Avaya Solution & Interoperability Test Lab

Application Notes for an Aruba Networks Remote Access VPN Solution with GSM Failover using an Avaya Aura™ Telephony Infrastructure in a Converged Voice over IP and Data Network - Issue 1.0

Abstract

These Application Notes describe a solution for supporting an Aruba Networks VPN Solution with GSM Failover using Aruba Networks 3200 Controller and RAP 5 Access Point with an Avaya Aura™ Telephony Infrastructure consisting of Avaya Aura™ Communication Manager, Avaya Aura™ SIP Enablement Services, Avaya Modular Messaging and Avaya Aura™ Communication Manager Messaging in a converged Voice over IP and Data Network. This solution consists of an Aruba 3200 Controller managing a remote RAP-5 Access Points with a GSM card 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 VPN solution with GSM Failover. This solution ensures that the remote office users are subjected to the same high level of network and access security as the corporate office users while ensuring that there is no impact on their access rights. The Aruba RAP-5 solution requires connectivity to the Aruba Controller in the Corporate HQ to be able to establish the VPN.

Telecommuters working from a remote site or from home can register their wired and wireless Avaya IP Telephones to the Avaya Telephony Infrastructure sitting in the Corporate Office (CO) by connecting the devices to the wired / wireless interface of the RAP-5. The Aruba Remote RAP-5 establishes an IPSec tunnel to the corporate Aruba Networks Controller at the CO via a wired connection (internet) or over the failover card (GSM), allowing the corporate network to be extended over the Internet into their remote office/home in a secure manner. Using the Remote AP, the enterprise wireless LAN environment appears wherever the Remote RAP-5 is operating, with the same level of WiFi security – encryption, authentication and network access control, as available in the enterprise facility.

1.1. Interoperability Compliance Testing

Testing verified the ability of the Aruba Networks VPN Solution with GSM Failover to provide remote site and telecommuters 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 telephones with the Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services which were 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 over the VPN and to validate GSM failover.

1.2. Support

Aruba Networks technical support:
Phone: 408 227 4500
Email: support@arubanetworks.com

2. Reference Configuration

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

2.1. Corporate Site

The Corporate site consisted of Avaya Aura™ Communication Manager & Aura™ Communication Manager Messaging running on an Avaya S8300 Server with an Avaya G450 Media Gateway, an Avaya S8500 Server running Avaya Aura™ SIP Enablement Services, one Avaya Modular Messaging Application Server, one Avaya Modular Messaging Storage Server, one Avaya 9630 IP Telephone (SIP), one Avaya 9620 IP Telephone (H.323), one Avaya 2420 Digital Telephone, one Aruba 3200 Mobility Controller. One computer is present in the network providing network services such as DHCP, TFTP, HTTP and RADIUS.

2.2. Remote Site

The Remote Site of two Avaya 3631 Wireless IP Telephones, four Avaya 9600 Series IP Telephones, two H.323 and two SIP, one Aruba RAP-5, one laptop and one PC on the data network.

