



Carrier-Class Wireless LAN Networking

*Designing a Forward-Compatible Network Management
Solution for Wireless Networks*

Summary

From coverage of small, single “hot spots” just a year ago, wireless networking is now covering large-scale infrastructure applications – and WLAN technology is evolving rapidly. At the same time, the 802.11 “Wi-Fi” suite of standards continues to evolve quickly. All together, this fast pace can lead to quickly obsolete WLAN equipment. Wireless network operators need better return on their investments, especially through this period of transition.

This paper reviews some of the issues that make 802.11-based products difficult to scale and adapt. The requirements of a network management interface designed to address those issues are then outlined. Finally, key features of the BelAir Networks integrated outdoor WLAN solution are identified in terms of effective operation, administration and maintenance (OAM) and shown to support and enhance the solution’s carrier-class wireless networking capabilities by integrating with and leveraging existing off-the-shelf network management systems (NMS).

OAM: Key to Wireless Network Adaptability

The wireless local area network (WLAN) has grown substantially in the past few years. Today, service providers are looking to wireless networks to extend the reach of existing infrastructures, while enterprises are turning to wireless deployments as a means of facilitating productivity and untethered access for increasingly mobile workforces across large campuses.

From coverage of small, single “hot spots”, wireless networking is now considered for large-scale infrastructure applications—and WLAN technology is evolving rapidly. At the same time, the 802.11 “Wi-Fi” suite of standards continues to evolve. All together, this fast pace can lead to quickly obsolete WLAN equipment.

While better-performing, more cost-effective equipment is available on an almost monthly basis, current system investments are quickly outdated and even become liabilities. Wireless network operators need better return on their investments, especially through this period of transition.

In any network, the integration of the nodal network management interface (i.e. the interface used to manage each access point (AP)) with the network management system (NMS) is essential to successful network evolution. The nodal management interface must be robust, reliable, flexible and adaptive. It must also provide a standards-based (e.g. SNMP) interface, allowing users to leverage their existing NMS equipment.

This paper reviews some of the issues that make 802.11-based products difficult to adapt and scale. The requirements of a network management interface designed to address those issues are then outlined. Finally, key features of the BelAir Networks integrated outdoor WLAN solution are identified in terms of effective operations, administration and maintenance (OAM) functions and shown to support and enhance the solution's carrier-class wireless networking capabilities.

802.11: From Commodity-Class to Carrier-Class

As networks grow, it becomes more important that they provide high availability and clearly defined, in-service, network-wide firmware upgrade procedures. In carrier-class networks, this is typically achieved through effective network management techniques. But many WLANs, initially designed for small-scale deployments, lack these characteristics. Although wireless APs are relatively low in cost, upgrading an entire network of them or making in-field modifications significantly increases operational expenses and impacts service.

The bottom line is that today's WLAN equipment is meant for small-scale deployments—not for the enterprise or service provider installing WLANs for medium- and large-scale deployments and profitability.

Wireless network operators need better return on their wireless investments, especially through this period of transition from small-scale deployments to large, carrier-class applications. The longer a system can remain in service with little to no operator intervention, the greater the ROI will be. The keys to achieving solid ROI in a wireless network are:

- **Flexibility** in WLAN equipment, which must scale well
- **Clear upgrade paths** for equipment, providing responsiveness to changing requirements and adapting to new applications
- **An integrated network management interface** that provides robustness, flexibility and scalability, while facilitating remote upgrades
- **Ease of integration** into off-the-shelf or pre-deployed network management systems

Flexible Application Scope

The current generations of 802.11 WLAN systems were designed for a narrow range of localized applications in commodity consumer markets. These include residential applications, hot spots, conference halls, office floors and the like. What these applications have in common is the single AP—either only one AP is required, or a network of APs is deployed by wiring together numerous single units, either through conventional networking infrastructure or a wireless aggregation shelf.



