Avaya Solution & Interoperability Test Lab

Application Notes for Aruba Networks Remote Access Point Solution with Avaya Communication Manager, Avaya Modular Messaging and Avaya IP Telephones in a Converged VoIP and Data Network - Issue 1.0

Abstract

These Application Notes describe a solution for supporting telecommuters working from home using Aruba Networks Remote Access Point Solution. This solution consists of an Aruba Controller managing remote Access Points via a Virtual Private Network (VPN).

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the small office / home office solution for supporting telecommuters using the Aruba Networks Remote Access Point solution. This solution ensures that the remote office user is subjected to the same high level of network and access security as the corporate office user, while ensuring that there is no impact on their access rights. The Aruba Remote Access Point (AP) solution requires connectivity to the Aruba controllers that in turn manage the APs. The Remote AP solution is an add-on solution to any existing Aruba infrastructure and can be enabled by turning on the right licenses and configuring any Aruba Access Point as a Remote AP (software setting).

Telecommuters working from home can register their wired and wireless Avaya IP Telephones to the Avaya Communication Manager sitting in the Corporate Office (CO) by connecting the devices to the wired / wireless interface of the Aruba Remote AP. The Aruba Remote AP establishes an IPSec tunnel to the corporate controller at the CO, allowing the corporate network to be extended over the Internet into their remote office in a secure manner. The Remote APs can be either deployed directly on public Internet through any broadband connection or can sit behind a firewall. Using the Remote AP, the enterprise wireless LAN environment appears wherever the Remote AP is operating, with the same level of WiFi security – encryption, authentication and network access control, as available in the enterprise facility.

When deploying access points with dual Ethernet ports, the second port can also be used to transport wired traffic securely across the IPSec tunnel to an enterprise data center.

2. Test Environment

The following section describes the test setup used and the network topology. The Remote AP feature is supported on all Aruba controllers and can be enabled using a license. Any AP model supported by Aruba can be configured (software configuration change) as a Remote AP and does not require any special AP hardware support. The only requirement is that the Remote AP license be enabled on the controller to which these APs connect. The equipment used in the test labs to verify this solution included the Aruba 2400 series of controllers and the Aruba AP70 Access Point.

2.1. Aruba 2400 Mobility Controller

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. It delivers integrated mobility, security and convergence services for both wired and wireless users. The Aruba 2400 can be easily 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.

2.2. Aruba AP 70

The Aruba 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.

Aruba 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 60	802.11a or 802.11b/g	Dual mode, single radio AP with detachable antennas

2.3. Test Network Details

The network diagram shown in **Figure 1** illustrates the environment used for compliance testing.

Corporate Site
The network consisted of an Avaya Communication Manager running on an Avaya S8300 Server with an Avaya G700 Media Gateway, one Avaya 9630 IP Telephone (H.323), one Avaya 9620 IP Telephone (H.323), one Avaya 2410 digital telephone, one Avaya Voice Priority Processor, one PC on the data VLAN, one Aruba 2400 Mobility Controller and one Aruba AP 60 access points. One computer is present in the network providing network services such as DHCP, TFTP, HTTP and RADIUS.

Remote Location
The network consisted of one Avaya 3631 Wireless IP Telephone, one Avaya 1616 IP Telephone (H.323), one Aruba AP 70, one laptop and one PC on the data network.

The following Avaya Endpoints were also tested at the remote location but are not shown in **Figure 1.**

- Avaya 9600 Series IP Telephones
- Avaya 4600 Series IP Telephones
- Avaya 3645 Wireless Telephone
- Avaya 3641 Wireless Telephone