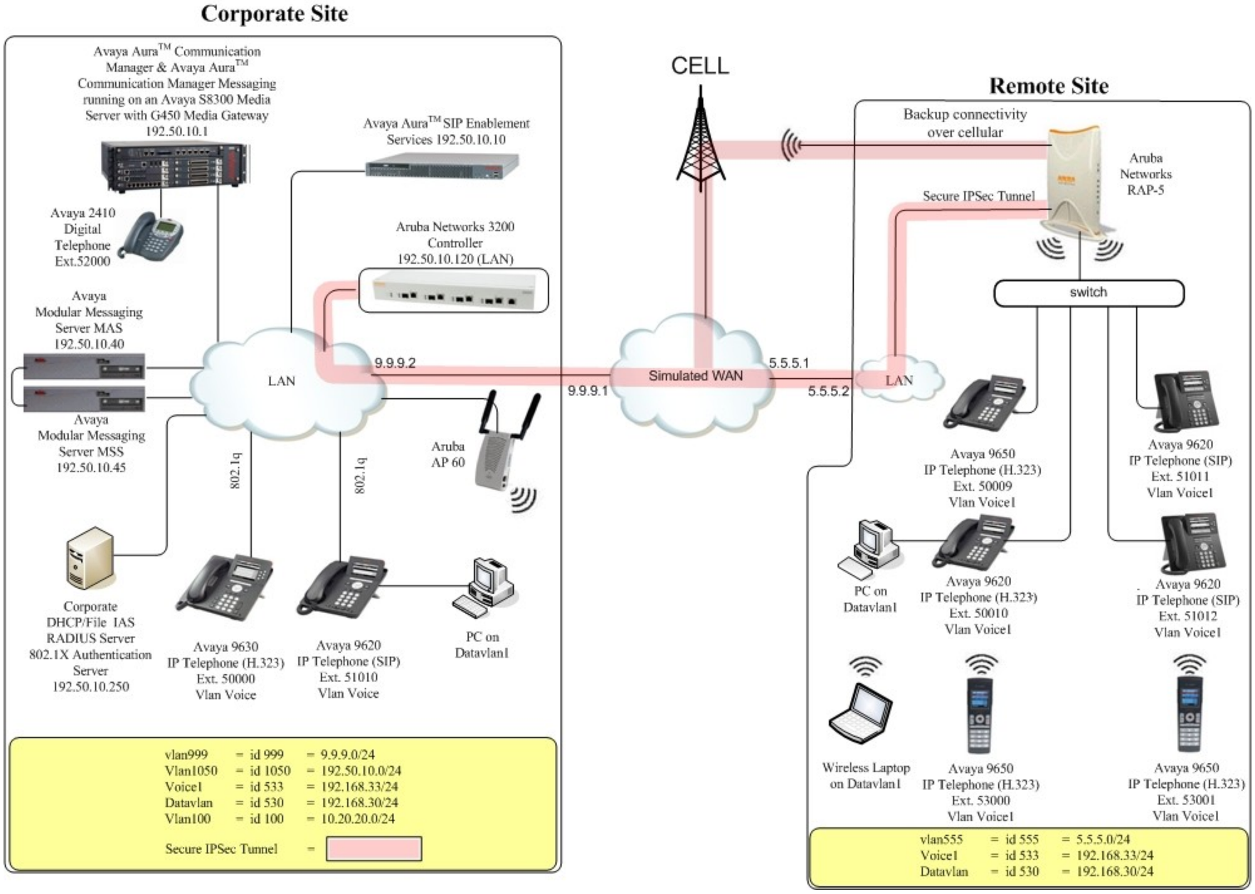

Corporate Site
Avaya Aura^{TM} Communication Manager & Avaya Aura^{TM} Communication Manager Messaging running on an Avaya S8300 Media Server with G450 Media Gateway 192.50.10.1
Avaya Aura^{TM} SIP Enablement Services 192.50.10.10
Avaya 2410 Digital Telephone Ext.52000
Aruba Networks 3200 Controller 192.50.10.120 (LAN)
Avaya Modular Messaging Server MAS 192.50.10.40
Avaya Modular Messaging Server MSS 192.50.10.45
LAN
9.9.9.2
9.9.9.1
802.1q
802.1q
Aruba AP 60
Corporate DHCP/File IAS RADIUS Server 802.1X Authentication Server 192.50.10.250
Avaya 9630 IP Telephone (H.323) Ext. 50000 Vlan Voice
Avaya 9620 IP Telephone (SIP) Ext. 51010 Vlan Voice
PC on Datavlan1
vlan999 = id 999 = 9.9.9.0/24
Vlan1050 = id 1050 = 192.50.10.0/24
Voice1 = id 533 = 192.168.33/24
Datavlan = id 530 = 192.168.30/24
Vlan100 = id 100 = 10.20.20.0/24
Secure IPSec Tunnel =
CELL
Simulated WAN
5.5.5.1
5.5.5.2
Remote Site
Backup connectivity over cellular
Secure IPSec Tunnel
Aruba Networks RAP-5
switch
LAN
Avaya 9650 IP Telephone (H.323) Ext. 50009 Vlan Voice1
Avaya 9620 IP Telephone (SIP) Ext. 51011 Vlan Voice1
PC on Datavlan1
Avaya 9620 IP Telephone (H.323) Ext. 50010 Vlan Voice1
Avaya 9620 IP Telephone (SIP) Ext. 51012 Vlan Voice1
Wireless Laptop on Datavlan1
Avaya 9650 IP Telephone (H.323) Ext. 53000 Vlan Voice1
Avaya 9650 IP Telephone (H.323) Ext. 53001 Vlan Voice1
vlan555 = id 555 = 5.5.5.0/24
Voice1 = id 533 = 192.168.33/24
Datavlan = id 530 = 192.168.30/24

Figure 1: Avaya and Aruba Networks Wireless LAN Configuration

3. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya PBX Products	
Avaya S8300 Server running Avaya Aura™ Communication Manager	Avaya Aura™ Communication Manager 5.2.1
Avaya G450 Media Gateway (Corporate Site) MGP MM712 DCP Media Module	 28.22.0 HW9
Avaya Aura™ SIP Enablement Services (SES)	
Avaya Aura™ SIP Enabled Services (SES) Server	5.2.1
Avaya Messaging (Voice Mail) Products	
Avaya Modular Messaging - Messaging Application Server (MAS)	5.0
Avaya Modular Messaging - Message Storage Server (MSS)	5.0
Avaya Aura™ Communication Manager Messaging (CMM)	5.2.1-13.0
Avaya Telephony Sets	
Avaya 9600 Series IP Telephones	Avaya one-X Deskphone Edition 3.0.1
Avaya 9600 Series IP Telephones	Avaya one-X Deskphone SIP 2.4
Avaya 2410 Digital Telephone	5.0
Aruba Products	
Aruba Networks 3200 Controller	ArubaOS version 5.0
Aruba Networks RAP-5	ArubaOS version 5.0
MS Products	
Microsoft Windows 2003 Server	Microsoft Windows 2003 Server

4. Configure Avaya Aura™ Communication Manager

This section describes the steps required for Communication Manager to support the configuration shown in **Figure 1**. The following pages provide instructions on how to administer the required configuration parameters. The assumption is that the appropriate license and authentication files have been installed on the servers and that login and password credentials are available. It is assumed that the reader has a basic understanding of the administration of Communication Manager and has access to the System Administration Terminal (SAT) screen. For detailed information on the installation, maintenance, and configuration of Communication Manager, please consult references in **Section 9 [1]** through **[4].**

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. QoS is now utilized to prioritize VoIP traffic and should be implemented throughout the entire network.

In order to achieve prioritization of VoIP traffic, the VoIP traffic must be classified. The Avaya Telephony Infrastructures supports both 802.1p and DiffServ.

There were two ip-network-region's used for this sample configuration, one for Avaya wired IP Telephones and one for Avaya wireless IP Telephones. The DiffServ and 802.1p/Q values configured here will be downloaded to the Avaya H.323 IP wired and wireless Telephones via Communication Manager. Avaya SIP IP Telephones will get QoS settings by downloading the 46xxsettings file from the HTTP server (not shown in this document). For more information on QoS settings please refer to **Section 9 [1]** through **[4]**.