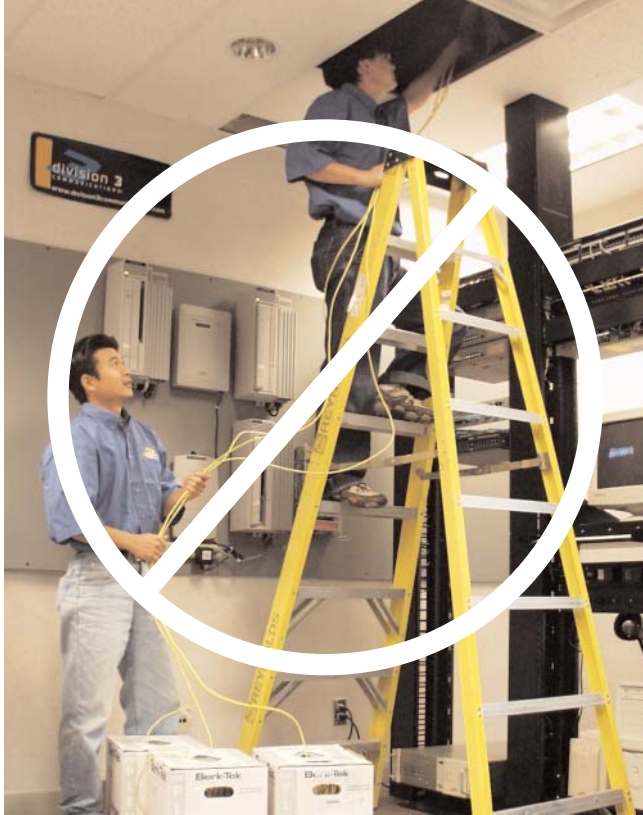
Today's WLAN is Growing Beyond the Conventional Hot spot

The design goal of these conventional small WLANs is a “plug-and-play” AP that requires little to no operator or user intervention. Service delivery is “what you get,” and performance is usually sacrificed for convenience or novelty. Nor are these solutions designed with an upgrade path; rather, the intent at this price point is disposability. The unit will be discarded and replaced, not upgraded. In fact, as most consumer

electronics are designed for planned obsolescence, they are counter-intuitive to more expansive network applications.

Clear Network Upgrade Path

The ability to upgrade a network with minimum cost and disruption is crucial to service providers and enterprise network operators. Without network-wide insight, WLAN solutions that consist of numerous autonomous APs cannot be reached remotely for firmware upgrades, service or trouble-shooting. In some cases, the unit may be reachable via local serial ports. Either method is problematic in a large network. “Truck rolls” to directly service units are costly, while serial port access is cumbersome and slow.



Enterprise WLANs Require Easy Management for Minimum Disruption During Service or Upgrade.

Two reasons for establishing a clear network upgrade path are: maximizing product life spans and minimizing service disruptions:

- Commissioning and installing equipment is labor-intensive and time consuming. Factory firmware upgrades or equipment replacement operations are tolerable for small numbers of APs, but operators need in-service upgrade mechanisms without recall or truck rolls.
- System upgrades or overbuilds often disrupt service for a significant period of time. In an enterprise deployment, this affects productivity and overall ROI, while for service providers it represents revenue loss. Firmware upgrade mechanisms must therefore be both timely and “invisible.” The goal is to avoid physical teardown of systems for modification.

Integrated Network Management

To be more versatile and suitable for infrastructure applications, a new class of WLAN products is required. Product design must be adaptable to accommodate change so the operator can optimize WLANs for specific new applications.

Among other characteristics, these next-generation WLANs need to resist obsolescence, even in a rapidly changing landscape. In this context, integrating the WLAN equipment into a network management system is crucial, and must enable operators to:

- **Re-configure** the settings of current features
- **Introduce** enhanced or new features
- **Query** the installed equipment inventory
- **Customize** deployment, policies, reporting and accounting functions
- **Automate** remote network upgrades
- **Detect** remote equipment failures in a timely and reliable fashion.

OAM functions must be designed into a network management interface that accommodates new features without disrupting resident features and operations. They must provide a means to grant a centralized NMS remote visibility into each unit, including diagnostics, fault alarms, link status, traffic metrics and more. Such network management interface integration, then, is vital in any infrastructure-scale WLAN deployment and in effect buffers the network from change.

Network Management Interface Requirements

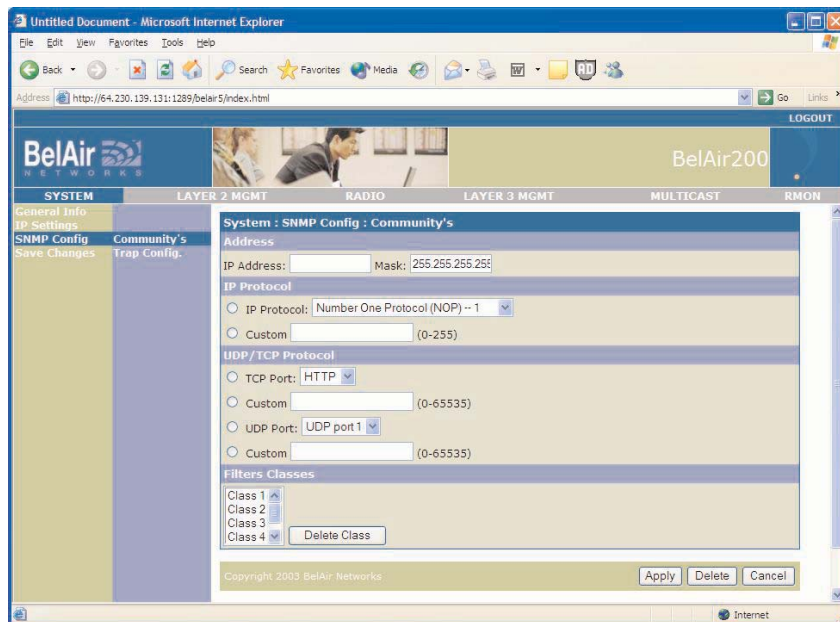
A network management interface suitable for the next generation of carrier-class WLANs must provide for at least six key capabilities, including application flexibility, maintainability, standards support, system availability, security and user customization.

