The Next WLAN Challenge:
The Emerging Requirement for Multi-Site Management

A Farpoint Group White Paper

Document FPG 2003-233.1
December 2003

With wireless LANs (WLANs) now seeing significant application in enterprises of all sizes, it's really not too early to begin thinking about how to manage WLAN networks as they, and the firms they serve, grow. As is often the case, a WLAN here and a WLAN there have a way of rapidly increasing in size and scope to the point of mission-criticality, with all of the accompanying concerns. Will the WLAN provide the coverage and capacity required over time? Will it integrate with already-installed enterprise LAN systems and procedures? Will it quickly become an unmanageable headache threatening corporate security, network equipment and operations budgets, and perhaps worse? Even for cheering fans of wireless LANs (and that's us), none of the above should be taken lightly. Growth beyond a single floor, building, or campus is now a given, and WLAN network management tools to address this growth are required.

What is Multi-Site Management?

We're thus quickly entering the era of *multi-site wireless LANs* and *multi-site management (MSM)*, which we'll define here as those in one or more of the following categories:

- *Geographically-distributed WLANs* – wireless LANs can now span huge geographies, from campuses to branch offices, sales offices, retail stores, warehouses, kiosks, and beyond, on a national or even multi-national scale. We believe that these multi-site installations will in fact become the norm over the next few years, as demand for WLAN service increases (driven primarily by notebooks with WLAN adapters as standard equipment) and as larger enterprises seek to provide coverage in many if not most of their locations. We even see the corporate wireless LAN extended to the residence, as home access points become nodes on the enterprise LAN, and to public spaces via managed services provided by the wireless ISPs (and cellular carriers) operating public-access WLAN systems but providing secure pass-though services to their key enterprise customers.

- *Mixed-vendor deployments* – While it's never really desirable to mix access points (APs) of differing manufacture (or even model or firmware revision) in a given deployment, it's inevitable that, given the technological evolution inherent in WLANs, and such additional realities as corporate mergers and acquisitions, more than a few network managers will wind up with this challenge. Network operations management is going to want the same usage policies, security features, and management interface for all of these otherwise incompatible systems – not to mention the ability to roam, securely, across infrastructure elements that inherently don't talk to one another. Again, multi-site management is the solution to smoothly integrating and operating the elements of this scenario.

- *Legacy WLAN installations* – The history of the WLAN has been typified by rapid technological and product evolution. This is certainly true in the radio space, with the original 1997 802.11 standard evolving rapidly through the current a, b, and g physical layers (PHYs). But there's an even higher-performance PHY on the horizon (.11n), and many new medium-access control (MAC) layer features that may also re-

quire hardware upgrades, such as the Advanced Encryption Standard (AES) functionality in 802.11i. Of course, just because new technology and products come along does not mean that a current installation is necessarily obsolete. However, said current installation will likely not have the most up-to-date management capabilities, nor is it likely to be interoperable with newer WLAN gear without a lot of help – and that help is available via multi-site management tools. Similarly, the integration of legacy distributed access points with equipment based on the newer "switched" (we prefer the term "centralized") architectures will also require multi-site management techniques. And finally, many WLAN-enabled devices, especially those in industrial and commercial applications like bar-code scanners and scales, are likely to be in service for a long time if for no other reason than to accommodate existing depreciation schedules. These devices can be easily integrated and updated for contemporary management and security via multi-site management tools.

And this leads to a very important point – *the requirement for multi-site management is independent of the architecture of a given WLAN system or product*. Moreover, multi-site management also implies that all sites to be managed are connected over a WAN. But note that it's critical that multi-site management services be available even when WAN connectivity is interrupted – local control is required for security enforcement at the very least.

Benefits of Multi-Site WLAN Management

In short, the issues relating to WLAN growth will soon be overwhelming to organizations that have not given sufficient consideration to the multi-site management challenge. Below, we'll address many specifics relating to multi-site management. For the moment, though, we need to review the key benefits that accrue from such an approach. These include:

- *Minimizing network management complexity* through *common, centralized tools*.