4.1. Configure the ip-network-region for wired IP Telephones

The Differentiated Services Code Point (DSCP) value of 46 will be used for both PHB values. DSCP 46 represents the traffic class of premium and the traffic type voice. Set the **Call Control PHB Value** to **46** and the **Audio PHB Value** to **46**. **Call Control 802.1p Priority** and **Audio 802.1p Priority** are set to **6**.

1. From the SAT, use the **change ip-network-region 1** command to change the DIFFSERV/TOS PARAMETERS and 802.1P/Q PARAMETERS settings. Change the following:

- **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: dev4.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
```

2. On **Page 3,** add the following options for **des rgn**:

- **codec** set set to **1**

Note: direct WAN, Units and IGAR will propagate automatically, hit Esc, e to continue

```
change ip-network-region 1                                      Page   3 of  19

 Source Region: 1     Inter Network Region Connection Management     I       M
                                                                     G  A    e
 dst codec direct   WAN-BW-limits   Video      Intervening      Dyn  A  G    a
 rgn  set   WAN  Units   Total Norm  Prio Shr Regions         CAC  R  L    s
 1    1                                                                all
 2
 3    1     y    NoLimit                                            n
```

4.2. Configure the ip-network-region for the Wireless IP Telephones

The Differentiated Services Code Point (DSCP) value of 52 will be used for both PHB values. DSCP 52 represents the traffic class of premium and the traffic type voice. Set the **Call Control PHB Value** to **52** and the **Audio PHB Value** to **52**. **Call Control 802.1p Priority** and **Audio 802.1p Priority** are set to **6**.

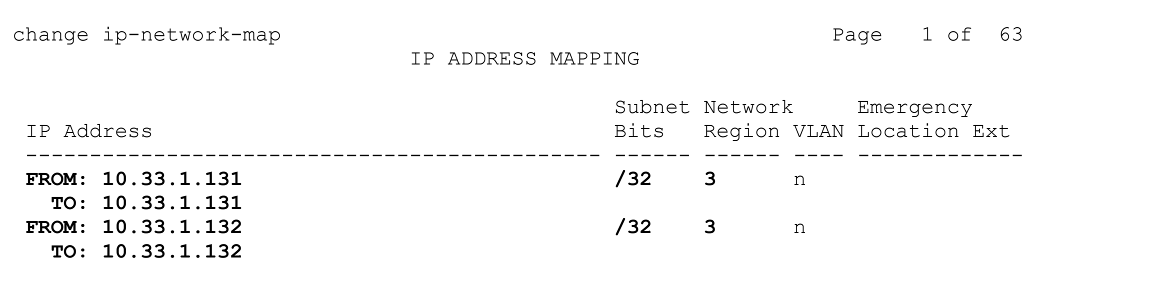
1. From the SAT, use the **change ip-network-region 3** command to change the DIFFSERV/TOS PARAMETERS and 802.1P/Q PARAMETERS settings. Change the following:

- **Call Control PHB Value** set to **52**
- **Audio PHB Value** set to **52**
- **Call Control 802.1p** set to **6**
- **Audio 802.1p priority** set to **6**

```
change ip-network-region 3                                     Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: dev4.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: 52      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 52       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
```

4.3. Configure the wireless Avaya IP Telephones to use ip-network-region 3

The Avaya 3631 Wireless IP Telephones use Wi-Fi Multimedia (WMM), for Quality of Service. WMM puts DSCP value 46 in the video queue and needs to be changed to 52 so the traffic is placed in the voice queue. This step is needed to assign the Avaya 3631 Wireless IP Telephones to use the ip-network-region 3 and DSCP value 52, configured in **Section 4.2, Step 1**.

Step	Description
1.	From the SAT, use the **change ip-network map** command to add the IP address of the Avaya 3631 Wireless IP Telephones individually or the subnet of where all of the Avaya 3631 Wireless IP Telephones reside. For compliance each Avaya 3631 Wireless IP Telephone was entered individually. • **FROM:** set to **IP address** of the Avaya 3631 Wireless IP Telephone • **TO:** set to **IP address** of the Avaya 3631 Wireless IP Telephone • **Subnet Bites:** set to **32** • **Network Region:** set to **3**
	

```
change ip-network-map                                           Page   1 of  63
                               IP ADDRESS MAPPING

                                               Subnet Network     Emergency
 IP Address                                    Bits   Region VLAN Location Ext
 --------------------------------------------- ------ ------ ---- -------------
 FROM: 10.33.1.131                             /32    3      n
   TO: 10.33.1.131
 FROM: 10.33.1.132                             /32    3      n
   TO: 10.33.1.132
```

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 3200 controller configuration guide.

5.1. Accessing the Aruba 3200 Controller CLI

Serial Console

Using a standard RS-232 cable, connect the Aruba mobility controller to the serial port of a terminal or PC. Run a terminal emulation program with the following configuration:

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

Use this mode of connection during the initialization phase of the controller to configure login credentials. Connections via SSH "ssh admin@<switch IP address>" and WEB "https://<ip_address_of_controller>:4343" can be used after the basic information, i.e., IP Address, is configured.

User: **admin**
Password: ***** < Refer to **Section 9, [8]** & **[9]** for password information.
(Aruba3200) >**enable**
Password:****** < Refer to **Section 9, [8]** & **[9]** for password information.
(Aruba3200) #

5.2. Creating VLANs and IP addresses:

Configure the following information:

- Create VLAN 1050 for management functions.
- Create VLAN 533 for voice users and traffic.
- Create VLAN 530 for data users and traffic.
- Configure loopback Address
- Add the default gateway

