

Avaya Solution & Interoperability Test Lab

# Application Notes for Aruba Networks Wireless LAN System with Avaya IP Office and Avaya IP Telephones in a Converged VoIP and Data Network - Issue 1.0

#### Abstract

These Application Notes describe a solution for supporting wireless voice traffic over an Avaya IP Telephony infrastructure using the Aruba Networks Wireless LAN System consisting of multiple Controllers managing multiple Access Points. Avaya Wireless IP Telephones and a wireless laptop running Avaya PhoneManager Pro gained network access through the Aruba Access Points and registered with the Avaya IP Office. The Avaya Voice Priority Processor (AVPP) was used to support SpectraLink Voice Priority (SVP) on the Avaya Wireless IP Telephones and the Aruba Access Points. Emphasis of the testing was placed on verifying good voice quality on calls associated with the Avaya wireless IP endpoints. Information in these Application Notes has been obtained through compliance additional technical discussions. testing and Testing was conducted via the DeveloperConnection Program at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

These Application Notes describe a solution for supporting wireless voice traffic over an Avaya IP Telephony infrastructure using the Aruba Networks Wireless LAN System consisting of one controller managing multiple Access Points. The Aruba Networks Controller, Aruba 2400 and Access Points AP60, AP65 and AP70 were used for testing. The Aruba APs connect the Avaya 3616/3626 Wireless IP Phones and the Wireless Laptops running the Avaya PhoneManager Pro to connect to the Aruba WLAN infrastructure. On the wired network, these devices primarily communicate with the Avaya IP Office and the Avaya Voice Priority Protocol Server. The Avaya Voice Priority Processor (AVPP) was used to support the SpectraLink Voice Priority (SVP) Protocol on the Avaya Wireless IP Telephones and the Aruba Access Points. Emphasis of the testing was placed on verifying good voice quality on calls associated with the Avaya wireless IP endpoints.

The compliance test verified the following features supported by the Aruba Wireless LAN System:

- Layer-2 and Layer-3 Connectivity
- 802.1X Security and WEP/WPA Encryption
- Quality of Service (QoS) based on Priority Queuing and Reserved Bandwidth
- VLANs and 802.1Q Trunking
- Layer-2 and Layer-3 Seamless Roaming
- SpectraLink Voice Protocol (SVP)
- IEEE 802.11b
- Dynamic IP Addressing using DHCP

#### 1.1. Aruba 2400

The Aruba 2400 is a wireless LAN mobility controller that aggregates up to 48 controlled Access Points (APs) and delivers centralized control and security for wireless deployments. The Aruba 2400 is designed for regional headquarters or dense office deployments, the Aruba 2400 mobility controller delivers integrated mobility, security and convergence services for both wired and wireless users and can be easily deployed as an overlay without any disruption to the existing wired network.

Controller Capacity				
Controller Model	# of APs	# of User		
Aruba 2400	48	768		

#### 1.2. Aruba Access Points

The Access Points (APs) discover the Aruba controllers, configure themselves and begin operating once connected to an IP network. The Mobility Controller is responsible for downloading software images, configuring and coordinating all dependent APs. The APs

continuously scan the RF environment, supplying information to optimize radio coverage and provide wireless intrusion prevention without having to deploy a separate sensor network.

AP	Radio	Description
Model	Support	
AP 70	802.11 b/g and	Dual mode, dual radio APs with additional Ethernet
	802.11 a	port for dual homing, external and built-in antennas
		supported
AP 65	802.11 b/g and	Dual mode, dual radio AP with built-in antennas
	802.11 a	
AP 60	802.11 b/g or	Dual mode, single radio AP with detachable antennas
	802.11 a	

**Figure 1** illustrates the Wireless LAN (WLAN) configuration used to verify the Avaya/Aruba Networks solution. All of the wireless IP devices depicted in the configuration roamed between the Aruba APs for full mobility.

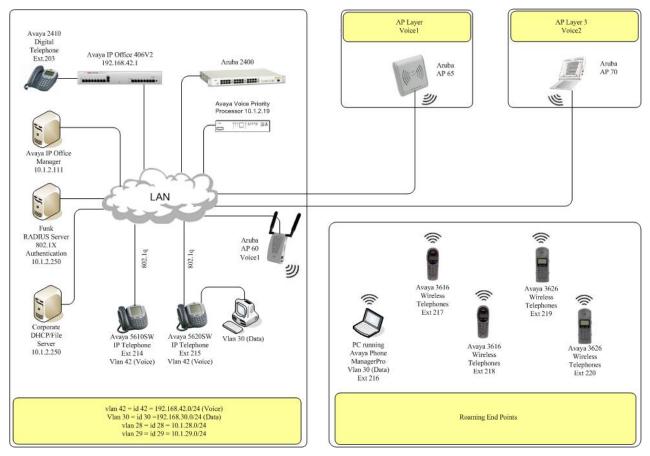


Figure 1: Avaya and Aruba Networks Wireless LAN Configuration

# 2. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment	Software
Avaya IP Office IP406V2	3.2(54)
Avaya Voice Priority Processor	33/02
Avaya 5620SW Telephones	2.3
Avaya 5610SW Telephones	3.2
Avaya 3616 wireless telephones	096.024
Avaya 3626 wireless telephones	096.024
Avaya 2410 Digital Telephone	N/A
Avaya Phone ManagerPro	2.1
Aruba 2400 Wireless LAN Switch	2.5.4.0
Aruba AP 70	2.5.4.0
Aruba AP 65	2.5.4.0
Aruba AP 60	2.5.4.0

## 3. Avaya IP Office Settings

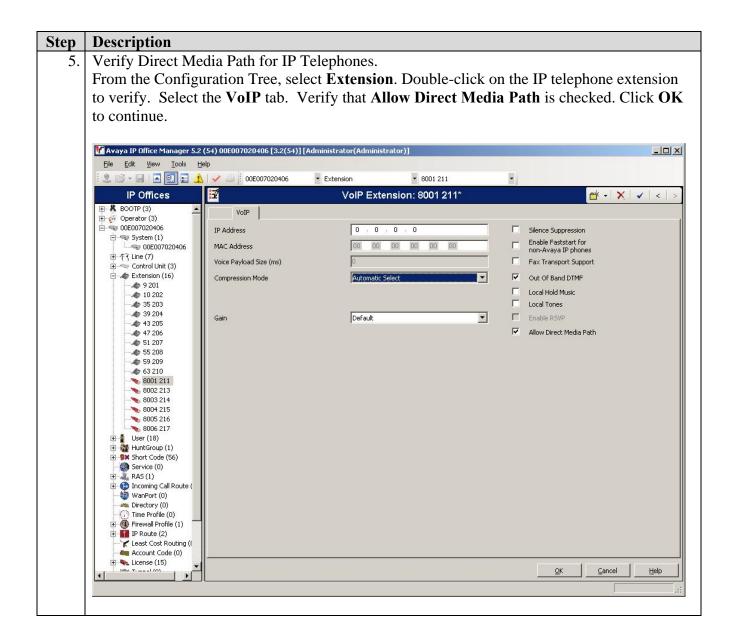
This section was included to verify that Avaya IP Office was configured correctly. Except where stated, the parameters in all steps are the default settings and are supplied for reference. For all other provisioning information such as provisioning of the trunks, call coverage, and extensions, please refer to the Avaya IP Office product documentation.

Step	Description
1.	IP Office is configured via the IP Office Manager program. Log into the IP Office Manager
	PC and select Start $\rightarrow$ Programs $\rightarrow$ IP Office $\rightarrow$ Manager to launch the Manager
	application. Log into the Manager application using the appropriate credentials.
	application. Log into the Manager application using the appropriate credentials.

Step	Description			
2.	IP Office Manager	Window.		
	The main IP Office	Manager win	dow appears. The following	ng steps refer to the Configuration
	Tree, which is in th	e left pane of	the window.	
		1		
	🎦 Avaya IP Office Manager 5.2 (	54) 00E007020406 [3.2(54)]	] [Administrator(Administrator)]	
	Eile Edit View Tools Hel			
	Contraction of the second s	00E007020406	User RemoteManager	
	IP Offices		RemoteManager:	
	Operator (3)     O0E007020406			ial In   Voice Recording   Button Programming   Menu Programmin( 💶 🕨
	System (1)	Name Password	RemoteManager	x
	⊞†ित् Line (7)	Confirm Password	****	
	Extension (16)	Full Name		
		Extension		
	Short Code (56)     Service (0)	Locale		
	E → RAS (1) E → D Incoming Call Route (8)	Priority	5	
			Ex Directory	
	- A Directory (0) - (j) Time Profile (0)	Device Type	Device Type Unknown	
	⊕	User Rights		
		User Rights view	User data	<b>•</b>
		Working hours time profile	<none></none>	<u></u>
		Working hours User Rights	Ĺ	
	Auto Attendant (0)	Out of hours User Rights		<u>×</u>
	⊞- <b>∦≭</b> E911 System (1)			
		<u>•</u>		
	4			<u>OK</u> <u>Cancel</u> <u>H</u> elp

<ul> <li>3. Verify H323 Gatekeeper information. The Avaya IP Telephones will get Differentiated Servic Office. This information will be utilized for QoS by the window, go to the Configuration Tree and double-click tab. Verify that the DiffServ Settings for DSCP and SIG respectively.</li> <li></li></ul>	Proxim MP.11. In the Manager System. Select the H323 Gatekeeper DSCP are set to 46 and 46,
Office. This information will be utilized for QoS by the window, go to the Configuration Tree and double-click tab. Verify that the <b>DiffServ Settings</b> for <b>DSCP</b> and <b>SIG</b> respectively.	Proxim MP.11. In the Manager System. Select the H323 Gatekeeper DSCP are set to 46 and 46,
window, go to the Configuration Tree and double-click tab. Verify that the DiffServ Settings for DSCP and SIG respectively.	System. Select the H323 Gatekeeper DSCP are set to 46 and 46,
tab. Verify that the DiffServ Settings for DSCP and SIG respectively.	DSCP are set to 46 and 46,
respectively.         IP Office Manager 5.2 (54) 00E007020406 [3.2(54)] [Administrator/Administrator)]         IP Office Manager 5.2 (54) 00E007020406 [3.2(54)] [Administrator/Administrator)]         IP Offices         ODE007020406         System I alvi 100         ODE007020406         System I alvi 0.1         ODE007020406         System I alvi 0.1         ODE007020406      <	)20406 ▼ ▲ → × ↓ ✓ ↓ >
Image: Service (0)         I	120406 ▼
Ele       Edit       Yew       Iools       Help         IP Offices       00E007020406       System       00E007020406         IP Offices       00E007020406       System       Itelephony       1323 Gatekeeper       LDAP       System       10AP         IP Offices       00E007020406       System       Itelephony       1323 Gatekeeper       LDAP       System       10AP       System       Itelephony       1323 Gatekeeper       LDAP       System       Itelephony       Itele	120406 ▼
Ele       Edit       Yew       Jools       Help         IP Offices       00E007020406       System       00E007020406         IP Offices       00E007020406       System       ODE007020406         IP Offices       System       Itelephony       H323 Gatekeeper       LDAP       System         IP Offices       ODE007020406       System       Telephony       H323 Gatekeeper       LDAP       System       Itelephony       H323 Gatekeeper       Itelephony       H323 Gatekeeper       Itelephony       H323 Gatekeeper       Itelephony       H323 Gatekeeper	120406 ▼
IP Offices       ODE007020406       System       ODE007020406         IP Operator (3)       ODE007020406       System (1)       Image: Control Unit (3)       System (1)         Image: Control Unit (3)         Image: Control Unit (3)       Image: Control Unit (3)       Image: Control Unit (3)       Image: Control Unit (3)       Image: Control Unit (3)         Image: Control Unit (3)       Image: Control Unit (3)       Image: Control Unit (3)       Image: Control Unit (3)       Image: Control Unit (3)         Image: Control Unit (3)       Image: Control Unit (3)       Image: Control Unit (3)       Image: Control Unit (3)       Image: Control Unit (3)         Image: Control Unit (3)       Image: Co	iii -   ×   ✓   <   >
IP Offices       OOE007020406         ●       © Operator (3)       System LANI DNS Voicemail Telephony H323 Gatekeeper LDAP (1)         ●       © 00E007020406       ●         ●       © 00E007020406       ●         ●       © 00E007020406       ●         ●       © 01007020406       ●         ●       © 01007020406       ●         ●       © 02007020406       ●         ●       © 02007020406       ●         ●       © 02007020406       ●         ●       © 02007020406       ●         ●       © 02007020406       ●         ●       © 02007020406       ●         ●       © 02007020406       ●         ●       © 02007020406       ●         ●       ●       ●         ●       ●       ●         ●       ●       ●         ●       ●       ●         ●       ●       ●	
Image: System (1)       System (1)         Image: System (1)       Image: System (1)	ystem Alarms   Twinning   CDR
← account Code (0)	
	OK Cancel Help