- *Reduced capital expense* (CAPEX) through the requirement of fewer (and standardized to a given site) hardware components, more rapid deployment, lower installation-related expense, a lessened requirement for upgrading and replacing hardware, and a reduced (or even eliminated) requirement for on-site network-skilled installation labor.

- *Reduced operating expenditures* (OPEX) as a function of improved management staff productivity, less opportunity for errors in configuration or in attempted corrections that ultimately don't work (or even exacerbate the problem), and automated processing of routine (or not) exceptional conditions. All of these factors also contribute to the optimization of total cost of ownership (TCO) and return on investment (ROI).

- *Improved scalability and adaptability* as a growth-oriented infrastructure is put in place.

- *Support for rapid deployment* when required, with common systems and procedures centrally enforced and controlled.

- *Improved reliability, security,* and *overall performance*.

The trend towards multi-site management has been evolving for some time. With the deployment of now-classic access points incorporating network management, security, and roaming functionality, it became clear that additional hardware would be necessary to extend these vital functions across the islands of connectivity that these APs otherwise represent. This led to the evolution of what we have been calling *enhancer/completer* products that provide enterprise-wide mobility, improved security, and management functions across multiple clusters of APs. The rise of switched architectures has simply shifted the focus of management to the control of APs via switches rather than control of APs directly. Regardless of the specific scenario, the "sea of devices", "sea of APs", and "sea of switches" across multiple sites coupled with the need to support legacy hardware and highly-distributed enterprises make the need for multi-site management more than clear.

Elements of a Multi-Site Management Solution

Let's begin with the hardware elements involved in multi-site management. We can group these elements into three categories, as follows (see Figure 1):

- *Client devices* – these include client adapters (which can be PC Cards, CF Cards, USB devices, built-in adapters of the Centrino variety and equivalents, etc.) along with related software (including drivers, 802.1x supplicants, encryption code, and other legacy code). This category also includes *RF probes*, a specialized fixed device for RF spectrum monitoring and related security/integrity functions available from a number of vendors.

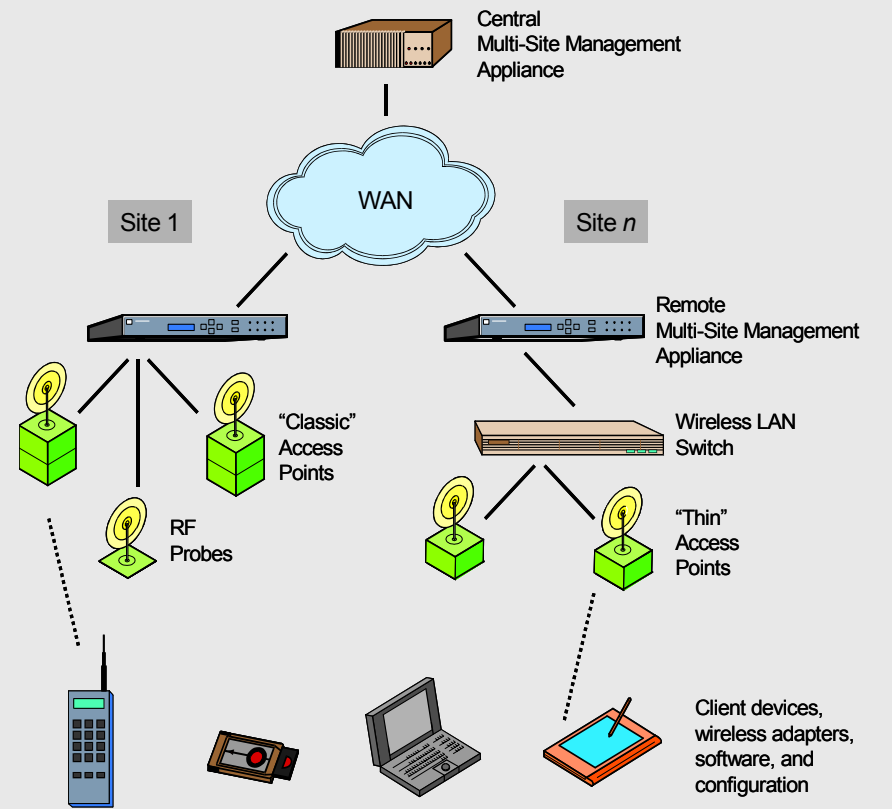

Figure 1: The hierarchy or elements considered in a multi-site management approach. *Source:* Farpoint Group

- *Remote site communication and RF infrastructure* - including access points, or switches and their related lightweight access points, as well as any enhancer/ completer hardware and software, security gateways, and other controller/ concentrator hardware.

