

Benefits at a glance:

- **ROI in time savings and man-power efforts:** Fewer support hours at HQ, streamlined configuration time, and simplified deployment process
- **Secure Wireless Infrastructure:** Allows remote teams to set up reach-back to HQ without being intrusive to the local bank network or having to depend on the security of a local network
- **Mesh:** Empowers deployed teams to quickly and easily expand the coverage of the remote WLAN without having to run cable and/or have network connectivity available
- **Remote AP:** Provides the ability to deploy small teams to necessary locations without having to supply excessive hardware
- **Local Switches:** provides scalable network to larger teams that require greater capacity and capability for the duration of the deployment
- **Central Management:** Allows HQ to have visibility and configuration baseline control across ALL connected users and deployed infrastructure whether large (“A Team”) or small (“B Team”) from one central location

LTI DataComm
23020 Eaglewood Ct. #100
Sterling, VA 20166
www.ltidata.com
800-677-5050

Copyright LTI DataComm, 2009.
All rights reserved.

Solution (Concluded)

The added features of these new tools allowed LTI to further tailor the solution to the FDIC requirements. For example, the Secure Remote Access Point service extends the FDIC corporate office to all necessary remote sites by connecting a field deployed AP to the master controller using standard Layer 2 tunneling protocol (L2TP) and Internet Protocol Security (IPSec) across the internet. All control and 802.11 data are carried through the secure encrypted tunnel protecting it while traversing any public network.

When a (B) team is tasked to a location, RAPs would be placed out at any remote location depending on the number of employees, and would in turn connect to the Aruba 6000 at FDIC HQ over the public internet and authenticate securely to the Master Switch establishing a VPN tunnel before allowing any FDIC wireless user to utilize the wireless service.

The second scenario that LTI helped to conceptualize and validate on-site with the FDIC engineers involved the deployment of the (A) team to a remote location that requires more coverage and capacity from the wireless network. To meet these specific needs LTI utilized the Point-to-Point VPN feature offered in the ArubaOS. This feature again takes advantage of securing all 802.11 data and control information in a secure IPSec tunnel, but this particular tunnel is sourced from an Aruba Switch configured as a Local controller terminating to the centrally configured master controller. The master controller in an Aruba architecture governs all RF and security settings, while additional controllers added to the same enterprise WLAN serve as subordinate switches to the master controller.

The local controller operates independently of the master and a pre-shared key (PSK) is used to create the IPSec tunnel between all controllers. The local controller depends on the master controller only for its security and RF settings, it needs to have connectivity to the master controller at all times to ensure that any changes on the master are propagated to all the local controllers in the network. The proven and tested design gives FDIC the ability to deploy as many local controllers to as many remote sites as needed.

Finally, due to the lack of prior knowledge regarding the existing network infrastructure at the remote location to be visited, it was essential that fielded teams have the capability to set up a secure wireless network without being deterred by the overall lack of on-site network connectivity. This is why LTI proposed implementing secure wireless mesh as it was an effective way of expanding enterprise wireless coverage without any wires.

By implementing mesh APs, the FDIC is now able to strategically place mesh units anywhere connectivity is a necessity while only having to power to the mesh node. The local Aruba controller still provides centralized configuration and management for Aruba APs in a mesh environment, but the mesh APs now additionally provide encryption and traffic forwarding through all the mesh links.

Results

LTI DataComm brought their knowledge and experience of wireless technology to design and administer the most appropriate solution - allowing their customer to meet Agency mission objectives. LTI was committed to fully understanding the requirements, and diligently worked with the customer's engineering team to simplify the deployment process and minimize the support efforts at HQ. By working as a consultative partner, LTI was able to bring a complete, applicable, secure, and expandable solution to contribute to the continued mission success of the agency.

Solutions to Serve, Solutions for Service