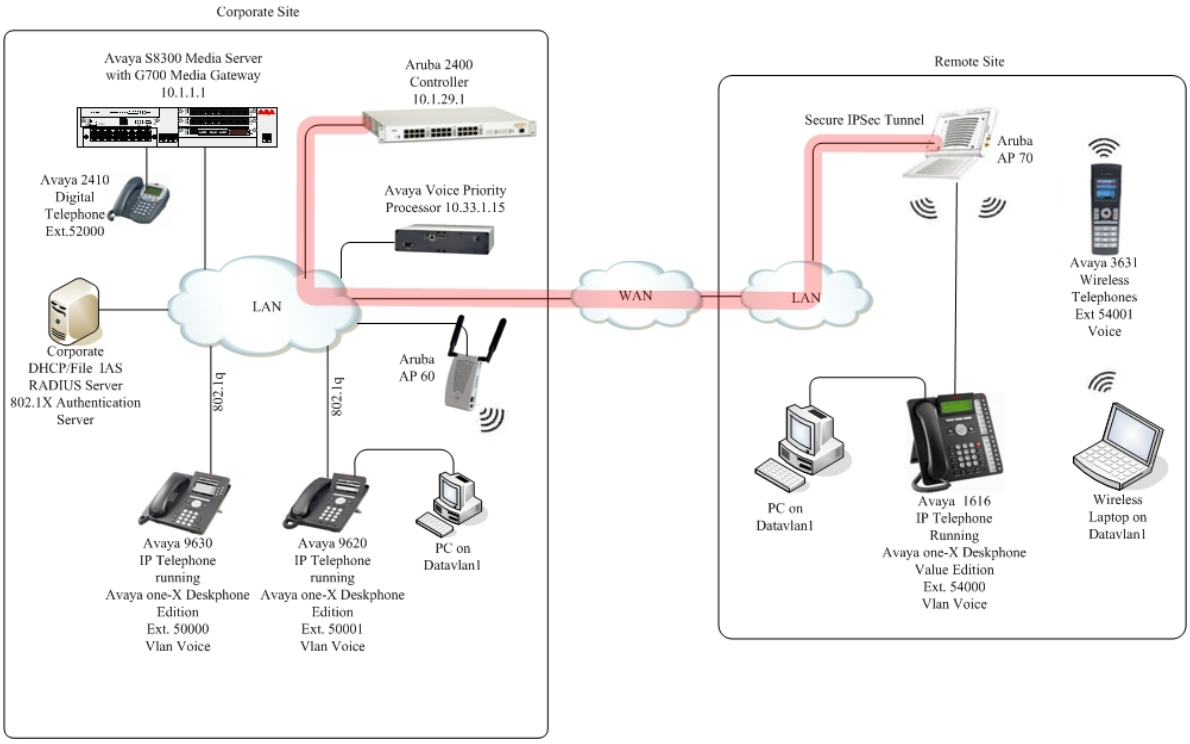


Figure 1: Avaya and Aruba Networks Wireless LAN Configuration

2.4. Equipment and Software Validated

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

Hardware Component	Software/Firmware
Avaya S8300 Server	Avaya Communication Manager 4.0 (R14x.00.1.731.2)
Avaya G700 Media Gateway MGP MM712 DCP Media Module	26.31.0 FW 008
Avaya 3631 Wireless Telephone	1.3.1
Avaya 3645 Wireless Telephone	117.016
Avaya 3641 Wireless Telephone	117.016
Avaya Voice Priority Processor	17x.028
Avaya 9620 IP Telephone	Avaya one-X Deskphone Edition 1.5 (H.323)
Avaya 9630 IP Telephone	Avaya one-X Deskphone Edition 1.5 (H.323)
Avaya 2410 Digital Telephone	5.0
Aruba 2400 Wireless LAN Switch	Aruba OS version 3.1.
Aruba AP 60	Aruba OS version 3.1.
Aruba AP 70	Aruba OS version 3.1.
Microsoft Windows 2003 Server	Internet Authentication Service (IAS)/Radius/File/DHCP

3. Configure Avaya Communication Manager

This section shows the necessary steps in configuring Avaya Communication Manager. Start a SAT terminal session to Avaya Communication Manager and access the system using valid login credentials. These Application Notes assume the proper licensing and customer options for Avaya Communication Manager have been installed. For detailed information on the installation, maintenance, and configuration of Avaya Communication Manager, please refer to **[1]** in **Section 13.**

All of the telephones configured in the sample network in **Figure 1** were administered as H.323 stations in Avaya Communication Manager. The Avaya Wireless IP Telephones should use **4620** as their station **Type** as in the example below. For complete references on how to administer these types of stations please refer to **[1]** and **[2].**

```
change station 40002                                      Page   1 of   5
                                    STATION

Extension: 40002                        Lock Messages? n               BCC: 0
     Type: 4620                         Security Code: 123456           TN: 1
     Port: S00000                     Coverage Path 1: 1               COR: 1
     Name: 3631-323                   Coverage Path 2:                 COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
              Loss Group: 19          Personalized Ringing Pattern: 1
                                                Message Lamp Ext: 40002
           Speakerphone: 2-way                Mute Button Enabled? y
        Display Language: english                Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal             Media Complex Ext:
   Survivable Trunk Dest? y                         IP SoftPhone? y

                                               IP Video Softphone? n


                                             Customizable Labels? y
```

3.1. Configure QoS on Avaya Communication Manager

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 Server, Avaya G700 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 Avaya Communication Manager.