- *Multi-site management infrastructure* – including any servers and software used just for management, and/or specialized WLAN management *appliances*. Farpoint Group defines a particular device as an appliance when it performs a set of specific functions and is not otherwise programmable by it owner, although updates and upgrades are usually provided by the manufacturer. We are increasingly recommending the use of an appliance-based approach because it often provides the best combination of functionality, scalability, and price/performance. This class of element is usually located in a network operations center (NOC) along with most other network management equipment, but may involve remote components as well.

Note that each of these elements also includes at least some software (and often firmware) that must be centrally managed as well. In this manner firmware updates, driver updates, and other software updates and upgrades can be centrally controlled with no action required on the part of a client device's end user. And that's really the goal of multi-site management – to consistently manage all hardware, software, and procedural/operational elements of a wireless-LAN infrastructure of any size or geographical distribution with minimal effort required on the part of operations staff.

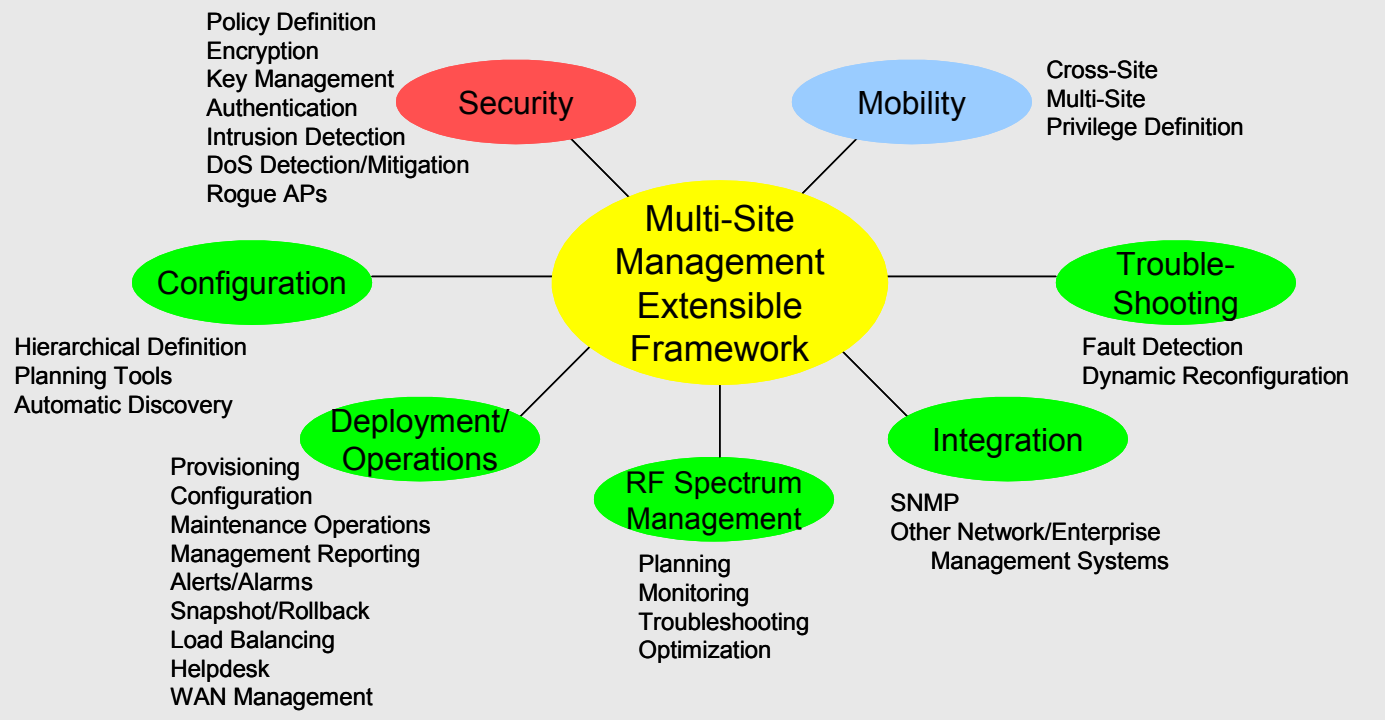

Figure 2: The many functions of multi-site management. Note the use of an extensible framework to specify and control other functions. *Source:* Farpoint Group

