WLAN Controller Applications Are Finding a New Home on the Network

Tim Zimmerman, Michael J. King

In the past, centralized wireless LAN (WLAN) controller applications and the platforms provided a single point of consolidation that eliminated the need to touch every autonomous access point. While controller hardware was a small part of the price tag for a large campus or enterprise, this requirement for a controller has made small or midsize business (SMB) or branch office solutions cost prohibitive. New WLAN architectures are eliminating the controller hardware and integrating the software into other parts of the network for all configurations.

Key Findings

- WLAN solutions that eliminate the requirement for a physical controller hardware platform can save a company, on average, $6,000 in upfront capital expenses, which for many SMB installations is the single most expensive component and may exceed the total cost of all access points.

- Pricing for controller platforms can range from a little over $1,000 to over $30,000, depending on the size of the solution and the need for redundancy in single-threaded architectures. Savings can include not only capital expenditure (capex), but also additional operating expenditure (opex) savings in annual hardware maintenance.

- Vendors are placing controller functionality and intelligence in the network for lower upfront capital expenses and lower WAN costs, as well as converged management/provisioning of wired and wireless solutions.

Recommendations

- Do not buy a dedicated, local physical WLAN controller platform for a wireless solution that is being deployed in a small business, branch or remote office.

- Leverage documented vendor APIs or secure browser connectivity for network application service changes and reporting. This allows the independent platform to reside anywhere on the network or locally, if required, but allows consolidation of information to meet the needs of enterprises with multiple sites.
STRATEGIC PLANNING ASSUMPTION(S)

By 2015, WLAN controller functionality will be integrated into other networking solutions, eliminating the need for stand-alone hardware platforms by over 80% of remote or branch offices.

ANALYSIS

WLANs at the edge of the network continue to grow; but for some usage scenarios, a large, bulky WLAN controller appliance distorts the implementation costs. The controller-centric architecture, introduced by Motorola (Symbol) and Cisco (Airespace), has been used to centralize management and policy enforcement of WLAN for more than 10 years. This solution, however, has required a dedicated WLAN controller for small and midsize office environments, and for any enterprises looking to install wireless only in conference rooms or reception areas. This architecture adds an expensive single-purpose WLAN controller that complicates the implementation by requiring additional power, cooling and physical space at every local site for a controller, or upstream to a large, centralized controller via the WAN. As a result, vendor-specific WLAN-centric platforms, which can cost over $30,000, are slowly disappearing as an architectural requirement, and the functionality is being integrated into wired switches on the network or existing WLAN access points for a more cost-effective solution.

WLAN Architectures Are Changing

It is clear that the industry is recognizing that the role of the WLAN controller is changing. The need to control and adjust the wireless medium — whether it is deep packet inspection, policy management or quality of service — still exists to ensure that the wireless experience provides the same reliability and functionality as its wired counterpart. What is changing is the location of this functionality. Gone are the days of sending every packet to a centralized controller appliance, whether it is required at each branch office or is tunneling everything back and forth through the WAN connection. As the wired and wireless access layers continue to converge, the role of the WLAN controller platform is optional.

Eliminating the Controller

Vendors are introducing architectures that eliminate the need for a separate WLAN controller platform. In these architectures, there are still three approaches:

- Integration of controller functionality in wired switches
- Integration into the access point
- Moving the controller application to the cloud

The first approach places the controller functionality into an existing switch as part of a single network vendor access layer solution or a coordinated strategic alliance that provides services for the wired and wireless infrastructures. Vendors such as Cisco with its ISR platform, HP, Enterasys and D-Link deliver this configuration. This solution maintains local WLAN functionality and seamless access to local resources into the switching platform, which also accommodates wired connections. Enterprises using this architecture should expect to get additional savings from wired and wireless integrated security and network management. Integration of controller functionality in wired switches is limited in that it requires the switch and access point solution to come from the same vendor. This is a good solution for users with existing infrastructure or that have relationships with service vendors already in place.
The second approach, and perhaps a little cleaner, is to integrate the controller functionality into the access point. This solution, which is currently available from Aerohive Networks, eliminates the need for any controller hardware because the wireless control plane is integrated into the access points with built-in redundancy to prevent a single point of failure. This solution also has a Remote Authentication Dial-In User Service (RADIUS) and Dynamic Host Configuration Protocol (DHCP) server as part of the integrated controller functionality that allows new users to be added at anytime to the wireless network, and to the wired infrastructure if the same security services are used. While this solution is self-contained and excellent for branch offices or SMBs, it requires separate panes of glass for managing wired and wireless resources at the edge of the network. This is an appropriate solution for enterprises that have many small branch offices, SMB users and those with a hosted LAN services model (provided by internal IT organizations).

The third approach is placing the wireless controller functionality “in the cloud,” which has been implemented by Meraki, Aerohive and Aruba. While this approach eliminates the controller hardware platform, it raises two important questions: To what extent is the controller functionality necessary to run the network, and what happens when the broadband connection to the cloud is unavailable? Cloud implementations have a centralized controller that may allow the WLAN to operate in the “last known state” and, depending on the usage scenario, this may be fine for temporary outages. This solution also allows multiple sites to be run from a single controller in the cloud, but requires the expense of the cloud service and may still require a separate application for managing wired and wireless access layer components. This is a good solution for enterprises with larger branch offices that require robust WAN links and failover, as well as those that have IT support on-site.

In the next five to seven years, Gartner expects that enterprises will have the ability to connect and configure any vendor’s access points to any switching components that form part of the upstream network infrastructure. Vendor-specific profiles will automatically configure the access point and the necessary communication, as the access point is automatically detected on the wired port. This profile will address a vendor-specific functionality or requirements on access points that differ from the switch vendor’s components. This scenario also will allow the access layer to be continually optimized and will provide a consistent interface to network application services that, in a converged wired and wireless model, provide homogeneous functionality for services from guest access to network management. Vendors such as Aerohive have the ability to deploy a WLAN without a controller to any upstream switch, but it still requires a separate management platform.

What About the Network Services?

Some WLAN vendors combine a dedicated hardware appliance with their required controller application, along with optional and separately licensed network services, such as guest access, network management or Wireless Intrusion Detection Systems/Wireless Intrusion Protection Systems (WIDS/WIPS) functionality. The key is not whether the hardware platform can serve as a multifunctional application platform. The critical point is enabling enterprises to eliminate the need for a site-specific or WLAN-centric platform that is required for a controller application. With the number of network services growing, the best place for these API-integrated or browser-based applications is an independent platform that can exist anywhere in the network. This strategy also fits with the convergence of wired and wireless converged policy solutions or on-demand multisite reporting solutions, where wireless functionality operates on its own.

Bottom Line

Enterprises need to review the architecture of their WLANs for the access-layer strategy they are trying to deploy to ensure that access layer availability metrics are met. Controllerless solutions make excellent sense in branch- or remote-office usage scenarios, where the cost of a WLAN-
specific controller hardware can be the single most expensive part of the solution and, in some cases, cost more than the access points being deployed.

Controllerless solutions are cost-effective for conference room or reception area wireless environments for any size organization with the ability to scale as WLAN requirements continue to grow. Enterprises need to ensure that when the physical platform has been displaced, their business needs will continue to be served. For larger home and headquarters office, campuses, and users who have limited WAN link choices, a controller-based architecture will remain the best choice. We expect that the majority of installations (65% to 70%) during the next three to five years will still require a physical controller.

RECOMMENDED READING

"Key Challenges in the Remote-Office Implementation of WOCs and WLANs"

"Magic Quadrant for Wireless LAN Infrastructure (Global)"

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Gianty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509