



Avaya Solution & Interoperability Test Lab

Application Notes for a Ruckus Wireless Solution consisting of the Ruckus ZoneDirector Controller and Ruckus ZoneFlex 2942 Access Points with an Avaya Telephony Infrastructure with Avaya Communication Manager Branch Edition in a Converged VoIP and Data Network - Issue 1.0

Abstract

These Application Notes describe a solution for supporting wireless voice traffic in an Avaya IP Telephony infrastructure using a Ruckus Wireless Solution, consisting of a Ruckus ZoneDirector 1000 controller managing multiple Ruckus ZoneFlex 2942 Access Points. Avaya 3600 Series Wireless IP Telephones gained network access through the Ruckus ZoneFlex 2942 Access Points and registered with Avaya Communication Manager Branch Edition (formally known as Avaya Distributed Office). Emphasis of the testing was placed on verifying prioritization of VoIP traffic on calls associated with the Avaya 3600 Series Wireless IP Telephones.

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 a solution for supporting wireless voice traffic in an Avaya IP Telephony infrastructure using a Ruckus ZoneDirector 1000 controller managing multiple Ruckus ZoneFlex 2942 Access Points. The Ruckus ZoneFlex 2942 Access Points connected the Avaya 3600 Series Wireless IP Telephones to the wired network and allowed them to register with Avaya Communication Manager Branch Edition. Emphasis of the testing was placed on verifying prioritization of VoIP traffic on calls associated with the Avaya wireless IP telephones.

1.1. Network Diagram

The network diagram shown in **Figure 1** illustrates the environment used for compliance testing. The network consists of an Avaya Communication Manager Branch Edition, two Avaya 3631 Wireless IP Telephones, one Avaya one-X 9630 Deskphone Edition IP Telephone, one Avaya one-X 9620 Deskphone Edition IP Telephone, one Ruckus ZoneDirector 1000 controller and three Ruckus ZoneFlex 2942 Access Points. One computer is present in the network providing network services such as DHCP, TFTP, HTTP and RADIUS.