Step	Description				
4.	Disable DHCP se				
	Select the LAN1	tab. Set the <b>I</b>	<b>DHCP Mode</b> to <b>D</b>	isabled. Click O	<b>DK</b> to continue.
			4)] [Administrator(Administrato	)]	
	Eile Edit View Iools He		▼ System	▼ 00E007020406 •	
	IP Offices		00E007	020406	<u> </u>
		IP Address IP Mask RIP Mode Number Of DHCP IP	Voicemail Telephony H323 Gatekee 192 · 168 · 42 · 1 255 · 255 · 255 · 0 None	eer   LDAP   System Alarms   Twinnin	ng CDR
	HuntGroup (1)     Sorvice (0)     Service (0)     Marconing Call Route (8)     WanPort (0)     Directory (0)     Time Profile (0)     Firewall Profile (1)     Firewall Profile (1)     Sorvice (2)     Least Cost Routing (0)     Least Routing (0)     Leas	Addresses DHCP Mode C Server	C Client	C Dialin	C Disabled
	×   )				QK Gancel Heip
					.:



# 4. Configure the Avaya Voice Priority Processor

The Avaya Voice Priority Processor (AVPP) utilizes SpectraLink Voice Priority (SVP) as the Quality of Service (QoS) mechanism supported by the Avaya 3616/3626 Wireless IP Telephones and the Aruba Access Point 100 to reduce jitter and delay for voice traffic over the wireless network.

The AVPP performs three major functions. First, it is a required component to utilize the 11Mbps maximum transmission speed available in the Avaya Wireless Telephones that support 802.11b. Secondly, SVP allows the Aruba Access Points and the Avaya Wireless IP Telephones to transmit their voice packets immediately, while other devices must wait a random backoff

TMA; Reviewed: SPOC 6/20/2007

Solution & Interoperability Test Lab Application Notes ©2007 Avaya Inc. All Rights Reserved. period as required by the 802.11 standard. This reduces delay for the voice packets. Lastly, the AVPP is required to serve as a "gateway" between the Avaya Wireless IP Telephones and the Avaya IP Telephony infrastructure. Since the wireless telephones support SVP, their packets are directed to the AVPP so that the SVP header information can be removed before the packets are forwarded to Avaya Communication Manager.

To configure the AVPP, connect a PC or laptop to the serial port of the AVPP. Run a terminal emulation program with the following configuration:

- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow Control: None

Once connected, the AVPP login screen is presented. Log in with the appropriate credentials. The **AVPP System Menu** is displayed as shown in **Figure 2**. After configuring an IP address to the AVPP, a Telnet session may be used to modify the AVPP configuration.

Hostna	NetLink SVP-I me: [slnk-000006],	-	10.1.2	.230		
	System Status SVP-II Configurati Network Configurat Change Password Exit					
Enter=Select	ESC=Exit	Use Arrow	Keys	to Move	Cursor	

Figure 2: AVPP System Menu

From the **AVPP System Menu**, select **Network Configuration** to configure the IP address, Subnet Mask, and Default Gateway of the AVPP.

		onfiguration						
Hostname	: [slnk-00000	06], Address:	: 10.1.	.2.19				
Ethernet Address (fix IP Address: Hostname: Subnet Mask: Default Gateway: SVP-II TFTP Download Primary DNS Server: Secondary DNS Server: DNS Domain: WINS Server: Workgroup: Syslog Server: Maintenance Lock:	ed): 00 10 sln 25 10 Master: NOI NOI NOI NOI	:90:7A:00:00: .1.2.230 ak-000006 5.255.255.0 .1.2.1 VE VE VE VE VE RE RE						
Enter=Change E	sc=Exit	Use	Arrow	Keys	to	Move	Cursor	

**Figure 3: Network Configuration** 

From the AVPP System Menu, select SVPP-II Configuration to configure the Phones per Access Point and the 802.11 Rate fields. In this configuration, the 802.11 Rate of the AVPP was configured to *Automatic*, as shown Figure 4, to allow the wireless telephones to determine its rate (up to 11Mbps), as opposed to the AVPP limiting the transmission rate of the wireless telephones to 1/2 Mbps. The Call Admission Control Feature on the Aruba Controller can be used to limit the number of calls per AP in a graceful manner. When using Call Admission Control, ensure that the setting the SVP server for the Phone per Access Point mirrors the settings on the controller or is greater than the value set on the controller. This allows the Aruba controller to effectively manage the maximum number of calls per AP

	SVP-II	[ Configuration
Hostn	ame: [slnk-0	000006], Address: 10.1.2.19
Phones per Access	Point:	10
802.11 Rate:		Automatic
SVP-II Master:		10.1.2.19
SVP-II Mode:		Netlink IP
Ethernet link:		100mbps/full duplex
System Locked:		N
Maintenance Lock:		N
Reset System		
Enter=Change	Esc=Exit	Use Arrow Keys to Move Cursor

**Figure 4: SVP-II Configuration** 

# 5. Configure the Aruba Controller and Access Points

This section covers the configuration of the Aruba Controller and Access Points. The switch configuration can be done using either a web-based interface or a command line interface (CLI). The following sections display the configuration using CLI. For web-based configuration, refer to the Aruba 2400 switch configuration guide (See Section 10).

The following section details the steps required to configure the controller to support voice on the WLAN. This section is broadly divided into 5 sub-sections based on the feature configured:

- Initialization
- L2/L3 settings
- WiFi Settings
- Session ACLs and QoS
- Authentication

#### 5.1. Aruba Solution Basics

#### **User Roles**

The Aruba Solution is role based. A user role defines the user's network privileges. A group of user's with similar access privileges will be assigned the same role. Session aware firewall policies assigned to the user roles define the network access rights. The right roles are assigned to the users on successful authentication. The authentication mechanisms in use can also influence the choice of roles assigned.

#### 5.2. Connecting to the Aruba Mobility Controller

- 1. Using a standard RS-232 cable, connect the Mobility Controller Switch to the serial port of a terminal or PC.
- 2. Run a terminal emulation program (such as HyperTerminal) or use a VT-100 terminal with the following configuration:

Bits per second: **9600** Data bits: **8** Parity: **None** Stop bits: **1** Flow control: **None** 

- 3. Log in with the appropriate credentials.
- 4. By default, only ssh access to the controller is permitted. From a management system that has network connectivity to the controller ssh to the switch.

#### ssh admin@<switch IP address>

Enter the admin password at the password prompt. Type **enable** at the ">" prompt to enter the enable mode. Type the enable password when prompted for a password.

**Note:** Configuration commands on the CLI can be issued only in the configuration mode on the controller. To enter the configuration mode, the following steps need to be executed.

(aruba) > ← exec mode (aruba) > enable (password): <enable password> (aruba) # ← enable mode (aruba) # configure terminal (aruba)(config) # ← config mode

### 5.3. Initialization

Before starting, please ensure that the Policy Enforcement Firewall module license is enabled on the Aruba controller. Please contact Aruba Networks for licenses and installation information. Refer to **Section 8**.

Step	Description: Initial startup of Aruba Controller
1.	On initial startup, the user is presented with a wizard.
1.	Enter System name [Aruba2400]: <b>Aruba</b> Enter VLAN 1 interface IP address [172.16.0.254]: Enter VLAN 1 interface subnet mask [255.255.255.0]: Enter IP Default gateway [none]: Enter Switch Role, (master local) [master]: <b>master</b> Enter Country code (ISO-3166), <ctrl-i> for supported list: <b>US</b> You have chosen Country code US for United States (yes no)?: yes Enter Password for admin login (up to 32 chars): xxxxx Re-type Password for admin login: xxxxx Enter Password for enable mode (up to 15 chars): enable Re-type Password for enable mode: enable Do you wish to shutdown all the ports (yes no)? [no]: no</ctrl-i>
	Current choices are:
	System name: aruba
	VLAN 1 interface IP address: 172.16.0.254
	VLAN 1 interface subnet mask: 255.255.255.0
	IP Default gateway: none

Switch Role: master
Country code: US
Ports shutdown: no

Confirm the choices. The system now reboots and the user is presented with the logon prompt.

