

# Rethinking Wireless LAN Infrastructure: *Virtualization is the Key*

*A Farpoint Group White Paper*

Document FPG 2010-341.1  
October 2010



As wireless LANs continue their rapid evolution to primary and even default connectivity across the facilities of enterprises (and similar venues) of all sizes and types around the planet, we continue to be impressed with the wide diversity of thought regarding strategies for designing, implementing, managing, and growing these crucial resources. Part of the reason for this divergence, to be sure, is the corresponding rapid evolution of both key industry standards as well as fundamental implementation technologies. And, of course, the faster/cheaper/better inherent in high technology products also serves to prompt a diversity of thought here as well. But, still, it's fair to ask: while we're not likely to see a single one-size-fits-all solution anytime soon, what are the key elements of WLAN system architecture and design that will have the greatest bearing on the success of large-scale enterprise deployments? That question, and a series of recent discussions with key industry players, provides the motivation for this Farpoint Group White Paper.

To begin, all key basic concerns regarding wireless technologies and wireless LANs have in fact been addressed, including most importantly:

- *Essential functionality* – Wireless LANs provide all of the services of a wired LAN without restriction. All network applications are supported, even those with time-bounded constraints, most notably voice, but also, increasingly, video. And wireless LANs can scale to provide access across even very large venues, including campuses and metropolitan settings. The only key differentiation with wire in terms of performance is the current lack of availability of wireless LANs with gigabit-plus throughput, but these will shortly be available.
- *Mobility* – Continuous connectivity and the improved user responsiveness it enables are simply not possible if users must be tied to their desks to gain access to network resources. And, after all, the network is now essential to virtually *all* business operations. Mobility, unique to wireless connectivity, is a key motivation for (and benefit of) migrating to a wireless LAN.
- *Cost* – The total cost of ownership (TCO) of WLANs is now well understood. While cost models differ, a given installation can often be justified on the savings over the life-cycle costs of a wired infrastructure alone. WLANs are usually *much* less expensive today than their wired counterparts, resulting primarily from decreasing product prices and the need to install and maintain far less cable at the edge of the network – oh, and clients are now essentially free as well. Adding in user convenience and productivity, and the financial case for the WLAN becomes overwhelming.

We should note here, however, that it's important to differentiate *capital expense* (CapEx), that which is required to plan, install, and make a given infrastructure operational, from *operating expense* (OpEx), which includes the often labor-intensive elements of support, troubleshooting, ongoing management, and related activities. OpEx can often be *much* greater than CapEx over the life-cycle of a given installation, and we'll return to this topic below.

The bottom line: *wire to the desktop simply can no longer compete*. Adding voice to the WLAN completes the picture, and finally cuts *all* cords to the desktop (other than those required to recharge batteries, of course!) once and for all. WLAN installations are thus proceeding at a rapid pace, but a few key challenges remain. These include:

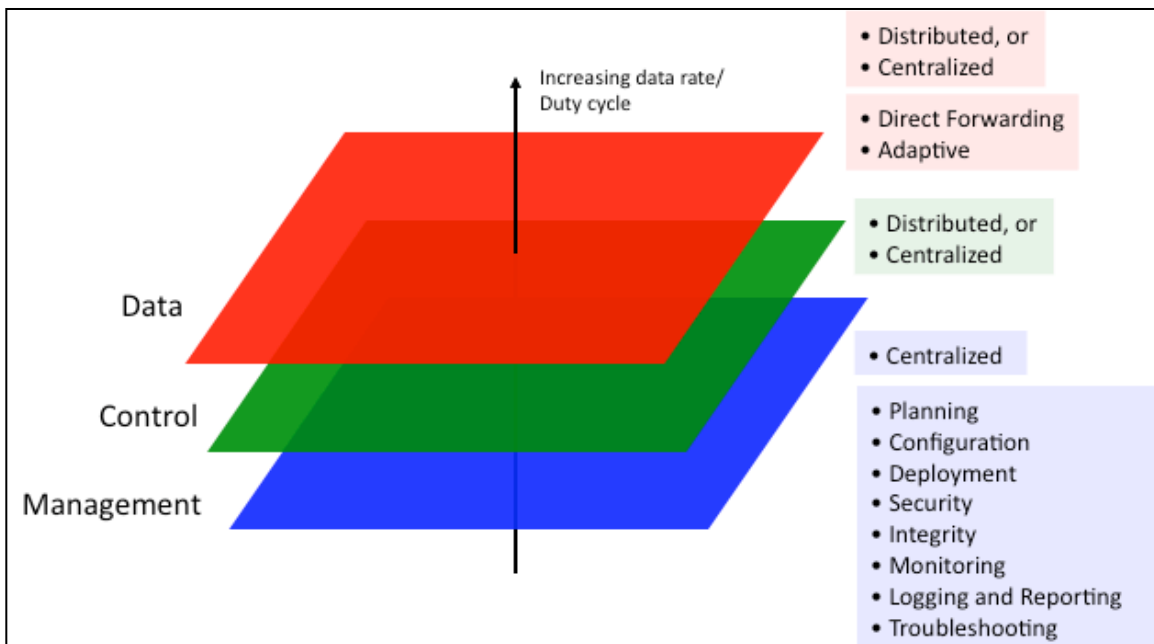
- *Performance* – While often used to denote throughput alone, performance in the domain of a wireless LAN must be viewed more broadly. WLAN performance metrics must also include *range* (more properly, the throughput available at any given distance, sometimes called *rate vs. range*) and, more importantly, *capacity*, which is the ability to handle the simultaneous requirements of a potentially large and diverse base of users and applications with the greatest efficiency possible, thereby contributing to the minimization of TCO. Most importantly, while the focus of WLAN technology has historically been on the radios required, the performance impact of *architectural choices* made by system vendors must be considered, especially in terms of potential bottlenecks as installations grow in scale and otherwise evolve.
- *Security* – While the IEEE 802.11 standard addresses basic link-layer security, new possibilities for attacks and other vulnerabilities are discovered on a regular basis. It's critical, then, for enterprise network managers to carefully discuss security capabilities and enterprise objectives with their vendors, and also to verify that solutions are both properly implemented and in concert with overall enterprise security policies and operational goals. And, similarly, all functional elements in any solution must be examined for potential impacts on security.
- *Reliability* – With WLANs taking on mission-critical roles, failure is never an option. But configuring for fault-tolerance and resilience can add significant cost to any enterprise solution, as redundant hardware is often required. Still, this is an area ripe with opportunity, as we will further discuss below.
- *Management* – Farpoint Group believes that WLAN network management capabilities will ultimately become *the* most significant differentiator between varying WLAN implementations. The importance of management is often overlooked by enterprises during the purchasing process, but we cannot stress enough just how vital this functionality is. Superior management capabilities are key to lowering both OpEx and CapEx and thus, again, to minimizing TCO.
- *Scalability* – Finally, it's vital that any installation be able to grow *non-disruptively* over its useful life, adding capacity, adapting to new missions, and providing additional coverage. Rip-and-replace is an occasional fact of life in networking, but such should be an infrequent strategy (after initial deployment) for 802.11n-based wireless LANs being installed today - assuming the requirements of growth are considered up front, when initial configurations are determined and purchasing decisions are made.

All of this leads back to a core question: what key characteristics must a WLAN infrastructure possess in order to best meet these challenges? And are there decisions that vendors and users alike can make to smooth the path to an optimal WLAN installation?

## Rethinking Wireless LAN Infrastructure

Conceptually, a wireless LAN is quite simple: imagine a black box with an antenna on one side, and a wired (Ethernet) connection on the other – and that’s it. The core element here is, of course, the ubiquitous *access point (AP)*, which performs this function. Enterprise-class systems, of course, are designed to include perhaps thousands of APs, and the wide variety of architectures that vendors use to implement these solutions is again intriguing – and *architecture*, as it turns out, can have a profound effect on the issues we enumerated above.