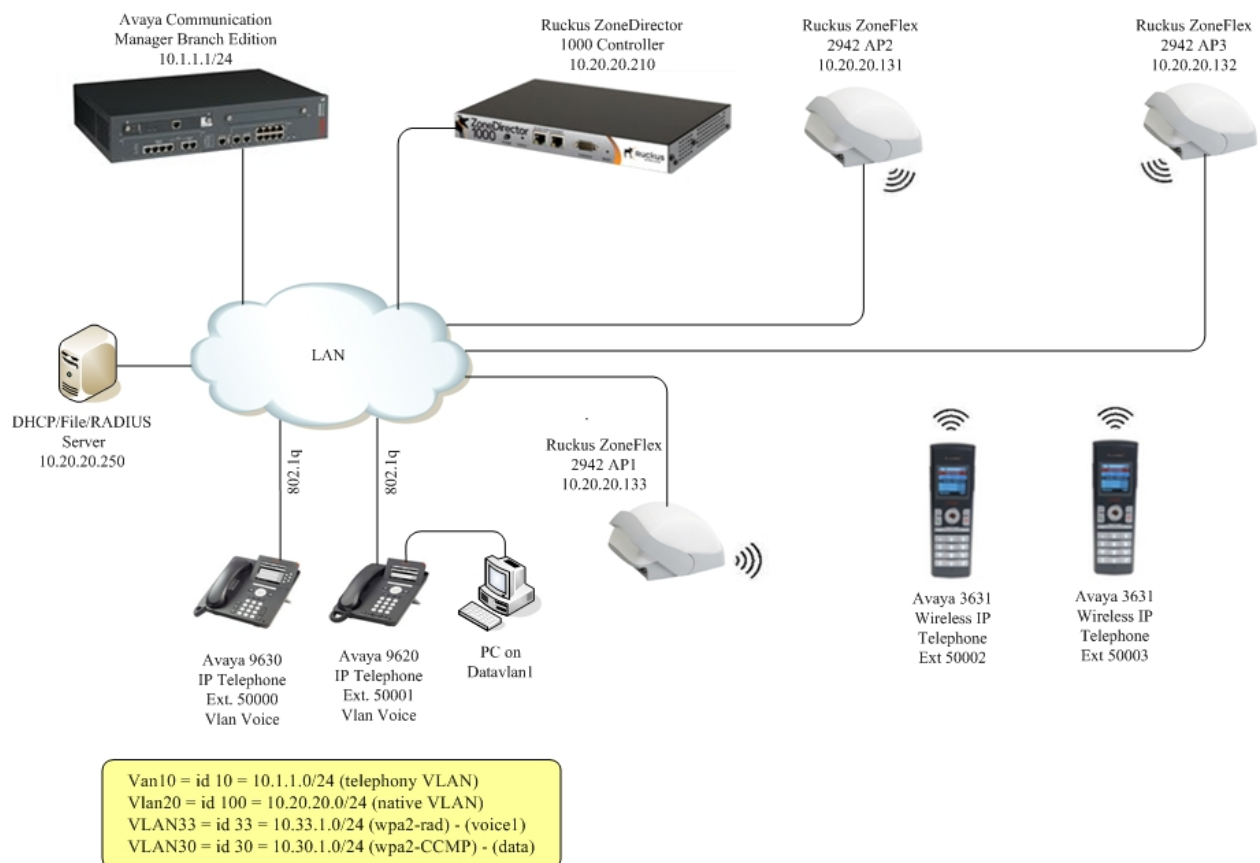


Figure 1: Avaya and Ruckus Wireless LAN Configuration

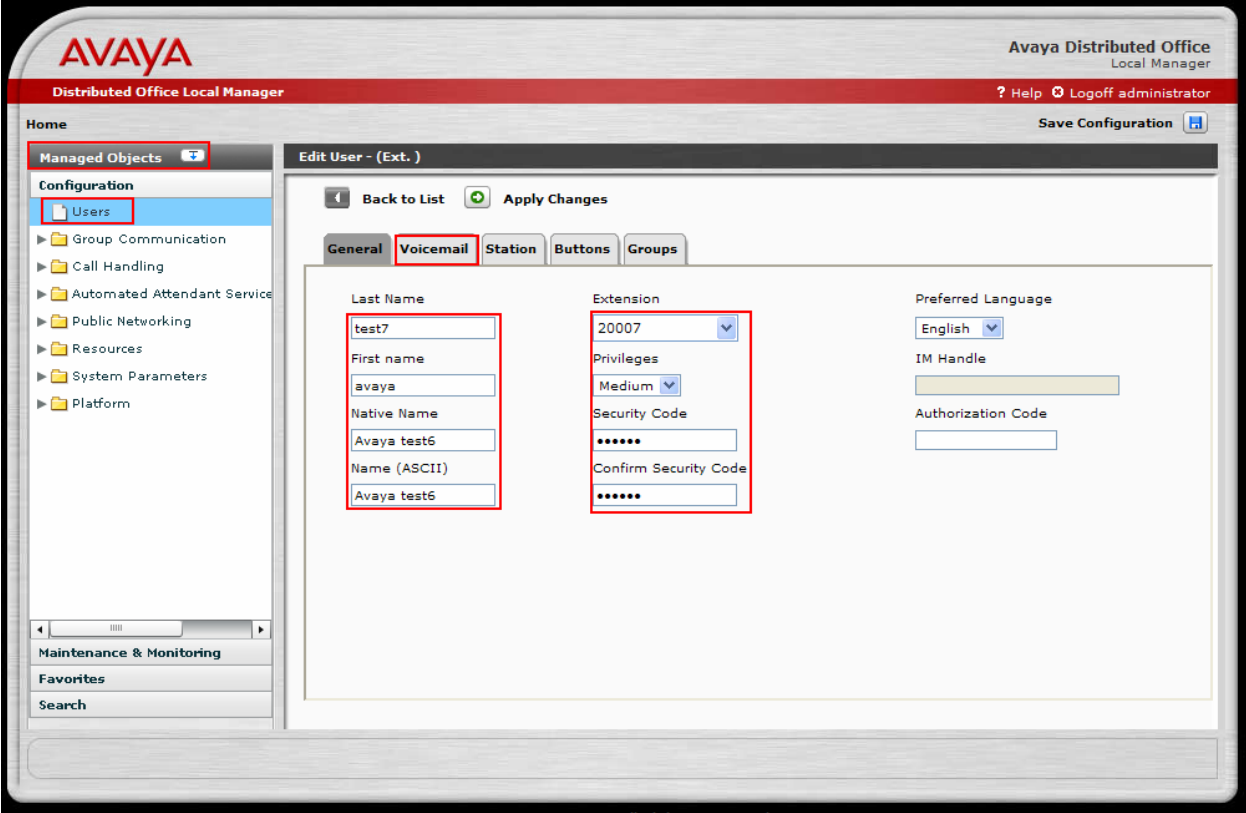
