Avaya Solution & Interoperability Test Lab

Application Notes for Aruba Networks Wireless LAN System with Avaya Communication Manager 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 Avaya IP one-X Desktop gained network access through the Aruba Access Points and registered to the Avaya Communication Manager. 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 multiple Controllers managing multiple Access Points. The Aruba Networks 6000 and 2400 Controllers and Access Points AP60, AP65 and AP70 were used for testing. The Aruba APs connected the Avaya 3616/3626 Wireless IP Telephones and the Avaya IP one-X Desktop Softphone running on wireless laptops to the wired network and allowed them to register with Avaya Communication Manager. 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 WPA2 PSK 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 6000

The Aruba 6000 is a modular wireless LAN mobility controller that aggregates up to 512 controlled Access Points (APs) and delivers mobility, centralized control, convergence services and security for wireless deployments. The Aruba 6000 is designed to support large deployments in a scaleable manner, and can be easily deployed as an overlay without any disruption to the existing wired network. The device is managed using the Aruba Mobility Management System.

1.2. 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 and delivers integrated mobility, security and convergence services for both wired and wireless users and can be deployed as an overlay without any disruption to the existing wired network. In large networks, the devices can optionally be managed using the Aruba Mobility Management System.

Controller Model	# of APs	# of User
Aruba 6000	512	8192
Aruba 2400	48	768

1.3. Aruba Access Points

The Access Points (APs) discover the Aruba controllers, download the configurations and become operational once they are 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, to gather information to optimize radio coverage and to provide wireless intrusion prevention without having to deploy a separate sensor network.