```
(Aruba3200) # configuration terminal
(Aruba3200) (config) # vlan 1050
(Aruba3200) (config) # interface vlan 1050
(Aruba3200) (config-subif)# description management
(Aruba3200) (config-subif)# no shutdown
(Aruba3200) (config-subif)# ip address 192.50.10.121 255.255.255.0
(Aruba3200) (config-subif)# ip helper-address  192.50.10.250
(Aruba3200) (config-subif)# !
(Aruba3200) (config) # vlan 533
(Aruba3200) (config) # interface vlan 533
(Aruba3200) (config-subif)# description voice
(Aruba3200) (config-subif)# no shutdown
(Aruba3200) (config-subif)# ip address 192.168.33.120 255.255.255.0
(Aruba3200) (config-subif)# ip helper-address  192.50.10.250
(Aruba3200) (config-subif)# !
(Aruba3200) (config) # vlan 530
(Aruba3200) (config) # interface vlan 530
(Aruba3200) (config-subif)# description data
(Aruba3200) (config-subif)# no shutdown
(Aruba3200) (config-subif)# ip address 192.168.30.120 255.255.255.0
(Aruba3200) (config-subif)# ip helper-address  192.50.10.250
(Aruba3200) (config-subif)# !
(Aruba3200) (config) # interface loopback 192.50.10.120
(Aruba3200) (config) # ip default-gateway 192.50.10.1
(Aruba3200) (config-subif)# !
```

5.3. Assigning physical ports on the controller

This topology assumes a single leg uplink from the controller into the corporate LAN. This port should be able to carry management and user VLAN traffic.

```
(Aruba3200) (config)# interface gigabitethernet 3/0
(Aruba3200) (config-if)# description controller-uplink
(Aruba3200) (config-if)# no shutdown
(Aruba3200) (config-if)# trusted
(Aruba3200) (config-if)# switchport trunk allowed vlan 1050,530,533
(Aruba3200) (config-if)# switchport trunk native vlan 1050
(Aruba3200) (config-if)# !
```

The Remote AP will attempt to reach the controller from the internet on UDP port 4500. So the corporate firewall should be made to forward all traffic to UDP 4500 to the controller. This UDP port will also serve user traffic.

If the controller is directly connected to the internet, create a new VLAN on the controller, assign an access-mode port to it and assign a static IP address to it. The default gateway of the controller should then be modified to the internet gateway. Please refer to the Aruba Virtual Branch Networks Validated Reference Design, http://www.arubanetworks.com/pdf/technology/VBN_VRD.pdf for comprehensive best practices.

5.4. Creating an IPSec L2TP Pool for RAPs:

The RAPs secure data over the WAN using IPSec tunnels. The RAPs get assigned an L2TP IP address for packets inside the tunnel (these addresses do not need to be externally routable). The controller acts as a DHCP server to administer IP addresses from this pool. This operation is quite similar to a traditional VPN client.

```
(Aruba3200) (config) # ip local pool remote-ap 10.1.1.1 10.1.1.100
```

5.5. Role-based Access Control Framework

This section enables the infrastructure to define the traffic handling for voice and data clients. This involves creating a session ACL, assigning rules to the session and assigning the ACL to the user-role created for the users.

5.5.1. Creating a firewall ACL for phones

```
(Aruba3200) (config) # ip access-list session rap-voice
(Aruba3200) (config-sess-rap-voice)# any any svc-sip-udp permit queue high tos 46
dot1p-priority 6
(Aruba3200) (config-sess-rap-voice)# any any svc-sip-tcp permit queue high tos 46
dot1p-priority 6
Aruba3200) (config-sess-rap-voice)# any any svc-sips permit queue high tos 46 dot1p-
priority 6
(Aruba3200) (config-sess-rap-voice)# any any svc-h323-udp permit queue high tos 46
dot1p-priority 6
(Aruba3200) (config-sess-rap-voice)# any any svc-h323-tcp permit queue high tos 46
dot1p-priority 6
(Aruba3200) (config-sess-rap-voice)# alias voice-subnet any any permit queue high tos
46 dot1p-priority 6
(Aruba3200) (config-sess-rap-voice)# any alias voice-subnet any permit queue high tos
46 dot1p-priority 6
(Aruba3200) (config-sess-rap-voice)# any any svc-http permit queue high tos 46 dot1p-
priority 6
(Aruba3200) (config-sess-rap-voice)# any any svc-icmp permit
(Aruba3200) (config-sess-rap-voice)# any any svc-dhcp permit queue high tos 46 dot1p-
priority 6
(Aruba3200) (config-sess-rap-voice)# any any svc-dns permit queue high tos 46 dot1p-
priority 6
(Aruba3200) (config-sess-rap-voice)# !
```

5.5.2. Creating a firewall ACL for data-clients

```
(Aruba3200) (config) # ip access-list session rap-data
(Aruba3200) (config-sess-rap-voice)# any any any permit
(Aruba3200) (config-sess-rap-voice)# !
```

5.5.3. Creating a user-role for voice clients on RAP

```
(Aruba3200) (config) # user-role rap-voice
(Aruba3200) (config-role) #access-list session rap-voice
(Aruba3200) (config-role) # !
```

5.5.4. Creating a user-role for data clients on RAP