2. Equipment and Software Validated

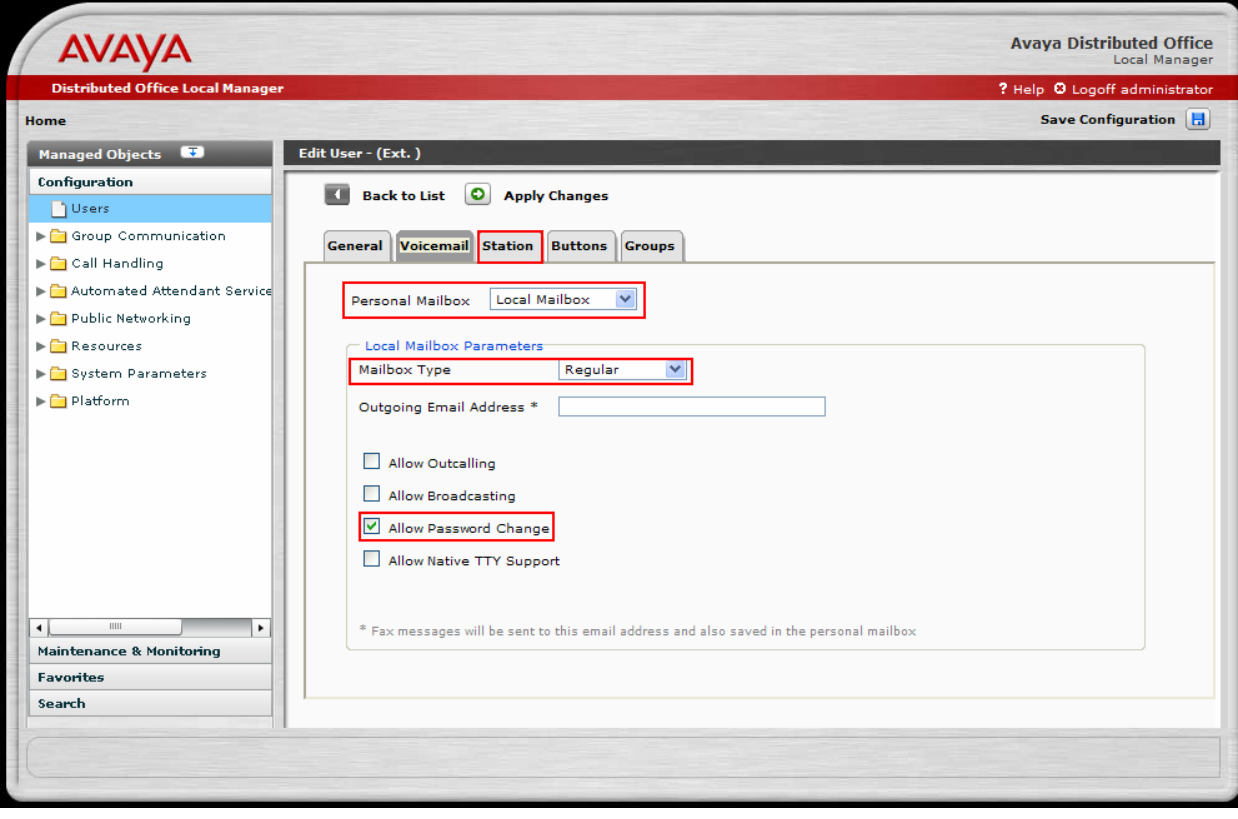
The following equipment and software were used for the sample configuration provided:

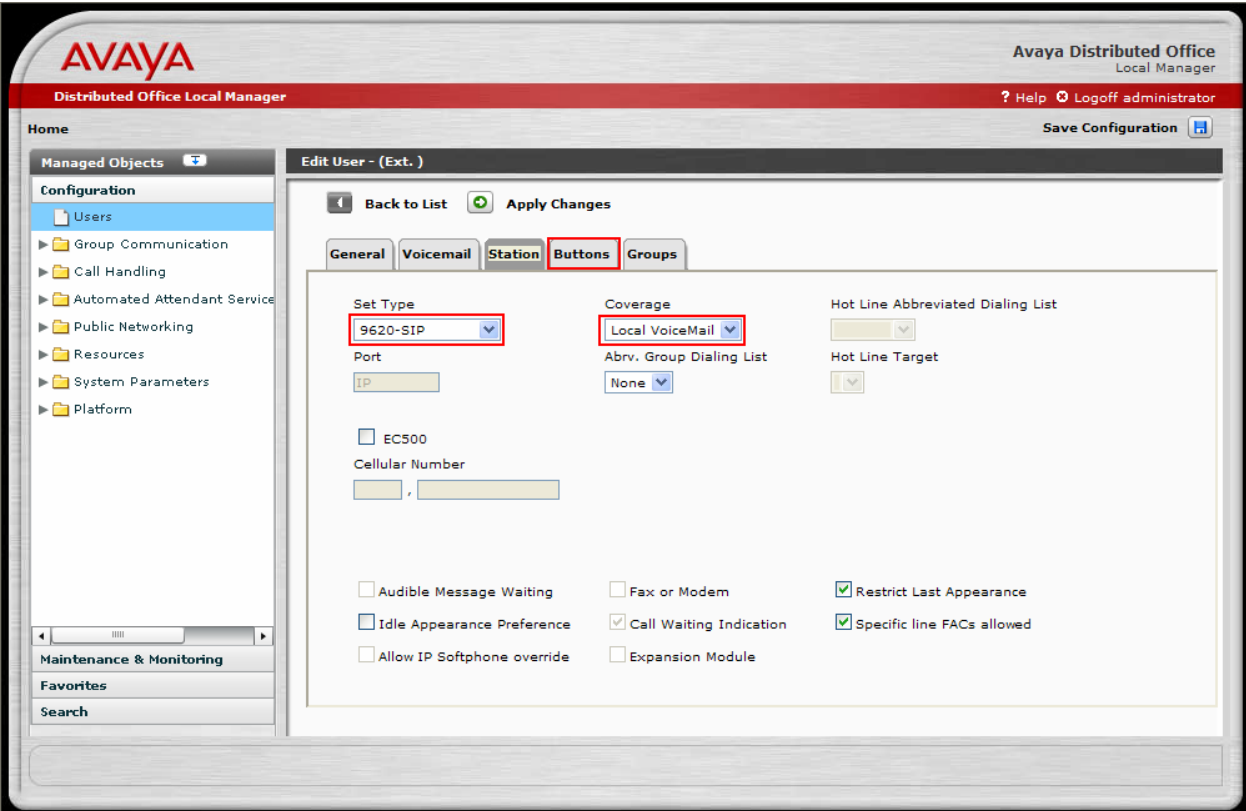
Hardware Component	Software/Firmware
Avaya Communication Manager Branch Edition i120 Avaya Communication Manager Branch Edition AM110	27.17.1 1.2
Avaya 3631 Wireless Telephone	1.5.3
Avaya 9600 Series IP Telephones	Avaya one-X Deskphone 2.0 (H.323)
Ruckus ZoneDirector 1000 controller	(6.0.1.0 build 159)
Ruckus ZoneFlex 2942 Access Point	(6.0.1.0 build 159)
Microsoft Windows 2003 Server	Internet Authentication Service (IAS)/Radius/File/DHCP