### 5.4. Aruba 2400 Controller Configuration Steps

Step	Description: Login into controller
1.	Configure the L2 / L3 network settings via the CLI.
	The voice over WiFi solution using the Avaya IP Office requires the handsets and the call server to belong to the same broadcast domain. A general guideline for such deployments is to place the voice devices and the call server in the same broadcast domain, a subnet dedicated for voice. The data users are assigned to the non-voice VLANs. Connect to the Aruba 2400 Controller. Log in using the appropriate Login ID and
	Password.
	Login: Password: (aruba) >

Step	Description: Configure Vlans and Interfaces
2.	(aruba) >
	(aruba) > <b>enable</b> Password:*****
	(aruba) # <b>configure terminal</b>
	(aruba) (config) #
	(aruba) (config) <b>#interface loopback</b>
	(aruba) (config-loop)#ip address 10.1.29.1
	(aruba) (config-loop)#!
	• Reboot the Aruba 2400 controller as requested.
	$(\operatorname{aruba})(\operatorname{config}) # \operatorname{vlan} 29 \leftarrow \operatorname{uplink}$ subnet and data user subnet
	(aruba) (config) <b>#interface vlan 29</b>
	(aruba) (config-subif)# <b>ip address 10.1.29.2 255.255.255.0</b> (aruba)(config-subif)# !
	(aruba)(comrg-subir)#:

(aruba) (config) #ip default-gateway 10.1.29.254
(aruba)(config)# vlan 42 ← voice vlan (aruba) (config) #interface vlan 42 (aruba) (config-subif)# ip address 192.168.42.15 255.255.255.0
(aruba)(config-subif)# !
(aruba)(config)# vlan 30 ← data vlan (aruba) (config) #interface vlan 30 (aruba) (config-subif)# ip address 192.168.30.15 255.255.255.0
(aruba)(config-subif)# <b>!</b>
(aruba)(config)# vlan 28 ← subnet for local APs (aruba) (config) #interface vlan 28 (aruba) (config-subif)# ip address 10.1.28.2 255.255.255.0 (aruba)(config-subif)# !
<ul> <li>Configure trunk port ← uplink trunk interface to the LAN         <ul> <li>(aruba) (config) #interface fastethernet 1/0</li> <li>(aruba) (config-if)#trusted</li> <li>(aruba) (config-if)#no shutdown</li> <li>(aruba) (config-if)#switchport mode trunk</li> <li>(aruba) (config-if)#switchport trunk allowed vlan 29,28,42</li> </ul> </li> </ul>

Step	Description: Configure Radius Server
3.	(aruba) (config) #aaa radius-server rad1 host 10.1.2.250 key testtesttest

## 5.5. Connecting Aruba APs

Before installing the Aruba APs in a network environment, ensure that the APs will be able to locate and connect to the Mobility Controller when powered on. Specifically, ensure the following:

- When connected to the network, each AP is assigned a valid IP address
- APs are able to locate the Mobility Controller "(L2/L3 connectivity)"

Each Aruba AP requires a unique IP address on a subnet work that has connectivity to a Mobility Controller. The Aruba APs can communicate with the controller over a L2 or L3 network. Aruba recommends using the Dynamic Host Configuration Protocol (DHCP) to provide IP addresses for APs. For compliance testing the DHCP server function on the Aruba controller

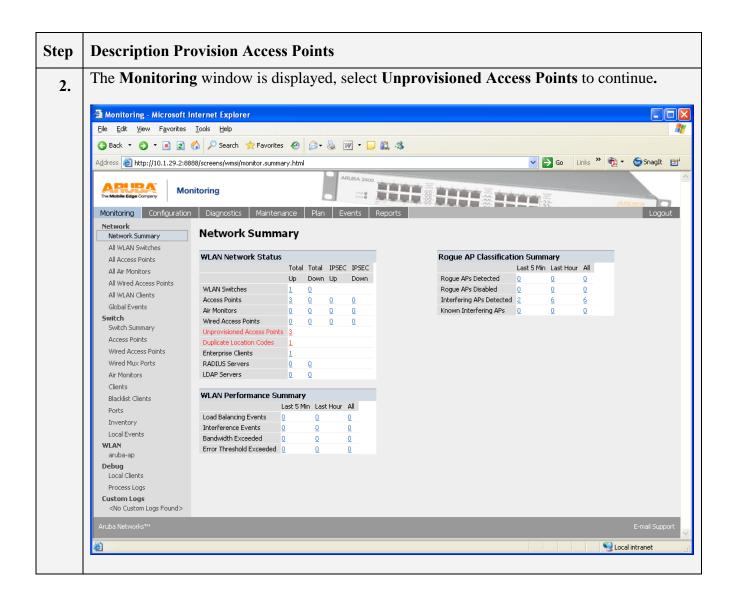
TMA; Reviewed:	Solution & Interoperability Test Lab Application Notes	14 of 30
SPOC 6/20/2007	©2007 Avaya Inc. All Rights Reserved.	Aruba-IPO-APP

was not used and instead a centralized corporate DHCP server was put in place. To better manage the different traffic types at each site, the voice and data traffic were separated onto different VLANs.

Note: DHCP Scope Options 43 and 60 need to be configured for DHCP to work correctly. Refer to the Configuring DHCP with Vendor-Specific Options Section in the ArubaOS User Guide (0510249-02)

Step	Description	
1.	Log into the Aruba 2400 Controller using the appropriate credentials.	
	Local intranet	

#### 5.5.1. Aruba 2400 Controller Configuration Steps

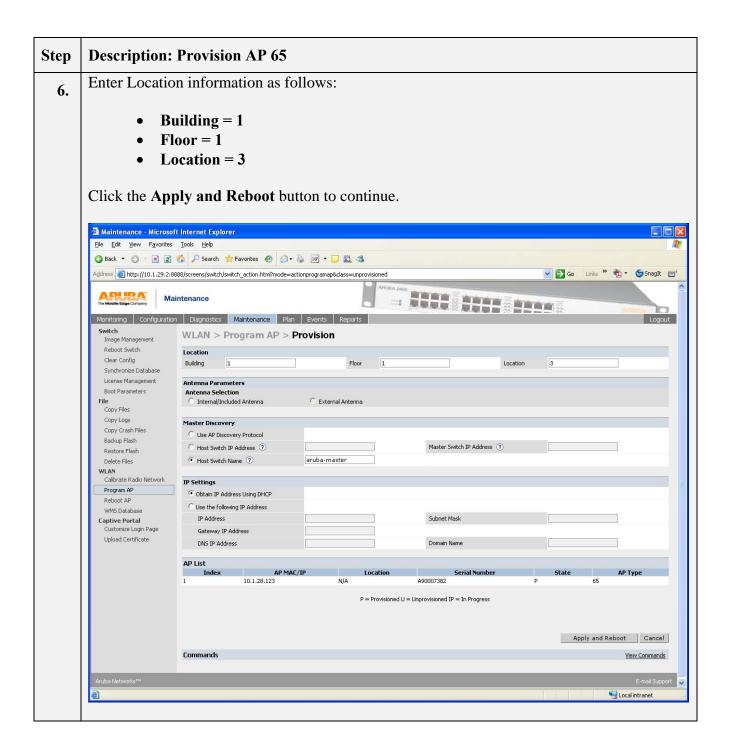


The Maintenance  $\rightarrow$  WLAN  $\rightarrow$  Program AP window appears. Select each AP and configure them.

Switch Image Management Reboot Switch         WLAN > Program AP           Search         Search	Back	4	🖹 Maintenance - Microsoft	Intern	et Explorer					
Address @ http://10.1.2.9.2:8888/srceens/switch/switch_action.html?mode=actionprogramap&dass=upprovisioned       Image Configuration       Diagnostics       Maintenance       Plan       Events       Reports       Americana         Monitoring       Configuration       Diagnostics       Maintenance       Plan       Events       Reports       Image Management         Reboot Switch       Image Management       Boot Parameters       Image Management       Search       Sear	Address in http://10.1.29.2:8888/screens/switch/switch_action.html*mode=actionprogramap8dass=unprovisioned in the information of the information o									
Maintenance       Plan       Events       Reports       American         Monitoring       Configuration       Diagnostics       Maintenance       Plan       Events       Reports       Lice         Switch       Image Management       Reboot Switch       Search	Maintenance       Maintenance       Plan       Events       Reports         Switch       Tage Management       Reports       Multiclassic       AP Secial Number *       Status         Switch       Clear Config       Synchronize Database       Location       AP IP *       AP Mac Address *       AP Secial Number *       Status         Synchronize Database       Location       AP IP *       AP Type *       AP MAC Address *       AP Secial Number *       Status         Synchronize Database       Location       AP IP *       AP Type *       AP MAC Address *       AP Secial Number *       Status         Synchronize Database       Location       AP IP *       AP Outbusic:2:0a:2:0       A30068156       up         Boot Parameters       Not set       10.1:28.1:22       70       00:0b::66::59:98       A50076308       up         File       Not set       10.1:28.1:23       65       00:0b::66::00::81:4       A90007382       up         Copy Crash Files       Backup Filesh       Restore Files       MULN       Calbrate Radio Network       Program AP       Reboot AP         WLN       Calbrate Radio Network       Program AP       Reboot AP       Status       Provision         VLN       Calbrate Radio Network       Coptive Portal <th></th> <th>🄇 Back 🔻 🐑 🝸 😰 (</th> <th>6</th> <th>Search 👷 Favorite</th> <th>es 🙆 🔗 🎍</th> <th>w • 🖵 🛍 🎕</th> <th></th> <th></th> <th></th>		🄇 Back 🔻 🐑 🝸 😰 (	6	Search 👷 Favorite	es 🙆 🔗 🎍	w • 🖵 🛍 🎕			
Maintenace     Monitoring Configuration Diagnostics Maintenance Plan Events Reports     Switch   Image Management:   Reboot Switch   Clear Config   Synchronize Dababase   License Management:   Boot Parameters   File   Copy Files   Copy Crash Files   Bachup Filash   Delete Files   WLAN   Reboot AP   WILAN   Castomice Login Page	Maintenance Plan Events Reports     Monitoring Configuration Diagnostics Maintenance Plan Events Reports     Switch   Switch   Raboot Switch   Clear Config   Synchronice Database   License Management   Boot Parameters   Copy Files   Copy Crash Files   Backup Flash   Delete Files   WLM   Calbrate Radio Network   Program AP   Reboot AP   WLM   Cabre Potal		Address 🗿 http://10.1.29.2:88	38/scree	ns/switch/switch_actio	on.html?mode=action	programap&class=unp	rovisioned	Go Links 🌺	🔁 🔹 🌀 Snagl
Image Management.       Search       Search       Search       Status         Clear Config       Synchronize Database       Image Management       AP Type ^       AP MAC Address ^       AP Serial Number ^       Status         Boot Parameters       Not set       10.1.28.121       61       00:0b:86:c2:0a:20       A30068156       up         Copy Files       Not set       10.1.28.122       70       00:0b:86:c2:0a:20       A30069156       up         Copy Files       Not set       10.1.28.123       65       00:0b:86:c2:0a:20       A30007382       up         Copy Files       Not set       10.1.28.123       65       00:0b:86:c2:0a:20       A90007382       up         Copy Files       Not set       10.1.28.123       65       00:0b:86:c2:0a:20       A90007382       up         Copy Crash Files       Backup Flash       Not set       10.1.28.123       65       00:0b:86:c2:0a:20       A90007382       up         WLN       Calibrate Radio Network       Program AP       Reboot AP       WMS Database       Search       Search       Search         Gaptive Portal       Customize Login Page       Customize Login Page       Search       Search       Search       Search	Image Management       Search         Synchronize Database       I       Location ^       AP IP ^       AP MAC Address ^       AP Serial Number ^       Statu         Synchronize Database       I       Location ^       AP IP ^       AP MAC Address ^       AP Serial Number ^       Statu         Boot Parameters       I       Not set       10.1.28.121       61       00:0b:86:c2:0a:20       A30068156       up         Boot Parameters       I       Not set       10.1.28.122       70       00:0b:86:c0:c8:e4       A9007382       up         Copy Files       I       Not set       10.1.28.123       65       00:0b:86:c0:c8:e4       A9007382       up         Copy Logs       I       I -3 of 3 10 ▼       I       I       I -3 of 3 10 ▼       IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII		Monitoring Configuration	Diag	gnostics Mainter					Anuces
Clear Config       Synchronize Database         License Management       Not set       10.1.28.121       61       00:0b:66:c2:0a:20       A30068156       up         Boot Parameters       Image: Copy Class       Image: Copy Class <th>Synchronize Database         Location         Are regiment         Are regiment         Are regiment         Are second and an adverted and advected andvected and advected and advected and advected and advected</th> <th></th> <th></th> <th></th> <th>-</th> <th>IM AP</th> <th></th> <th></th> <th></th> <th>Sea</th>	Synchronize Database         Location         Are regiment         Are regiment         Are regiment         Are second and an adverted and advected andvected and advected and advected and advected and advected				-	IM AP				Sea
License Management Boot Parameters         Mot set         10.1.28.121         61         0000:06:62:20:020         A30068156         up           Boot Parameters         Not set         10.1.28.122         70         00:0b:66:55:6:98         A50076308         up           File         Not set         10.1.28.122         70         00:0b:66:C5:6:98         A50076308         up           Copy Files         Not set         10.1.28.123         65         00:0b:86:C0:c8:64         A90007382         up           Copy Crash Files         Copy Crash Files         E	V         Not set         10.1.28.121         61         0000636:22:03:20         A30068156         up           Boot Parameters         Not set         10.1.28.122         70         00:0b:86:c5:56:98         A50076308         up           File         Not set         10.1.28.123         65         00:0b:86:c5:56:98         A50076308         up           Copy Files         Not set         10.1.28.123         65         00:0b:86:c0:c8:e4         A9007382         up           Copy Logs         Copy Crash Files         Provision         P		-	Г	Location	AP IP 🔺	AP Type 🔺	AP MAC Address 🔷	AP Serial Number 🔺	Status 🕈
Boot Parameters         Not set         10.1.28.122         70         00.0b:86:c5:6:98         A50076308         up           File         Not set         10.1.28.123         65         00.0b:86:c0:68:e4         A90007382         up           Copy Class         Copy Class         I   1-3 of 3         I @         I         I @         I	Boot Parameters         Not set         10.1.28.122         70         00:0b:66:c5:56:98         A50076308         up           File         Not set         10.1.28.123         65         00:0b:66:c0:c8:e4         A90007382         up           Copy Files         Copy Crash Files         Provision         Provision         Provision         Provision           WLAN         Calbrate Radio Network         Program AP         Reboot AP         WMS Database         L <thl< th=""> <thl< th="">         L         L</thl<></thl<>			$\overline{\mathbf{v}}$	Not set	10.1.28.121	61	00:0b:86:c2:0a:20	A30068156	up
File       Not set       10.1.28.123 65       00:0b:66:c0:c8:e4       A90007382       up         Copy Logs       I   I-3 of 3 10 v       IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	File   Copy Files   Copy Cash Files   Backup Flash   Delete Files   WLAN   Calbrate Radio Network   Program AP   Reboot AP   WMS Database   Captive Portal		-		Not set	10.1.28.122	70	00:0b:86:c5:5e:98	A50076308	up
Copy Logs Copy Crash Files Backup Flash Restore Flash Delete Files WLAN Calibrate Radio Network Program AP Reboot AP WMS Database Captive Portal Customize Login Page	Copy Logs Copy Crash Files Backup Flash Restore Flash Delete Files WLAN Calibrate Radio Network Program AP Reboot AP WMS Database Captive Portal		File		Not set	10.1.28.123	65	00:0b:86:c0:c8:e4	A90007382	up
Copy Crash Files       Provision         Badup Flash       Provision         Restore Flash       Delete Files         WLAN       Calibrate Radio Network         Program AP       Reboot AP         WMS Database       Captive Portal         Customize Login Page       Customize Login Page	Copy Crash Files       Provision         Backup Flash       Provision         Restore Flash       Delete Files         WLAN       Calibrate Radio Network         Program AP       Reboot AP         Reboot AP       WMS Database         Captive Portal       Eaptive Portal							1   1-3 of 3 10 🔽		
Backup Flash Restore Flash Delete Files WLAN Calibrate Radio Network Program AP Reboot AP WMS Database Captive Portal Customize Login Page	Backup Flash     Provision       Restore Flash     Delete Files       WLAN     Calibrate Radio Network       Program AP       Reboot AP       WMS Database       Captive Portal									
Restore Flash         Delete Files         WLAN         Calibrate Radio Network         Program AP         Reboot AP         WMS Database         Captive Portal         Customize Login Page	Restore Flash Delete Files WLAN Calibrate Radio Network Program AP Reboot AP WMS Database Captive Portal							Provision		
WLAN         Calibrate Radio Network         Program AP         Reboot AP         WMS Database         Captive Portal         Customize Login Page	WLAN         Calibrate Radio Network         Program AP         Reboot AP         WMS Database         Captive Portal									
Calibrate Radio Network Program AP Reboot AP WMS Database Captive Portal Customize Login Page	Calibrate Radio Network  Program AP  Reboot AP  WMS Database  Captive Portal		Delete Files							
Program AP Reboot AP WMS Database Captive Portal Customize Login Page	Program AP Reboot AP WMS Database Captive Portal		WLAN							
Reboot AP WMS Database Captive Portal Customize Login Page	Reboot AP WMS Database Captive Portal									
WMS Database Captive Portal Customize Login Page	WMS Database Captive Portal		Calibrate Radio Network							
Captive Portal Customize Login Page	Captive Portal		Calibrate Radio Network Program AP							
	Customize Login Page		Calibrate Radio Network Program AP Reboot AP							
Upload Certificate			Calibrate Radio Network Program AP Reboot AP WMS Database							
	Upload Certificate		Calibrate Radio Network Program AP Reboot AP WMS Database Captive Portal Customize Login Page							