For this example configuration, the DIFFSERV/TOS PARAMETERS and 802.1P/Q PARAMETERS were set to 46 and 6. From the SAT prompt in Avaya Communication Manager, use the **change ip-network-region 1** to change the values.

- **Call Control PHB Value** set to **46**
- **Audio PHB Value** set to **46**
- **Call Control 802.1p** set to **6**
- **Audio 802.1p priority** set to **6**

```
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 3641/3645 Wireless IP Telephones and the Aruba Access Point 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 maximum transmission speed available in the Avaya Wireless Telephones that support 802.11b and 80211g. 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 using a straight through serial cable. 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 1**. After configuring an IP address for the AVPP, a Telnet session may be used to modify the AVPP configuration.

```
                          NetLink SVP-II System
                 Hostname: [slnk-000006], Address: 10.33.1.15

                       System Status
                       SVP-II Configuration
                       Network Configuration
                       Change Password
                       Exit

     Enter=Select            ESC=Exit     Use Arrow Keys to Move Cursor
```

Figure 1: 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:                    10.33.1.15
    Hostname:                      slnk-000006
    Subnet Mask:                   255.255.255.0
    Default Gateway:               10.33.1.254
    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 2: 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 in **Figure 3**, to allow the wireless telephones to determine its rate (up to 54Mbps), 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: 10.33.1.15

    Phones per Access Point:       10
    802.11 Rate:                   Automatic
    SVP-II Master:                 10.33.1.15
    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 3: SVP-II Configuration

5. Configuring the Aruba WLAN Solution

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 2400 controller 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 sub-sections based on the feature configured.

5.1. Aruba Solution Basics

The Aruba WLAN solution is a user centric solution. Each user on the Aruba network is assigned a role based on the authentication policies and the network access rights assigned to the user. A user on successful association to the WiFi network is forced to authenticate (L2 or L3 authentication) before the user is granted network access. During the authentication process, the user is assigned a user role. The user role is assigned based on the success/failure state of authentication and based on any authentication VSAs that the authentication server returns. The user role is associated with session polices which are session aware firewall rules configured on the system to define the access rights of the user.

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 "(aruba)>" 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

To exit from the config mode, type **end.** To go the previous level in the config mode, type **exit.**

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 or refer to [8].

aruba) >
(aruba) > **enable**
(aruba) # show license

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):
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 Aruba APs in the LAN mode communicate to the controller over a Layer-2 / Layer-3 network. The APs boot up by default in the LAN mode. For more information on AP installation and configuration, refer to the AP installation guide from Aruba.

The Aruba AP can be provisioned as a Remote AP to connect to the controller over the internet. This section describes the steps required to enable Remote AP feature on the Aruba controller

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 Aruba 2400 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 33** (aruba) (config-subif)# **ip address 10.33.1.15 255.255.255.0** (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**

