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 testing and additional technical discussions. Testing was conducted via the Developer*Connection* 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 Model	Radio Support	Description
AP 70	802.11 b/g and 802.11 a	Dual mode , dual radio APs with additional Ethernet port for dual homing, external and built-in antennas supported
AP 65	802.11 b/g and 802.11 a	Dual mode, dual radio AP with built-in antennas
AP 60	802.11 b/g or 802.11 a	Dual mode, single radio AP with detachable antennas

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.

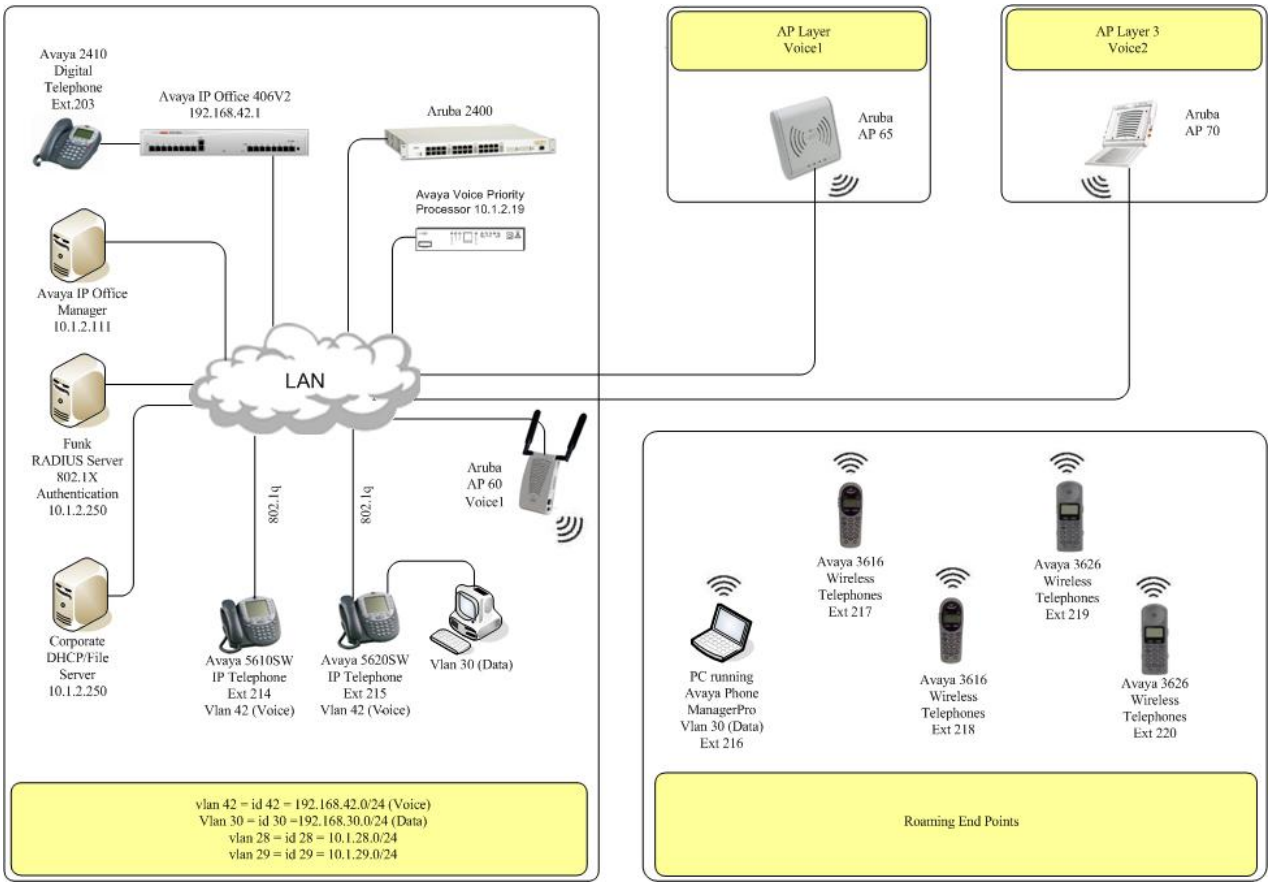


Figure 1: Avaya and Aruba Networks Wireless LAN Configuration

2. Equipment and Software Validated

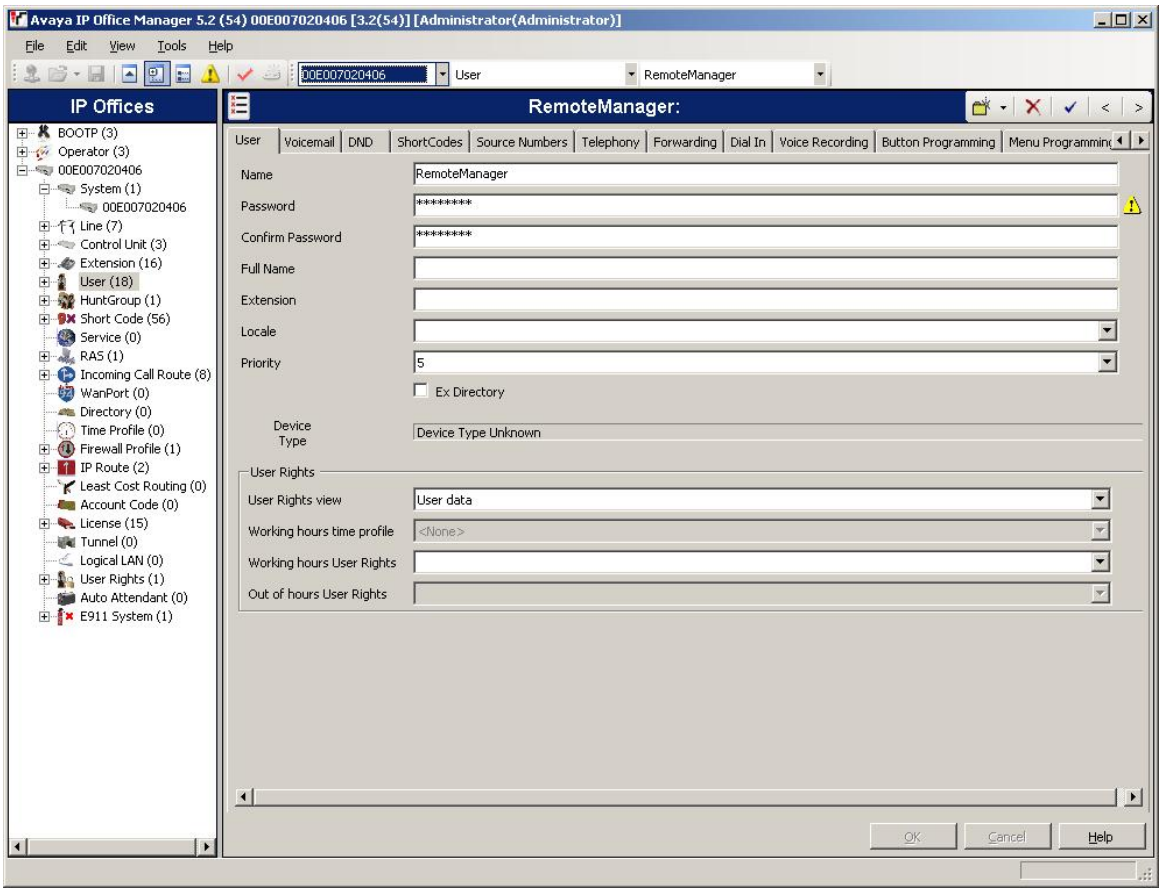
The following equipment and software were used for the sample configuration provided:

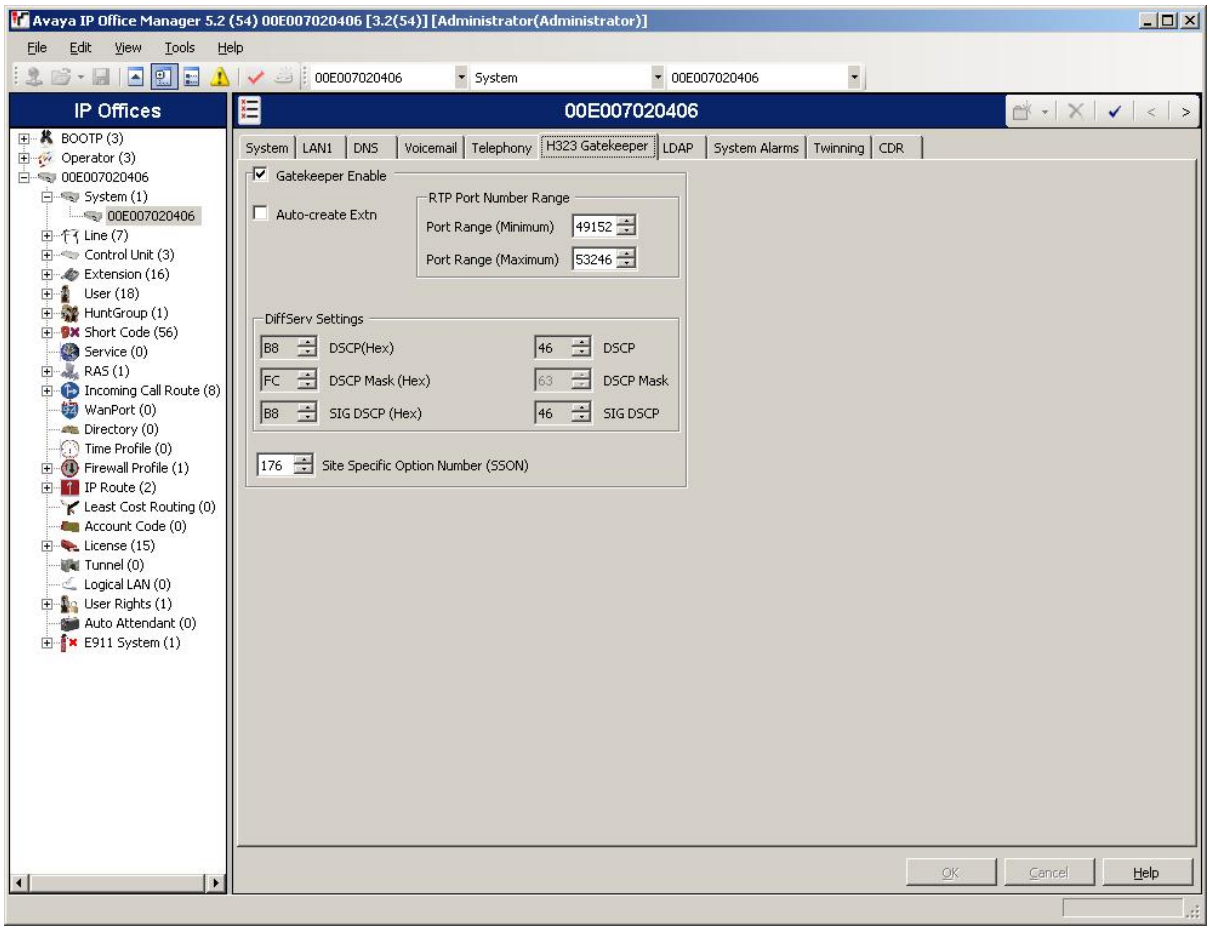
Equipment	Software
Avaya IP Office IP406V2	3.2(54)
Avaya Voice Priority Processor	33/02
Avaya 5620SW Telephones	2.3
Avaya 5610SW Telephones	3.2
Avaya 3616 wireless telephones	096.024
Avaya 3626 wireless telephones	096.024
Avaya 2410 Digital Telephone	N/A
Avaya Phone ManagerPro	2.1
Aruba 2400 Wireless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