р	Description:	Provision AP 61				
۱.	Enter Location	n information as fo	ollows:			
	• Flo • Lo	nilding = 1 por = 1 pocation = 1 poly and Reboot but	utton to continue			
	Maintenance - Microso		ation to continue.			
	Eile Edit View Favorites					
		🏠 🔎 Search 👷 Favorites  👔				
	Address 🙆 http://10.1.29.2:8	8888/screens/switch/switch_action.html?moc			Go Links	» 📆 ▾ 🌀 SnagIt 📷
	The Mobile Edge Company	aintenance	ARUBA 2400			
	Image Management Reboot Switch Clear Config Synchronize Database License Management Boot Parameters File Copy Files	Location Building 1 Antenna Parameters Antenna Selection C Internal/Included Antenna	Floor 1	Location	1	
	Copy Logs Copy Crash Files	Master Discovery				
	Backup Flash	Use AP Discovery Protocol     Host Switch IP Address ⑦		Master Switch IP Address 🥥		
	Restore Flash Delete Files WLAN	Host Switch Name	aruba-master	Marcel Switch & Modess ()	L	
	Calibrate Radio Network	IP Settings				
	Program AP	Obtain IP Address Using DHCP				
	Reboot AP WMS Database	C Use the following IP Address				
	Captive Portal	IP Address		Subnet Mask		
	Customize Login Page Upload Certificate	Gateway IP Address				
		DNS IP Address		Domain Name	-	
		AP List Index AP M	AC/IP Location	Serial Number	State	AP Type
		1 10.1.28.121	N/A	A30068156	P 61	
			P = Provisioned I	J = Unprovisioned IP = In Progress		
					Apply and	Reboot Cancel
		Commands				View Commands

р	<b>Description:</b>	Provision AP 70		
•	Enter Locatio	on information as follows:		
	<ul> <li>F</li> <li>L</li> <li>A</li> </ul>	uilding = 1 loor = 1 ocation = 2 ntenna Parameters i. 5 GHz Antenna Gain (d ii. 2 GHz Antenna Gain (d ply and Reboot button to conti	Bi) = 20	
	Maintenance - Microso	Iools <u>H</u> elp		
		🏠 🔎 Search 🚖 Favorites 🤣 🎯 + 🌺 📝 + 📮 🏭 🦄		🗸 🏹 Go 🛛 Links 🎽 🖓 🔹 🌍 SnagIt
		8888/screens/switch/switch_action.html?mode=actionprogramap&class=unprov	APUBA 2400	
	Monitoring Configuratio	n Diagnostics Maintenance Plan Events Reports		Alluse Logout
	Image Management Reboot Switch Clear Config Synchronize Database License Management Boot Parameters File	Location Building 1 Floor Antenna Parameters Antenna Selection	5 GHz Antenna Gain (dBi) 20 5 Ghz Antenna	2 2 GHz Antenna Gain (dbi) 20
	Copy Files Copy Logs Copy Crash Files Backup Flash	C Internal/Included Antenna C External Antenna	<ul> <li>Automatic (recommended)</li> <li>2 Ghz Antenna</li> <li>Automatic (recommended)</li> </ul>	C Antenna 1 C Antenna 2
	Copy Logs Copy Crash Files		2 Ghz Antenna	
	Copy Logs Copy Crash Files Backup Flash Restore Flash Delete Files <b>WLAN</b> Calibrate Radio Network <b>Program AP</b>	Internal/Included Antenna     External Antenna  Master Discovery     Use AP Discovery Protocol     Host Switch IP Address     Host Switch Name ⑦     aruba-master  IP Settings     Obtain IP Address Using DHCP     Use the following IP Address     IP Address     Gateway IP Address	2 Ghz Antenna <sup>(*</sup> Automatic (recommended)	
	Copy Logs Copy Crash Files Backup Flash Nestore Flash Delete Files <b>WLAN</b> Calibrate Radio Network <b>Program AP</b> Reboot AP WMS Database <b>Captive Portal</b> Customize Login Page	Internal/Included Antenna     External Antenna  Master Discovery     Use AP Discovery Protocol     Host Switch IP Address ⑦     aruba-master  IP Settings     Obtain IP Address Using DHCP     Use the following IP Address     IP Address     IP Address     DNS IP Address     DNS IP Address  AP List Index     AP MAC/IP     Lo	2 Ghz Antenna  Automatic (recommended)  Master Switch IP Address ()  Subnet Mask  Domain Name  Cation Serial Number	C Antenna 1 C Antenna 2
	Copy Logs Copy Crash Files Backup Flash Nestore Flash Delete Files <b>WLAN</b> Calibrate Radio Network <b>Program AP</b> Reboot AP WMS Database <b>Captive Portal</b> Customize Login Page	Internal/Included Antenna     External Antenna  Master Discovery     Use AP Discovery Protocol     Host Switch IP Address     Obtain IP Address     Use the following IP Address     IP Address     JP Address     DNS IP Address     DNS IP Address     DNS IP Address     DNS IP Address     Index AP MAC/IP     Lot     IOL.28.122     N/A	2 Ghz Antenna Automatic (recommended) Master Switch IP Address () Subnet Mask Domain Name	C Antenna 1 C Antenna 2
	Copy Logs Copy Crash Files Backup Flash Nestore Flash Delete Files <b>WLAN</b> Calibrate Radio Network <b>Program AP</b> Reboot AP WMS Database <b>Captive Portal</b> Customize Login Page	Internal/Included Antenna     External Antenna  Master Discovery     Use AP Discovery Protocol     Host Switch IP Address     Obtain IP Address     Use the following IP Address     IP Address     JP Address     DNS IP Address     DNS IP Address     DNS IP Address     DNS IP Address     Index AP MAC/IP     Lot     IOL.28.122     N/A	2 Ghz Antenna Automatic (recommended) Master Switch IP Address () Subnet Mask Domain Name Section Serial Number A50076308	C Antenna 1 C Antenna 2



