CENTRALIZED MANAGEMENT AND RF SECURITY MOVES ARIBA TO ARUBA

ARIBA®

At Ariba, the world's leading provider of enterprise commerce software systems, nearly every new employee is presented a laptop with integrated Wi-Fi. So for Ariba's IT department, building an enterprise-class Wi-Fi infrastructure wasn't an option. Ariba needed to cost-effectively rollout 802.11a+b/g services campus-wide to a technically-savy community of more than 200 wireless laptops users that was quickly growing. Doing this required a new approach that conventional wireless systems couldn't uniformly deliver.

"We needed an enterprise-class wireless system that centralized the control and security of our entire environment," said Kevin Smith, manager of IT Global Communications at Ariba. "Aruba built that system and Ariba has standardized on it."

Ariba's goal was to integrate a centralized wireless system to support some 600 employees at their four-story campus headquarters in Sunnyvale, California and then roll Wi-Fi out to branch offices around the world. "Frankly because we don't have IT staff in our branch offices, without a centralized wireless system, we just wouldn't offer wireless there. Now we can." said Smith.

While Ariba had deployed a small wireless testbed of conventional fat APs, this environment proved too costly to manage, difficult to scale and impossible to remotely troubleshoot. Firmware and code upgrades for each AP had to be individually performed through a console connection.

The legacy, distributed system was also arduous to deploy. A separate VLAN had to be configured for the fat APs and trunks created to the VPN concentrator for each specified port. Wireless users had to then tunnel into the intranet through the VPN.

Topping the list of Ariba requirements for wireless was centralized management control that eliminated the complexity associated with monitoring a large wireless environment. Multiple layers of wireless security such as RF security to identify and disable rogue APs, link layer encryption and VPN support was also a must have. "We wanted a security architecture that addressed authentication, encryption, rogue AP detection along with a rich policy management infrastructure to control access for different types of users," said Smith. "Wireless is all about knowing the user."

REQUIREMENTS:

- Integrate a seamless 802.11 wireless solution without disrupting wired network
- VPN support for a diverse OS environment including Mac, Linux and Windows clients
- Add centralized wireless management and RF spectrum management
- Scale to support hundreds of simultaneous users
- Multi-layered wireless security that addressed authentication, encryption, rogue AP detection and policy management

SOLUTION:

- One Aruba MMC-5000 Mobility Controller
- 44 Aruba 52 dual-purpose 802.11a+b/g access points
- Three Aruba 800 Mobility Controllers
- ArubaOS Mobility Software

BENEFITS:

- Enhanced user experience
- Centralized security and control for entire WLAN
- Remote RF visibility and monitoring
- Seamless integration with existing wired network

"When I see 200 concurrent wireless users on the WLAN during the day, and I get no support calls, that's when I know I've made the right decision. Aruba has given IT more control and robust security over our wireless environment and our users a better overall experience."

Kevin Smith
Manager, IT Global Communications
Ariba, Inc.

ARUBA networks

Another key requirement for the wireless network was seamless integration with the existing wired network. Ariba wanted a wireless overlay that used the existing IP network as transport without any disruptions to the wired network. Aruba APs connected to existing L2/L3 wired switches and an Aruba Mobility Controller in the data center controlling them was the preferred architecture.

To address wireless management and security concerns, Ariba deployed an Aruba centralized mobility solution consisting of 44 802.11a+b/g Aruba 52 APs, the full suite of ArubaOS application software, and the Aruba 5000 modular controller.

Access points were deployed in the data center, on all four floors of Ariba's headquarters building as well as in Ariba's cafeteria. APs connect to existing L2/L3 IDF (intermediate distribution frame) switches in every wiring closet. Aruba's 5000 Mobility Controller is centralized in Ariba's data center and connected via a gigabit uplink to an L2/L3 MDF (main distribution frame) backbone switch. ArubaOS applications are enabled at the controller in the data center.

Aruba APs indirectly connected to the Aruba 5000 create a logical wireless overlay that uses the wired IP nework as transport without requiring any physical or logical reconfiguration. This also gives Ariba a rich policy management infrastructure for tailoring wireless services and security profiles to different users and user groups as they roam. A Web-based captive portal within the Aruba 5000 provides guest access and authentication.

With Aruba's centralized WLAN switching system, Ariba now has in place a scalable 802.11 infrastructure that allows them quickly adapt to change and closely monitor the performance and security of their global wireless environment from a single point. This translates into lower operational cost due to the elimination of labor intensive wireless monitoring. Additionally, Ariba has found a higher satisfaction among users as problems and optimization of the wireless network can now be performed quickly from a single point.

Finally remote deployment of wireless is now possible and cost effective from the ability to manage and secure remote office wireless environments from Ariba corporate headquarters.

ORGANIZATION OVERVIEW:

Headquartered in Sunnyvale, California, Ariba is a leading provider of online enterprise commerce solutions and pioneered the market for Enterprise Spend Management (ESM). The company employs a staff of more that 900 worldwide.

www.arubanetworks.com

1344 Crossman Avenue. Sunnyvale, CA 94089
1-866-55-ARUBA | Tel. +1 408.227.4500 | Fax. +1 408.227.4550 | info@arubanetworks.com