



Design and Implementation Guide

Apple® iPhone™ Compatibility



Introduction

Security in wireless LANs has long been a concern for network administrators. While securing laptop devices is well understood, new threats to the network are appearing as converged devices are being constantly introduced in the market. The devices are as almost as powerful as a regular computer, but lack the security controls found in a regular computer system. Some of the devices carry a powerful CPUs and large amounts of memory, running striped down versions of operating system that run on a personal computer.

Universities are a good example of the kind of network where wireless devices on converged devices are likely to appear. It is common to find different versions of OS, laptops, and wifi enabled handsets all existing on the same common network. It is a nightmare for the network admin to try to secure these devices in an open access network.

Currently the devices offer little or no control on what should and should not be executed. These devices become easy targets for hackers and viruses. In addition, some of the networking protocols implemented on these devices could be non-standards based, causing the network to behave in an erratic manner.

These devices are a cause for great concern among network administrators. The devices not only poses productivity risks to individual, but could cause a situation which affects all of the users having access to the common resource, in this case the wireless LAN network.

The Aruba Advantage

Aruba Networks is uniquely positioned to reduce the effects of these kinds problems. Aruba Networks make it easier to mitigate the risks posed by such open access environments through the use of an integrated firewall and multilayered authentication. Scalability and battery life enhancements are available through VLAN pooling, Proxy ARP, and seamless layer 3 mobility.

Integrated ICSA certified Firewall

Aruba's role based firewall helps assign roles to users and devices based on parameters provided by the network administrator. These roles can be defined on the basis of user identity, device identity, device type, authentication mechanism, etc. This is a stateful firewall that is able to enforce security and access requirements. Violations can be acted upon to quarantine or blacklist users whose machines violate predetermined policy.

Devices like iPhones can be provided a unique role in the system with access to network resources appropriate to the network policy needs. E.g. one can disable access to iTunes by limiting access to the multicast address and the port that the service runs on.

Multilayered Authentication

Converged phones and PDA devices usually use legacy security and authentication protocols (e.g. WEP, PSK). This security limitation can be overcome through additional layered security mechanisms to enhance the security of the device and user.

As an example, a user or a device may be allowed to enter the network using a SSID that uses WEP encryption, but can be forced to authenticate with captive portal on VPN technologies to gain access to core resources (servers, file systems etc) on the network.

VLAN Pooling and Proxy ARP

VLANs are typically used not only to separate broadcast domains but also to separate users by class. A prime example would be to have a series of VLANs for students, and a separate VLAN for faculty use. The default method of mapping wireless users to VLANs is to associate an SSID with a VLAN. This is typically not a problem until the number of users grows beyond a reasonable subnet size, as would occur in very large classrooms or auditoriums.

A VLAN typically cannot handle more than 200 users very effectively. Increased broadcast traffic on large VLANs not only causes performance problems and consumes precious over-the-air bandwidth, but also drains battery life on mobile devices.

VLAN pooling, delivers the flexibility of VLAN-based network planning without any of the negative side effects. In VLAN Pooling, multiple VLANs form a VLAN pool, and all VLANs belonging to the VLAN pool are available at any location on the campus. VLAN assignment is performed dynamically at the time a user logs into the network and is based on current user loads on the different VLANs that form the VLAN pool.

Aruba's Proxy ARP helps reduce the broadcast on a VLAN and helps improve client battery life by not flooding unneeded packets to the client, thus forcing it to wake up. Instead, the system answers ARP requests on behalf of the client, reducing the amount of time the client must be awake and transmitting to deal with routine network requests.

Seamless Layer 3 Mobility Domains

Creating multiple subnets allows the network to be structured more efficiently, and allows different VLANs and network segments to have their own IP ranges. This segmentation enhances troubleshooting and the maintainability of large networks.

The downside is that if a user crosses a Layer 3 boundary, it may cause the active sessions to break (voice, data). Aruba's WLAN system provides Layer 3 mobility features that seamlessly connect across Layer 3 subnets, thus causing "zero disruption" to the application. This is achieved through IP mobility, allowing the client to keep their IP address as they roam through different subnets, with their traffic tunneled back to their original subnet for standard Layer 3 routing.