2.	**Configuring the User Role, Session Policies and Queuing Settings** Traffic prioritization and access control are managed on the Aruba system using session ACLs. Traffic can be prioritized and tagged on a per session basis. Session ACLs are assigned to the user roles, these roles are assigned to the users on authentication. ▪ Configuring the Session ACLs The following session ACL permits voice traffic for the Avaya 3600 Series VoWLAN phones. CLI based configuration: (Aruba) #**configure terminal** Enter Configuration commands, one per line. End with **CNTL/Z** (Aruba) (config) # **ip access-list session Voice** (Aruba) (config-sess-Voice)# **any any svc-svp permit queue high tos 63 dot1p-priority 6** (Aruba) (config-sess-Voice)# **any any svc-sip-udp permit queue high tos 63 dot1p-priority 6** (Aruba) (config-sess-Voice)# **any any svc-sip-tcp permit queue high tos 63 dot1p-priority 6** (Aruba) (config-sess-Voice)# **any any svc-dhcp permit** (Aruba) (config-sess-Voice)# **any any svc-tftp permit** ▪ Configuring the user roles for the phones (Aruba) (config) # **user-role Phones** (Aruba) (config-role) # **session-acl Voice** (Aruba) (config-role) # **!**
3.	**Configuring the Authentication Profile** Based on the authentication support available on the handset, the authentication profile needs to be created on the controller. The Avaya 3641 and 3645 Wireless Telephones support WPA2-PSK with OUI based or MAC based authentication. The Avaya 3631 Wireless Telephones support 802.1x authentication so the supported authentication method is 802.1x or 802.11i (WPA2) Refer to the Aruba user guide for steps to configure the various authentication methods on the controller. For the purpose of this document, the authentication profile is called **Auth_dot1x** for dot1x authentication and **AVPP_Auth_OUI** for the MAC based authentication.

4.	**Configuring the AP Profile** (Aruba) (config) # **wlan ssid-profile "Avaya-avpp**" (Aruba) (SSID Profile "Avaya-avpp") # **essid "AVPP"** (Aruba) (SSID Profile "Avaya-avpp") # **opmode wpa2-psk-aes** (Aruba) (SSID Profile "Avaya-avpp") # **wpa-passphrase key1** (Aruba) (SSID Profile "Avaya-avpp") # **vlan <vlan-id>** (Aruba) (SSID Profile "Avaya-avpp") # **!** (Aruba) (config) # **wlan ssid-profile "Avaya-corp"** (Aruba) (SSID Profile "Avaya-corp") # **essid "Corp-user"** (Aruba) (SSID Profile "Avaya-corp") # **opmode wpa2-aes** (Aruba) (SSID Profile "Avaya-corp") # **wmm** (Aruba) (SSID Profile "Avaya-corp") # **vlan <vlan-id>** (Aruba) (SSID Profile "Avaya-corp") # **!** (Aruba) (config) # **wlan virtual-ap AVPP-Voice** (Aruba) (config) # **aaa-profile "AVPP_Auth_OUI"** (Aruba) (config) # **ssid-profile "Avaya-avpp**" (Aruba) (config) # **!** (Aruba) (config) # **wlan virtual-ap Corp** (Aruba) (config) # **aaa-profile Auth_dot1x** (Aruba) (config) # **ssid-profile Avaya-corp** (Aruba) (config) # **!** (Aruba) (config) # **ap wired-ap-profile "wiredAP"** (Aruba) (Wired AP profile "wiredAP") # **wired-ap-enable** (Aruba) (Wired AP profile "wiredAP") # **forward-mode bridge** (Aruba) (Wired AP profile "wiredAP") # **!** (Aruba) (config) # **ap-group "Avaya_Remote_AP"** (Aruba) (AP group "Avaya_Remote_AP") # **virtual-ap AVPP-Voice** (Aruba) (AP group "Avaya_Remote_AP") # **virtual-ap Corp** (Aruba) (AP group "Avaya_Remote_AP") # **wired-ap-profile "wiredAP"** (Aruba) (AP group "Avaya_Remote_AP") # **!** (Aruba) (config) # *Note: The 3631 H.323 phones support WMM. Enable WMM on the SSID profile corresponding to the SSID that these phones would associate to. In this example, the SSID is Avaya-corp.*

5. **Configuring the VPN Information for the Remote AP**

- Cofigure a public address for the controller
- Configure the vpn parameters

(Aruba) (config) #
(Aruba) (config) #**vpdn group l2tp**
(Aruba) (config-vpdn-l2tp**)# ppp authentication PAP**
(Aruba) (config-vpdn-l2tp)# **client configuration dns 10.6.1.1 10.7.1.2**
(Aruba) (config-vpdn-l2tp)# **!**