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

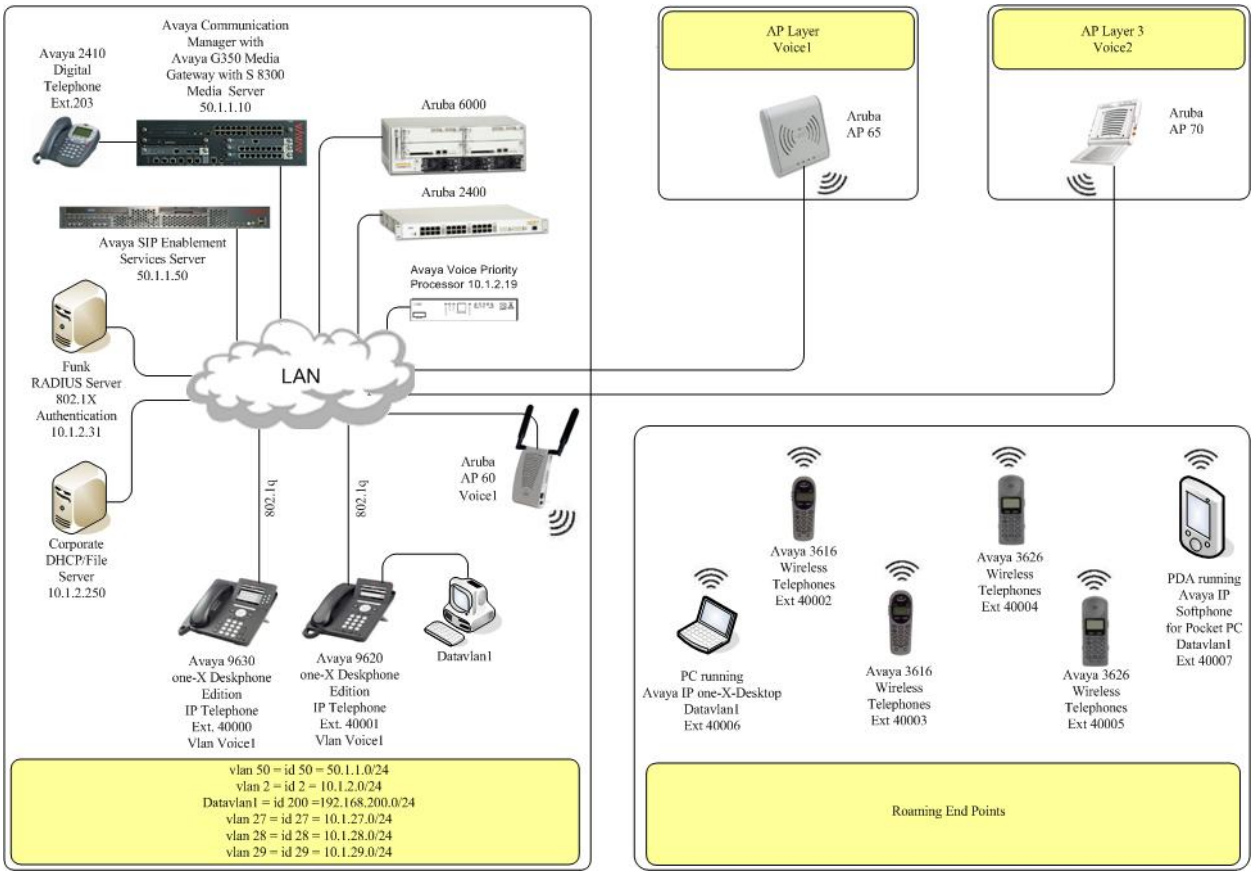

Figure 1: Avaya and Aruba Networks Wireless LAN Configuration

2. Equipment and Software Validated

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

Equipment	Software
Avaya S8300 Media Server with Avaya G350 Media Gateway	Avaya Communication Manager 3.1.2
Avaya Voice Priority Processor	33/02
Avaya SIP Enablement Services Server	3.1.1
Avaya 9620 one-X Deskphone Edition IP Telephone	1.1 (H.323)
Avaya 9630 one-X Deskphone Edition IP Telephone	1.1 (H.323)
Avaya 4620SW IP Telephones	2.2.2 (SIP)
Avaya 3616 wireless telephones	096.024
Avaya 3626 wireless telephones	096.024
Avaya IP one-X Desktop Softphone	2.1
Avaya IP Softphone for Pocket PC	2.3
Aruba 6000 Wireless LAN Switch	2.5.4.0
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
Funk Odyssey Radius Server	2.01.00.653
Funk Odyssey Client	3.03.0.119

3. Configure Avaya Communication Manager

This section shows the necessary steps in configuring Avaya Communication Manager. For detailed information on the installation, maintenance, and configuration of Avaya Communication Manager, please consult references [1] and [2].

IP networks were originally designed to carry data on a best-effort delivery basis, which meant that all traffic had equal priority and an equal chance of being delivered in a timely manner. As a result, all traffic had an equal chance of being dropped when congestion occurred. To carry voice, Quality of Service (QoS) has to be implemented throughout the entire network.

In order to achieve good voice quality, the VoIP traffic must be classified. The Avaya S8300 Media Server, Avaya G350 Media Gateway and Avaya IP Telephones support both Layer 2 802.1.p/Q priority and Layer 3 Differentiated Services (DiffServ). The Aruba Controllers can be configured to prioritize VoIP traffic based on these values.

All network components are in network region 1 for this sample configuration. The DiffServ and 802.1p/Q values configured here will be downloaded to the Avaya IP Telephones via the Avaya Communication Manager.

