UNITED STATES AIR FORCE WORLDWIDE NETWORK TAKES TO THE AIR

U.S. AIR FORCE

The United States Air Force had a unique challenge. Their technicians needed the ability to access technical information directly from the runway and on the flightline. Due to the number of different aircraft they supported, the large variety of potential systems and armaments and the high complexity of the equipment they needed to maintain in top working order, this became a very daunting task. The issue was further complicated by the fact that the system needed to be deployed at over 100 Air Force bases around the world.

The Air Force had already tested a first-generation solution comprised of multiple vendors and components; however this solution proved too expensive and too complex to manage. To maintain their technological edge, and ensure top performance from all combat assets, it became apparent a different solution would be necessary.

STREAMLINING THE WIRELESS NETWORK

To meet the demanding network requirements needed for flightline maintenance, as well as base-wide communications and medical applications, the Air Force would need a new class of wireless solutions that could deliver reliable high speed, highly flexible networks without sacrificing security. While examining the requirements for the CITS deployment it was clear that older traditional 'thick' APs wouldn't meet their needs. What the Air Force required was a more streamlined solution with fewer potential points of failure that was easier to manage and more cost effective.

To accomplish this, the Air Force determined they needed a single wireless platform that could incorporate Layer 2 encryption and Wireless Intrusion Detection Systems, could support complex applications, and most importantly, would meet or exceed all Department of Defense (DoD) security standards including FIPS 140-2 certification and the requirements outlined in DoD Directive 8100.2.

REQUIREMENTS:

- FIPS 140-2 Certification
- Integration with legacy Air Force Wi-Fi equipment
- Seamless roaming between APs
- No mass management of WEP keys on individual user stations
- Centralized security and RF management for thousands of APs
- Centralized management of devices and authentication
- Support for all current student wireless cards (a/b/g) and PDAs
- Ability to deny given protocols (i.e., ICMP, NetBIOS, etc.)
- Power-over-Ethernet and VoIP capable

SOLUTION:

- Aruba 6000 and 800 Mobility Controllers
- Aruba AP61, 65 and 70 dualpurpose 802.11a + b/g access points

BENEFITS:

- Anytime access to critical information from runways and hangars
- Centralized RF management
- Thin AP model providing security as well as lower cost of ownership
- Wi-Fi "overlay" simplifying deployment

After evaluating several solutions, the Air Force selected the next-generation wireless mobility platform from Aruba based on security, ease of installation and cost.

ARUBA networks

They determined a centralized architecture would provide the ideal platform to not only meet their requirements for access and security, but would also enable greater mobility for users. In a centralized architecture, all encryption, authentication, and access control is done by a single controller. The controller provides identity-based security making use of "thin" access points in contrast to traditional access control methods, which determine security settings at point of network entry. The centralized architecture allows Air Force Technicians to roam from one AP coverage area to another without losing connectivity or having to reestablish access to secure information.

After evaluating several solutions, the Air Force selected the next-generation wireless mobility platform from Aruba based on security, ease of installation and cost.

MEETING MILITARY-GRADE REQUIREMENTS

During the installation, Aruba demonstrated not only ease-of-installation, but a superior knowledge of applicable Federal oriented requirements (i.e., Call Admission Control, FIPS, end-to-end encryption, and legacy integration). The Air Force utilizes the Aruba Wi-Fi access to provide greater flexibility to their most important resource, their people. It has proven critical in allowing the Air Force to enhance their ability to perform their missions in numerous areas. For example, the crews on the flightline rely on wireless to gain access to critical information such as technical orders and maintenance records in a timely manner. It also provides the medical professionals the mobility needed to move from room to room, or even building to building, and still have access to critical medical records or other information to evaluate and treat patients. This has greatly enhanced patient care in these facilities.

To ensure wireless coverage is extended to all required locations, such as flightlines, runways, and hangars, the Air Force has installed Aruba AP60 and AP70 series access points that communicate directly to the Aruba mobility controller using GRE tunnels.

An even greater challenge than coverage in deploying a standard enterprise wireless networking solution within the Air Force is securing the large number of client devices that must be supported. The Air Force currently uses various versions of laptops including special ruggedized versions. These laptops are being used across the base by the aircraft technicians on the flightline and the doctors in the medical facilities. Inventory on bases is tracked using several different models of handheld devices, including Symbol and Intermec, running on various operating systems. Many of these devices are being secured by the use of the Aruba's FIPS-validated xSec client.

ORGANIZATION OVERVIEW:

The mission of the United States Air Force is to deliver sovereign options for the defense of the United States of America and its global interests to fly and fight in air, space and cyberspace.

To achieve that mission, the Air Force has a vision of Global Vigilance, Reach and Power. That vision orbits around three core competencies: Developing Airmen, Technology-to-Warfighting and Integrating Operations.

For new remote deployments, administrators simply send Aruba APs, pre-configured with only the IP address of the central mobility controller, to staff in remote offices. Remote office staff require no technical expertise and need only plug in the AP to a power source and an Internet connection. The AP automatically builds an IPsec tunnel to the Aruba mobility controller maintaining full FIPS 140 Certification and appropriate access levels based on clearance, role or location. Upon authentication, the AP's configuration, power levels and channel assignments are controlled from headquarters. Users have access to the corporate network as if they were at their primary location and do not require VPN client software on their laptops.

ARUBA networks

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