```
(Aruba3200) (config) # user-role rap-data
(Aruba3200) (config-role) # access-list session rap-data
(Aruba3200) (config-role) # !
```

5.6. Authentication Framework

Now that user-roles have been defined, this section defines the authentication mechanisms for wired and wireless clients to get assigned those user-roles. Wired phones are Avaya phones and hence each deployment would have a determinate set of MAC OUIs. The first 6 octets of the client are used to identify wired phones and assign them the rap-voice role. Wireless clients use 802.1x to authenticate against a RADIUS server. Based on the success of 802.1x authentication the Aruba wireless infrastructure assigns a client the rap-voice role. In case of both wired and wireless, it is assumed that clients that fail the criteria for rap-voice would get assigned rap-data roles. Wireless phones will be configured to use EAP-PEAP with inner-EAP type mschapv2.

5.6.1. Creating a user-derivation rule for wired phones

```
(Aruba3200) (config) # aaa derivation-rules user rap-voice
(Aruba3200) (user-rule) # set role condition macaddr starts-with xx:xx:xx set-value
rap-voice
(Aruba3200) (user-rule) # set role condition macaddr starts-with yy:yy:yy set-value
rap-voice
(Aruba3200) (user-rule) # !
```

5.6.2. Creating an AAA Profile for wired phones

```
(Aruba3200) (config) # aaa profile rap-wired-voice
(Aruba3200) (AAA Profile "rap-wired-voice ") # initial-role rap-data
(Aruba3200) (AAA Profile "rap-wired-voice ") # user-derivation-rules rap-voice
(Aruba3200) (AAA Profile "rap-wireless-voice-wpa2") # !
```

5.6.3. Creating RADIUS server instance for wireless 802.1x phones

```
(Aruba3200) (config) # aaa authentication-server radius aruba-devcon
(Aruba3200) (RADIUS Server "aruba-devcon") # host 192.50.10.250
(Aruba3200) (RADIUS Server "aruba-devcon") # key arubademo
(Aruba3200) (RADIUS Server "aruba-devcon") # enable
(Aruba3200) (RADIUS Server "aruba-devcon") # !
```

Note: The same key must be used for the RADIUS client definition on the RADIUS server.

5.6.4. Creating an authentication server group for wireless 802.1x phones

```
(Aruba3200) (config) # aaa server-group aruba-devcon
(Aruba3200) (Server Group "aruba-devcon") # auth-server aruba-devcon
(Aruba3200) (Server Group "aruba-devcon") # !
```

5.6.5. Creating a L2 802.1x Authentication Profile for wireless dot1x phones

```
(Aruba3200) (config) # aaa authentication dot1x "rap-voice-dot1x"
(Aruba3200) (802.1X Authentication Profile "rap-voice-dot1x") # validate-pmkid
(Aruba3200) (802.1X Authentication Profile "rap-voice-dot1x") # termination eap-type
eap-peap
(Aruba3200) (802.1X Authentication Profile "rap-voice-dot1x") # termination inner-eap-
type eap-mschapv2
(Aruba3200) (802.1X Authentication Profile "rap-voice-dot1x") # !
```

5.6.6. Creating an AAA Profile for wireless phones

```
(Aruba3200) (config) # aaa profile rap-wireless-voice-wpa2
(Aruba3200) (AAA Profile "rap-wireless-voice-wpa2") # initial-role rap-data
(Aruba3200) (AAA Profile "rap-wireless-voice-wpa2") # authentication-dot1x rap-voice-
dot1x
(Aruba3200) (AAA Profile "rap-wireless-voice-wpa2") # dot1x-default-role rap-voice
(Aruba3200) (AAA Profile "rap-wireless-voice-wpa2") # dot1x-server-group aruba-devcon
(Aruba3200) (AAA Profile "rap-wireless-voice-wpa2") # !
```

5.7. Wireless Phone Connectivity to RAP

This section defines the wireless parameters to be configured to maintain a reliable link between wireless phones and the access point. A SSID profile is created with best-practice settings. High-throughput is disabled on this SSID, even though it is enabled on the radio, so that all transmissions to and from these voice clients will use legacy methods. A virtual-AP profile is created to tie the SSID profile with the authentication profile and define the forwarding mode for packets as split-tunnel.

5.7.1. Create an SSID Profile for the phones

```
(Aruba3200) (config) # wlan ssid-profile avaya-voice
(Aruba3200) (SSID Profile "avaya-voice") # opmode wpa2-aes
(Aruba3200) (SSID Profile "avaya-voice") # max-retries 3
(Aruba3200) (SSID Profile "avaya-voice") # max-tx-fail 20
(Aruba3200) (SSID Profile "avaya-voice") # dtim-period 2
(Aruba3200) (SSID Profile "avaya-voice") # mcast-rate-opt
(Aruba3200) (SSID Profile "avaya-voice") # no short-preamble
(Aruba3200) (SSID Profile "avaya-voice") # wmm
(Aruba3200) (SSID Profile "avaya-voice") # wmm-uapsd
(Aruba3200) (SSID Profile "avaya-voice") # wmm-vo-dscp 46
(Aruba3200) (SSID Profile "avaya-voice") # strict-svp
(Aruba3200) (SSID Profile "avaya-voice") # essid avaya-voice
(Aruba3200) (SSID Profile "avaya-voice") # a-tx-rates 6 9 12 18 24 36 48 54
(Aruba3200) (SSID Profile "avaya-voice") # g-basic-rates 5
(Aruba3200) (SSID Profile "avaya-voice") # g-tx-rates 5 6 11 12 18 24 36 48 54
(Aruba3200) (SSID Profile "avaya-voice") # !
```

5.7.2. Create a high-throughput SSID profile for the phones

