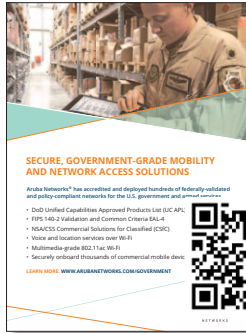


Jon Green

Senior Director, Security Architecture
Aruba Networks

Mobility Is Not Monolithic



Building mobile infrastructure, security, authentication, device management, applications and storage capabilities all at the same time can be daunting.

“Don’t tackle mobility as one big monolithic thing; there are a lot of pieces to it. If you can break it into more bite sized pieces you can actually be more effective,” **Jon**

Green from Aruba Networks told OTFL in a recent interview.

Phase 1 is to look at network infrastructure. Phase 2 is to look at what types of devices are going on the networks.

“So laptops, we’ll do that from day one; then we can look at adding tablets to that; from there we can look at adding guest and visitor; then we can look at adding personally owned devices or BYOD,” Mr. Green explained.

“Phasing these things in is actually important. From my experience I don’t see a lot of people thinking about it that way. They throw their hands up and say: ‘How are we going to tackle all this stuff at the same time?’”

Mobility Defined Networks

In the mobility marketplace, Aruba is primarily known as a wireless LAN and WiFi vendor. The company has deployed hundreds of federally-validated and policy-compliant networks. Its Mobility-Defined Networks™ allows general-purpose commercial mobile devices to access networks that handle classified, sensitive but unclassified and confidential information.

Mr. Green said they unify and automate all aspects of secure mobility — access management, network infrastructure and mobile applications — into one cohesive system for employees, contractors, visitors, and military personnel in garrison or in deployment.

The result is leveraging contextual data-user roles, device types, application flows, location and time-of-day — to enforce standards-based security and access policies across the network all the way to devices and mobile applications.

“We’ve always thought of ourselves as a mobility infrastructure vendor,” Mr. Green noted. “The vision has always been that we all walk around with our cell phones on mobile networks, so why don’t we have the same type of experience, the same advantages when we are in an enterprise setting on an internal type of network? So that’s what we set out to build.”

More Reach, Less Cost

The Number One and easiest way to increase your mobile capability is to install more WiFi, putting up wireless even where you don’t necessarily have a need for it today.

“Laptops work great on this and people forget mobility also involves things like laptops. And if you are talking Windows 8 tablets, it’s effectively the same as dealing with a laptop,” Mr. Green said.

“You don’t have to make huge changes to policy because your enterprise management systems already work and you are just changing the method by which devices connect into the network.”

That has a couple of implications Mr. Green explained.

“One is, if you are looking at something such as Bring Your Own Device (BYOD) or some other type of mobility program, WiFi is running the function for that on the network side,” he said.

“Once you’ve deployed WiFi, you’ve solved a huge part of this whole mobility challenge. Putting in a pervasive WiFi network reaching everywhere in your agency is a huge step towards that.”

Mr. Green noted further that WiFi is a lot cheaper than wired networks. As agencies look to refresh programs for their wired networks, they can actually take a hard look at what they actually need.

Does an agency need to replace 200 switches to provide 4 ports per work location? By putting in WiFi, agencies can scale the wired network so that it meets today’s needs. There’s a huge cost savings involved in doing that and it can more than pay for the installation of the WiFi piece, Mr. Green declared.

Also, by deploying WiFi you are also improving network security; now you must do authentication, encryption and access control because you need to authenticate the user and potentially the device as it joins on to the network.

“Instead of seeing something plugged in, a PC plugged into an Internet port, we can actually recognize ‘this is the CEO and he’s on an iPad, or this is a Three Star General and he’s on an Android phone,’” noted Mr. Green.

“That type of stuff gives you a lot of power. You can actually make a case for security going up and costs going down by going to a WiFi network.” ■