The next question, of course, is what centralized management functionality is required to deal with all of the above. What follows is the list of requirements, broken down within the three primary functional areas of multi-site management (see Figure 2).

Security

The issues in WLAN *encryption* have been well-documented since the fundamental flaws in the 802.11's Wired Equivalent Privacy (WEP) first came to light a couple of years ago. While we have long argued that WEP was never designed to be a complete WLAN security solution (partially because it's easily broken, and partially because it secures only the airlink and not the entire value chain from client to server), it can at least be agreed that the huge exposure this issue has received has made enterprise managers more aware of the need to take additional measures to secure their WLANs, and, in many cases, to think about the security of their *entire network* (wired and wireless) in a new light.

The current baseline solution to the WEP problem is the Wi-Fi Alliance's Wireless Protected Access (WPA) specification, now being implemented by many WLAN equipment vendors. We also recommend the use of Virtual Private Networks (VPNs), usually based on IPsec or SSL, as a much better approach to end-to-end encryption. But the diversity of security solutions which results from both rapidly-evolving technology as well as legacy and mixed-vendor installations dictates a multi-site management solution to security, ideally from the early days of operation of any wireless LAN. Security management functions include the specification of the security techniques to be used for any given user or device, encryption key management, and security policy definition and enforcement.

Of equal importance with encryption are *authentication* and *policy management*, which together define the valid users of, and their permissions on, a given network. Highly-mobile users crossing subnet boundaries can be a major challenge in enterprise authentication, since this functionality is often based on a user's location and not just identity. Wireless authentication often requires validation of both the mobile client devices as well as the user, along with the requirement for access to common network authentication databases, such as RADIUS, LDAP, PKI, Microsoft Windows domains, or others defined in the increasingly-popular 802.1x standard and the Extensible Authentication Protocol (EAP) and all of its potential variations. Central (and often hierarchical, multi-level) control of authentication procedures, passwords, and digital certificates is critical no matter what a given network's size. Policy control defines how each user or device may access the network, including allowable hosts/applications, protocols, bandwidth allocation/prioritization, and encryption types. Policy control is the foundation for enabling multi-application (or "mixed-use") wireless LANs at each location. It's also important that the privileges granted to network managers be hierarchical and auditable as well.

The final elements in wireless security are *intrusion detection*, dealing with various wireless *denial-of service (DoS) attacks*, and *unauthorized (rogue) AP detection*. While effective techniques now exist for all of these potentially-critical possibilities, a centralized implementation eliminates the need to have local staff on hand at each site to deal with these chal-

lenges. Centralized monitoring, detection, and countermeasures are easy to implement within a multi-site management framework.

Like many elements of a network or IT infrastructure, security techniques and implementations are constantly evolving. It's therefore critical that uniform, auditable security management be a part of any WLAN network designed to grow without compromising either critical corporate information or IT department budgets.

Mobility

It goes without saying that one of the core benefits of a wireless LAN is in the ability of mobile users to roam, subject to policy, of course, wherever the enterprise has provided appropriate infrastructure. This may include the relatively simple matter of roaming across IP subnets, or more complex requirements related to a given user's potential presence in (and ability to roam across) multiple physical locations – what we call *cross-site mobility*. A given user's privileges on the network, including quality of service via traffic prioritization, or access to network resources such as printers, may vary by location, and thus central definition and control of user profiles and usage policies is essential. Such *identity-based networking* is again quite different from the approach taken on wired LANs.