Monitoring       Outloging       Name       Nam       Name       Name<	Back     Image: Back <th>Back   Image: Back  <th>Back</th><th>Course are been been been been been been been be</th></th>	Back   Image: Back     Image: Back <th>Back</th> <th>Course are been been been been been been been be</th>	Back	Course are been been been been been been been be
Matterial procession       Matterial procession <th< th=""><th>Image: The problem in the problem i</th><th>Image: With the state of t</th><th>Address       Ettp://10.1.29.2:8888/screens/wmsi/monitor.summary.html         Monitoring       Monitoring         Monitoring       Network         Metwork       Network         Network       Network         All Access Points       Valued Access Points         All WLAN Clients       Up       Down       Up       Down         All WLAN Clients       1       0         Switch       3.0       0       0         Switch       Switch       0       0       0         Switch       Supplicate Location Codes       0       0       0</th><th>Rogue AP Classification Summary Last 5 Min Last Hour All Rogue APs Detected 0 0 0 Rogue APs Detected 0 0 0 Interfering APs Detected 0 1 0</th></th<>	Image: The problem in the problem i	Image: With the state of t	Address       Ettp://10.1.29.2:8888/screens/wmsi/monitor.summary.html         Monitoring       Monitoring         Monitoring       Network         Metwork       Network         Network       Network         All Access Points       Valued Access Points         All WLAN Clients       Up       Down       Up       Down         All WLAN Clients       1       0         Switch       3.0       0       0         Switch       Switch       0       0       0         Switch       Supplicate Location Codes       0       0       0	Rogue AP Classification Summary Last 5 Min Last Hour All Rogue APs Detected 0 0 0 Rogue APs Detected 0 0 0 Interfering APs Detected 0 1 0
Variation	Monitoring       Configuration       Diagnostics       Maintenance       Real       Vector       Configuration       Diagnostics       Maintenance       Real       Vector         Network       Summary       Al Weak Swetches       Al Access Points       Al Weak Access Points       Al Q Q Q Q       Q       Al Weak Access Points       Al Q Q Q Q       Q       Al Weak Access Points       Al Weak Access Points       Q	Nonitoring       Monitoring       Monitoring       Monitoring       Monitoring       Monitoring       Manitability       Manitabilit	Monitoring         Monitoring           Monitoring         Configuration         Diagnostics         Maintenance         Plan         Events         Report           Network         Network         Network         Network         Network         Network         Network           All WLAN Switches         All Access Points         Network Status         VLAN Network Status         Network           All Wired Access Points         All Wired Access Points         Up         Down         Up         Down           All Wired Access Points         All Monitors         Q	Rogue AP Classification Summary Last 5 Min Last Hour All Rogue APs Detected 0 0 0 Rogue APs Detected 0 0 0 Interfering APs Detected 0 1 0
Network     Network       Network     Network Stammary       Al WLAN Switches     Network Status       Al Ar Monitors     Na Metwork Status       Al Wred Access Points     0       Al WLAN Switches     0       Al WLAN Switches     0       Switch     0       Switch     0       Switch Summary     Unprovisioned Access Points       Ar Monitors     0       Access Points     0       Wred Access Points     0       Wred Access Points     0       Bladidst Clients     0       Ports     0       Inventory     1.coad Balancing Events       MutAn     0       Wired Access Points     0       Bladidst Clients     0       Ports     0       Inventory     1.coad Balancing Events       Bandwidt Exceeded     0       Inventory     1.coad Clents       Ports     0       Debug     0       Load Clents     0       Ports     0       Debug     0       Load Clents     0       Process Logs       Close Tougs       Close Tougs       Close Tougs	Network     Network       Network Summary       All WLAN Switches       All Are Montors       All Wied Access Points       All WLAN Switches       All Wied Access Points       All WLAN Clenks       Switch       Switch Summary       Unprovisioned Access Points       Ale Montors       Access Points       Bibdilet Clenks       Ports       Unprovisioned Access Points       Bibdilet Clenks       Ports       Unanter Statis       Debing       Local Clenks       Ports       Debing       Local Clenks       Process Logs       Custom Logs Found>       Chords Clenks       Ports       Debing       Local Clenks       Process Logs       Custom Logs Found>	Network     Network       Network       Network       Network       Network       All van Switches       All van Switches       All Wred Access Points       All Wired Access Points       All Wired Access Points       All Wired Access Points       Switch       Switch       Switch       Wired Access Points       All Montors       All Montors       All Wired Access Points       All Montors       Switch       Switch       Switch       Wired Access Points       Duplicate Location Codes       Diversioned Access Points       Bladkist Clients       Ports       Inventory       Locad Balancing Events       Locad Balancing Events       David Clients       Ports       Debug       Locad Clients       Process Logs       Custom Logs       Loton Events       Locad Balancing Events       Divertioned Clients       Process Logs       Custom Logs       Loton Events       Duplotate Location C	Network         Network Summary         All WLAN Switches         All Access Points         All Arcess Points         All Wired Access Points         Switch         Switch         Switch Summary         Access Points         Access Points         Duplicate Location Codes	Rogue AP Classification Summary         Last 5 Min       Last Hour       All         Rogue APs Detected       Q       Q         Rogue APs Detected       Q       Q         Interfering APs Detected       Q       Q         Interfering APs Detected       Q       4
Network       Network Summary         All WLAN Switches       I         All Wred Access Points       I         All Wred Access Points       I         All Wred Access Points       I         Global Events       I         Switch       I         Switch       Improvisioned Access Points         Ar Montors       Improvisioned Access Points         Access Points       Improvisioned Access Points         Ar Montors       Improvisioned Access Points         Blackist Clients       Improvisioned Access Points         Blackist Clients       Improvisioned Access Points         Ports       Improvisioned Access Points         Inventory       Icat S Min         Icat S Min       Last S Min         Inventory       Icat S Min         Icad Balancing Events       Improvisioned Access Points         Prits       Improvisioned Balancing Events         Inventory       Icad Balancing Events         Icad Clients       Improvisioned I Diago         Prits       Improvisioned I Diago         Inventory       Icad Clients         Process Logs       Improvisioned I Diago         Clients       Improvisioned I Diago         Potos       Improvisione	Network         Network Summary         All Access Points         All An Network Status         All An Network Status         All Access Points         All An Network Status         All An Network Status         All An Network Status         All Michaitors         All An Network Status         All An Network Status         Weed Access Points         Switch         Switch         Switch Summary         Access Points         Duplicate Location Codes         Dupolicate Location Codes	Network     Network Summary       All vers Norks     All Acress Points       All Art Monitors     Total Total Total TPSEC IPSEC       All Art Monitors     Down Up Down Up Down       All Wired Access Points     Q     Q       All Wired Access Points     Q     Q       All Wired Access Points     Q     Q       Mired Access Points     Q     Q       Mired Access Points     Q     Q       Mired Access Points     Q     Q       Wired Access Points     Q     Q       Baddist Clents     Ports       Portes	Network         Network Summary         All WLAN Switches         All Access Points         All Arcess Points         All Wired Access Points         Switch         Switch         Switch Summary         Access Points         Access Points         Duplicate Location Codes	Rogue AP Classification Summary         Last 5 Min       Last Hour       All         Rogue APs Detected       0       0       0         Rogue APs Disabled       0       0       0         Interfering APs Detected       0       1       1
All WLAN Switches         All Access Points         All Mark Monitors         All WLAN Clenks         All WLAN Clenks         All WLAN Clenks         Global Events         Switch         Switch         Switch Summary         Access Points         Duploxisioned Access Points         Duploxisioned Access Points         Duploxisioned Access Points         Wired Access Points         Wired Access Points         Duploxisioned Access Points         Duploxisioned Access Points         Clenks         Blacklist Clenks         Ports         Inventory         Load Blancing Events         Ports         Ducal Clenks         Blacklist Clenks         Ports         Load Blancing Events         Ports         Load Blancing Events         Ports         Load Clenks         Process Logs         Cual Clenks         Process Logs         Cual Clenks         Process Logs         Cual Clenks         Process Logs         Cual Clenks         Process Logs	All WLAN Switches         All Access Points         All Ar Monitors         All Weak Access Points         All Weak Access Points         All Weak Access Points         Global Events         Switch         Switch Summary         Duplocate Location Codes         Duprovisioned Access Points         Duplocate Location Codes         Vired Access Points         Backlist Clients         All Weak Networks         Backlist Clients         Duplocate Location Codes         Clients         Backlist Clients         Ports         Invertences         Debug         Locad Clients         Protes         Potos         Potos         Cuad Clients         Protess Logs         Cuad Clients         Protess         Doplocate Code         Doplocate Solition Codes         Debug         Load Clients         Protess Logs         Cuad Clients         Protess Logs         Cuad Clients         Protess Logs         Cuad Clients         Process Logs         Custom Log	All VAN Switches All Access Points All Viced Access Points All Viced Access Points All Viced Access Points All Viced Access Points Switch Switc	All WLAN Switches All Access Points All Air Monitors All WLAN Clients All WLAN Clients Global Events Switch Summary Upprovisioned Access Points Duplicate Location Codes O	Last 5 Min     Last Hour     All       Rogue APs Detected     0     0     0       Rogue APs Disabled     0     0     0       Interfering APs Detected     0     1     1
All Access Points       Val.AN Network Status         All Air Monitors       Total Total IPSEC IPSEC         All Access Points       Up Down Up Down         All Wired Access Points       Q Q Q         All Wired Access Points       Q Q Q         Global Events       Arr Monitors         Switch       Wired Access Points         Switch Summary       Upprovisioned Access Points         Duplicate Location Codes       Q         Wired Access Points       Q         Duplicate Location Codes       Q         Wired Access Points       Q         Duplicate Location Codes       Q         Vired Mux Ports       RADIUS Servers       Q         Clerits       Load Balancing Events       Q       Q         Inventory       Load Balancing Events       Q       Q         Inventory       Load Balancing Events       Q       Q         Load Events       Q       Q       Q         Bandwidth Exceeded       Q       Q       Q         Load Clerits       Q       Q       Q         Inventory       Load Balancing Events       Q       Q         Load Events       Dow       Q       Q         Bandwidth Exceeded	All Access Points       Total Total Total PSPC IPSPC       Rogue AP Classification Summary         All Air Monitors       Up Down Up Down       Down       Rogue APs Detected       Q       Q         All Wired Access Points       Access Points       Q<	All Access Points       MLAN Network Status         All Air Monitors       Total Total Total Total Total TipSC TIPSC         All Mired Access Points       1         All Wired Access Points       2       0         Global Events       Air Monitors         Switch       Wired Access Points       0       0         Switch       Wired Access Points       0       0       0         Switch       Wired Access Points       0       0       0         Switch       Wired Access Points       0       0       0         Switch       Upprovisioned Access Points       0       0       0         Wired Access Points       0       0       0       0         Wired Access Points       0       0       0       0         Switch       Upprovisioned Access Points       0       0       0         Access Points       0       0       0       0       0         Access Points       0       0       0       0       0       0       0         Bidolist Cleints       1       -       -       0       0       0       0       0       0       0       0       0       0       0       0<	All Access Points     Total     Tot	Last 5 Min     Last Hour     All       Rogue APs Detected     0     0     0       Rogue APs Disabled     0     0     0       Interfering APs Detected     0     1     1
Minkcess Points       Total Total Total TSEC TPSEC         All Air Monitors       Up Down Up Down         All Wired Access Points       1         All Wired Access Points       1         All Wired Access Points       0         Global Events       Air Monitors         Switch       Mired Access Points         Switch Summary       Unprovisioned Access Points         Julicate Location Codes       0         Access Points       0         Access Points       0         Access Points       0         Switch Summary       Unprovisioned Access Points         Duplicate Location Codes       0         Wired Mux Ports       RADIUS Servers         Access Points       0         Air Monitors       0         Load Estist Clients       1         Backlist Clients       0         Inventory       Interfering Events         Local Events       0       0         Bandwidt Exceeded       0       0         Verkal Muxaph       0       0         Debug       0       0         Local Clients       Bandwidt Exceeded       0         Protess Logis       Custom Logs Found>	Minkess       Total       <	All Air Monitors   All Air Monitors   All WLAN Clents   All WLAN Clents   Access Points   Global Events   Switch   Switch   Switch Summary   Unprovisioned Access Points   Inventory   Load Balancing Events   Inventory   Load Balancing Events   Unprovisioned Access Points   Caccess Points   Load Cleants	Mill And Markows Folints     Total     TPSEC     IPSEC       All Air Monkors     Up     Down     Up     Down       All Wired Access Points     Up     Down     Up     Down       All Wired Access Points     1     0     Down     Up       All Wired Access Points     2     0     0       Global Events     Air Monitors     0     0     0       Switch     Wired Access Points     0     0     0       Switch Summary     Upprovisioned Access Points     0	Last 5 Min     Last Hour     All       Rogue APs Detected     0     0     0       Rogue APs Disabled     0     0     0       Interfering APs Detected     0     1     1
All Wind Access Points       1       0 <td>All Wed Access Points       1       0</td> <td>All Wind Access Points       1       0<td>Up         Down         Up         Down           All Wred Access Points         L         0         -           All WLAN Clients         L         0         -         -           All WLAN Clients         All WLAN Switches         L         0         -         -           Global Events         Air Monitors         Q</td><td>Rogue APs Detected     0     0       Rogue APs Disabled     0     0     0       Interfering APs Detected     0     4     4</td></td>	All Wed Access Points       1       0	All Wind Access Points       1       0 <td>Up         Down         Up         Down           All Wred Access Points         L         0         -           All WLAN Clients         L         0         -         -           All WLAN Clients         All WLAN Switches         L         0         -         -           Global Events         Air Monitors         Q</td> <td>Rogue APs Detected     0     0       Rogue APs Disabled     0     0     0       Interfering APs Detected     0     4     4</td>	Up         Down         Up         Down           All Wred Access Points         L         0         -           All WLAN Clients         L         0         -         -           All WLAN Clients         All WLAN Switches         L         0         -         -           Global Events         Air Monitors         Q	Rogue APs Detected     0     0       Rogue APs Disabled     0     0     0       Interfering APs Detected     0     4     4
All WLAN Clients       1.       0.       0.0	All WLAN Clients       1.       0	All WLAN Clients       Access Points       1       0 <td< td=""><td>All WLAN Clients         L         Q.           Global Events         A:r Monitors         3         Q         Q.           Switch         Wired Access Points         Q         Q.         Q.           Switch         Wired Access Points         Q.         Q.         Q.           Access Points         Dupprovisioned Access Points         Q.         Q.         Q.           Access Points         Duplicate Location Codes         Q.         Q.         Q.</td><td>Interfering APs Detected 0 4</td></td<>	All WLAN Clients         L         Q.           Global Events         A:r Monitors         3         Q         Q.           Switch         Wired Access Points         Q         Q.         Q.           Switch         Wired Access Points         Q.         Q.         Q.           Access Points         Dupprovisioned Access Points         Q.         Q.         Q.           Access Points         Duplicate Location Codes         Q.         Q.         Q.	Interfering APs Detected 0 4