- **Application flexibility** – in order to optimize the WLAN solution for unique or specific applications, the network management interface must be adaptable so that settings and features are easily reconfigured or added. At the same time, resident features and operations must not be disrupted in the process of change. The interface must accommodate numerous network topologies and be forward-compatible to next-release products.
- **Maintainability** – uniform OAM functions are required for system maintainability, in order to deliver reliable services with good performance at low operating costs. This includes flow-through provisioning, firmware upgrades, billing statistics collection, commissioning, a comprehensive test suite for field testing, and querying for equipment inventories.
- **Standards support** – the interface must provide support for industry accepted network management standards, such as SNMP.
- **System availability** – for carrier-class applications, a node must not be a single source of failure in a multi-point WLAN. The network must tolerate the loss of an individual AP or cluster with minimal impact on overall operations. Fail-over and redundancy features must be built in. The nodal network management interface and overall network structure must support this availability.
- **Security** – network traffic, including management traffic, must be protected during transmission on both the access and backhaul data paths. Thus, the network management interface must provide authentication for access and encryption for the backhaul. Layered security is required for local craft access with challenge password, secure shell, and the ability to originate or terminate a virtual private network (VPN) tunnel.
- **User customization** – network operators will have both unique and common requirements for their WLAN deployments. Unique requirements typically involve OAM functions, as network architectures and the way they are managed vary. The network management interface must accommodate unique policies for traffic handling, reporting and accounting, and contingencies for various states (e.g. failure, overload, idle, etc.). This also allows value added resellers (VARs) to easily customize and evolve products for smaller applications or spot solutions.

Carrier-Class WLANs from BelAir Networks

BelAir Networks unique outdoor WLAN solution provides the mandatory OAM functions outlined above, allowing straightforward integration with carrier-class network management systems. The BelAir Networks network management interface provides effortless remote access to the company's patent-pending, multiple point-to-point mesh architecture, which uniquely integrates wireless access and backhaul in a single mesh.

The BelAir Networks architecture combines the best of WLAN and cellular technologies to simplify WLAN infrastructures and eliminate backhaul costs. It allows multiple communication paths to each unit, therefore providing built-in redundancy.



BelAir Networks Network Management Interface

This integrated solution includes a network management interface that provides sophisticated OAM functions and is unique in wireless networking for its advanced nodal architecture.

Nodal-Based Management

The BelAir Networks solution is a nodal-based management interface that integrates into a pre-deployed or

off-the-shelf NMS. This approach allows the solution to scale and achieve high system performance, as well as reduce initial capital expenditures.

Each node in the network incorporates a self-contained OAM network management interface with its own IP address. Each interface can be accessed directly through other APs, by a local operator or from a remotely located network operations center (NOC). This provides the network operator with the ability to easily commission, monitor, reconfigure and upgrade each node without impact on the operation of other nodes.

In addition, having individual OAM systems that can either report network problems or be interrogated on a periodic basis enables the operator to easily obtain a network-wide view and drill down for specific information as required.

Each node can either operate in local autonomous mode with no external management system required, or be integrated with an NMS residing in a central network operations

center (NOC). Thus, larger carriers can easily integrate the BelAir Networks equipment into their pre-deployed network management systems, while smaller Wi-Fi operators can bypass the need for an NMS by using BelAir Networks nodal interfaces.

High-Availability Management

In cluster (multi-nodal) mesh WLAN deployments, it is critical that the failure of any one AP does not result in the loss of overall network management operations. The BelAir Networks mesh architecture tolerates the loss of individual nodes without causing a system-wide outage or loss of overall network visibility to the operator.

For example, in the case of a failed node, the traffic can be redirected via other paths in the mesh. Although the individual node's local coverage is lost, the impact on the overall system is minimal.

This approach also results in additional benefits with:

- **Fail-over:** Single or redundant operator network management systems can manage the cluster network
- **Multiple network gateway APs:** APs can be deployed as gateways to link into the public network, providing multiple paths for an operator's network management system to maintain contact with the WLAN OAM system.