Operations and Life-Cycle Management

MSM forms the basis for all ongoing, day-to-day operations management across all phases of a given installation's useful life::

- *Configuration/Re-Configuration* – One of the most challenging tasks in any WLAN installation is initial planning and network configuration. What's required is knowledge of site layout, building construction, user population, traffic characterization (including peak loading by specific location), and the ability to easily review and modify configurations over time as operational parameters change. Flexibility is important here: Farpoint Group suggests that the best approach to configuration is essentially object-oriented, with the ability to define classes of installations (such as "small branch office" or "conference room") and then push configuration information to the relevant access points or switches. A hierarchical definition is also important here, allowing the specification of functionality on, for example, a campus, building, per-floor, or location basis. Also critical are the automatic discovery and validation of new network elements (such as an additional access point, if for no other reason than to make sure it's not a rogue), and maintaining an audit trail. Logs and configuration databases, along with appropriate reporting tools, are a must.

- *Deployment and operations* – configuration-related information provides the basis for the next set of processes involved in multi-site management, network deployment and ongoing operations. Perhaps the most important function in the deployment/operations phase is *provisioning*, which defines the capabilities and permissions of devices, users, and applications across a given site and the entire enterprise. This in-

cludes bandwidth management and prioritization on a per user/device basis. The management and control of software pushed to these devices, including applications, firmware updates, and upgrades, is also a key requirement. Support for routine and exceptional maintenance, the prediction of possible equipment failures, and equipment swapout/replacement/upgrade is essential. The ability to snapshot and even roll back configurations is required, as is linking configuration and operational information to the Helpdesk function. A complete set of alerts and reports is required; the ability to audit the system's actions is vital. And of course, all management functions must be under strict security control themselves; again, a hierarchical approach is desirable allowing, for example, permission to execute specific functions to be applied to different classes of management staff.

Finally, management and optimization of WAN connections is also an important element in multi-site management. Important functions here include minimizing traffic across the WAN connection for reasons of both cost and responsiveness (there's no point, for example, of backhauling traffic across the WAN if it otherwise starts at ends at a single remote site), and the ability to continue to operate if WAN connectivity is interrupted. This is another excellent justification for an appliance-based multi-site management approach.

- *RF Spectrum Management* – We've discussed this topic in detail in a previous Farpoint Group White Paper (see FPG 2003-201.1), so suffice it to say here that centralized management of RF planning, monitoring, troubleshooting, and optimization is critical. Such an approach minimizes the number of RF-trained staff that must be maintained, and allows central repair of any RF-related problems (such an interference, out-of-range conditions, and capacity exhaustion) that may appear.

- *Troubleshooting* – One of the key features of any management system is the handling of exceptional conditions. This includes intelligent monitoring, predicting problems based on data gathered, automatic responses to alerts, performance monitoring, analysis, and reporting for such items as RF utilization and error rates. Dynamic reconfiguration should also be a feature of any multi-site management solution, according to installation-specific rules defined within the system itself.

- *Integration* – It probably goes without saying that integration of any multi-site management tools with existing network and enterprise management systems (including HP OpenView, CA Unicenter, and IBM Tivoli) is essential, as is integration with authentication and related databases. And, of course, support for the Simple Network Management Protocol (SNMP) is required.

- *Extensibility* – Finally, a good multi-site management tool is really a *framework* for current and future functionality – with the emphasis on *future* here, because no one can predict the need for additional general-purpose or enterprise/site-specific functionality that may be required as WLANs, and the enterprise itself, evolves.

Figure 3 shows an example of a production multi-site management installation.