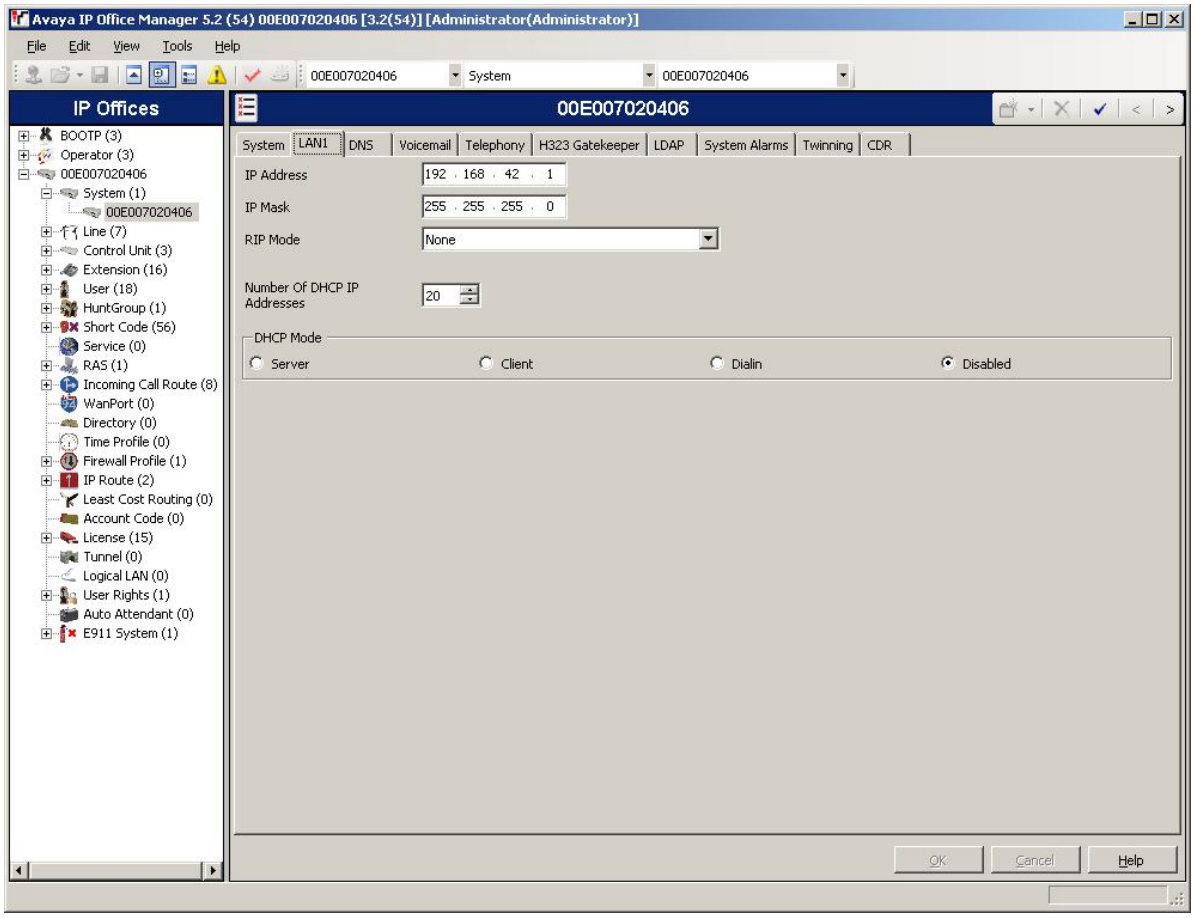
3. Avaya IP Office Settings

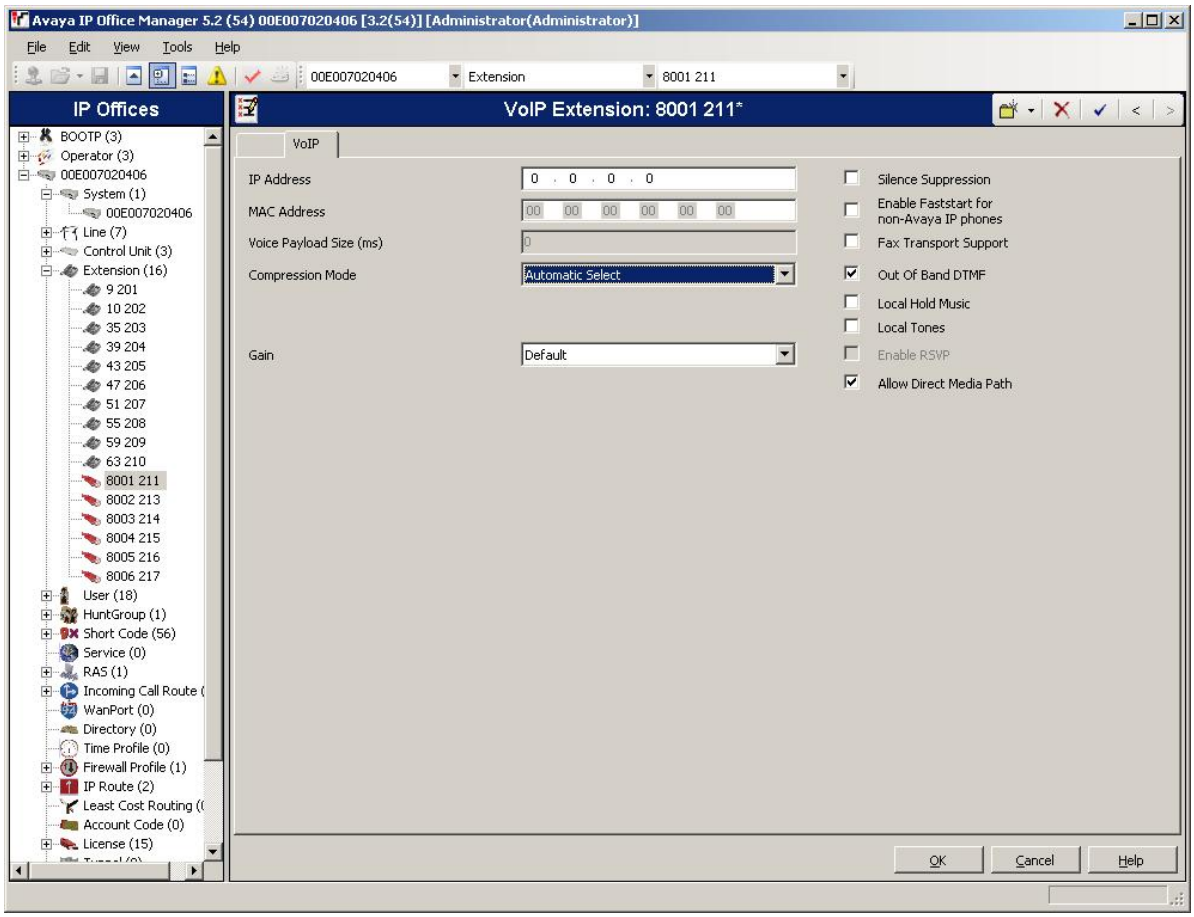
This section was included to verify that Avaya IP Office was configured correctly. Except where stated, the parameters in all steps are the default settings and are supplied for reference. For all other provisioning information such as provisioning of the trunks, call coverage, and extensions, please 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 → Programs → IP Office → Manager** to launch the Manager application. Log into the Manager application using the appropriate credentials.

Step	Description
2.	IP Office Manager Window. The main IP Office Manager window appears. The following steps refer to the Configuration Tree, which is in the left pane of the window. 

Step	Description
3.	Verify H323 Gatekeeper information. The Avaya IP Telephones will get Differentiated Services information from the Avaya IP Office. This information will be utilized for QoS by the Proxim MP.11. In the Manager window, go to the Configuration Tree and double-click **System**. Select the **H323 Gatekeeper** tab. Verify that the **DiffServ Settings** for **DSCP** and **SIG DSCP** are set to **46** and **46,** respectively. 

Step	Description
4.	Disable DHCP server on Avaya IP Office. Select the **LAN1** tab. Set the **DHCP Mode** to **Disabled**. Click **OK** to continue. 

Step	Description
5.	Verify Direct Media Path for IP Telephones. From the Configuration Tree, select **Extension**. Double-click on the IP telephone extension to verify. Select the **VoIP** tab. Verify that **Allow Direct Media Path** is checked. Click **OK** to continue. 

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

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.

```
                              NetLink SVP-II System
                    Hostname: [slnk-000006], Address: 10.1.2.230

                          System Status
                          SVP-II Configuration
                          Network Configuration
                          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.

```
                              Network Configuration
                   Hostname: [slnk-000006], Address: 10.1.2.19

     Ethernet Address (fixed):      00:90:7A:00:00:06
     IP Address:                    10.1.2.230
     Hostname:                      slnk-000006
     Subnet Mask:                   255.255.255.0
     Default Gateway:               10.1.2.1
     SVP-II TFTP Download Master:   NONE
     Primary DNS Server:            NONE
     Secondary DNS Server:          NONE
     DNS Domain:                    NONE
     WINS Server:                   NONE
     Workgroup:                     WORKGROUP
     Syslog Server:                 NONE
     Maintenance Lock:              N

       Enter=Change      Esc=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
                   Hostname: [slnk-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. Enter System name [Aruba2400]: **Aruba** 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]: **master** Enter Country code (ISO-3166), <ctrl-I> for supported list: **US** 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** 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) >**enable** Password:****** (aruba) #**configure terminal** (aruba) (config) # (aruba) (config) #**interface loopback** (aruba) (config-loop)#**ip address 10.1.29.1** (aruba) (config-loop)#**!** • Reboot the Aruba 2400 controller as requested. (aruba)(config)# **vlan 29** ← uplink subnet and data user subnet (aruba) (config) #**interface vlan 29** (aruba) (config-subif)# **ip address 10.1.29.2 255.255.255.0** (aruba)(config-subif)# **!**

	(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)# **!** (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)# **!** • Configure trunk port ← uplink trunk interface to the LAN (aruba) (config) #**interface fastethernet 1/0** (aruba) (config-if)#**trusted** (aruba) (config-if)#**no shutdown** (aruba) (config-if)#**switchport mode trunk** (aruba) (config-if)#**switchport trunk allowed vlan 29,28,42**

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:

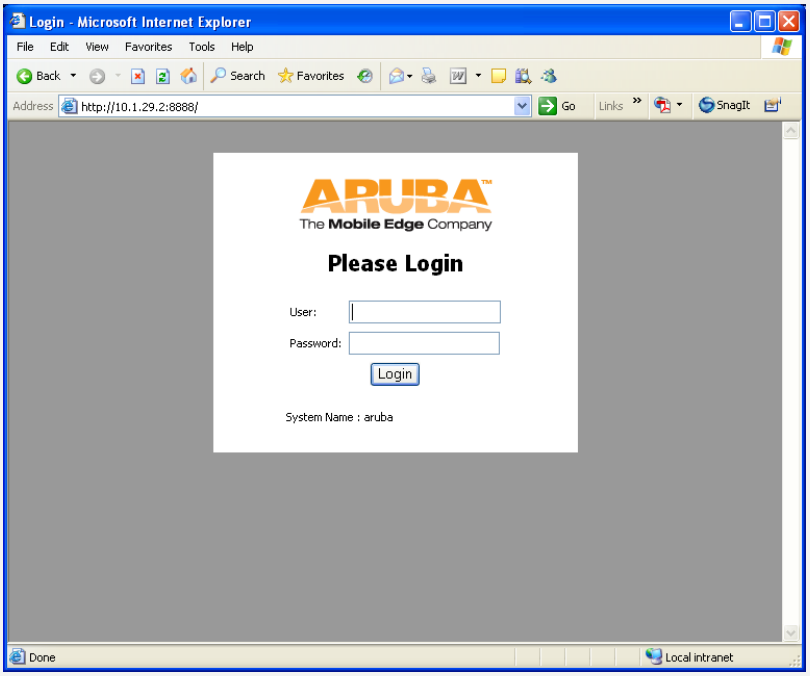
- When connected to the network, each AP is assigned a valid IP address
- APs are able to locate the Mobility Controller "(L2/L3 connectivity)"