Global Events       3       0       <	Global Events       Air Monitors       Q </td <td>Air Monitors Q</td> <td>Access Points         3         0         0         0           Switch         Air Monitors         0         0         0         0           Switch         Wired Access Points         0         0         0         0           Switch Summary         Upprovisioned Access Points         0         0         0         0           Access Points         Duplicate Location Codes         0        </td> <td></td>	Air Monitors Q	Access Points         3         0         0         0           Switch         Air Monitors         0         0         0         0           Switch         Wired Access Points         0         0         0         0           Switch Summary         Upprovisioned Access Points         0         0         0         0           Access Points         Duplicate Location Codes         0	
Switch       Wired Access Points       0 </td <td>Switch       Mired Access Points       0<!--</td--><td>Switch Air Monitors 0 0 0 0 0   Switch Summary Unprovisioned Access Points 0 0 0 0   Access Points Dublicate Location Codes 0 0 0   Wired Access Points 0 0 0 0   Wired Mux Ports RADUID Servers 0 0 0   Air Monitors DAP Servers 0 0 0   Blackist Clients Last S Min Last Hour All 0 0   Ports Load Balancing Events 0 0 0   Inventory Load Balancing Events 0 0 0   Inventory Load Balancing Events 0 0 0   WLAN Error Threshold Exceeded 0 0 0   Artuba-ap Error Threshold Exceeded 0 0 0   Potes Structure Structure Structure Structure   VLAN Error Threshold Exceeded 0 0 0   Cilents Forotape Foundo Structure Structure   Photos Structure Structure Structure   VLAN Structure Structure Structure   Local Clie</td><td>Switch         Wired Access Points         0         0         0         0           Switch Summary         Upprovisioned Access Points         0         0         0         0           Access Points         Duplicate Location Codes         0         0         0         0</td><td>Known Interfering APs 0 0</td></td>	Switch       Mired Access Points       0 </td <td>Switch Air Monitors 0 0 0 0 0   Switch Summary Unprovisioned Access Points 0 0 0 0   Access Points Dublicate Location Codes 0 0 0   Wired Access Points 0 0 0 0   Wired Mux Ports RADUID Servers 0 0 0   Air Monitors DAP Servers 0 0 0   Blackist Clients Last S Min Last Hour All 0 0   Ports Load Balancing Events 0 0 0   Inventory Load Balancing Events 0 0 0   Inventory Load Balancing Events 0 0 0   WLAN Error Threshold Exceeded 0 0 0   Artuba-ap Error Threshold Exceeded 0 0 0   Potes Structure Structure Structure Structure   VLAN Error Threshold Exceeded 0 0 0   Cilents Forotape Foundo Structure Structure   Photos Structure Structure Structure   VLAN Structure Structure Structure   Local Clie</td> <td>Switch         Wired Access Points         0         0         0         0           Switch Summary         Upprovisioned Access Points         0         0         0         0           Access Points         Duplicate Location Codes         0         0         0         0</td> <td>Known Interfering APs 0 0</td>	Switch Air Monitors 0 0 0 0 0   Switch Summary Unprovisioned Access Points 0 0 0 0   Access Points Dublicate Location Codes 0 0 0   Wired Access Points 0 0 0 0   Wired Mux Ports RADUID Servers 0 0 0   Air Monitors DAP Servers 0 0 0   Blackist Clients Last S Min Last Hour All 0 0   Ports Load Balancing Events 0 0 0   Inventory Load Balancing Events 0 0 0   Inventory Load Balancing Events 0 0 0   WLAN Error Threshold Exceeded 0 0 0   Artuba-ap Error Threshold Exceeded 0 0 0   Potes Structure Structure Structure Structure   VLAN Error Threshold Exceeded 0 0 0   Cilents Forotape Foundo Structure Structure   Photos Structure Structure Structure   VLAN Structure Structure Structure   Local Clie	Switch         Wired Access Points         0         0         0         0           Switch Summary         Upprovisioned Access Points         0         0         0         0           Access Points         Duplicate Location Codes         0         0         0         0	Known Interfering APs 0 0
Switch Summary     Unprovisioned Access Points       Access Points     Duplicate Location Codes       Wired Mucess Points     Enterprise Clients       Wired Muc Ports     RADIUS Servers       Air Monitors     LDAP Servers       Clients     Unprovisioned Excess Points       Blacklist Clients     Inventory       Local Events     Bandwidth Exceeded       Bandwidth Exceeded     Q       Verd Muces Founds	Switch Summary     Unprovisioned Access Points     0     0       Access Points     Duplicate Location Codes     0     0       Wired Mccess Points     Enterprise Clients     1     0       Air Monitors     LDAP Servers     0     0       Air Monitors     LDAP Servers     0     0       Blacklet Clients     Inventory     Last SMn     Last SMn       Inventory     Interference Events     0     0       Local Events     Bandwith Exceeded     0     0       Debug     Local Clients     Error Threshold Exceeded     0     0       Voc Custom Logs     Logs Found>     Inventory     Interference Events     0	Switch Summary Unprovisioned Access Points   Access Points Duplicate Location Codes   Wired Access Points Enterprise Clients   Wired Access Points Enterprise Clients   Wired Mack Norts LDAP Servers   Q Q   Air Monitors LDAP Servers   Q Q   Air Monitors LDAP Servers   Q Q   Clients Laat S Min Last Hour All   Blacklist Clients Q   Q Q   Local Balancing Events Q   Q Q   Local Events Q   Bandwitch Exceeded Q   Q Q   Ports Enter Threshold Exceeded   Bandwitch Exceeded Q   Q Q	Switch Summary Unprovides Control Cont	
Access Points     Duplicate Location Codes       Wired Access Points     Enterprise Clients       Wired Mux Ports     RADIUS Servers     Q       Air Monitors     LDAP Servers     Q       Clients     Last SMin     Last SMin       Blacklist Clients     Load Balancing Events     Q       Inventory     Interference Events     Q       Load Events     Bandwidth Exceeded     Q       Ports     Error Threshold Exceeded     Q       Pobug     Load Clients     Error Threshold Exceeded       Process Logs     Custom Logs Found>	Access Points     Duplicate Location Codes       Wired Access Points     Enterprise Clients       Wired Mux Ports     RADIUS Servers     Q       Air Monitors     LDAP Servers     Q       Clients     Last 5 Min     Last 5 Min       Blacklist Clients     Load Balancing Events     Q       Inventory     Interference Events     Q       Load Events     Bandwich Exceeded     Q       Ports     Dadius Exceeded     Q       VLAN     Error Threshold Exceeded     Q       Potoss     Error Threshold Exceeded     Q       VLAN     Error Threshold Exceeded     Q       Vio Custom Logs Found>     Vio Custom Logs Found>	Access Points     Duplicate Location Codes       Wired Access Points     Enterprise Clients       Mired Access Points     Enterprise Clients       Air Monitors     LDAP Servers     Q       Clients     Immerify       Biadkist Clients     Q     Q       Inventory     Load Balancing Events     Q       Local Events     Q     Q       Biadkist Clients     Interference Events     Q       Debug     Error Threshold Exceeded     Q       Ports     Error Threshold Exceeded     Q       Posts     Error Threshold Exceeded     Q	Access Points Duplicate Location Codes 0	
Wired Access Points     Enterprise Clients       Wired Mux Ports     RADUS Servers     0       LDAP Servers     0     0       Air Monitors     LDAP Servers     0       Clients	Wired Access Points     Enterprise Clients     I       Wired Mux Ports     RADUDS Servers     Q       LDAP Servers     Q     Q       Air Monitors     LDAP Servers     Q       Clients     Inventors     Last SMn       Blacklist Clients     Last SMn     Last SMn       Inventory     Load Balancing Events     Q     Q       Local Events     Bandwich Exceeded     Q     Q       WLAN     Error Threshold Exceeded     Q     Q       Debug     Local Clients     Error Threshold Exceeded     Q     Q       VLAN     Error Threshold Exceeded     Q     Q       Vita Custom Logs     Foundation     Error Threshold Exceeded     Q	Wired Access Points     Enterprise Clients     I       Wired Access Points     RADIUS Servers     Q       Air Monitors     LDAP Servers     Q       Clients     VMLAN Performance Summary       Blackist Clients     Load Balancing Events     Q       Inventory     Load Balancing Events     Q       Local Events     Q     Q       Blackist Clients     Q     Q       Inventory     East SMin Last Hour All       Local Events     Q     Q       Blackist Clients     Q     Q       Local Events     Q     Q       Blackist Clients     Q     Q       Local Events     D     Q       Blackist Clients     Q     Q       Local Events     D     Q       Blackist Clients     Q     Q       Blackist Clients     Q     Q       Blackist Clients     Q     Q       Blackist Events     Q     Q       Blackist Clients     Events     B       Blackist Events     Events     B       Blackist Events <td></td> <td></td>		
Wired Mux Ports     RADIUS Servers     0       Air Monitors     LDAP Servers     0       Clents     LDAP Servers     0       Blacklist Clents     VLAN Performance Summary       Inventory     Load Balancing Events     0       Local Events     Bandwidth Exceeded     0     0       WLAN     Error Threshold Exceeded     0     0       Debug     Load Clents     Error Threshold Exceeded     0       Custom Logs Found>     V     V	Wired Mux Ports     RADIUS Servers     Q       Air Monitors     LDAP Servers     Q     Q       Clients     LDAP Servers     Q     Q       Blacklist Clients     Last S Min     Last Hour     All       Drots     Load Balancing Events     Q     Q       Local Events     Bandwidth Exceeded     Q     Q       WLAN     Error Threshold Exceeded     Q     Q       Debug     Local Clients     Error Threshold Exceeded     Q     Q       Vacial Clients     Error Threshold Exceeded     Q     Q       Voc Custom Logs Found>     V     V     V	Wired Mux Ports RADIUS Servers   Air Monitors LDAP Servers   Q Q   Clents WLAN Performance Summary   Blacklist Clients Last S Min   Inventory Load Balancing Events   Local Clevents Bandwidth Exceeded   Q Q   WLAN   aruba-ap		
Air Monitors LDAP Servers   Clients   Bicklist Clients   Bicklist Clients   Dotts   Load Balancing Events   Load Balancing Events   Load Balancing Events   Load Events   Bandwidt Exceeded   Q   VLAN   aruba-ap   Debug   Load Clients   Process Logs   Custom Logs Found>	Air Monitors LDAP Servers   Clients   Blacklist Clients   Blacklist Clients   Ports   Load Balancing Events   Q   Local Events   Bandwidth Exceeded   Q   Q   WLAN   aruba-ap   Debug   Local Clients   Process Logs   Custom Logs Found>	Air Monitors LDAP Servers   Q Q   Clients   Blackils Clients   Blackils Clients   Dorts   Load Balancing Events   Q   Q   Local Events   Bandwidh Exceeded   Q   Q   VLAN   aruba-ap   Process Logs   Custom Logs Foundo		
Clients     WLAN Performance Summary       Blacklist Clients     Last 5 Min       Ports     Last 5 Min       Inventory     Load Balancing Events     0     0       Load Events     Bandwidth Exceeded     0     0       Bandwidth Exceeded     0     0     0       Ucal Clients     Bandwidth Exceeded     0     0       Debug     Local Clients     Frore Threshold Exceeded     0     0       Process Logs     Custom Logs Found>     V     V	Clients   Blacklist Clients   Ports   Load Balancing Events   Load Balancing Events   Q   Load Events   Bandwidth Exceeded   Q   Q   Loal Events   Bandwidth Exceeded   Q   Q   Debug   Local Clients   Process Logs   Custom Logs Found>	Clients   Blackist Clients   Ports   Load Balancing Events   Load Balancing Events   Q   Load Events   Bandwidth Exceeded   Q   VELAN   Bandwidth Exceeded   Q   Q   Debug   Local Clients   Process Logs   Custom Logs Found>		
Blackist Clients     WLAN Performance Summary       Ports     Last 5 Min     Last Hour     All       Inventory     Load Balancing Events     Q     Q     Q       Inventory     Intefference Events     Q     Q     Q       Load Events     Bandwidth Exceeded     Q     Q     Q       wLAN     Error Threshold Exceeded     Q     Q     Q       Debug     Error Threshold Exceeded     Q     Q     Q       Load Clients     Process Logs     Error Threshold Exceeded     V     V	Bladdist Clients     WLAN Performance Summary       Ports     Last S Min     Last Hour     All       Inventory     Load Balancing Events     Q     Q     Q       Inventory     Interference Events     Q     Q     Q       Load Events     Bandwidth Exceeded     Q     Q     Q       aruba-ap     Error Threshold Exceeded     Q     Q     Q       Debug     Error Threshold Exceeded     Q     Q     Q       Load Clients     Process Logs     Error Threshold Exceeded     V     V	Blacklist Clients     WLAN Performance Summaria       Ports     Last S Min Last Hour All       Inventory     Load Balancing Events     Q     Q       Inventory     Interference Events     Q     Q       Bandwidth Exceeded     Q     Q     Q       aruba-ap     Error Threshold Exceeded     Q     Q       Podg     Error Threshold Exceeded     Q     Q       Load Clients     Process Logs     Error Threshold Exceeded     Q		
Ports     Last SMn     Last Hour     All       Inventory     Load Bancing Events     Q     Q     Q       Local Events     Bandwidth Exceeded     Q     Q     Q       VLAN     Bandwidth Exceeded     Q     Q     Q       aruba-ap     Error Threshold Exceeded     Q     Q     Q       Debug     Local Clerks     Frore Stogs     Froe Stogs     Froe Stogs	Ports     Last SMn     Last Hour     All       Inventory     Load Balancing Events     Q     Q     Q       Local Events     Bandwidth Exceeded     Q     Q     Q       VLAN     Bandwidth Exceeded     Q     Q     Q       VLAN     Error Threshold Exceeded     Q     Q     Q       Debug     Local Clents     Frore Stops     Froe Stops     Froe Stops       Custom Logs Found>     V     V     V     V	Parts         Last SMin         Last Hour         All           Inventory         Load Banding Events         Q         Q         Q           Interference Events         Q         Q         Q           Local Stvents         Bandwidth Exceeded         Q         Q           wLAN         Error Threshold Exceeded         Q         Q           Poly         Error Threshold Exceeded         Q         Q           Polog         Exceeded         Q         Q           Local Cleints         Fortes         V         V           Protess Logs         Exceeded         V         V	In AND Design and Design and	
Inventory Local Events Bandwidt Exceeded Q Q Q Q Q Q Q Q Q Q Q Q Q Q Q Q Q	Inventory Interference Events 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Inventory         Load Balancing Events         Q         Q         Q           Local Events         Interference Events         Q         Q         Q           Bandwidth Exceeded         Q         Q         Q           wLAN         Error Threshold Exceeded         Q         Q         Q           Pbug         Error Threshold Exceeded         Q         Q         Q           Process Logs         Front Second         V         V         V           Custom Logs Found>         V         V         V         V	Last 5 Min Last Hour All	
Local Events 0 0 0 0 WLAN Error Threshold Exceeded 0 0 0 Debug Local Clents Process Logs Custom Logs Found>	Local Events Dandwich Exceeded Q Q Q WLAN Error Threshold Exceeded Q Q Q aruba-ap Debug Local Clients Process Logs Custom Logs Found>	Local Events     Interference Events     0     0     0       WLAN     Bandwidh Exceeded     0     0     0       aruba-ap     Error Threshold Exceeded     0     0     0       Debug     Local Clents     Fror Threshold Exceeded     0     0     0       Process Logs     Custom Logs Found>     Custom Logs Found>     Custom Logs Found>	Load Balancing Events 0 0 0	
Bandwidth Exceeded     U     U     U       aruba-ap     Error Threshold Exceeded     0     0     0       Debug     Local Gents     V     V     V     V       Process Logs     Custom Logs Found>     V     V     V     V	Bandwidth Exceeded     U     U       aruba-ap     Error Threshold Exceeded     Q     Q       Debug       Local Clients       Process Logs       Custom Logs Found>	WLAN     Bandwidth Exceeded     U     U       aruba-ap     Error Threshold Exceeded     Q     Q       Debug     Local Clients     Process Logs       Process Logs     Custom Logs Found>	Interference Events 0 0 0	
aruba-ap Debug Local Clients Process Logs Custom Logs Found>	aruba-ap Error Inreshold Exceeded u u u Debug Local Clients Process Logs Custom Logs Found>	aruba-ap. Debug Local Clients Process Logs Custom Logs Custom Logs	Bandwidth Exceeded U U U	
Local Clients Process Logs Custom Logs <no custom="" found="" logs=""></no>	Local Clients Process Logs <b>Custom Logs</b> <no custom="" found="" logs=""></no>	Local Clients Process Logs Custom Logs <no custom="" found="" logs=""></no>	Error Inreshold Exceeded U U U	
Process Logs Custom Logs <no custom="" found="" logs=""></no>	Process Lags <b>Custom Lags</b> <no custom="" found="" lags=""></no>	Process Logs Custom Logs    Clustom Logs Found>		
Custom Logs <no custom="" found="" logs=""></no>	Custom Logs <no custom="" found="" logs=""></no>	Custom Logs <no custom="" found="" logs=""></no>	Local Clients	
<no custom="" found="" logs=""></no>	<no custom="" found="" logs=""></no>	<no custom="" found="" logs=""></no>	Process Logs	
Aruba Networks1**	Aruba Networks™		<no custom="" found="" logs=""></no>	
			Aruba Networks™	