```
(Aruba3200) (config) # wlan ht-ssid-profile ht-disabled
(Aruba3200) (High-throughput SSID profile "ht-disabled") # no high-throughput-enable
(Aruba3200) (High-throughput SSID profile "ht-disabled") # no 40MHz-enable
(Aruba3200) (High-throughput SSID profile "ht-disabled") # no mpdu-agg
(Aruba3200) (High-throughput SSID profile "ht-disabled") # !
```

5.7.3. Assign the high-throughput SSID profile to the SSID profile

```
(Aruba3200) (config) # wlan ssid-profile avaya-voice
(Aruba3200) (SSID Profile "avaya-voice") # ht-ssid-profile ht-disabled
(Aruba3200) (SSID Profile "avaya-voice") # !
```

5.7.4. Create a virtual-AP for the wireless phones

```
(Aruba3200) (config) # wlan virtual-ap avaya-voice
(Aruba3200) (Virtual AP profile "avaya-voice") # vlan 533
(Aruba3200) (Virtual AP profile "avaya-voice") # aaa-profile rap-wireless-voice-wpa2
(Aruba3200) (Virtual AP profile "avaya-voice") # ssid-profile avaya-voice
(Aruba3200) (Virtual AP profile "avaya-voice") # allowed-band g
(Aruba3200) (Virtual AP profile "avaya-voice") # forward-mode split-tunnel
(Aruba3200) (Virtual AP profile "avaya-voice") # !
```

5.8. Radio Configuration on RAP for Wireless Phones:

The radio profile is common to all SSIDs on the RAP. So high-throughput must be enabled if data clients require 802.11n connectivity. In most cases, one can use the default Radio-profile, HT-Radio profile and ARM profile and modify them as required. If there are multiple AP-groups on the network that require different radio profiles, please ensure the following radio-configuration options are in place for voice operation. This section also lists the Adaptive Radio Management (ARM) settings that must be in place. Please refer to the ArubaOS configuration guide and Validated Reference Design Guide for Mobile Devices for best-practices.

5.8.1. Enable legacy station workaround on the radios

```
(Aruba3200) (config) # rf ht-radio-profile default-g
(Aruba3600) (High-throughput radio profile "default-g") # single-chain-legacy
(Aruba3600) (High-throughput radio profile "default-g") # !
(Aruba3200) (config) # rf ht-radio-profile default-a
(Aruba3600) (High-throughput radio profile "default-a") # single-chain-legacy
(Aruba3600) (High-throughput radio profile "default-a") # !
```

5.8.2. Enable Voice-aware and Power-save-aware ARM scanning

```
(Aruba3200) (config) # rf arm-profile default
(Aruba3200) (ARM-profile “default”) # voip-aware-scan
(Aruba3200) (ARM-profile “default”) # power-save-aware scan
(Aruba3200) (ARM-profile “default”) #!
(Aruba3200) (ARM-profile “default”) # write memory
```

5.8.3. Save the configuration

```
(Aruba3200) (config) # write memory
```

5.9. Wired Phone Connectivity to RAP

Downlink to Switch: The branch topology assumes a managed L2 switch connected to ports 1-4 of the RAP5. Phones and data clients are connected to the switch. The Avaya phones are capable of dot1q VLAN tagging and hence would tag their traffic as VLAN 533. Any data clients connecting to the switch would get assigned a native VLAN 530. The uplink from the switch to the RAP is a trunk port with these two VLANs.

5.9.1. Wired AP profile

```
(Aruba3200) (config) # ap wired-ap-profile rap-downlink
(Aruba3200) (Wired AP profile "rap-downlink") # forward-mode split-tunnel
(Aruba3200) (Wired AP profile "rap-downlink") # switchport trunk allowed vlan 530,533
(Aruba3200) (Wired AP profile "rap-downlink") # switchport trunk native vlan 530
(Aruba3200) (Wired AP profile "rap-downlink") # wired-ap-enable
(Aruba3200) (Wired AP profile "rap-downlink") # !
```

5.9.2. Wired Port profile

```
(Aruba3200) (config) # ap wired-port-profile rap-downlink
(Aruba3200) (AP wired port profile "rap-downlink") # wired-ap-profile rap-downlink
(Aruba3200) (AP wired port profile "rap-downlink") # aaa-profile rap-wired-voice
(Aruba3200) (AP wired port profile "rap-downlink") # no shutdown
(Aruba3200) (AP wired port profile "rap-downlink") # !
```

5.10. AP System Configuration:

Uplink to internet: The RAP uses port 0 as its uplink to the internet. This port is a trusted access port.

5.10.1. Wired AP profile

```
(Aruba3200) (config) # ap wired-ap-profile rap-uplink
(Aruba3200) (Wired AP profile "rap-uplink") # trusted
(Aruba3200) (Wired AP profile "rap-uplink") # wired-ap-enable
(Aruba3200) (Wired AP profile "rap-uplink") # !
```

5.10.2. Wired Port profile

```
(Aruba3200) (config) # ap wired-port-profile rap-uplink
(Aruba3200) (AP wired port profile "rap-uplink") # wired-ap-profile rap-uplink
(Aruba3200) (AP wired port profile "rap-uplink") # no shutdown
(Aruba3200) (AP wired port profile "rap-uplink") # !
```

5.10.3. AP Provisioning Profile

This step is primarily to configure the USB type that will be used for cellular backhaul. Executing ‘usb-type ?’ will produce a list of options. Also, link-priority between Ethernet and cellular backhaul is configured here. Higher the priority value, higher the precedence. Alternately, this provisioning can be done on a per-AP basis on the AP Provisioning page once the AP has initialized on an Ethernet backhaul.