Conclusion

In summary, the Aruba Networks Mobility Controller and thin Access Point solution provides a powerful feature set making it possible to deploy a secure, scalable and a versatile network. Network administrators are free to open their network to devices they do not have direct control of, secure in the knowledge that their network is protected from malicious activity and potential capacity issues.

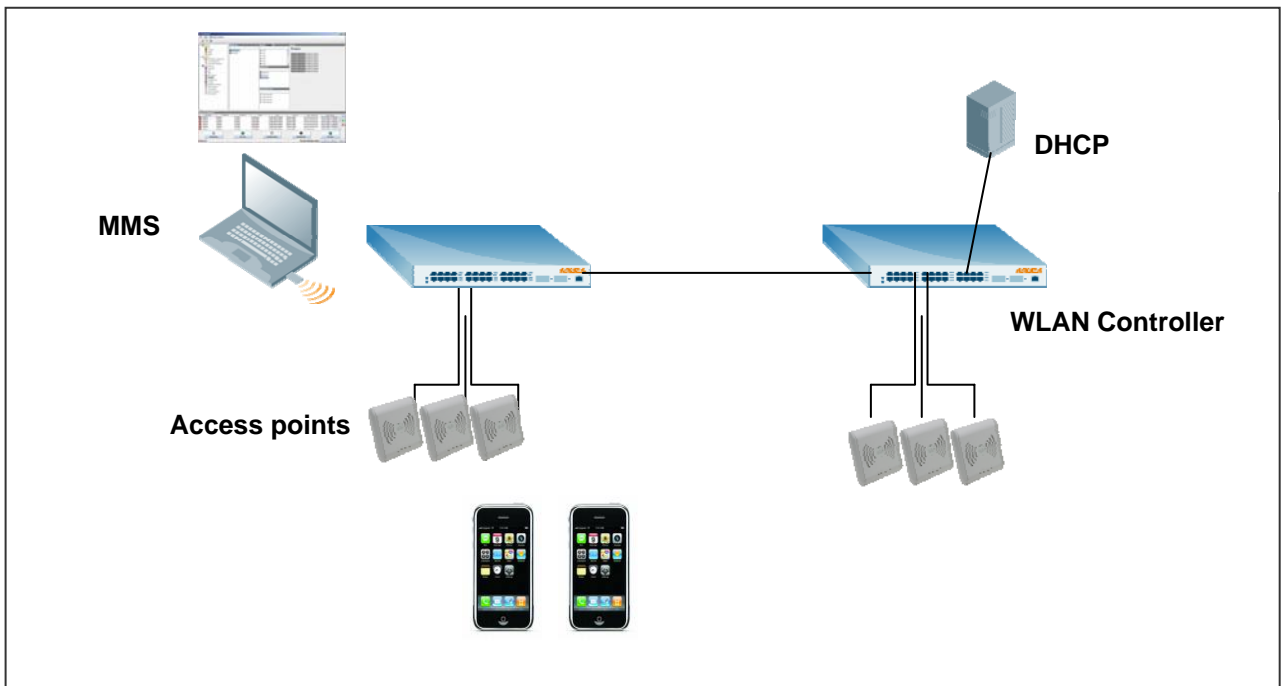
About Aruba Networks, Inc.

Aruba Networks provides an enterprise mobility solution that enables secure access to data, voice and video applications across wireless and wireline enterprise networks. The Aruba Mobile Edge Architecture allows end-users to roam to different locations within an enterprise campus or office building, as well as to remote locations such as branch and home offices, while maintaining secure and consistent access to all of their network resources. Using the Aruba Mobile Edge Architecture, IT departments can manage user-based network access and enforce application delivery policies from a single integrated point of control in a consistent manner. Aruba's user-centric enterprise mobility solution integrates the ArubaOS operating system, optional value-added software modules, a centralized mobility management system, high-performance programmable mobility controllers, and wired and wireless access points. Based in Sunnyvale, California, Aruba has operations in the United States, Europe, the Middle East and Asia Pacific, and employs staff around the world. To learn more, visit Aruba at <http://www.arubanetworks.com>.

