# Remote AP Module

Aruba Networks' Remote AP software module enables any Aruba access point to be securely and easily connected from a remote location to an Aruba mobility controller across the Internet. Ideally suited for small remote offices, home offices, telecommuters and mobile executives, Aruba's Remote AP software module extends the mobile edge to any remote location by enabling seamless corporate wireless data and voice wherever a user finds an Internet-connected Ethernet port.
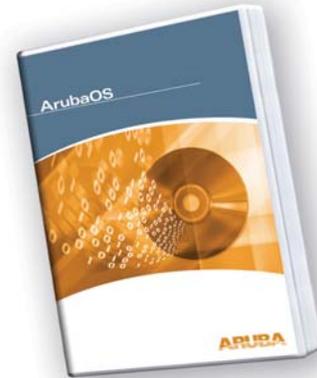
SECURE MOBILE CONNECTIVITY
Secure corporate voice and data connectivity at any remote location
Standards based IPSec encryption

CENTRALIZED MANAGEMENT AND SECURITY
Centrally defined and managed access policies
Works with existing 802.1x supplicant on client machines
No IPsec client or SSL VPN software required

IDEAL SOLUTION FOR TELECOMMUTERS
Plug-and-play simplicity for mobile executives
Remote troubleshooting and management
Works with any Aruba 60, 61 or 70 access point

SURVIVABILITY AND LOCAL RESOURCE ACCESS
Local bridging capability to access local resources such as printers and local servers
Continued service to users in the absence of connectivity to headquarters

SECURE WIRELESS MOBILE CONNECTIVITY AND VOIP ANYWHERE

The Remote AP software module activates secure communications from an Aruba mobility controller to a designated Aruba access point (AP) at a remote location, seamlessly extending the corporate WLAN over the Internet anywhere it is needed. The user experience at the home office, remote office, or at any other location is exactly the same as it would be at the corporate headquarters.

A remote Aruba AP communicates with an Aruba mobility controller using the IPsec protocol, widely trusted for deploying Virtual Private Network (VPN) connections across the Internet. This standards-based, end-to-end encryption support enables a remote AP to be plugged directly into an Internet-connected DSL router, eliminating the need for a mobility controller to be installed at the remote location.

Corporate-issued Voice-over-wireless phones connect through a remote Aruba AP and function as if they were at the central corporate site. Aruba's QoS-enabled, voice protocol-aware architecture delivers a toll-quality voice experience, even over remote links. Additionally, available security features, such as encryption and the Policy Enforcement Firewall, ensure that all voice communications have the highest levels of security available to prevent eavesdropping.

CENTRALIZED MANAGEMENT AND SECURITY

Aruba's Remote AP module enables the network administrator to access all the remote Aruba AP's parameters, such as operating channel, radio type, SSID, BSSID and all associated clients, and enables centralized configuration changes. Additionally, the network administrator can see detailed client status reports showing the client MAC address, client manufacturer, channel, radio, status and last activity date and time.

A remotely-connected Aruba AP works with existing 802.1x supplicants on client machines to provide secure authentication with IPsec encryption of all authentication information between the client and the mobility controller. The Remote AP supports end-to-end WPA2 and 802.11i security from the client to the mobility controller, regardless of whether the client is wireless or wired.

After successful authentication, all communication is tunneled or encrypted inside the IPsec connection. There is no need to install and maintain a VPN client or download a temporary SSL VPN client on the remote machine, significantly reducing the cost of management.

A remote Aruba AP downloads its configuration and security policy from the Aruba mobility controller. This eliminates any risk of security policy misconfiguration and the need for any technical expertise at the remote location. No security credentials are stored on the remote AP, so there is no risk of a security breach in the event that an AP is lost or stolen.
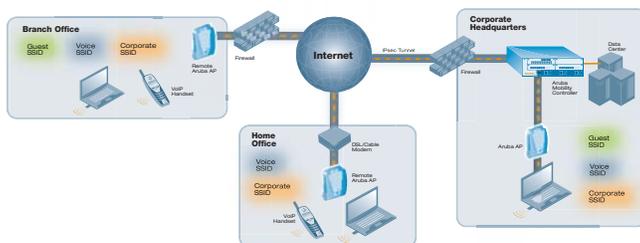
The remote Aruba AP communicates user attributes such as authentication method, application, device type and protocol used to the available Policy Enforcement Firewall module in the mobility controller. This communication enables highly granular and dynamic security policies, further improving the security posture of the enterprise WLAN. For example, a remote user can be restricted from using a particular application or network resource. This advanced capability allows workers to safely connect to the network via a remote AP regardless of location because users' security policies always follow them.

Aruba Remote APs are ideally suited for providing secure mobile connectivity to branch and home offices. All security policies are centrally defined and enforced on Aruba's mobility controller.

Detailed client status report

Aruba Remote APs are ideally suited for providing secure mobile connectivity to branch and home offices. All security policies are centrally defined and enforced on Aruba's mobility controller.

IDEAL SOLUTION FOR TELECOMMUTERS

With remote users who have VPN clients, the network administrator often has to support or troubleshoot a non-corporate client device. A remotely-connected Aruba AP operates independently of the home network, requiring no maintenance, troubleshooting or reconfiguration of existing networks.

A remote Aruba AP is so easy to deploy that a mobile executive can simply plug it into a DSL router, cable modem or other broadband connection in their home or at a remote location. The remote AP automatically contacts the corporate mobility controller, authenticates, self-configures, and begins operation. If the broadband connection is behind a firewall, the remote AP uses its built-in NAT-T capability to connect to the corporate mobility controller without requiring any user intervention.

Aruba APs support the 802.11af Power-over-Ethernet (PoE) standard, so the AP can be directly connected to a PoE-enabled port without requiring a separate power line. Additionally, Aruba APs have multi-directional, movable, and interchangeable antennas that provide excellent wireless coverage and eliminate the need for costly site surveys or expensive installation.

If problems arise, Aruba's Remote AP module allows the network administrator to remotely capture packets for traffic analysis and troubleshooting, eliminating a "truck roll" to the remote site.

SURVIVABILITY AND ACCESS TO LOCAL RESOURCES

The remote access points can be configured to locally bridge all traffic on selected SSIDs, thereby allowing access to local resources without tunneling all traffic back to the main site. This is enabled by performing encryption and decryption on the access point, rather than the mobility controller, for these selected SSIDs. These SSIDs can also be used as a backup for providing network access if the link to the main site is lost. The users at the remote site will still be provided with access, although new users may be unable to authenticate to the network.

SPECIFICATIONS

Supported Aruba Access Points

All Aruba Access Points currently available

Supported Protocols

L2TP/IPsec
IPSEC over NAT-T (Network Address Translation Traversal)
802.11af compliant Power-over-Ethernet

FEATURE	BENEFIT
Authentication	• Variety of options to authenticate users, devices and access points including Captive Portal, 802 1X, MAC-based, RADIUS, LDAP and SecurID.
Mobile Security	• Apply Identity-based per-user security policies that follow the user regardless of their connection location.
Centralized Key Storage	• No critical information is stored on a remote Aruba AP. In the event that the AP is lost or stolen, no vital security information is compromised and the AP can simply be disabled by the administrator.
Wireless Encryption	• Support for the latest security standards including 802.11i, WPA and WPA2 guarantees proven security and interoperability.

The Mobile Edge Company

www.arubanetworks.com

1322 Crossman Avenue
Sunnyvale, California 94089
Tel: 408.227.4500 • Fax: 408.227.4550