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

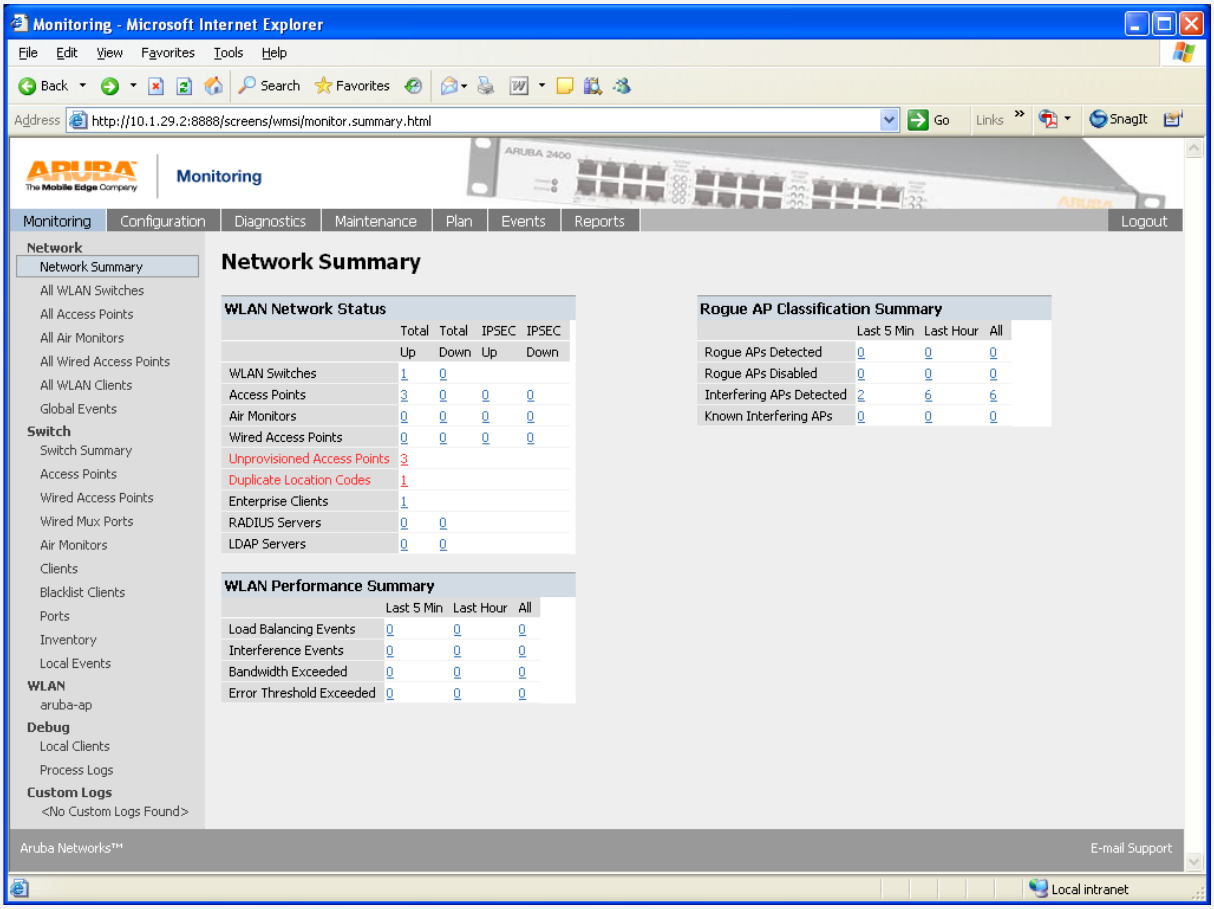
was not used and instead a centralized corporate DHCP server was put in place. To better manage the different traffic types at each site, the voice and data traffic were separated onto different VLANs.

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)**

5.5.1. Aruba 2400 Controller Configuration Steps

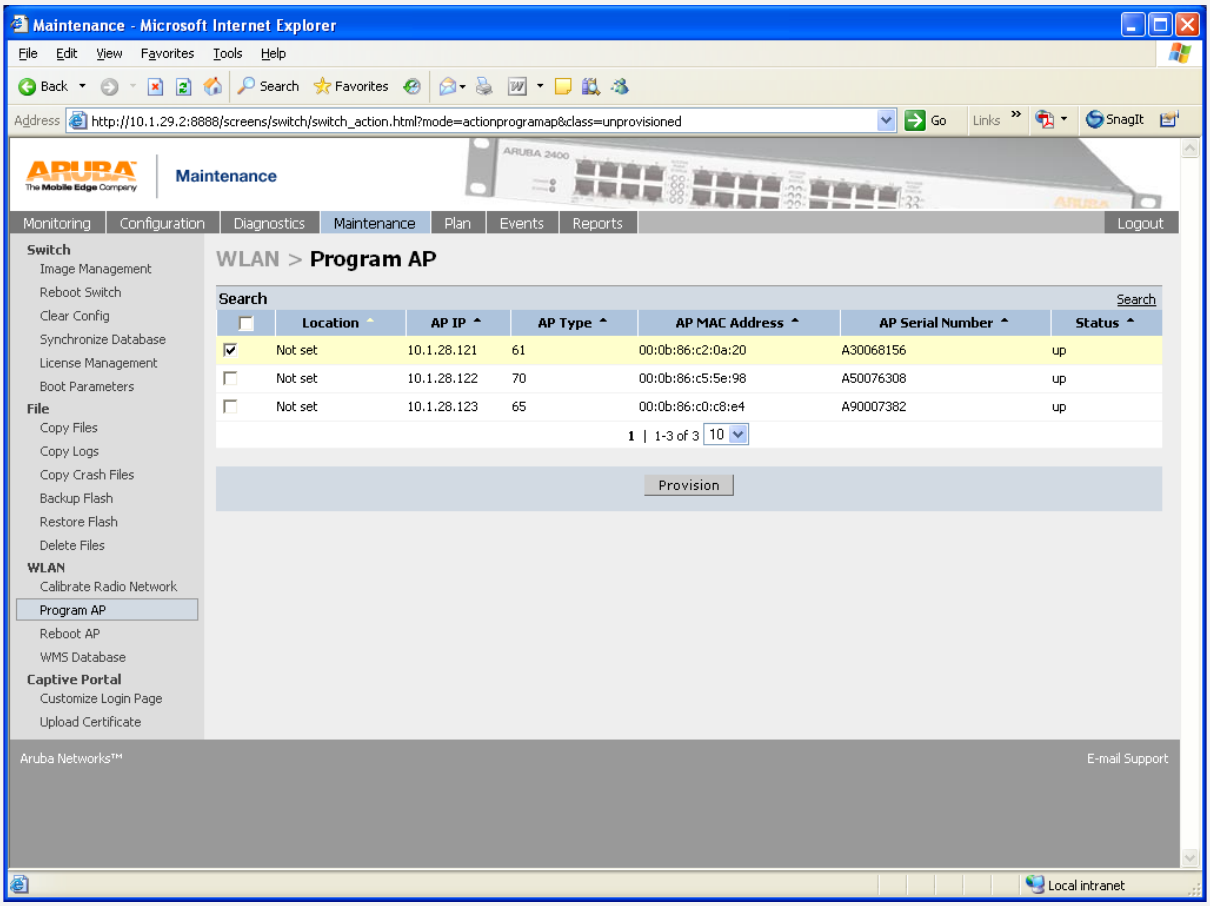
Step	Description
1.	Log into the Aruba 2400 Controller using the appropriate credentials. 