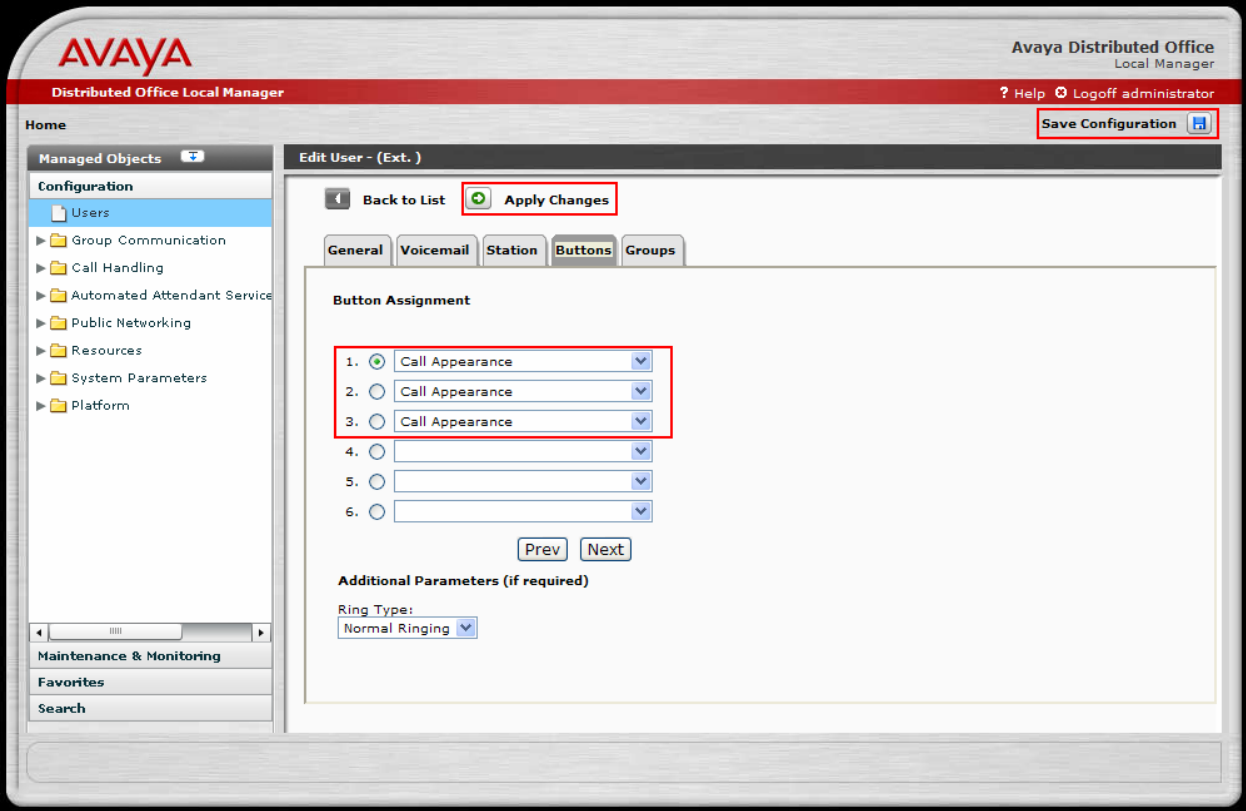
3. Avaya Communication Manager Branch Edition Configuration

Avaya Communication Manager Branch Edition is administered via a web interface. In the sample network, the Avaya Communication Manager Branch Edition was assigned the IP address 10.1.1.1 and the URL <http://10.1.1.1> was used to access the administration interface. For information on how to access and setup a factory default system, refer to **Section 10 [1]**.

Step	Description
1.	<p>Navigate to the Edit User frame by clicking Managed Objects → Users. Under General, enter the values displayed below and then click Apply Changes. Last Name, First name and Native Name can be any descriptive text that identifies this user. Name (ASCII) may be populated with the same information that is entered in Native Name. Security Code and Confirm Security code are numeric codes that must match. Use the drop-down list for Extension and select any available extension. The remaining parameters were left to default values. Click the Voicemail tab to continue.</p> 

Step	Description
2.	<p>Navigate to the Voicemail tab by clicking Voicemail. Click the drop-down list for Personal Mailbox and select Local Mailbox. Under Local Mailbox Parameters, click the drop-down list for Mailbox Type and select Regular. Check the Allow Password Change check box. Click the Station tab to continue.</p>
	 <p>The screenshot shows the Avaya Distributed Office Local Manager interface. The 'Station' tab is selected under the 'Voicemail' section. The 'Local Mailbox Parameters' section is expanded, showing the 'Mailbox Type' dropdown set to 'Regular' and the 'Allow Password Change' checkbox checked. The 'Outgoing Email Address' field is empty. The 'Allow Outcalling', 'Allow Broadcasting', and 'Allow Native TTY Support' checkboxes are unchecked. The 'Personal Mailbox' dropdown is set to 'Local Mailbox'.</p>

Step	Description
3.	<p>Navigate to the Station tab by clicking Station. Use the drop-down list for Set Type to select 9620-SIP. This release of Avaya Communication Manager Branch Edition has no specific Set Type for the Avaya 3631 Wireless Telephone. Therefore, the 9620-SIP Set Type was used. Use the drop-down list for Coverage to select Local VoiceMail. The remaining parameters were left to default values. Click the Buttons tab to continue.</p> 

Step	Description
4.	<p>Navigate to the Buttons tab by clicking Buttons. Use the drop-down list for Button Assignment 1 – 3 and select Call Appearance. The remaining parameters were left to default values. Click Apply Changes and then click Save Configuration. Note the user may receive a message indicating the system is busy if Save Configuration is clicked immediately after Apply Changes. If that occurs, simply click Save Configuration after one or two minutes. Repeat this process for each Avaya 3631 Wireless Telephone. Click Apply Changes and then click Save Configuration.</p> 


4. Configure Ruckus ZoneDirector 1000 controller and Ruckus ZoneFlex 2942 Access Points

The following steps detail the initial configuration for the Ruckus Mobility Solution used for the compliance testing.