```
(Aruba3200) (config) # ap provisioning-profile default
(Aruba3200) (Provisioning profile "default") # remote-ap
(Aruba3200) (Provisioning profile "default") # master <controller ip>
(Aruba3200) (Provisioning profile "default") # usb-type option
(Aruba3200) (Provisioning profile "default") # link-priority-ethernet 1
(Aruba3200) (Provisioning profile "default") # !
```

5.11. Configuring the AP-Group

This step assigns the virtual-AP and the port profiles to the RAP.

```
(Aruba3200) (config) # ap-group remote-ap
(Aruba3200) (AP group "remote-ap") # virtual-ap avaya-voice
(Aruba3200) (AP group "remote-ap") # enet0-port-profile rap-uplink
(Aruba3200) (AP group "remote-ap") # enet2-port-profile rap-downlink
(Aruba3200) (AP group "remote-ap") # enet3-port-profile rap-downlink
(Aruba3200) (AP group "remote-ap") # enet4-port-profile rap-downlink
(Aruba3200) (AP group "remote-ap") # provisioning-profile default
(Aruba3200) (AP group "remote-ap") # !
```

5.12. Configuration for RAP Uplink bandwidth reservation:

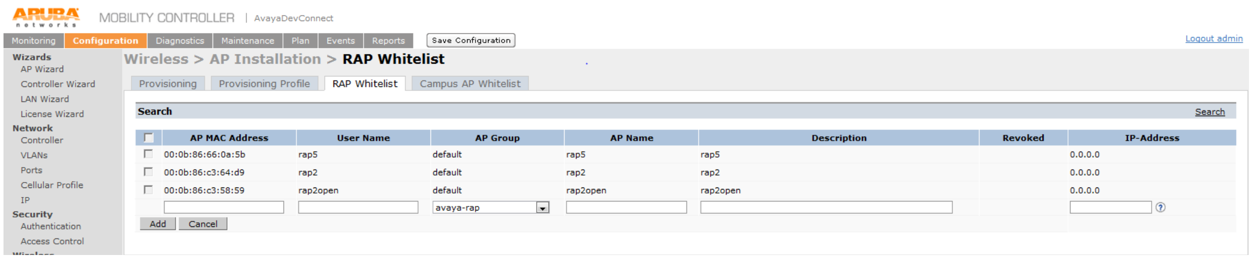
This step reserves uplink bandwidth for priority voice traffic. The tests assumed that the RAP had a total uplink bandwidth of 20 Mbps of which 5 Mbps was to be reserved for voice. In a deployment, the uplink would typically be around 10 Mbps. A reservation of 1 Mbps for voice should be sufficient to accommodate the voice traffic for 10 calls reliably.