(Aruba) (config) #**ip local pool pool1 10.4.1.1 10.4.10.200**
(Aruba) (config) #**crypto isakmp key test123 address 10.4.1.0 netmask 255.255.255.0**
(Aruba) (config) #

- Configure the Remote AP user role

(Aruba) (config) #**ip access-list session Remote_AP_policy**
(Aruba) (config-sess-Remote_AP_policy)#**any any svc-papi permit**
(Aruba) (config-sess-Remote_AP_policy)#**any any svc-gre permit**
(Aruba) (config-sess-Remote_AP_policy)#**any any svc-l2tp permit**
(Aruba) (config-sess-Remote_AP_policy)#**any alias mswitch svc-tftp permit**
(Aruba) (config-sess-Remote_AP_policy)#**any alias mswitch svc-ftp permit**
(Aruba) (config-sess-Remote_AP_policy)#**user-role Remote_AP**
(Aruba) (config-role) #**session-acl Remote_AP_policy**
(Aruba) (config-role) #**!**

- Configure the VPN authentication

(Aruba) (config) #**aaa server-group Remote_AP**
(Aruba) (Server Group "Remote_AP") #**auth-server Internal**
(Aruba) (Server Group "Remote_AP") #**aaa authentication vpn**
(Aruba) (VPN Authentication Profile) #**default-role Remote_AP**

(Aruba) (VPN Authentication Profile) #**server-group Remote_AP**
(Aruba) (VPN Authentication Profile) #**!**

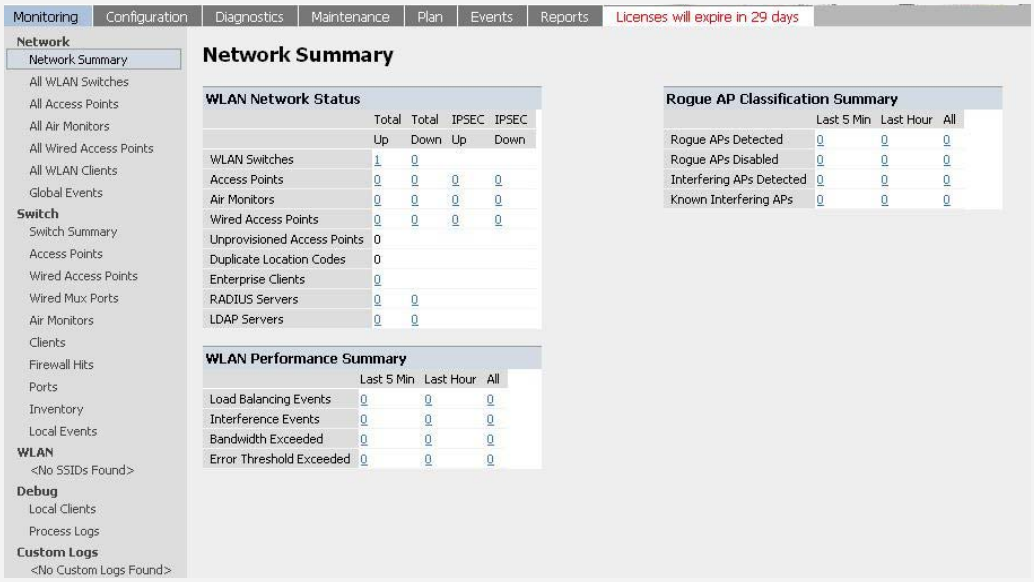
- Create the user name and password the AP will use to authenticate on the Internal database

Local-userdb add user username <*username*> password <*password*>
(Aruba) #local-userdb add username abc password abc

6. **Provision the AP as the Remote AP.**

The switch can be accessed using http, **http://<switch IP Address>**

Enter the username and password configured (in the example above, the username / password configured is admin / admin). On successful login the following Network Summary page is displayed:



Navigate to the **Configuration > Wireless > AP Installation > Provisioning** page. Select the Remote AP and click **Provision**.

- Under **Authentication Method**, select **IPSec Parameters**. Enter the **Internet Key Exchange (IKE) Pre-Shared Key (PSK), username**, and **password**.

NOTE: The username and password you enter must match the username and password configured on the authentication server for the remote AP.

- Under **Master Discovery**, set the **Master IP Address** to **Host Controller IP Address** and enter the the IP address **10.1.29.1**:

- Under **IP Settings**, make sure that **Obtain IP Address Using DHCP** is selected.

Click **Apply** and **Reboot.**

NOTE: Regardless of the deployment type, Aruba recommends that the LMS IP in the AP system profile for the AP be set to the Mobility Controller IP address (either the loopback address of the Mobility Controller or the VLAN 1 IP address).

6. Configure Avaya 3631 Wireless IP Telephone

For complete details on configuring the Avaya 3631 Wireless IP Telephone refer to [5].

7. Configure Avaya 3641 Wireless IP Telephone

For complete details on configuring the Avaya 3641 Wireless IP Telephone refer to [7].

8. Configure Avaya 3645 Wireless IP Telephone

For complete details on configuring the Avaya 3645 Wireless IP Telephone refer to [7].

9. Interoperability Compliance Testing

Testing verified the ability of the Aruba Networks Remote AP Solution to provide telecommuters working for home offices with the same connectivity and user experience, as they would have at the corporate network. This includes the ability to register the wired and wireless Avaya IP phones with the Avaya Communication Manager, which may be located in the corporate network, over the internet. The emphasis of the testing was on the ability to enforce the same encryption, authentication and access control policies that would be used in the enterprise facility.

9.1. General Test Approach

The general test approach was to register the Avaya Wireless IP Telephones with Avaya Communication Manager through the through the VPN using Aruba Networks Remote Access Point Solution. Calls were made between both wired and wireless telephones and specific calling features were exercised. To validate Quality of Service, low priority background traffic was injected into the network and the Aruba Networks Remote Access Point Solution was verified to maintain voice calls while dropping the low priority traffic. Network level tests included verifying Quality of Service for voice traffic.

