

ArubaOS

Remote AP Module

ArubaOS

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, mobile executives, and for business continuity applications, Aruba's Remote AP software module extends the enterprise network to any remote location by enabling seamless wireless data and voice wherever a user finds an Internet-connected Ethernet port or cellular connection.

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 enterprise 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 site. 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. IT-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.

Rogue AP Prevention

- Rogue AP detection, Classification, Location and automatic containment

Denial of Service (DoS) Attack Detection

- Management frame floods, Deauthentication attacks, Authentication floods, Probe request floods, Fake AP floods, Null probe responses, EAP handshake floods

Probing and Network Discovery

- Detection of NetStumbler and broadcast probes

Client Intrusion Prevention

- Honeypot AP protection, Valid station protection

Network Intrusion Detection

- Wireless bridges, ASLEAP attacks

Surveillance

- Detection of weak encryption implementation

Impersonation Detection and Prevention

- MAC address spoofing, AP impersonations, Man-in-the-middle attacks, sequence number anomaly detection

Product Overview



Benefits:

Ideal Solution for Road Warriors and Business Continuity

- Extends the enterprise network to remote locations without compromising security
- Plug-and-play simplicity for mobile executives
- Remote troubleshooting and management
- Works with any Aruba access point

Secure Mobile Connectivity

- Secure corporate voice and data connectivity at any remote location
- Standards based IPsec and AES encryption for secure mobile connectivity over the Internet
- Split tunneling for optimized local traffic performance
- Reliable connectivity over slow links

Product Overview

More Benefits:

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
- Stateful firewall and NAT for local and centralized traffic
- DNS-based Mobility Controller lookup for ease-of-use, load balancing, and fault tolerance

Nomadic and Mobile Network Access Using Cellular Backhaul

- Enables instant network extension for temporary secure access, first responders, disaster recovery and tactical applications
- Increased reliability and resiliency by using cellular link as back-up to wired Internet connection

Specifications:

Supported Aruba Access Points

- AP-60/61, AP-65, AP-70, AP-85

Supported Protocols

- L2TP/IPsec
- IPSEC over NAT-T (Network Address Translation Traversal)
- 802.11af compliant Power-over-Ethernet
- Minimum link speed required: 64 Kbps per SSID

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

Centralized Management and Security

Aruba's Remote AP module enables the network administrator to centrally assign all the remote Aruba AP's parameters, such as operating mode, fault tolerance, SSID, and security settings. Additionally, the network administrator can see detailed statistics and local client status reports showing the client MAC address, client manufacturer, channel, radio, status and last activity date and time.

A remote AP works with existing 802.1X supplicants on client machines to provide secure authentication and encryption of all authentication information between the client and the mobility controller. The module supports both a centralized mode, with end-to-end WPA2 and 802.11i security from the client to the mobility controller, as well as a distributed mode with WPA2 and 802.11i termination on the access point. 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 a Mobility Controller, eliminating the 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, minimizing the 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, as well as the policy enforcement module on the access point. 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.

Ideal Business Continuity Solution

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 employee 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 primary or back-up Mobility Controllers, 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. The Aruba Remote AP also offers the capability to connect from a hotel room equipped with wired Internet access without requiring a separate VPN software client, even where the connection needs to be initially activated using a browser-based mechanism or captive portal. This is ideal for road warriors as well as hotel meeting room sessions as the remote AP can extend the office network in a plug-and-play manner for the duration of the stay or meeting.

Nomadic Access Using Cellular Backhaul

The Aruba AP-70 can use a USB-based EVDO or 3G modem to connect to the Internet over a cellular network. The cellular network is used as a transport mechanism to reach the Aruba Mobility Controller and enable all Remote AP capabilities. This eliminates the requirement for a wired Internet connection to extend the network and enables multiple applications including temporary offices in environments where wired Internet connections are not feasible or available, first responder access, disaster recovery and tactical applications. This also allows companies to set up instant branch offices almost anywhere – thus truly utilizing the power of the ubiquitous cellular network. Until now, enterprises have been forced to quarantine wireless users into a DMZ, where they were authenticated and firewalled as if they were coming in from the Internet. While this mechanism works from a security standpoint, the performance offered to the wireless user is severely impacted due to limitations with DMZ-based VPN gateways and firewalls. Aruba allows corporate users to be authenticated, encrypted and firewalled within the corporate intranet with the highest degree of security and performance, providing the connecting point between mobile users and the wired network.