Aerohive, in a recent conversation. "It's the same set of capabilities in the standalone HiveManager product, but available on an on-demand basis. Customers can start small and grow with the same management platform over time, minimizing training and other operational costs."

We also spoke with Ty Puckett, Director of Information Technology for Greenway Medical, a vendor of electronic health record solutions based in Carrollton, Georgia. Mr. Puckett recently converted to Aerohive equipment from another vendor, and the availability of HiveManager Online was a key driver for the switch. "The financial savings inherent in HiveManager Online literally enabled us to upgrade our entire Wi-Fi infrastructure, which is currently 27 APs but which will grow significantly over the next few years," he told us. He's also used HiveManager Online for a large off-site event, with configuration of a fairly complex multi-service network was performed, again literally, in minutes. And location-independence is also a key benefit, Mr. Puckett told us, with staff being able to monitor and operate the network literally from anywhere.

The Evolution of Cloud-Based Network Management

While we may be a little bit out on a limb here (but only, we believe, a little), cloud-based WLAN management is poised to become a major alternative in the network-management space. In fact, we believe that a majority of WLAN installations will be using cloud-based management over the next five years. The appeal to entry-level enterprise installations and small/medium businesses (SMBs) is obvious, but we believe that a simple financial cost/benefit analysis and a verification of the reliability of a given

solution (again, in concert with an enterprise's overall IT continuity plans) will show the wisdom of a strategy based on cloud services for almost all WLAN installations.

Local, dedicated management facilities will still be the preferable alternative, we believe, in many if not most high-security applications (particularly governmental departments and agencies), larger installations (tens of thousands of access points and beyond), and other special situations. Many of these organizations will take advantage of extant NOC facilities and network management organizations, as well as capturing the cost advantages of server virtualization that may already be in place. But many installations will start with cloud-based management and stick with this strategy even as they grow to considerable size and scope, and the NOC as we know it may have seen its best days.

The key advantage, we believe, to a cloud-based management strategy will be in the ability of an installation to maintain operational continuity as their network scales up, minimizing rip-and-replace expenses, re-training, downtime, service disruptions, and operational errors which may occur during a cutover. And even the smallest installations get "big system" capability and other features that to this point have been economically or operationally infeasible, or simply unavailable in entry-level products.

And it's also intriguing to think how a cloud-based network-management strategy might itself evolve over time. Among the new capabilities here are wired-network integration, noted above as *unified networking*. We've previously expounded on our belief that unified networking, with unification especially at the management plane, will become essential if for no other reason than cost minimization (as it is less expensive to operate one network instead of two) and the requirement for unified functionality is such capabilities as IDS/IPS and AAA. It's regardless no longer adequate to describe the WLAN as an "overlay" on the wired network; rather, the wireless LAN *is* today the primary or default access mechanism for the enterprise, with the wired network serving in a supporting role in terms of the interconnection of key WLAN components (and, of course, fixed elements like printers and servers). Unified management is in the early days of its evolution, but this is a key direction that will eventually become the dominant operational model in organizations of all types and sizes. We also believe that *mobile device management*, which extends operational control to what is today the new edge of the enterprise network – PCs, tablets, and handsets – will also eventually be integrated into network management consoles, including in the cloud.

It's clear that a competitive market in cloud-based WLAN management services is now in its infancy, and, as this market grows, the cost and service benefits for enterprises and other organizations will be enormous. As we noted above, the cloud is the future of much of IT today, and network management is certainly no exception.

Ashland MA USA
508-881-6467
www.farpointgroup.com
info@farpointgroup.com

The information and analysis contained in this document are based upon actual testing and publicly-available information sources believed to be correct as of the date of publication. Farpoint Group assumes no liability for any inaccuracies that may be present herein. Revisions to this document may be issued, without notice, from time to time.