9.2. Test Results

The Avaya Wireless IP Telephones registered with Avaya Communication Manager utilizing Aruba Networks Remote Access Point Solution passed all test cases. The Avaya Wireless IP Telephones successfully register with Avaya Communication Manager using the Aruba Networks Remote Access Point Solution. The compliance testing also focused on verifying Quality of Service for voice traffic while low priority background traffic was competing for bandwidth.

Four different security schemas were tested: Clear, WEP-128 and WPA2-PSK TKIP on the Avaya 3641 Wireless IP Telephones and Avaya 3645 Wireless IP Telephones, and Clear, WEP-128, WPA2-PSK TKIP and WPA2-CCMP-802.1X on the Avaya 3631 Wireless IP Telephone. Two codecs were used for testing: G.711MU and G.729AB. Telephone calls were verified to operate correctly with the media path direct between the telephones (shuffling enabled) and with

the media path centralized through Avaya Communication Manager (shuffling disabled). Calls were maintained for durations over one minute without degradation to voice quality.

The telephony features verified to operate correctly included attended/unattended transfer, conference call participation, conference call add/drop, multiple call appearances, caller ID operation, call forwarding unconditional, call forwarding on busy, call forwarding clear, call pick-up, bridged call appearances, voicemail using Avaya Modular Messaging, Message Waiting Indicator (MWI), hold and return from hold.

10. Verification Steps

This section provides the verification steps that may be performed to verify that the wireless IP endpoints have connectivity to the network and that good voice quality is being provided on wireless calls.

- Place calls between the corporate and remote sites and verify good voice quality in both directions.
- Ensure that the **ESSID** field value configured in **Step 5.5.4**, on the the Aruba Networks 2400 controller matches the **ESSID** field value on the Avaya Wireless IP Telephones.
- Check that the Avaya Wireless IP Telephones and Avaya IP Telephones have successfully registered with Avaya Communication Manager by typing the **list registered-ip-station** command on the SAT in Avaya Communication Manager.

11. 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.

12. Conclusion

These Application Notes illustrate the procedures necessary for configuring Aruba Networks Remote Access Point Solution to support Avaya 3600 Series IP Wireless Telephones, Avaya 1600 Series IP Telephones, Avaya 9600 Series IP Telephones and Avaya Communication Manager. The Aruba Networks 2400 controller, as well as the Aruba APs were successfully compliance-tested in a converged voice and data network configuration. The Aruba Networks 2400 controller, as well as the Aruba APs were able to support 802.11 b/g/a radio, VLAN Tagging, QoS, and 802.1x authentication with digital CA certificates as well as WPA2 AES and TKIP Encryption.

13. Additional References

The following Avaya product documentation can be found at http://support.avaya.com.

[1] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 3.1, February 2007
[2] *Avaya Communication Manager Advanced Administration Quick Reference*, Doc # 03-300364, Issue 3, February 2007
[3] *Administration for Network Connectivity for Avaya Communication Manager*, Doc # 555-233-504, Issue 12, February 2007
[4] *Avaya IP Telephony Implementation Guide*, May 1, 2006
[5] *Avaya 3631 Wireless Telephone Administrator Guide*, March 2007, Issue 2, Document Number 16-602203
[6] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide*
[7] *Avaya 3641/3645 Wireless Telephone and Accessories User Guide*, August 2007

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

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.