Use the **change ip-network-region 1** command to change the DIFFSERV/TOS PARAMETERS and 802.1P/Q PARAMETERS settings configured in Avaya Communication Manager. The **Call Control PHB Value** should be **46** and the Audio PHB Value should be **46**. The Call Control and Audio 802.1P priority are set to **6**. These values will be used in **Step 5** in **Section 5.5**.

```
change ip-network-region 1                                    Page   1 of  19
                              IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: devcon.com
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? y
   UDP Port Max: 3027
DIFFSERV/TOS PARAMETERS                 RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

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 as *admin*. 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 Controllers and Access Points. The controller configuration can be done using either a web-based interface or a command line interface (CLI). The following sessions display the configuration using CLI. For web-based configuration, refer to the Aruba 6000 and 2400 controllers configuration guide. The Aruba 6000 controller is configured as a master switch and the Aruba 2400 is configured as a backup switch in an active stand by setup.

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
- Redundancy

5.1. Aruba Solution Basics

The Aruba Solution is roles based. A user *role* corresponds to a logical user classification in an organization. Users belonging to a particular *role* will be assigned access rights associated with that role. *Role* assignment to users can be done based on authentication mechanism used and the outcome of the authentication process (success or failure).

5.2. Connecting to the 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.

On initial startup, the user is presented with a wizard.

Enter System name [Aruba800]: **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):
Re-type Password for admin login:
Enter Password for enable mode (up to 15 chars):
Re-type Password for enable mode:
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. Connecting APs

The APs need to be provisioned. The Aruba APs can be provisioned manually or be configured for automatic provisioning. For manual provisioning, use the web-based AP provisioning web page. Refer to the AP Provisioning User Guide for instructions on provisioning the AP.

The APs can communicate with the controller over a L2 or L3 network. The only requirement is that each AP be assigned an IP address and default gateway using DHCP.

5.5. Configuration Steps

Step	Description
1.	Configuring the L2 / L3 network settings via the CLI. The Avaya Communication Manager Voice over WiFi (VoWiFi) solution requires the

	handsets and the call servers to be members of the same broadcast domain. A general guideline for such deployments is to place the voice devices and the call servers in the same broadcast domain, a subnet dedicated for voice. The data users are assigned to the non-voice VLANs. • Configurations for the lab network on the Master-6000 controller (aruba) (config) #**interface loopback** (aruba) (config-loop)#**ip address 10.1.29.1** (aruba) (config-loop)#**!** (aruba) (config) #**ip default-gateway 10.1.29.254** (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)# **vlan 2** ← voice vlan (aruba) (config) #**interface vlan 2** (aruba) (config-subif)# **ip address 10.1.2.15 255.255.255.0** (aruba)(config-subif)# **!** (aruba)(config)# **vlan 28** ← subnet for local APs (aruba) (config) #**interface vlan 28** (aruba) (config-subif)# **ip address 10.1.28.3 255.255.255.0** (aruba)(config-subif)# **!** (aruba) (config) #**interface fastethernet 2/0** (aruba) (config-if)#**trusted** (aruba) (config-if)#**no shutdown** (aruba) (config-if)#**switchport mode trunk** (aruba) (config-if)#**switchport trunk allowed vlan add 29,28,42** • Verifying Connectivity Ping the default gateway from the switch's console. Ping the switch's IP address from the management station.
2.	Configuring the WiFi Network – SSID configuration. APs can be configured using the CLI or the Web Interface. Each AP on an Aruba WLAN System is identified by a unique location code. These location codes help in configuring unique WiFi settings on the AP. A group of APs can be configured globally using the wildcard location, "0" is used as the wildcard. • Configurations for the lab network on the Master-6000 controller

	(aruba)#**configure terminal** (aruba) (config)# **ap location 0.0.0** (aruba)(sap-config)#**essid corp_wpa2** ← corporate / data SSID (aruba) (sap-config)#**opmode dynamicTkip** ← encryption for the corporate SSID (aruba) (sap-config)# **phy-type g** (aruba)(sap-config)# **virtual-ap VOIPAVPP vlan-id 42 opmode wpa2-aes-psk wpa-passphrase max-retries 1 local-probe-response enable wpa-passphrase avaya123 dtim-period 3** ← voice SSID (aruba) (sap-config)# **!** (aruba)(config)# **write mem**
3.	Configuring the WiFi Network – RF settings. • Configurations for the lab network on the Master-6000 controller (aruba) (config) #**ap location 0.0.0** (aruba) (sap-config)#**phy-type g** (aruba) (sap-config)#**rates 1,2,6,9,18,24** (aruba) (sap-config)#**txrates 1,2,5,11,6,9,24,36,48,54** (aruba) (sap-config)#**mode ap_mode**
4.	Dynamic RF management – ARM aware scanning. If ARM Aware Scanning (RF scanning) is included in the firmware release, it can be enabled through the command line interface (CLI) as follows: • Configurations for the lab network on the Master-6000 controller. (aruba) (config) #**ap location 0.0.0** (aruba) (sap-config)#**phy-type g** (aruba) (sap-config)#**arm scanning enable** (aruba) (sap-config)#**arm assignment single-band** (aruba) (sap-config)#**arm voip-aware-scan enable** (aruba) (sap-config)#**exit** (aruba) (config)# **write memory**