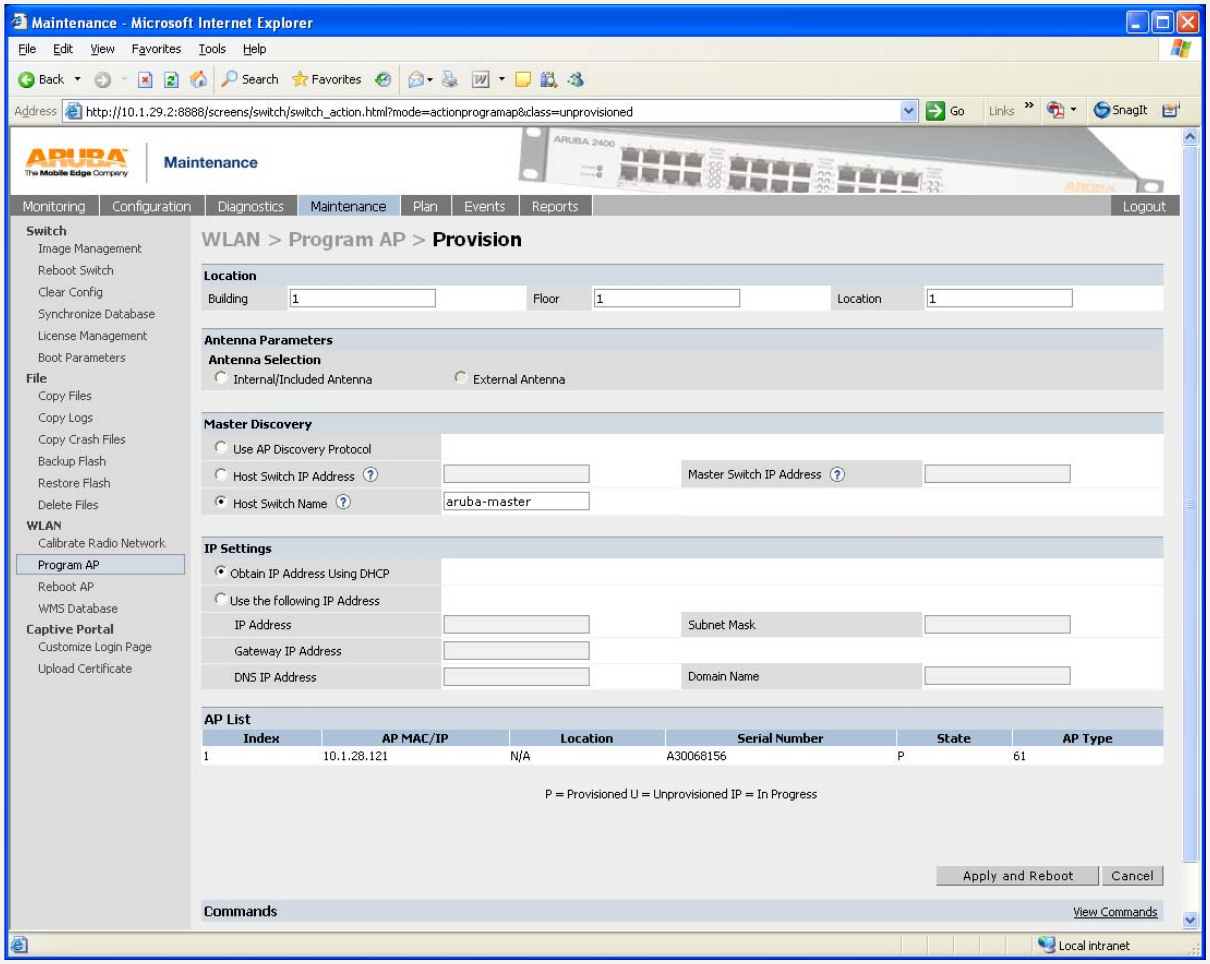
Step	Description Provision Access Points
2.	The **Monitoring** window is displayed, select **Unprovisioned Access Points** to continue**.**



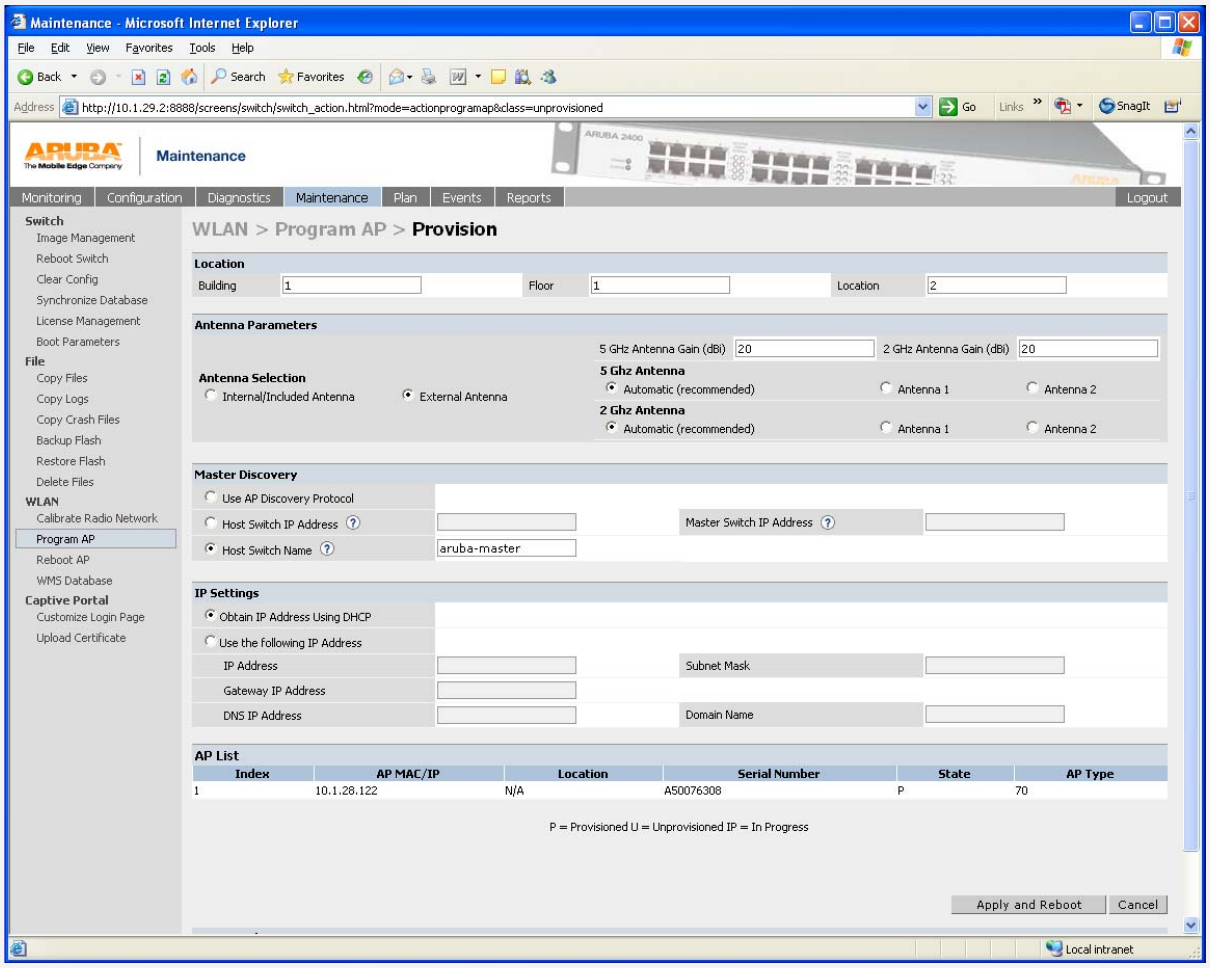
The **Maintenance → WLAN → Program AP** window appears. Select each AP and configure them**.**