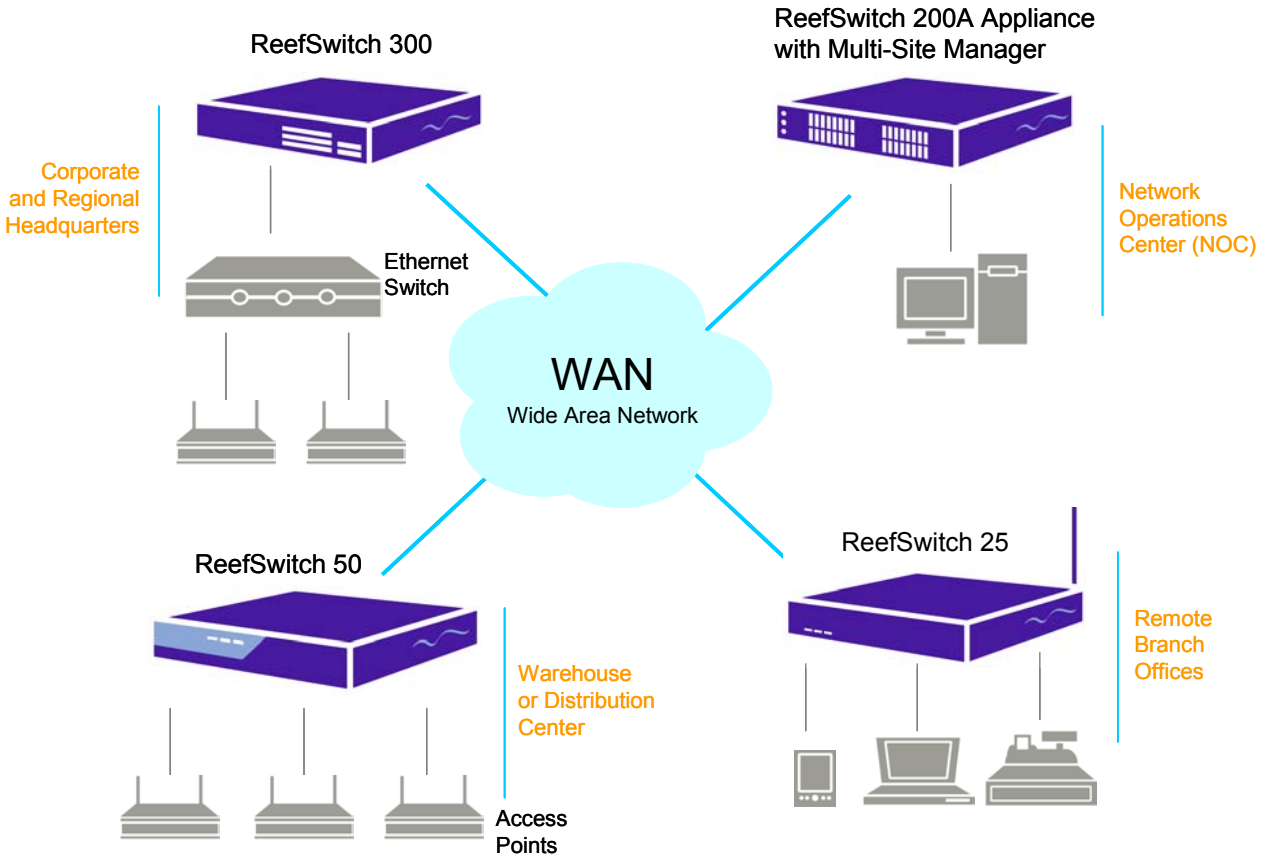

Figure 3: A production multi-site management example. (*source:* ReefEdge)

Multi-Site Management is the Future – and the Present

The most critical element in any successful networking installation is ensuring that the network meets the needs of the user community while also satisfying enterprise security, cost, and scalability goals. Multi-site management – *implemented as early as possible in the life-cycle of any enterprise-class wireless LAN installation* – is critical in obtaining these goals under the unique set of requirements and conditions defined in wireless LAN management itself. Multi-site management is also key to minimizing both CAPEX and OPEX (through extending the life of installed equipment and in lowering labor-related costs), and in providing the bridge between legacy and future WLAN installations that is certain to be needed as WLAN technology, systems, and corporate requirements evolve. We believe that a single, *uniform* multi-site management platform is the best approach to assuring smooth operations through the many technology and product transitions that an enterprise is likely to see over time

There is undeniable appeal in applying to wireless LANs the same techniques network managers have enjoyed for years in the world of wire – a single management hierarchy, with control centralized in the Network Operations Center (NOC), incorporating all functionality, automation, and scope required to minimize costs and maximize ROI with minimal effort. Such capabilities are available today, and we see their adoption as a major trend – *and key enabling factor* – in the eventual ubiquity of wireless LANs in the enterprise.

7 Whippoorwill Lane
Ashland MA 01721
508-881-6467
www.farpointgroup.com
info@farpointgroup.com

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