The configuration on the Ruckus ZoneDirector 1000 controller was administered via the Web configuration tool. Except where stated, the parameters in all steps are the default settings and are supplied for reference.

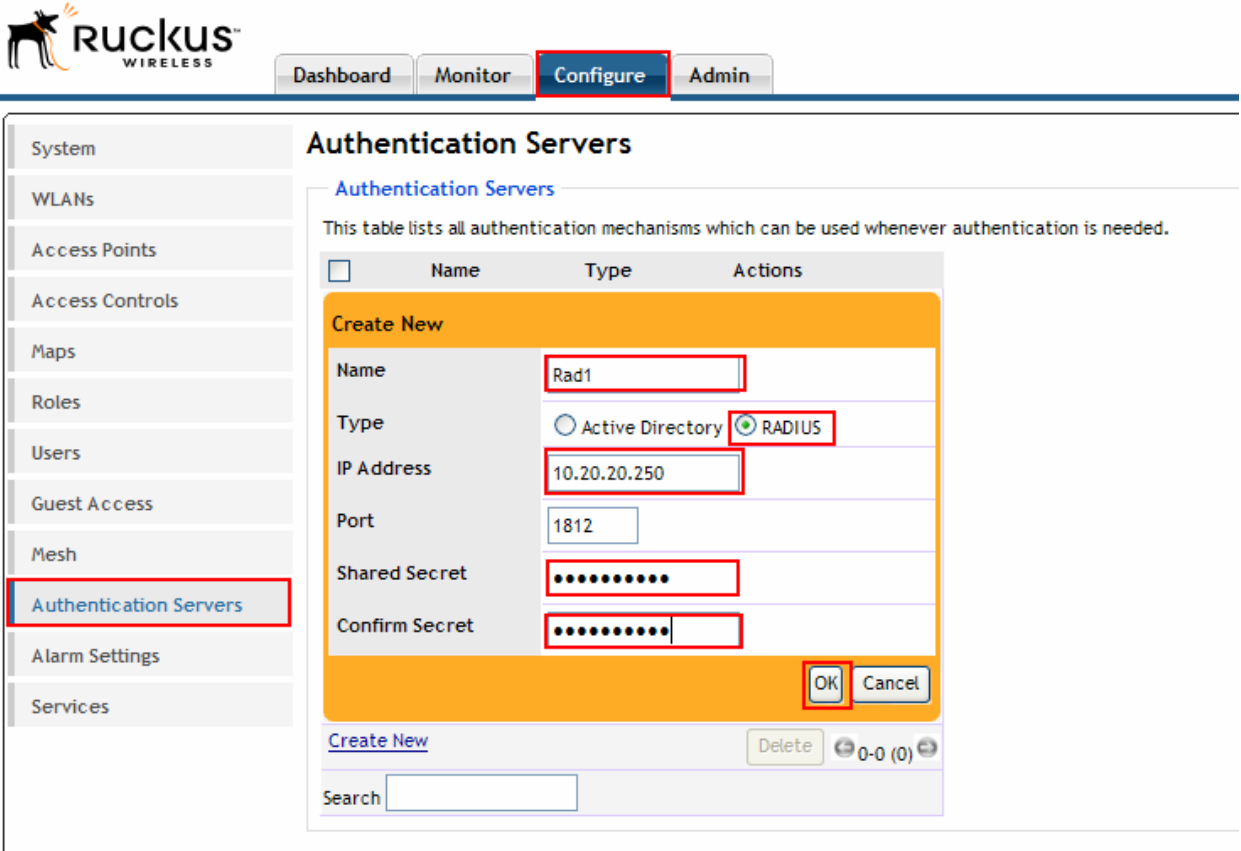
4.1. Configure Ruckus ZoneDirector 1000 controller

Step	
------	--

Step	
	<p>1. Configure the Ruckus ZoneDirector 1000 using the built-in web-based Management Tool. Access this tool by establishing a web browser connection to the Ruckus ZoneDirector 1000 controller. It is assumed that basic IP information has been completed on the Ruckus ZoneDirector 1000 controller. Refer to Section 10 [4].</p> <ol style="list-style-type: none"> 1. Start the Management Tool as follows: Start your web browser and enter https://10.20.20.31 Press Enter. 2. Log in to the Ruckus ZoneDirector 1000 controller using default credentials which can be obtained from the Ruckus ZoneDirector 1000 controller documentation. 