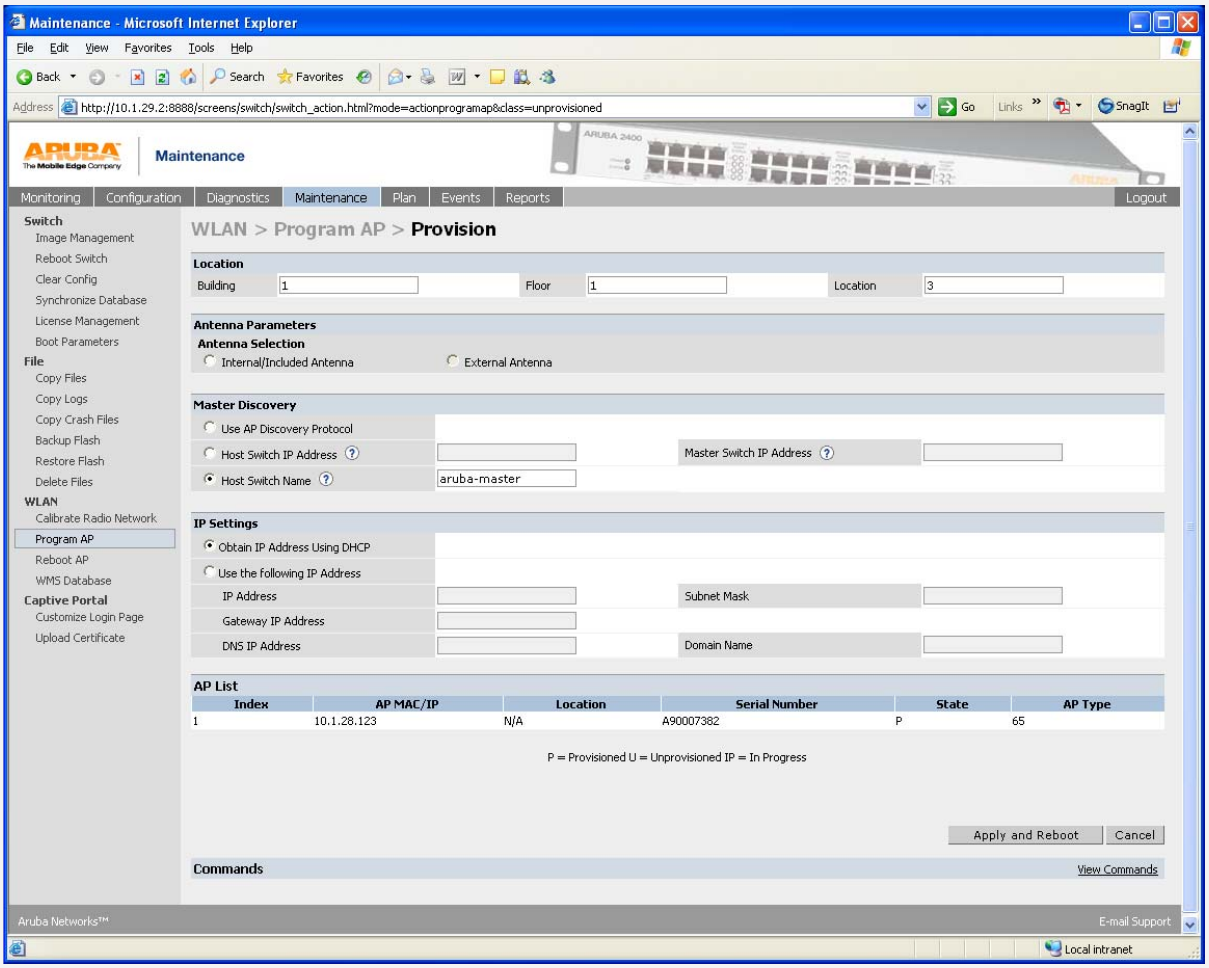
Step	Description: Provision APs
3.	Select one Unprovisioned Access Point and click the **Provision** button.



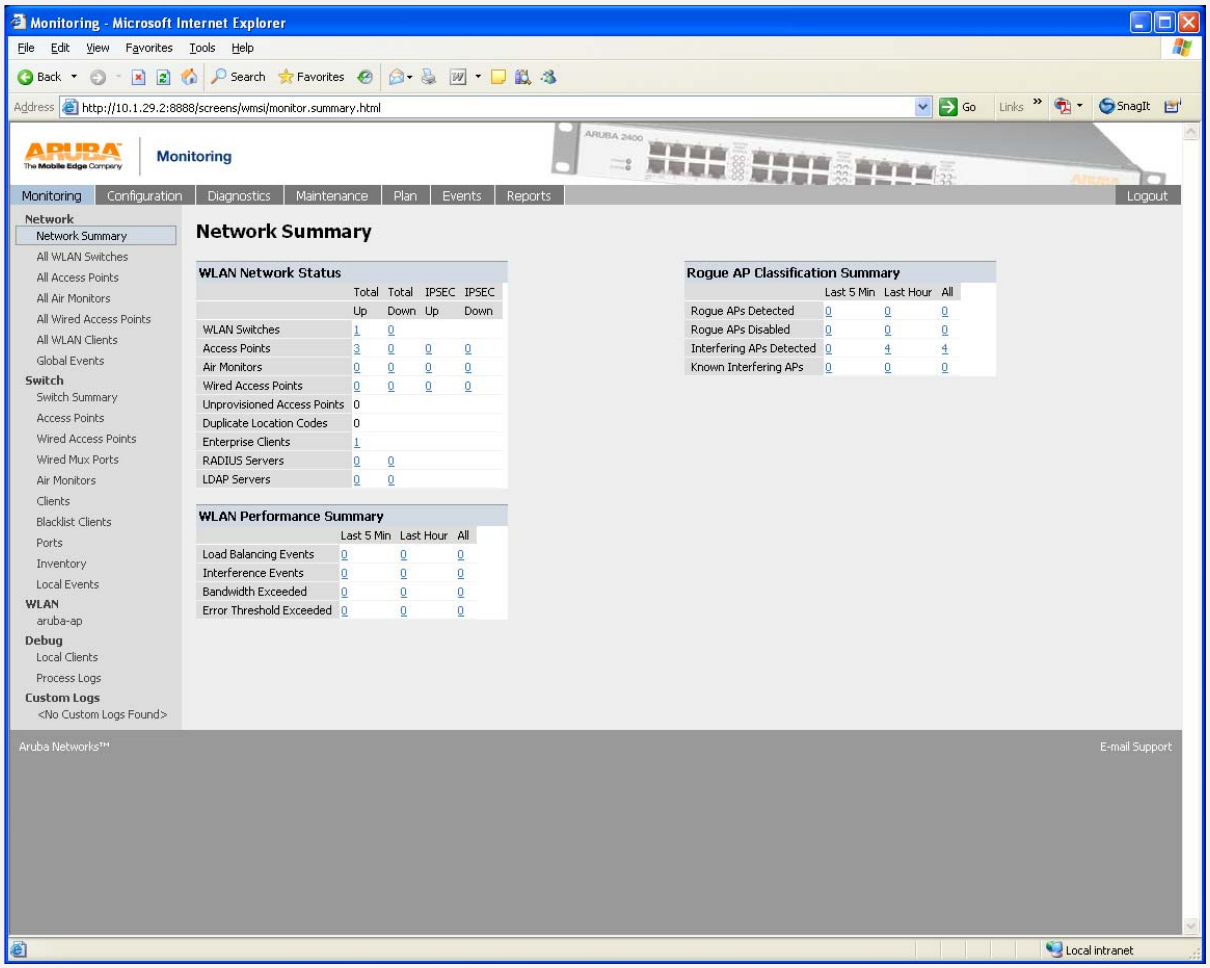
Step	Description: Provision AP 61
4.	Enter Location information as follows: • Building = 1 • Floor = 1 • Location = 1 Click the **Apply and Reboot** button to continue. 