### 5.5.2. SSID Configuration Steps

Step	Description:	Configure SSID a	ruba-voice	
8.	<ul> <li>Netwo</li> <li>Netwo</li> <li>Encry</li> <li>PSK A</li> <li>Retype</li> <li>Forma</li> </ul>	rk Name (SSID) = rk Authentication ption = AES .ES Key/Passphra	n = WPA-PSK ase = testtesttest Passphrase = testtesttest	options
	WLAN Configuration - Mil Elle Edit View Favorites Address Address Http://10.1.29.2:888	<u>T</u> ools <u>H</u> elp	ARUBA 2000	Go Links » 🔁 • 🕞 Snagit 📬
	Monitoring Configuration Basic   Advanced WLAN Security Network Management Access Point Installation Wizard	Diagnostics     Maintenance     Plan       WLAN > New       aruba-ap/Global     New       Network     New       Network Name (SSID)     Radio Type       B02.11 Security     Network Authentication       Encryption     Advanced Authentication       Advanced Authentication     Auth Server Type       Keys     PSK AES Key/Passphrase       Pormat     Format	Events Reports	
	Aruba Networks™	Authentication Server ServerName Add VLAN VLAN ID Commands	IP. Address Authentication Por: Arct Por: 42	Shared Key Actions Apply View Commands E-mail Support

Solution & Interoperability Test Lab Application Notes ©2007 Avaya Inc. All Rights Reserved.