Farpoint Group uses what we call the “Planes Model” of wireless-LAN architecture (see Figure 1) to describe the required conceptual architectural elements of a WLAN system and where they can reside. There are three key functional components here, as follows:



**Figure 1** – The “Planes Model” of WLAN architecture. *Source:* Farpoint Group.

- *Data Plane* – The data plane describes how user data moves within a particular architecture. There are two alternatives here:
  - *Classic Thin AP* – Introduced about a decade ago, this innovation began with the creation of a new physical element, the *Wireless-LAN Controller* (which we’ll discuss below), and the relocation of functionality

historically based in the AP to this separate physical unit. Most importantly for our discussion here, *all* user traffic in this model flows between the AP and the Controller, and is subsequently redirected to its destination at either of these endpoints.

- *Direct Forwarding* – This model is sometimes viewed as a return to the classic “thick” AP model that dominated during the 1990s, but such is not entirely fair, again as we’ll discuss below. In this approach, regardless, the AP forwards traffic directly to a destination address and user traffic does not flow through the Controller. The Controller is still present here, managing operational functions as determined by a given vendor.

While both of these models clearly work, the Classic Thin AP approach places additional load on both the Controller and the data network connecting it to the AP. A bottleneck here can impact performance, and new Controllers and even network infrastructure (primarily gigabit – or faster – Ethernet switches) may be required midway through the life of a given installation as network loads scale up. Note that Farpoint Group recommends gigabit Ethernet for all AP interconnection today, as 1 Gb can easily swamp Fast Ethernet. But the *aggregate* traffic flowing into a Controller in the Thin AP model can easily outrun even gigabit Ethernet, necessitating careful network planning, monitoring, management, and upgrades.

- *Management Plane* – Management is, of course a large collection of functions including but not limited to installation planning, configuration, policy definition,



**Figure 2** – A partial list of the functions of the management plane in a WLAN architecture. Management must be centralized, and the importance of these capabilities in successful installations cannot be overestimated. *Source:* Farpoint Group.

security policy, deployment, alerts/alarms, monitoring, reporting, and many more (see Figure 2). The management console and its constituent databases are thus critical elements in the success of any enterprise-class infrastructure. But while the data rates and volumes involved at the Data Plane can indeed be enormous, the data load in the Management Plane is exactly the opposite – small amounts of data, usually moved on a low-duty-cycle basis. It is convenient to think of the bulk of activity occurring in the management plane as essentially the setting of policies and otherwise making entries in security and other management databases, along with monitoring (primarily alerts and alarms) and *ad-hoc* queries and reporting. It's also important that management systems be able to handle all relevant functions across large and widely-distributed operations.

So while the data plane needs to be *distributed*, the management plane must be *centralized*. But one more functional plane is required to complete our operational model:

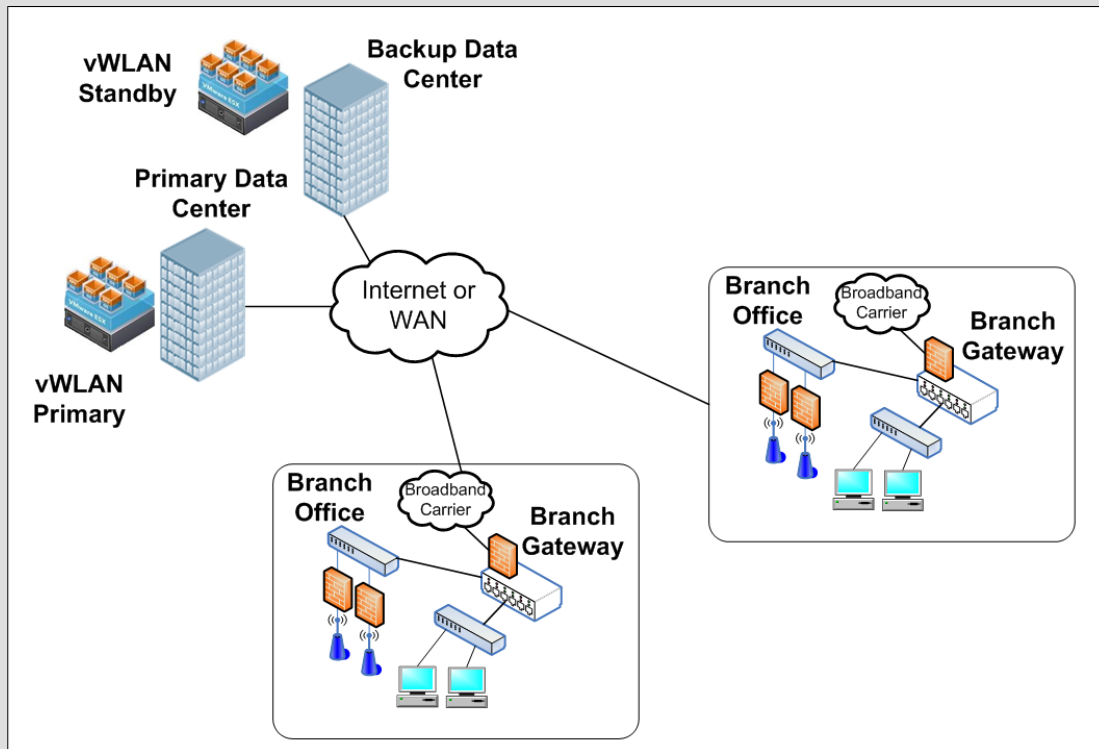
- *Control Plane* – We like to think of the control plane as the “operating system” of the wireless LAN. Whereas the management plane defines policies, it is the control plane that carries these out. Thus key functions related to the implementation of security, integrity, scheduling, policy enforcement, and other system-level tasks occur here. Traditionally, the control plane has been fully distributed, there being no alternative in the case of traditional (sometimes called “thick” or “fat”) APs. The rise of the Thin AP model, however, with its dependence upon a physical Controller, has resulted in control planes that are in many architectures completely centralized. While the debate continues to rage here, Farpoint Group believes that the increasing momentum towards direct-forwarding architectures minimizes the requirements placed on the control plane, allowing the centralized-control model to compete without having to deal with the potential enormous data loads presented by the Thin AP model. We therefore, consequently, see the Control and Management Planes merging, as both can now be realized as purely-software functions with low data-load and duty-cycle requirements. Thus the Control Plane and the Controller itself continue to evolve - and we can take this evolution one very important step further.

## Virtualizing the Control Plane

*Virtualization* is a very hot topic in IT today, and with good reason: this technique, broadly applicable across many IT functions, can dramatically reduce the requirement for additional hardware, along with its operational-expense components, including requirements for physical space, power, cooling, and maintenance and upgrades. As there is significant variability in terminology here, we use the term virtualization here in the sense of *virtual machines*. For those unfamiliar, most modern PC-class microprocessors implement machine instructions that allow the creation of software constructs, called virtual machines, which emulate real computers under the control of component of system software known as a *hypervisor*. The popular VMware products serve as examples here. The bottom line regardless is that a single server or appliance can be

## Bluesocket's vWLAN Architecture

One of the more intriguing approaches to addressing the Control Plane question comes from Bluesocket, a leading wireless LAN company based in Burlington, MA. We recently spent some time with the firm exploring their unique strategy for meeting the challenges that we outlined in this White Paper, and were more than interested when a discussion of their *Virtual Wireless LAN (vWLAN)* architecture (see Figure 3) revealed a number of innovations complementing our thesis here. Of course, the term “virtual” now has somewhat indeterminate status throughout all of information technology, and is used in a variety of ways within the wireless-LAN industry. Bluesocket's terminology fits the most common definition, using virtual machines to host key elements of their solutions. Company executives stress flexibility, fault-tolerance (which they describe as “zero failover time”), scalability, and of course, security, which has always been a featured element in the company's strategy. vWLAN installations are now underway and we've been promised access to a customer for a real-world evaluation of just how well this architecture works. We hope to have that soon, and we will issue an update to this White Paper once our explorations here are complete.



**Figure 3** – An example of Bluesocket's vWLAN architecture in a specific application. Controller appliances or virtual machines can be located wherever it is convenient, and fault-tolerance is and scalability are both simplified via virtualization. *Source:* Bluesocket Inc.