Apple iPhone Compatibility Test Description

Aruba tested the Apple iPhone in our labs to ensure seamless interoperability. The test specifics are summarized below:

Test Topology



Aruba WLAN Test Set-up

Results summary

Vendor / Device	Model	Static WEP	WPA-PSK	WPA2-PSK	Fast Roaming	Standby Roaming	VPN
Apple iPhone	4Gb model 1.0 (1A5423a)	✓	✓	✓	✓	✓	✓

Test Details

The compatibility test plan consisted of the following:

Network Connectivity: L2 and L3 connectivity was verified when the iPhone was associated to a Aruba network.

Association Modes: The mobile device is configured for the chosen security mode and then connected to the Aruba infrastructure. Successful data transfers upon connection are required to pass the test. The security modes tested are as follows.

1. **Static WEP:** In this mode, the mobile device under test is configured to encrypt traffic using the WEP (Wired Equivalent Privacy) standard, using pre-shared keys.
2. **WPA-PSK:** In this mode, the mobile device under test is configured to encrypt traffic using the WPA (Wi-Fi Protected Access that using TKIP) standard, using pre-shared keys i.e. no authentication.
3. **WPA2-PSK:** device under test is configured to encrypt traffic using the WPA2 (Wi-Fi Protected Access using AES-CCMP) standard, using pre-shared keys i.e. no authentication.
4. **Open**

Roaming test: Roaming tests were performed on this device with and across controllers. Roaming tests were also done when the device woke up on a different access point than it has last associated on the same network.

VPN tests: VPN connections were tested with L2TP and PPTP modes available on the phones terminating on the Aruba controller.

Captive Portal: The phone was made to authenticate via the captive portal in addition to PSK to gain access to the internet resources are a guest user on the Aruba WLAN network.

iTunes policy enforcement: The Aruba WLAN controller was configured to block requests to the iTunes service when on the corporate network. The multicast address and the port that subscribes to this service can be blocked using the in built L4-L7 session firewall on the WLAN controller.

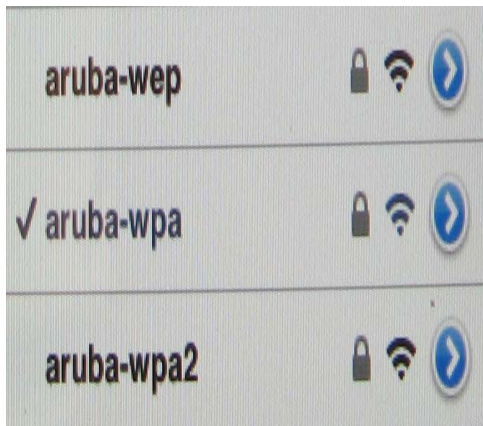
Notes

- WEP is not a recommend method of encryption due to known security weaknesses
- 802.1x is not currently supported on the iPhone.

Apple iPhone Configuration

A. Steps to associate the phone to a WLAN network.

1. Press Menu button on the phone
2. Navigate to Settings→Wi-Fi
3. All the SSIDs available will be listed in the screen.



4. If the SSID you are trying to is hidden or not shown select “Other” option.



5. Select the SSID you wish to connect.
6. If you are connecting to a open SSID you will be automatically connected.
7. If you are connecting to WEP/WPA/WPA2 then you will be prompted for the password.

B. Steps to configure the L2TP/PPTP VPN client on the iPhone

1. Press Menu button on the phone
2. Navigate to Settings→VPN→Settings
3. Select the type of VPN you want to create L2TP/PPTP
4. Type the server name
5. Type in the password



© 2007 Aruba Networks, Inc. All rights reserved. Aruba Networks and Aruba Mobile Edge Architecture are trademarks of Aruba Networks, Inc. Apple is a trademark of Apple Inc., registered in the U.S. and other countries. iPhone is a trademark of Apple Inc. All other trademarks or registered trademarks are the property of their respective holders. Specifications are subject to change without notice.

DIG_IPHON_US_070730