Sophisticated Node Architecture

In order to achieve carrier-class network management, the architecture of the nodal system must be responsive, flexible and robust.

The BelAir Networks solution provides a central processor, or switch control module (SCM), to host the OAM and switch management functions. The SCM in the node inter-works with each radio module, which also incorporates OAM sub-functions. Using this arrangement, the management system can uniquely address each node for operator reconfiguration, enable or disable operations, software or firmware upgrade and monitoring (alarms and statistics).

The BelAir solution leverages the highly reliable, open source Linux operating system, which provides the option of incorporating specialized applications on the processor platforms. Thus, a node can be given a unique set of features that enables the product to be used in a range of WLAN applications.

For example, gateway features such as network address translation (NAT), firewall and IP filtering can be added on an as-needed and per-node basis.

Key Features

The following table summarizes key features of the BelAir Networks network management interface.

Feature	Description
Flexible Architecture Features	
Innovative inter-processor communication (IPC)	Internal communications architecture allows efficient access to each module under control of the node's OAM system. Thus, an operator can easily "drill down" to each radio module and retrieve its parameters, monitor its performance and check or reconfigure its operational settings.
Self recovery	Full system self-recovery requires no operator intervention to bring WLAN services and management back online after outages due to prolonged power failures. The configuration and network settings of each AP are stored in non-volatile memory, allowing full restoration of the node and its network context. This greatly reduces the number of maintenance calls for craft personnel as well as reducing operational expenditures for the system.
Platform-independent firmware	BelAir Networks firmware can be upgraded with new features without requiring hardware changes.
Firmware modularity	The BelAir Networks modular software architecture enables operators to add new specialized functions to BelAir Networks equipment with minimal system impact.
Customizable	Flexible access and reporting structures can be customized for the operator to better match business requirements and existing network management systems in use. Supports web, SNMP and other reporting mechanisms, as well as forward compatibility to new OAM trends employing XML and Java-based management.
Integrated management	BelAir Networks node management functions can be integrated with "off the shelf" NMS products and are thus easily accessible from a centralized location.
Support for automated configuration	The BelAir Networks command line interface (CLI) allows operators to develop automated scripts for rapid network deployment and upgrade.
Traffic independence	OAM functions are independent of traffic flows, ensuring deployment flexibility by isolating OAM functions from the application and traffic management. The system can thus absorb new features and accommodate new standards without disruption or a major system rebuild.
Security Features	
Access Control	Each node's management system enables setup of access control tables and firewalls to ensure that it is reachable only by authorized users.
Virtual private networks	Provides additional security through the use of VPNs to the NMS of each node.
Encryption	All backhaul mesh radio channels are encrypted, preventing illegal access.

Carrier-Class WLANs: Node-NMS Integration is the Key

Today, the wireless local area network (WLAN) has grown to the point that service providers and enterprises require carrier-class WLAN infrastructure solutions. As WLANs grow, they must provide high network availability through system redundancy and effective network management techniques.

In any network, the ability to integrate new equipment with pre-deployed or off-the-shelf network management systems is essential to the initial acceptance of equipment and to network operation and evolution. But many WLAN products, initially designed for small-scale deployments, lack the ability to easily integrate into a centralized management system, which can provide the robustness and redundancy features required for carrier-class networks.

The BelAir Networks unique, integrated outdoor WLAN solution was designed for carrier-class deployments. It leverages industry-accepted network management standards (such as SNMP) and paradigms (like intuitive Web-based interface and text-based command line interface). It incorporates a network management interface with all required operation, administration and maintenance functions for medium- and large-scale WLAN applications. But it also allows smaller Wi-Fi operators to bypass the need for an NMS by using BelAir Networks nodal interfaces.

With BelAir Networks, profitable public and cost-effective private WLANs can be deployed. That means service providers can make wireless networking profitable, while enterprises can cost-effectively deploy it across campuses for truly untethered productivity.

About BelAir Networks

BelAir Networks is a wireless infrastructure supplier that provides advanced, multi-service, mobile networking solutions optimized for medium and large public and private cellular LAN networks.

Combining the best of WLAN and cellular technologies, BelAir Networks solutions go beyond basic Wi-Fi to overcome the limitations associated with traditional WLANs. They are built on a patented multiple point-to-point mesh enabled by outdoor platforms, indoor nodes, and network management software. Together, the mesh and the products that enable it are designed to simplify wireless infrastructures, reduce capital and operating expenditures, and deliver ubiquitous high capacity data, video and voice services where and when needed.

For More Information Contact:

Joe Aragona
Director, Marketing
BelAir Networks
t: 613.254-7070 ext. 134
e: jaragona@belairnetworks.com

Or Visit Our Web Site at
www.belairnetworks.com