5.	Configuring Security and Queuing. 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**
6.	Configuring Authentication. 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.

	• 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**
7.	Configuring Call Admission Control 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 Master-6000 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**
8.	Additional Voice Settings <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**
9.	Enabling Redundancy The redundancy design that was tested in the lab uses two controllers in a master-local with the master controller acting as a backup for the local controller. The local controller derives all of its WiFi, authentications and IDS settings from the master controller. Only the L2 and L3 settings need to be locally configured on the controller. VRRP is used as the redundancy protocol. The requirements are – The VRRP subnet needs to be shared between the 2 controllers and the 2 controllers needs to be on the same broadcast domain. – The APs are configured to use the VRRP address as the lms-ip address Refer to the Aruba documentation for more information on redundancy,VRRP and LMS IP settings. Local controller settings (aruba) (config) **#interface loopback** (aruba) (config-loop)#**ip address 10.1.27.1** (aruba) (config-loop)#**!** (aruba) (config) #**ip default-gateway 10.1.27.2** (aruba)(config)# **vlan 27** ← uplink subnet and data user subnet (aruba) (config) #**interface vlan 27** (aruba) (config-subif)# **ip address 10.1.27.2 255.255.255.0** (aruba)(config-subif)# **!** (aruba)(config)# **vlan 2** ← voice vlan (aruba) (config) #**interface vlan 2** (aruba) (config-subif)# **ip address 10.1.2.15 255.255.255.0** (aruba)(config-subif)# **!** (aruba)(config)# **vlan 28** ← subnet for local APs (aruba) (config) #**interface vlan 28** (aruba) (config-subif)# **ip address 10.1.28.3 255.255.255.0** (aruba)(config-subif)# **!** (aruba) (config) #**interface fastethernet 1/23** (aruba) (config-if)#**trusted** (aruba) (config-if)#**no shutdown** (aruba) (config-if)#**switchport mode trunk** (aruba) (config-if)#**switchport trunk allowed vlan add 27,28,42**

	(aruba) (config-if)#**masterip 10.1.29.1** (aruba)(config)#**vrrp 28** (aruba)(config-vrrp)#**priority 110** (aruba)(config-vrrp)#**authentication avaya** (aruba)(config-vrrp)#**ip address 10.1.28.5** (aruba)(config-vrrp)#**vlan 28** (aruba)(config-vrrp)#**no preempt** (aruba)(config-vrrp)#**no shutdown** Master controller settings VRRP Settings on the Master (aruba)# **configure terminal** (aruba)(config)#**vrrp 28** (aruba)(config-vrrp)#**authentication avaya** (aruba)(config-vrrp)#**ip address 10.1.28.5** (aruba)(config-vrrp)#**vlan 28** (aruba)(config-vrrp)#**no preempt** (aruba)(config-vrrp)#**no shutdown** Configuring the LMS IP Settings for the APs to use the VRRP interface (aruba) (config) #**ap location 1.10.0** (aruba) (sap-config)#**lms-ip 10.1.28.5** (aruba) (sap-config)# **exit** (aruba)(config)# **write memory**

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 IP one-X Desktop Softphone, and other wireless clients. The emphasis of testing was on the QoS implementation in order to achieve good voice quality, Radius authentication, WPA2 PSK and 802.1x encryption methods, 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 WPA2 PSK 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 WPA2 PSK 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 verification steps that may be performed in the field to verify that the wireless IP endpoints have connectivity to the network and that good voice quality is being provided on wireless calls.

1. Check that the Avaya wireless IP endpoints have successfully registered with Avaya Communication Manager by typing the **list registered-station** command on the SAT.

2. Verify that the Aruba APs are recognized by the Aruba Controller. Using the web UI or the CLI (*show ap registered location <x.y.z>)* to verify if all the APs are up and registered

3. Verify that the associated handset gets the right role. Using the Web UI or CLI verify that the clients have obtained their IP and registered with the call servers and PBXs.

4. Place a call between two wireless IP endpoints and verify good voice quality in both directions.

8. Support

If you encounter difficulties or have questions regarding the configuration process, please 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 equipment to support Avaya IP Wireless Telephones and Avaya IP one-X Desktop Softphone on wireless PCs. The Aruba Networks 6000 and 2400 controllers, 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 WPA2 PSK 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.

Product documentation for Avaya products may be found at http://support.avaya.com/.

[1] *Administrator Guide for Avaya Communication Manager*, Issue 2.1, May 2006, Document Number 03-300509
[2] *Administration for Network Connectivity for Avaya Communication Manager*, Issue 11, February 2006, Document Number 555-233-504
[3] *SIP Support in Release 3.1 of Avaya Communication Manager*, Issue 6, February 2006, Document Number 555-245-206
[4] *Installing and Administering SIP Enablement Services R3.1.1*, Issue 2.0, August 2006, Document Number 03-600768

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