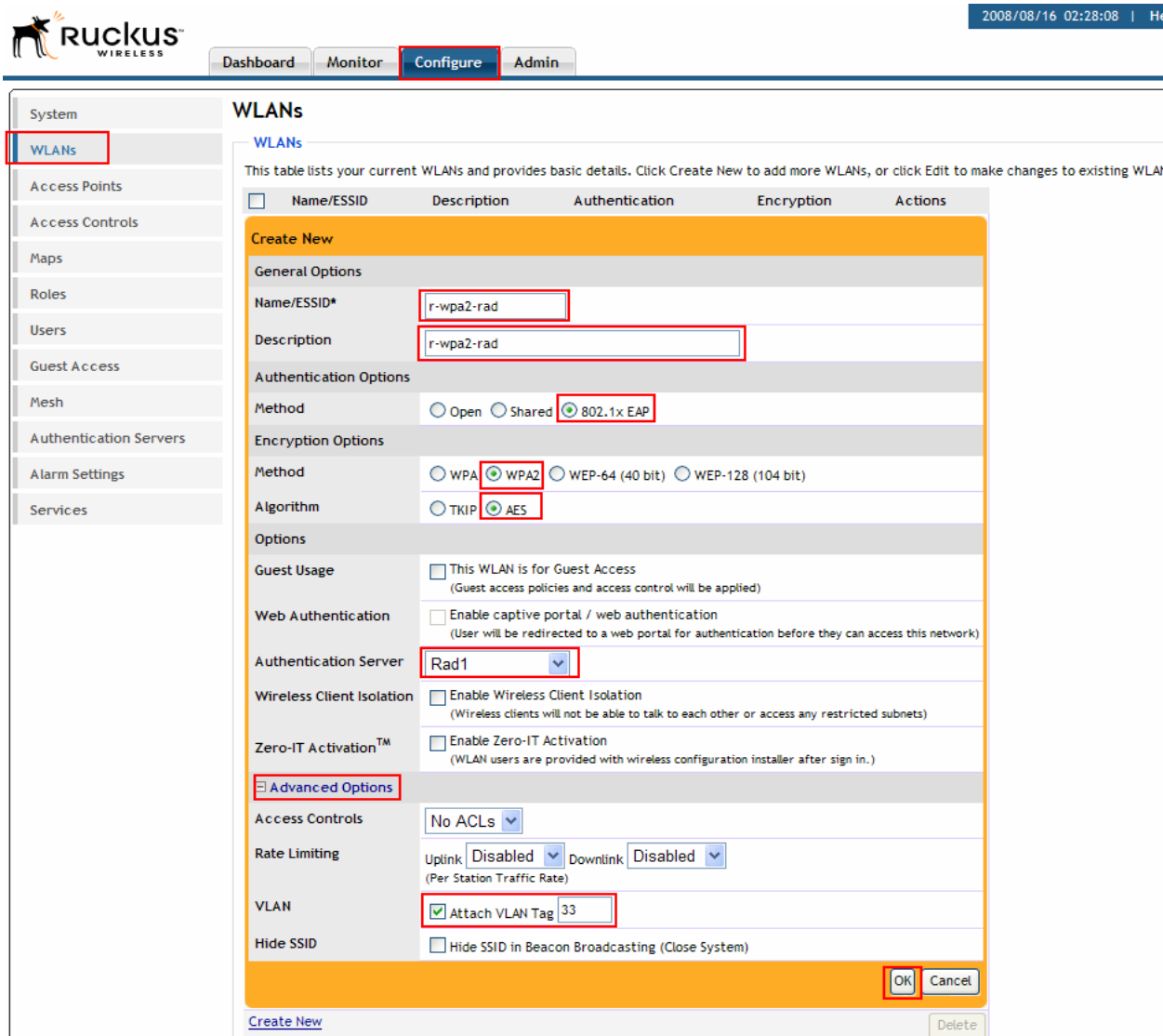
4.2. Configure Authentication Server entry (Radius)

