



Aruba's Secure Mobility Solution for Legacy WLANs

Many forward-looking organizations recognized the benefits of wireless LAN (WLAN) technology long ago and deployed it to increase employee productivity, enable new applications, and deliver network mobility. At that time, the state of the art in WLAN consisted of stand-alone “thick” access points and the WEP encryption protocol. Today, these technologies are recognized as cumbersome at best and dangerous at worst, yet many organizations have made a sizeable investment in the technology and can't afford a wholesale upgrade. Aruba Networks allows these organizations to augment their existing WLAN access points to deliver today's user-centric network.

The Need for Augmenting Legacy WLANs

LACK OF MOBILITY

Legacy APs are anchored to VLANs and IP subnets, meaning that wireless clients are also anchored to these VLANs. When a client roams to an AP connected to a different VLAN, the transition is not seamless. Clients are forced to obtain a new IP address and existing sessions must be restarted.

GAPS IN WLAN SECURITY

Many older APs only support WEP and cannot be upgraded to support WPA2, the current wireless security standard. This exposes the organization to great risk since WEP is extremely simple to break. Legacy WLANs also provide “one size fits all” access – once a user is on the network, access is wide open. This makes it impossible to safely provide

guest access and opens holes in the network where simple devices, such as wireless barcode scanners, are given excessive privileges.

LACK OF WLAN VISIBILITY

Legacy WLANs provide limited or no visibility into what's happening in the RF domain. Troubleshooting, rogue AP detection and location, and attack detection are all manual processes that require in-depth WLAN knowledge.

CUMBERSOME TROUBLESHOOTING

When a legacy AP becomes unreachable from the network, often administrators must pull out ladders and climb above ceiling tiles to troubleshoot the AP. This is both time consuming and expensive.

How Aruba Secures and Mobilizes Legacy WLANs

By installing an Aruba Mobility Controller in the network and connecting legacy APs through the Controller, either physically or logically, many of the benefits of a modern centralized WLAN can be provided to legacy APs.

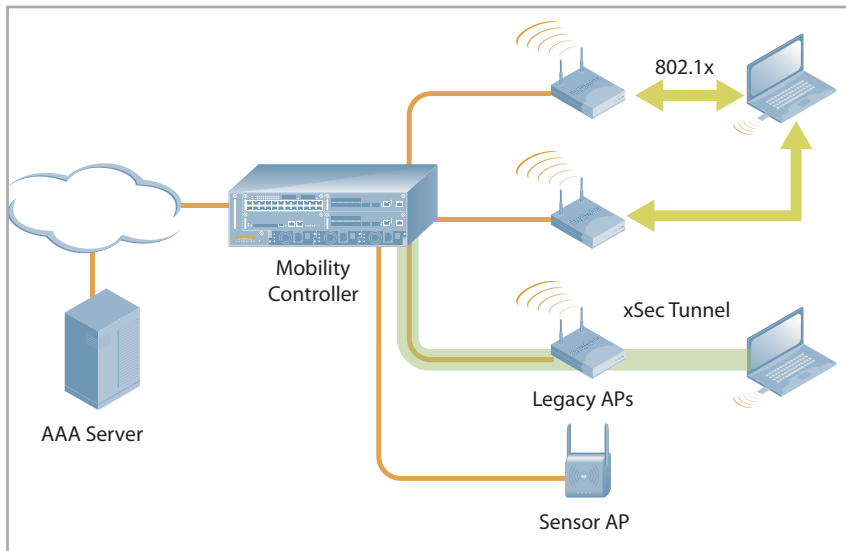
SEAMLESS ROAMING

Aruba's proxy DHCP enables seamless roaming to work regardless of which VLAN an AP is physically connected. When a client first joins the network, it is assigned an IP address according to normal rules (the VLAN on which the AP exists). When the client roams,

Benefits:

- Instant upgrade for WLAN security without replacing APs
- Eliminate inter-VLAN roaming failures
- Strengthen overall security using Wireless Intrusion Protection
- Better policy enforcement using Aruba's stateful firewall
- Simple migration path from legacy WLAN to modern centralized WLAN

Secure Mobility for Legacy WLANs



it will issue a DHCP renew each time it associates to a new AP. The Mobility Controller will capture the DHCP request and respond to it, telling the client to keep the same IP address. This lets the client keep a consistent view of the network, while the network keeps a consistent view of the client. In this manner, a client can roam throughout the network, within and across VLANs, without sessions being reset.

STATEFUL 802.1X

Stateful 802.1x allows the Mobility Controller to learn the identity and role of a user connected to a third-party AP. When an 802.1x-capable access point sends a RADIUS request to the AAA server, the Mobility Controller inspects this request and the associated response to learn the authentication state of the user. It then applies identity-based security through the Policy Enforcement Firewall.

POLICY ENFORCEMENT FIREWALL

Using Aruba's ICSA-certified Policy Enforcement Firewall (PEF), the Mobility Controller can enforce identity-based access control for users on third-party APs. This lets users be mapped into roles based on group membership, with different access rights provided to each role. Using PEF, open access can be provided to employees on laptops while very restricted access is provided to devices such as barcode scanners – even with both devices on the same

SSID. In addition, guest access can be restricted to Internet-only while contractors are given limited rights to the internal network.

SERIAL- AND POWER-OVER-ETHERNET

When third-party APs are connected directly to a Mobility Controller, Power-over-Ethernet as well as Serial-over-Ethernet (SOE) are provided by the Mobility Controller. Using SOE with the appropriate splitter, console connectivity to the AP can be provided through the Mobility Controller's built-in terminal server by carrying RS-232 serial lines over spare wires in standard twisted-pair cables. Administrators no longer need to climb ladders to connect console ports to APs when troubleshooting must be performed. Instead, administrators simply connect to the Mobility Controller over telnet or SSH and can immediately console into the third-party AP.

XSEC LAYER-2 VPN

Some legacy APs cannot be upgraded to support modern security standards such as WPA or WPA2. For these APs, Aruba's xSec provides a way to bypass the security of the AP entirely while still providing all the benefits of WPA2 with AES encryption. Using xSec client software, a secure tunnel is formed across the wireless link to an Aruba Mobility Controller. While the AP can be operating in "open" mode, all traffic

Secure Mobility for Legacy WLANs

going through the AP is authenticated and encrypted just as in WPA2. Client software is available for a number of popular operating systems.

RF VISIBILITY

By adding a small number of Aruba APs to the network to act as monitoring devices, RF visibility is provided to the network administrator to visualize activity, interference, and error conditions. For troubleshooting sessions, live remote packet captures can be streamed to the Aruba Enterprise Analyzer.

WIRELESS INTRUSION PREVENTION

To enhance wireless security, Aruba provides the Wireless Intrusion Prevention module embedded within each Mobility Controller. This system monitors both Aruba APs as well as third-party APs and can identify a number of vulnerabilities and attacks against wireless LANs including rogue APs, bridging client devices, and denial of service attacks. For greater capabilities including event correlation and advanced visualization, Aruba also offers the stand-alone RFprotect™ software application that integrates with Aruba wireless APs acting as sensors.



WWW.ARUBANETWORKS.COM

1322 Crossman Avenue, Sunnyvale, CA 94089 | Tel. +1 408.227.4500 | Fax. +1 408.227.4550