```
(Aruba3200) (config) # ap system-profile rap-uplink
(Aruba3200) (AP system profile "rap-uplink") # rap-bw-total 20000
(Aruba3200) (AP system profile "rap-uplink") # rap-bw-resv-1 acl rap-voice 5000
priority 1
(Aruba3200) (AP system profile "rap-uplink") # !
(Aruba3200) (config) # ap-group remote-ap
(Aruba3200) (AP group "remote-ap") #ap-system-profile rap-uplink
(Aruba3200) (AP group "remote-ap") #!
```

5.13. AP Provisioning: Adding a RAP to the controller Whitelist

From a PC on Vlan1050, open a web-browser and input the IP address of the Aruba controller, assigned in **Section 5.3**, into the URL address, http://192.50.10.121, login using appropriate login credentials. Input the appropriate login credentials, which can be obtained by reading the Aruba documents found in **Section 10** [**5**].

- On the controller WebUI, navigate to **Configuration → AP Installation**.
- Go to the RAP Whitelist tab.
- Click '**New**'. Add the RAP MAC address, a user-name and specify the AP-Group from the drop-down list.
- Click '**Add**' and '**Save Configuration**'.



□	AP MAC Address	User Name	AP Group	AP Name	Description	Revoked	IP-Address
□	00:0b:86:66:0a:5b	rap5	default	rap5	rap5		0.0.0.0
□	00:0b:86:c3:64:d9	rap2	default	rap2	rap2		0.0.0.0
□	00:0b:86:c3:58:59	rap2open	default	rap2open	rap2open		0.0.0.0
			avaya-rap				

5.14. Initializing the Remote AP

Configure the Aruba RAP-5 with the following:

- Connect the AP's port 0 to the internet at the remote location.
- Connect a computer to port 1.
- Wait till the AP boots. Ensure that the computer gets a 192.168.11.x IP address. Open a browser window on the computer.
- The browser should redirect to **rapconsole.arubanetworks.com**
- Type in the IP address of the controller (should be routable over the internet).
- Follow the prompts as the AP attempts to reach the controller, upgrades image and reboots.
- Plug a Layer-2 switch to Ethernet port 1-4. Connect phones to the switch or directly to the AP.

6. General Test Approach and Test Results

6.1. General Test Approach

All feature functionality test cases were performed manually. The general test approach entailed verifying the following:

- Registration, re-registration of the wired and wireless Avaya IP Telephone from the remote site through the VPN using Aruba Networks Remote Access Point Solution with Communication Manager (H.323 Endpoints) and SIP Enablement Services (SIP Endpoints).
- Verify Message Waiting Indicator and message retrieval from Modular Messaging Server & Communication Manager Messaging
- VoIP calls between all Avaya Digital Telephones, Avaya SIP and Avaya H.323 IP Telephones.
- Inter-office calls using SIP, G.711 codec, shuffling, conferencing, voice mail, DTMF and sending low priority data traffic over the LAN.
- Wireless Security, Wireless Authentication and Wireless Quality of Service.
- Verifying that QoS directed the voice signaling and voice media to the higher priority queues for wireless and wired Avaya endpoints.
- Failover to GSM network (See Observations in **Section 6.3**)
- 802.1x Authentication using RADIUS (3631 only)
- WPA2 Enterprise Encryption (3631 only)

6.2. Test Results

All feature functionality, serviceability, and performance test cases passed. The Aruba Networks Remote Access Point Solution consisting of Aruba 3200 Controller and RAP-5 Access Point with GSM failover, (See **Observation**s in **Section 6.3**), yielded good voice quality and no calls were lost. The stability of the Avaya/Aruba solution was successfully verified through performance and serviceability testing.

The Avaya wired and wireless IP Telephones from the remote site registered with Communication Manager (H.323 Endpoints) and SIP Enablement Services (SIP Endpoints) utilizing Aruba Networks Remote Access Point Solution consisting of Aruba 3200 Controller and RAP-5 Access Point with GSM failover passed all test cases. The compliance testing also focused on verifying Quality of Service, WMM for wireless and Layer 2 Priority (802.1p) and Layer 3 Differentiated Services (DiffServ) for wired endpoints for voice traffic. Multiple security schemas, OPEN and WPA2-AES-CCMP with 802.1x Authentication and G7.11MU codec were used for testing. Telephone calls were verified to operate correctly with the media path direct between the telephones (shuffling enabled) and with the media path centralized through Communication Manager (shuffling disabled). Calls were maintained for durations over one minute without degradation to voice quality. Failover testing verified that when the WAN connection is lost, the Aruba RAP-5 access Point with a GSM card, setup a VPN from the Remote Site to the Corporate Site over the to GSM network, (See Observations in Section).

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, pick groups, call pickup, bridged appearance alerting, voicemail using Modular Messaging & Communication Manager Messaging, MWI, hold and return from hold.

6.3. Observations

It needs to be noted that failover capabilities will vary depending on the signal strength and Cell plans. The Signal strength observer during compliance testing was 87dbm.

- There were 6 wired Avaya IP telephones, 2 wireless Avaya IP telephones and 1 PC running Avaya Softphone registered to the Communication Manager (H.323 Endpoints) and SIP Enablement Services (SIP Endpoints).

- The amount of calls able to be made varied from 1 to 5 active calls.

- Failover times to GSM constantly took about 1.25 minutes.

- Failover times back from GSM constantly took about 2.30 minutes.

- The amount of calls able to be made varied from 1 to 5 active calls before the GSM connection would drop. On average, 1 to 2 calls could be made before the GSM connection would drop.

7. Verification Steps

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

- Place calls to and from all wired and wireless Avaya IP Telephones and verify two-way audio.

- Place a calls to the wired and wireless Avaya IP Telephones in the Remote Site, allow the calls to be directed to voicemail, leave a voicemail message and verify the MWI message is received.

- From Avaya IP Telephones in the Remote Site, connect to the voicemail system to retrieve the voicemail and verify the MWI message clears.

- From Avaya IP Telephones in the Remote Site, exercise calling features such as transfer, conference and hold.

- Place calls between the corporate and remote sites and verify good voice quality in both directions.

- Check that the Avaya wired & wireless IP Telephones a have successfully registered with Communication Manager (H.323 Endpoints), by typing the **list registered-ip-station** command on the SAT prompt.

8. Conclusion

These Application Notes illustrate the procedures necessary for configuring Aruba Networks Remote Access Point Solution using the Aruba 3200 Controller and RAP-5 Access Point with an Avaya Aura™ Telephony Infrastructure using Avaya Aura™ Communication Manager, Avaya Aura™ SIP Enablement Services, Avaya Modular Messaging, Avaya Aura™ Communication Manager Messaging, Avaya 3631 Wireless IP Telephones and Avaya 9600 Series IP Telephones. All feature functionality test cases described in **Section 6.1** passed.

9. Additional References

Avaya documentation was obtained from http://support.avaya.com.

[1] *Administering Avaya Aura™ Communication Manager,* May 2009, Issue 5.0, Document Number 03-300509..

[2] *Administering Avaya Aura™ SIP Enablement Services*, May 2009, Issue 2.1, Document 03-602508.

[3] *Avaya Aura™ SIP Enablement Services (SES) Implementation Guide*, May 2009, Issue 6, Document 16-300140.

[4] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 3.0,* Document Number 16-300698.

[5] *Avaya one-X Deskphone SIP for 9600 Series IP Telephones Administrator Guide, Release 2.0,* Document Number 16-601944.

[6] *Modular Messaging, Release 5.0 with the Avaya MSS Messaging Application Server (MAS) Administration Guide,* January 2009.

[7] *Avaya* Aura™ *Communication Manager Messaging Application Release* 5.1 *Administering. Communication Manager Servers to Work with IA 770*, June 2008.

The following Aruba Validated Reference Design Guides can be found at http://www.arubanetworks.com/technology/design_guides.php

[8] Virtual Branch Networks Validated Reference Design v3.0RN

[9] Optimizing Aruba WLANs for Roaming Devices v3.3

Aruba configuration notes can be found on the Aruba support site https://support.arubanetworks.com/

The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.