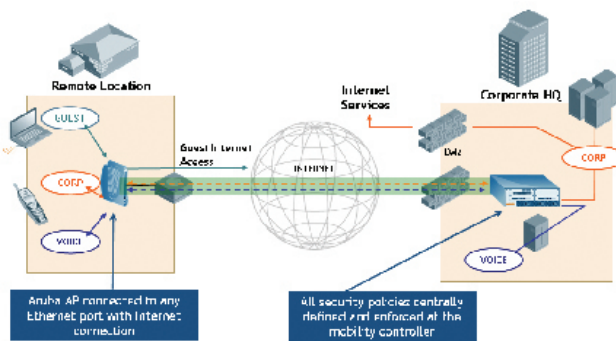


# Small Office, Home Office, and Road Warrior Mobile Networks

The mobile edge must transcend the enterprise network perimeter and extend to wherever employees need access to enterprise voice and data resources. Aruba's solution for small offices/home offices (SOHO) and road warriors allows secure corporate "hot spots" to be set up wherever an Internet-connected Ethernet port is available.

Remote sites are protected against WAN link failures, and can be selectively granted access to local resources as needed. In locations where a wired Ethernet port is not available, Aruba's Mobile Edge Client gives mobile users a secure VPN connection back to the corporate network.



## Remote AP with Centralized Termination

Aruba's Flex-MAC architecture permits a Remote AP to operate with user traffic terminating at a centralized mobility controller. In this model, the Remote AP accepts encrypted wireless traffic from clients, adds an IPSEC header, and forwards the traffic across a WAN or the Internet to a mobility controller at a corporate site. The mobility controller is responsible for all encryption, forwarding, and other traffic processing. This model results in the highest level of security, since user data is encrypted from the client all the way to the corporate network.

## Remote AP with Local Termination

Aruba's Flex-MAC architecture also permits a Remote AP to terminate user traffic locally. When local resources are present, such as file servers or printers, it can be inefficient or impossible for traffic to cross the WAN multiple times. For these circumstances, the Remote AP operating in local termination mode handles all encryption and traffic forwarding, while the mobility controller performs authentication and management of the AP.

## Multi-ESSID Support

The Aruba Remote AP supports multiple ESSIDs with different profiles and different traffic termination. Aruba's Flex-MAC architecture allows both centralized encryption and local bridging to be supported at the same time on multiple ESSIDs. This can be used to provide a corporate ESSID, secured using 802.11i, that is terminated centrally at a corporate mobility controller. At the same time, a voice ESSID secured using static-key encryption can be supported with central termination, and a guest ESSID without encryption can be terminated locally to provide direct Internet access to guests.

## Remote Site Survivability

A Remote AP using centralized encryption will cease to operate if the WAN link to the central mobility controller fails. To handle this failure scenario, an SSID may be configured for local bridging with static-key encryption, and client devices can be configured to automatically connect to the backup SSID when the primary fails. Using this technique, users can still access local resources, such as servers and printers, even when the link to the corporate site is unavailable. As an alternate method, Remote APs may be con-

## Highlights

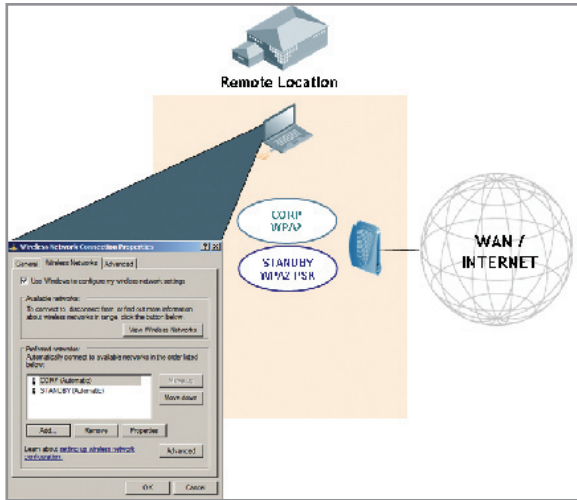
- Secure mobile connectivity at any remote location including small offices, homes, hotel rooms, and public wireless hotspots
- Data and voice devices both supported with full security
- Security and management controlled centrally by IT staff

## Solution Benefits

- Keeps employees in touch with enterprise resources wherever they travel
- Extends corporate wireless policies and security to remote locations
- Lets multiple employees at a remote location share the same secure wireless connection
- Gives remote access capabilities to wireless voice over IP handsets
- Secures access from employee homes without IT staff needing to manage consumer equipment
- Allows a wired device in a small office or home office to be securely connected to the corporate network



figured for full-time local bridging. Under a failure scenario, clients that are already associated and authenticated will remain connected to the network.



WLAN Backup

### Wired Port Tunneling

Unique to the Aruba 70, wired port tunneling permits the second Ethernet port of an Aruba 70 to provide secure connectivity to a central mobility controller. When wired port tunneling is enabled, the second Ethernet port is designated as a logical extension of the mobility controller. Authentication using 802.1x, captive portal, VPN, or MAC address may be optionally enabled, and all traffic entering the wired port will be sent through an encrypted IPSEC tunnel back to the corporate site. This capability allows wired devices, such as VoIP desktop phones or printers, to be part of the corporate network without the need for an expensive VPN gateway at the remote site.



AP 70

### 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 public wireless hotspots where a Remote AP cannot be used, the Mobile Edge Client is preconfigured by the network administrator with all the settings needed to secure the end-to-end connection using VPN tunnels. Using the Mobile Edge Client, users and administrators are never forced to configure complex VPN settings on client devices.



Mobile Edge Client

### Required Components

<b>Mobility Controller</b>
Any Aruba Mobility Controller Aruba 6000 Aruba 2400 Aruba 800
<b>System Software</b>
Policy Enforcement Firewall Module Remote AP Module
<b>Controlled Access Points</b>
Aruba-Compatible Wireless Access Point Aruba 41 Aruba 60 Aruba 61 Aruba 65 Aruba 70