Step	Description: Provision AP 70

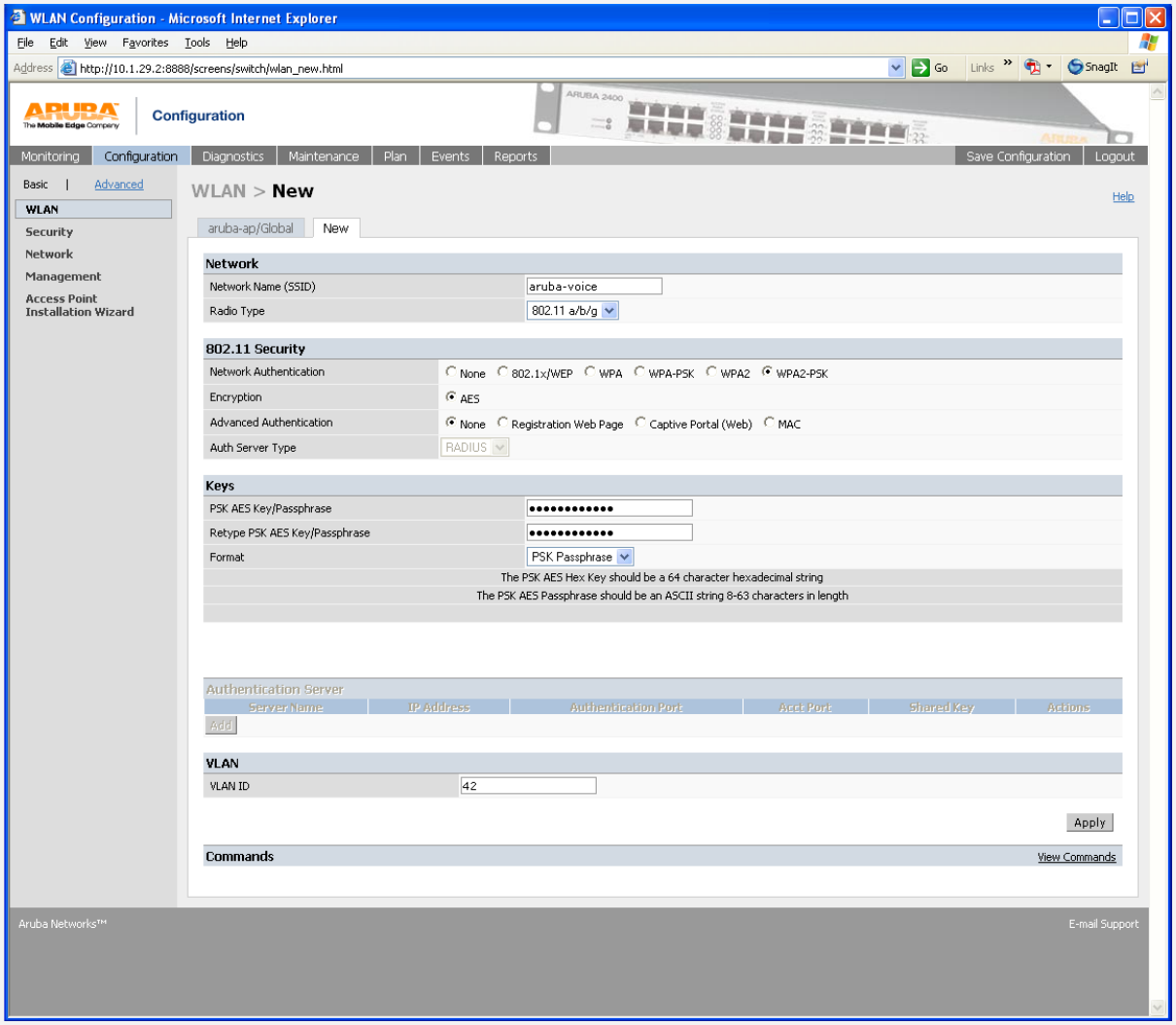
5.	Enter Location information as follows:
	
	• **Building = 1**
	• **Floor = 1**
	• **Location = 2**
	• **Antenna Parameters**
	  i. **5 GHz Antenna Gain (dBi) = 20**
	  ii. **2 GHz Antenna Gain (dBi) = 20**
	
	Click the **Apply and Reboot** button to continue.
	
	 

Step	Description: Provision AP 65
6.	Enter Location information as follows: • **Building = 1** • **Floor = 1** • **Location = 3** Click the **Apply and Reboot** button to continue. 

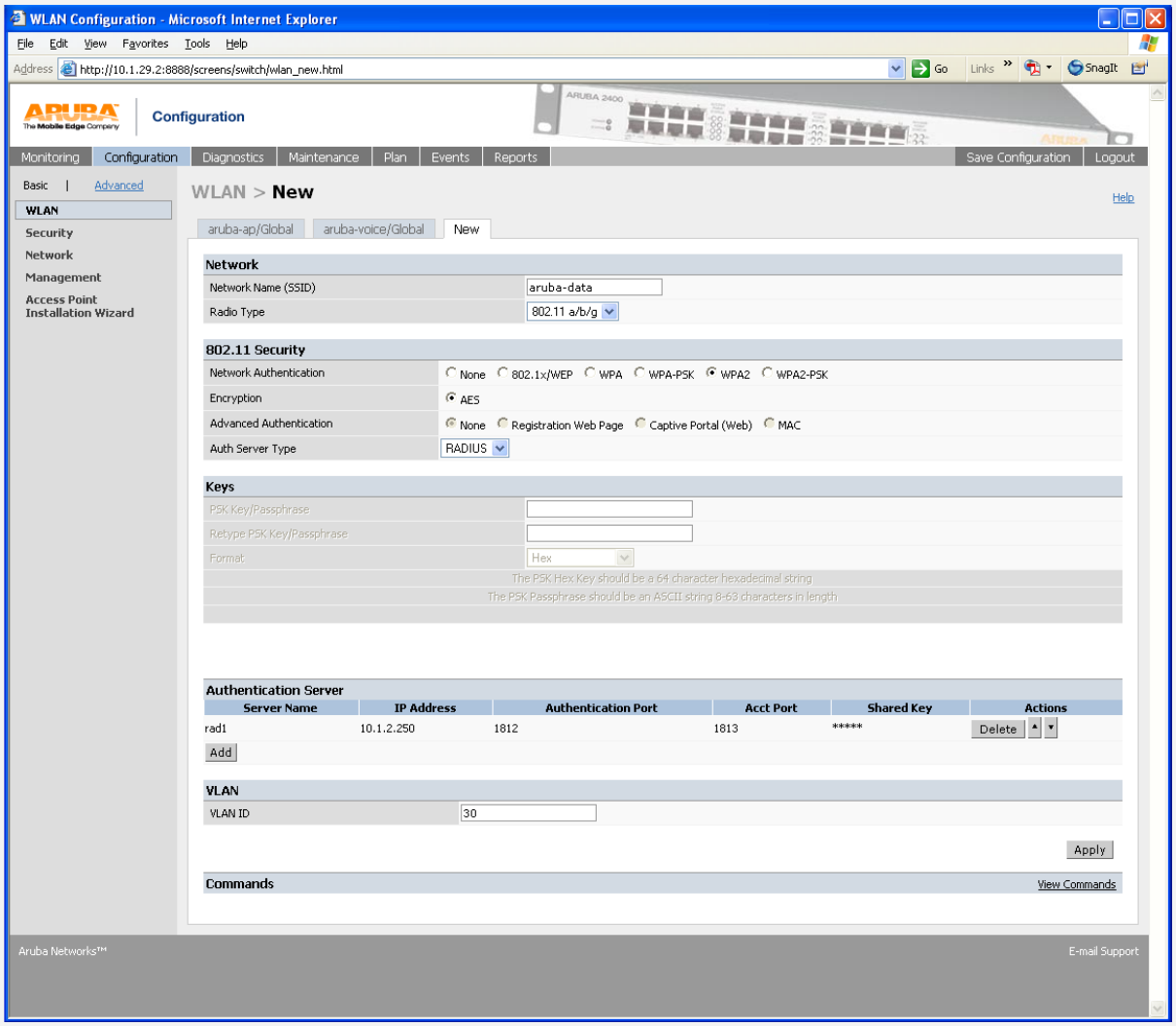
Step	Description: Verify APs
7.	Click **Monitoring → Network Summary** to verify APs have been provisioned.