In the meantime, a statement made by Parick Foy, VP of Engineering at Bluesocket, caught our attention. “The future of the enterprise-class WLAN is inextricably tied to software and virtualization. Since configurations, mission, volumes of users and traffic, and overall scale will change – often dramatically – over the useful life of a given deployment, we think our greatest value-add is in our ability to respond to these challenges with an unparalleled degree of flexibility and cost-effectiveness. That's why we're here.”

running several simultaneous operating systems with their own applications and users, and isolation between these virtual machines assures both security and integrity. Modern server-class microprocessors are in most cases easily powerful enough to handle this type of load with no real concerns about performance, and, again, many IT shops today depend upon (and, we believe, *should* depend upon!) virtualization as a matter of course.

This brings us to an interesting possibility: given that the Control Plane will see lower data rates in a direct-forward architecture, and given that the Control Plane and the Management Plane are both essentially software functions, and given that the Management Plane in many cases already runs on servers using virtual machine hypervisors, it clearly makes sense to combine the Control and Management Planes on a single server, and perhaps even in a single software element. So doing offers opportunities to minimize both CapEx and OpEx, as the Controller is now virtualized, and scaling up a WLAN infrastructure becomes little more than an exercise in server configuration. Growth is inexpensive, smooth, and non-disruptive, with the addition of new Controller capacity reduced to loading new software onto a virtual machine.

There are three important additional benefits to the virtualization strategy worth mentioning here, as follows:

- *Reliability* – Fault-tolerance is critical in any enterprise network. All enterprise-class WLAN architectures provide some degree of failover, from APs that re-configure should one of their number fail, to redundant Controllers that automatically assume the load of a failed unit. A Controller running in a virtual machine provides the ultimate in capability here, as it's easy to bring up a new Controller or have the software in hot standby as required. And TCO is certainly minimized via this approach, as fully-redundant configurations of dedicated-hardware Controllers can add significant cost to any given solution.
- *Flexibility* – Software-based Controllers can reside essentially anywhere in a network that's convenient, and it's easy for WLAN vendors to revise and enhance Controller functionality, both in terms of fixing bugs and in adding new features. The term "software-defined WLAN" comes to mind, but it is perhaps a bit early to be thinking as such. Still, we do, and the possibilities are intriguing.
- *Managed Configuration Options* – Finally, Farpoint Group believes that many organizations, particularly SMBs but also some larger organizations, will take full advantage of the savings in both cost and complexity that come with a managed-services offering. Placing the Control and Management Planes in the cloud is already seeing some success, and we expect the installed base here to grow as both the economics become clear and third-party service organizations roll out their capabilities in this space.

## An Increasing Role for Virtualization

As the number of users, number of applications, application requirements (including time-boundedness), and even non-traditional services (for the WLAN, anyway) like machine-to-machine (M2M) communications all increase, the WLAN is increasing its roles as the enterprise's mission-critical access network. As we have discussed above, we see the virtualization of key elements of this resource as a key direction going forward, and one that meets all enterprise networking requirements – including all of those that we listed as challenges above – without compromise. It's important to keep in mind that:

- Integrity, reliability, and availability must extend across *all* elements of a given installation; AP-based fault tolerance is only one component here. Virtualizing the Control and Management Planes augments a cost-effective path to this end.
- Scalability isn't just about adding new APs – the remainder of the infrastructure, as illustrated in our Planes Model, must non-disruptively scale as well.
- Virtualization is a key to the minimization of TCO. While we don't expect Controllers based on dedicated hardware to disappear anytime soon (indeed, they can be quite valuable in smaller configurations), moving as much function as possible into software has enormous benefits for vendors and customers alike.
- And, as we noted above, virtualization has real appeal for service providers who, we believe, will take on larger roles in the operation of WLANs in the future.

And even security can be enhanced, as virtualized implementations can be more easily secured and managed. In short, Farpoint Group believes that virtualization will play a key role in establishing the inevitable ubiquity of WLANs - and investments here on the part of both system vendors and users alike will continue to yield a clear advantage.



Ashland MA USA

508-881-6467

[www.farpointgroup.com](http://www.farpointgroup.com)

[info@farpointgroup.com](mailto: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.

**Copyright 2010 – All rights reserved**

Permission to reproduce and distribute this document is granted provided this copyright notice is included and that no modifications are made to the original.