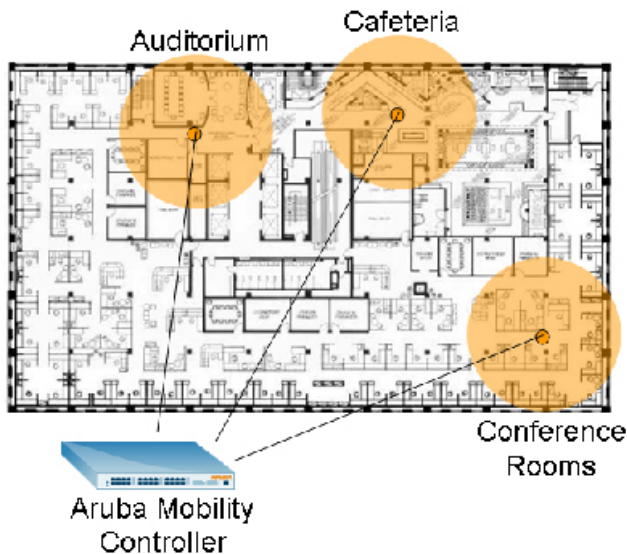


Internal WLAN Hotspots

The Aruba Networks solution for internal WLAN hotspots allows IT managers to quickly and easily install wireless LAN access in strategic locations such as conference rooms, cafeterias, auditoriums, and lounges. This type of access is provided as a convenience service rather than a mission critical network to allow secure access to the internal network and the Internet. For these internal WLAN hotspots, Aruba Networks provides a secure, convenient solution that installs with a minimum of cost and effort and without disrupting the existing network. This system can easily accommodate guest access as well, and also grows to accommodate future enterprise-wide wireless LAN access as the mobile edge of the network expands.



Highlights

- Internal “convenience” wireless access in conference rooms and other strategic locations
- Gives employees mobility in places they demand it most
- Easy to combine with guest access solution

Solution Benefits

- Convenient wireless access for employees in common areas
- Requires a minimum of involvement from IT staff
- Minimal client configuration requirements
- Maximum client compatibility to reduce helpdesk calls
- Strong security to prevent intrusion or eavesdropping
- APs are installed using existing cabling, reducing installation costs

Centralized Wireless LAN Control

Provides high security and scalability by placing security, management, mobility, and RF calibration in a centralized mobility controller instead of distributed access points. This allows APs to be placed wherever it is convenient, without regard to RF planning or physical security. Secure mounting options can be used to lock down an AP, but even in the event that an AP is stolen, it contains no configuration or security information and is useless without the centralized controller.

Adaptive Radio Management (ARM)

Provides automatic self-configuration of all radio parameters, including transmit power level, channel, load-balancing, and interference avoidance. With ARM, network administrators can simply place an access point wherever it is convenient and need not worry about expensive site surveys or manual performance tuning.

Non-Disruptive Deployment

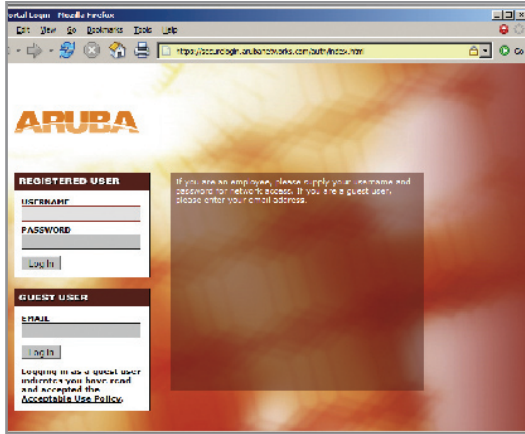
Treats the existing network a “no-touch” zone to allow for rapid on-demand deployments. Aruba APs and mobility controllers securely communicate with each other over IP networks. No reconfiguration of closet switches, routers, VLANs, or ports is required. Administrators simply connect an Aruba AP to an existing Ethernet port and it automatically discovers a controller, connects to it, and begins operation.

Captive Portal

Provides secure web-based authentication. Client devices connect to the network and are blocked from all access until a web browser is opened and authentication credentials are entered. The exchange of authentication credentials is secured using industry-standard



SSL. The system can require a valid username and password, or may be configured only to collect non-validated email addresses for guest access. The captive portal pages may be customized by uploading custom backgrounds, acceptable use policies, and other text.



Captive Portal

VPN Server Emulation

Allows existing VPN clients on employee laptops, used for Internet remote access, to also secure the wireless network. An employee with a self-installed wireless LAN card can be given instructions to connect to a wireless SSID with a pre-shared encryption key and then launch a VPN client, just as they would while at home or while traveling. The VPN connection will be intercepted by the Aruba mobility controller and terminated locally, preventing internal wireless users from overloading external VPN concentrators.

Mobile Edge Client

The Mobile Edge Client is a small software application that can be automatically downloaded to a client device through the Aruba Captive Portal. The Mobile Edge Client is a front-end to the VPN client built into Microsoft Windows 2000 and XP. Used in environments where a VPN client is not already installed, the Mobile Edge Client is preconfigured by the network administrator with all the settings needed to secure the wireless network using VPN technology. Using the Mobile Edge Client, users and administrators are never forced to configure complex VPN settings on client devices.



Mobile Edge Client

Required Components

Mobility Controller

Any Aruba Mobility Controller
 Aruba 6000
 Aruba 2400
 Aruba 800

System Software

Policy Enforcement Firewall Module
 VPN Server Module

Controlled Access Points

Aruba Controlled Wireless Access Point
 Aruba 41
 Aruba 60
 Aruba 61
 Aruba 65
 Aruba 70