5.5.2. SSID Configuration Steps

Step	Description: Configure SSID aruba-voice
8.	Select **Configuration → WLAN → New**. Configure the following options • **Network Name (SSID) = aruba-voice** • **Network Authentication = WPA-PSK** • **Encryption = AES** • **PSK AES Key/Passphrase = testtesttest** • **Retype PSK AES Key/Passphrase = testtesttest** • **Format = PSK Passphrase** • **VLAN ID = 42** 

Step	Description: Configure SSID aruba-data
9.	Select **Configuration → WLAN → New**. Configure the following options • **Network Name (SSID) = aruba-data** • **Network Authentication = WPA** • **Encryption = AES** • **VLAN ID = 30** Click **Add** under **Authentication Server**. Click on the pull down tab under **Choose an Authentication Server** and select **rad1 [IP Address:10.1.2.250]**, and click **Add. Click Apply** to continue.



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 **Section 3**. • 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) #**ip access-list session <acl-name>** (aruba) (config-sess-phone_acl)#**any host 10.100.117.250 svc-svp permit queue high tos 46 dot1p-priority 6** (aruba) (config-sess-phone_acl)#**host 10.100.117.253 any svc-svp permit queue 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. • Configurations for the lab network on the Master-6000 controller (aruba)(config)# configure terminal ## Phone role (aruba) (config) #**ip access-list session AVPP-acl** (aruba) (config-sess-phone_acl)#**any any svc-svp permit queue high** (aruba) (config-sess-phone_acl)#**any any svc-tftp permit queue high** (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.	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. 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). • 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 <role>** **The OUI for the phones is 00:90:7a** • 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)#**exit** (aruba)(config)# **write memory**

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. • 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**

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

Step	Description: Additional Voice Settings
4.	<u>Proxy-arp</u> 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. • CLI based Configuration (aruba) #**configure terminal** (aruba) (config) #**firewall voip proxy-arp** <u>Miscellaneous settings</u> Disable RF roaming assist on the controller for VoIP clients and RF fast roaming • CLI based Configuration (aruba) #**configure terminal** (aruba) (config) # **wms station-policy handoff-assist disable** (aruba) (config) #**stm fast-roaming disable**

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)

- 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

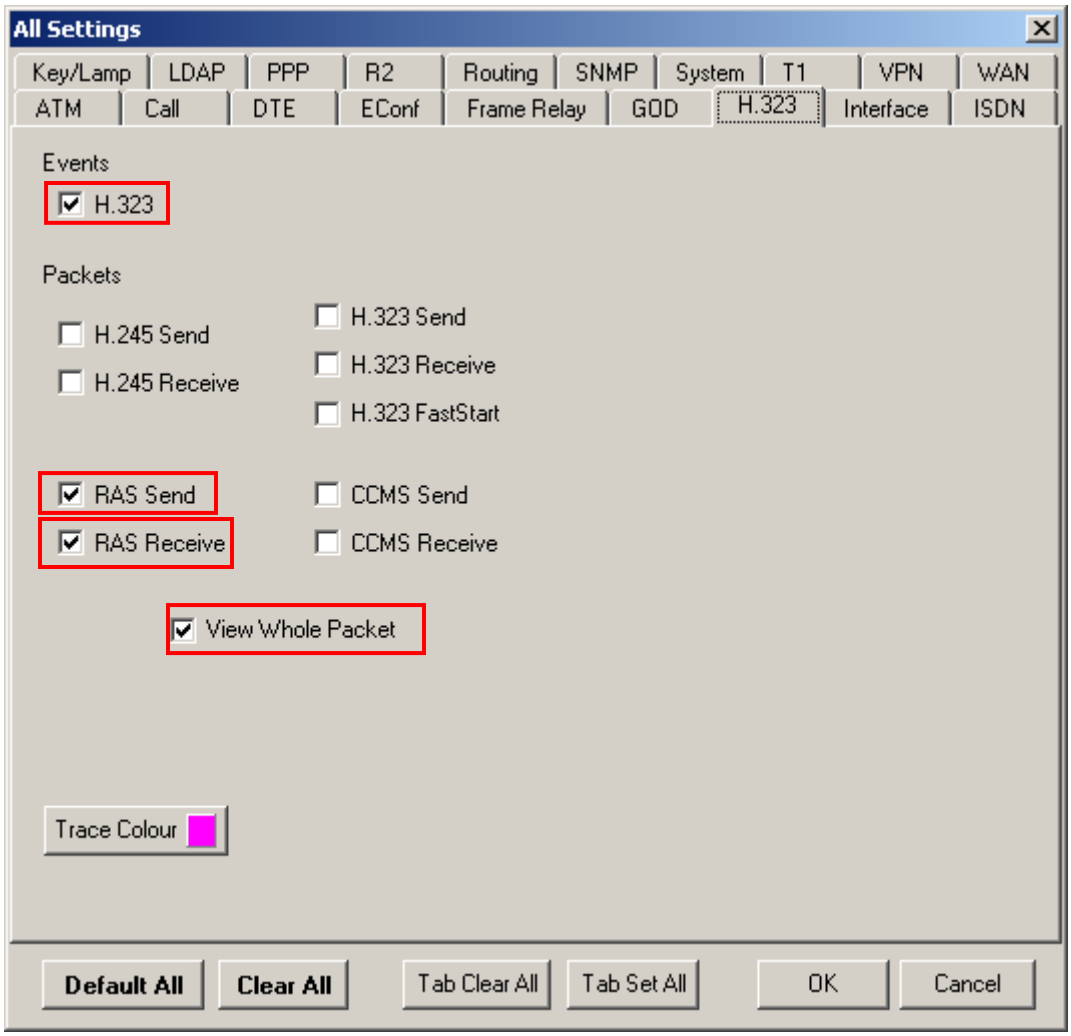
This section provides the steps for verifying end-to-end network connectivity and QoS. In general, the verification steps include:

- 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 → Programs → IP Office → 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.



8. Aruba Networks Support

If there aredifficulties or questions regarding the configuration process, contact Aruba Networks technical support at 408 227 4500, www.support.arubanetworks.com 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.

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:
http://marketingtools.avaya.com/knowledgebase/

The Aruba Networks product documentation can be found at:
http://www.arubanetworks.com/
http://www.arubanetworks.com/products/mobility_controllers.php

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