Select Config • Netwo • Netwo • Encry • VLAN Click Add un	on Server and se	N → New. Conf = aruba-data on = WPA ion Server. Cl	ick on the pull	down tab under Choos 250], and click Add. (
WLAN Configuration - M	licrosoft Internet Explorer			
File Edit View Favorites	Tools Help 188/screens/switch/wlan_new.html			🗸 🏹 Go 🛛 Links » 📆 🗸 🌀 Snagi
Network Management Access Point Installation Wizard	Network Network Name (SSID) Radio Type B02.11 Security Network Authentication Encryption Advanced Authentication Auth Server Type Keys PSK Key/Passphrase Retype PSK Key/Passphrase	AES	WPA C WPA-PSK C WPA2 C WPA2 Page C Captive Portal (Web) C MAC	:PSK
	Format Authentication Server Server Name II rad1 10.1.2.2 Add VLAN VLAN ID	The PSK Passphrase st P Address Authenti	ishould be a 64 character hexadecimal strin hould be an ASCII string 8+63 characters in cation Port Acct Port 1813	length
	Commands			Apply View Command

## 5.5.3. Configuring Security and Queuing

Step	Description: Configuring Security and Queuing				
1.	Traffic prioritization and access control are managed on the Aruba system using session ACLs. Traffic can be prioritized and tagged on a session basis. Session ACLs are then assigned to roles. These values are from <b>Section 3</b> .				
	• Defining Session ACLs.				
	Create a session ACL that permits the voice traffic for the Avaya 36XX series VoWLAN phones. These phones run the SVP protocol. CLI based Configuration. Configuring the policies. (aruba) (config) <b>#ip access-list session <acl-name></acl-name></b> (aruba) (config-sess-phone_acl) <b>#any host 10.100.117.250 svc-svp permit queue</b>				
	high tos 46 dot1p-priority 6				
	(aruba) (config-sess-phone_acl)#host 10.100.117.253 any svc-svp permit que high tos 46 dot1p-priority 6				
	(aruba) (config-sess-phone_acl)#any host 224.0.1.116 svc-svp permit queue high (aruba) (config-sess-phone_acl)#any any svc-tftp permit (aruba) (config-sess-phone_acl)#any any svc-dhcp permit				
	Add additional policies to open up the ports required for the VoIP communication.				
	Configuring the phone roles				
	Once the device successfully associates and authenticates t the Aruba WiFi network, the user is assigned a role and the access rights are defined by the policies assigned to the role. Create a user-role (phones) and assign the previously configured acl to it.				
	<ul> <li>Configurations for the lab network on the Master-6000 controller (aruba)(config)# configure terminal ## Phone role</li> </ul>				
	(aruba) (config) #ip access-list session AVPP-acl				
	(aruba) (config-sess-phone_acl) <b>#any any svc-svp permit queue high</b> (aruba) (config-sess-phone_acl) <b>#any any svc-tftp permit queue high</b>				
	(aruba) (config-sess-phone_acl)#any any svc-dhcp permit queue high				
	(aruba)(config-sess-phone acl)#exit (aruba) (config)#user-role AVPP				
	(aruba) (config-role)#session-acl AVPP-acl				
	(aruba)(config-role)#exit				

Step	Description: Configuring Authentication
2.	<ul> <li>Aruba recommends that authentication always be used to validate the devices before permitting access to the network. Refer to the Aruba documentation for a complete description of all the authentication methods that can be supported and the corresponding configuration steps. In this example, the data users use 802.1x / 802.11i authentication whereas the handsets do not support any authentication. Aruba recommends using basic authentication methods like SSID auth (validating based on SSID association), MAC-auth (validating based on MAC address) is used.</li> <li>Aruba recommends the use of MAC authentication to authenticate the 36XX series handsets. On the Aruba System, the roles for Wireless Telephones are derived using MAC-authentication (since the handsets themselves do not support advanced authentication mechanisms). The Wireless Telephones can be authenticated individually using MAC-authentication or as a group using the vendor derivation rules. For instruction on enabling MAC-authentication refer to Aruba's User Guide (See Section 10).</li> <li>CLI based Configuration For the OUI based derivation rule, configure the following from the CLI: (aruba)(config)#aaa derivation rules user (Aruba)(user-rule)#set role condition macaddr [starts-with / equals / contains] <value> set-value <rol> <li>Configurations for the lab network on the Master-6000 controller (aruba) (config)# aaa derivation rules user (aruba)(user-rule)# set role condition macaddr starts-with 00:90:7a set-value AVPP (aruba)(user-rule)# set role condition macaddr starts-with 00:90:7a set-value AVPP (aruba)(user-rule)# set role condition macaddr starts-with 00:90:7a set-value AVPP (aruba)(config)# write memory</li> </rol></value></li></ul>

Step	Description: Configuring Call Admission Control (CAC)	
3.	Call Admission Control (CAC) allows the WLAN system to control the call capacity in the air based on the number of active calls (or VoWiFi device on call) per AP rather than the number of WiFi associations. CAC is voice aware and load balances the handsets with no impact to the call quality of the devices already in-call. Settings for CAC based on the radio band.	
	<ul> <li>Configurations for the lab network on the Aruba 2400 controller (aruba) #configure terminal (aruba) (config) #ap location 0.0.0 (aruba) (sap-config) #voip call-admission-control enable (aruba) (sap-config) #voip active-load-balancing enable</li> </ul>	

(aruba) (sap-config) <b>#voip voip svp-call-capacity 12</b>
(aruba) (sap-config) <b>#voip call-handoff-reservation 20</b>
(aruba) (sap-config) <b>#voip high-capacity-threshold 20</b>
(aruba) (sap-config)#!
(aruba)(config)#write memory

Step	Description: Additional Voice Settings
4.	Proxy-arp
	<ul> <li>Enable the proxy-arp settings as this controls the generic broadcast traffic in the air. This will clear the WiFi bandwidth which would otherwise be used up for arp requests / STP packets etc.</li> <li>CLI based Configuration <ul> <li>(aruba) #configure terminal</li> <li>(aruba) (config) #firewall voip proxy-arp</li> </ul> </li> </ul>
	<ul> <li><u>Miscellaneous settings</u></li> <li>Disable RF roaming assist on the controller for VoIP clients and RF fast roaming</li> <li>CLI based Configuration         <ul> <li>(aruba) #configure terminal</li> <li>(aruba) (config) # wms station-policy handoff-assist disable</li> <li>(aruba) (config) #stm fast-roaming disable</li> </ul> </li> </ul>

## 6. Interoperability Compliance Testing

Interoperability compliance testing covered feature functionality, serviceability, and performance testing. Feature functionality testing verified the ability of the Aruba Networks Wireless LAN System to provide network access to the Avaya 3616/3626 Wireless IP Telephones, Avaya PhoneManager Pro, and other wireless clients. The emphasis of testing was on the QoS implementation in order to achieve good voice quality, Radius authentication, WEP encryption, and seamless roaming at layer-2 and layer-3.

#### 6.1. General Test Approach

All feature functionality test cases were performed manually. The following features and functionality were verified:

- Layer-2 and Layer-3 Connectivity
- 802.1X Security and WEP/WPA Encryption
- Quality of Service (QoS) based on Priority Queuing and Reserved Bandwidth
- VLANs and 802.1Q Trunking
- Layer-2 and Layer-3 Seamless Roaming
- SpectraLink Voice Protocol (SVP)

TMA; Reviewed:	Solution & Interoperability Test Lab Application Notes
SPOC 6/20/2007	©2007 Avaya Inc. All Rights Reserved.

- IEEE 802.11 a/b/g
- Dynamic IP Addressing using DHCP

Performance testing was accomplished by running a VoIP Test on a traffic generator. The VoIP Test generated audio (RTP) packets between two wireless clients and calculated a MOS score to quantify the voice quality. In addition, low-priority traffic was generated while empirically verifying the voice quality on an active wireless call.

#### 6.2. Test Results

All feature functionality, serviceability, and performance test cases passed. The Aruba Controllers and APs provide network access to the Avaya wireless IP endpoints using 802.1X Security and WEP/WPA Encryption. Good voice quality was achieved on wireless voice calls through the use of the Aruba Networks QoS implementation. The Aruba APs communicated with the wireless devices using 802.11b.

# 7. Verification Steps

This section provides the steps for verifying end-to-end network connectivity and QoS. In general, the verification steps include:

- Verify that the DHCP relay is functioning by confirming that the Avaya IP Telephones receive their IP addresses from the DHCP server connected to the network
- Check that the Avaya IP Telephones have successfully registered using the Avaya IP Office. See Section 7.1.
- Place calls between the Avaya 2410 Digital Telephone and Avaya IP Telephones.
- Verify good voice quality using a Chariot server and clients.

## 7.1. Troubleshooting

Troubleshooting can be performed on Avaya IP Office via the Avaya IP Office System Monitor application. Log into the IP Office Monitor PC and select Start  $\rightarrow$  Programs  $\rightarrow$  IP Office  $\rightarrow$  Monitor to launch the IP Office System Monitor application. Log into the application using the appropriate credentials.

To see the registration messages going to and from Avaya IP Office, select **Trace Options** under the **Filters** Menu. Select the **H.323** tab and configure as illustrated below. Click the **OK** button.

All Settings
Key/Lamp LDAP PPP R2 Routing SNMP System T1 VPN WAN
ATM Call DTE EConf Frame Relay GOD H.323 Interface ISDN
Events
Packets
H.245 Send
H.323 Receive
H.323 FastStart
RAS Send       CCMS Send         RAS Receive       CCMS Receive         View Whole Packet
Trace Colour
Default All         Clear All         Tab Clear All         Tab Set All         OK         Cancel

#### 8. Aruba Networks Support

If there are difficulties or questions regarding the configuration process, contact Aruba Networks technical support at 408 227 4500, <u>www.support.arubanetworks.com</u> or support@arubanetworks.com.

# 9. Conclusion

These Application Notes illustrate the procedures necessary for configuring Aruba Networks wireless LAN switches to support Avaya IP Office, Avaya IP Wireless Telephones and Avaya PhoneManager Pro on wireless PCs. The Aruba Networks 2400 wireless LAN switch, as well as the Aruba APs were successfully compliance-tested in the converged voice/data network configuration described in these Application Notes. These switches and APs were able to support 802.11 a/b/g radio, VLAN Tagging, QoS and 802.1x authentication as well as WEP/WPA encryption. They also support roaming at both Layer 2 and Layer 3.

TMA; Reviewed:	Solution & Interoperability Test Lab Application Notes	28 of 30
SPOC 6/20/2007	©2007 Avaya Inc. All Rights Reserved.	Aruba-IPO-APP

## 10. References

This section references the Avaya and Aruba product documentation that are relevant to these Application Notes.

The Avaya IP Office product documentation can be found at: <a href="http://marketingtools.avaya.com/knowledgebase/">http://marketingtools.avaya.com/knowledgebase/</a>

The Aruba Networks product documentation can be found at: <u>http://www.arubanetworks.com/</u> http://www.arubanetworks.com/products/mobility\_controllers.php

ArubaOS User Guide (0510249-02) ArubaOS Command Line Interface Reference Guide

#### ©2007 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by <sup>®</sup> and <sup>™</sup> are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at devconnect@avaya.com.