Step	
------	--

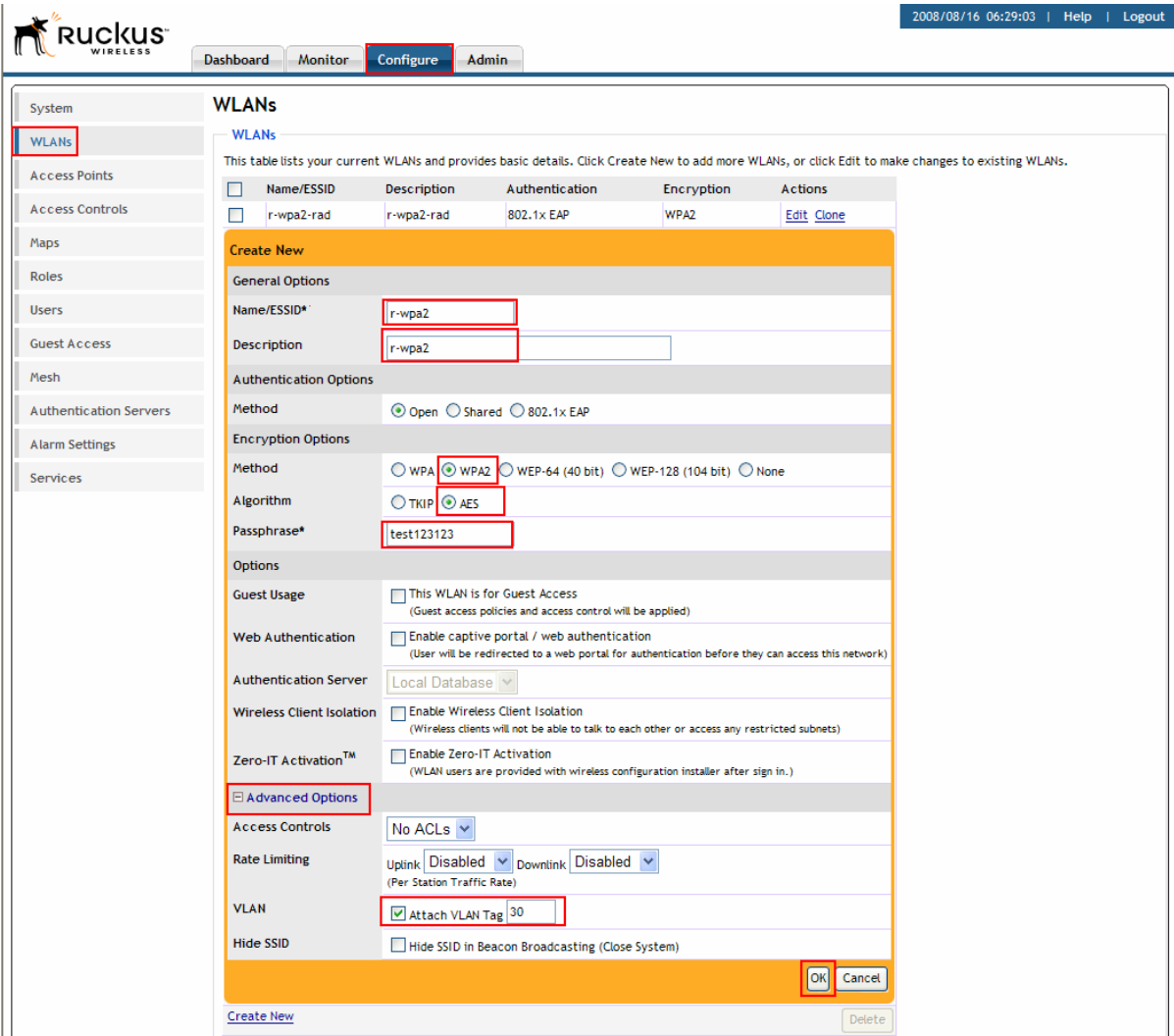
Step	
1.	<p>Navigate to Configure → Authentication Servers, select Create New (not shown) and enter a Name for the Authentication Server. Select the RADIUS check box and enter the IP Address of the radius server. Enter the Shared Secret and Confirm Secret information. Select OK to continue.</p> <p>Note: The RADIUS Shared Secret must match the Radius server and be obtained from the Radius administrator.</p> 

Create ESSIDs for the voice and data networks. Four different security schemas were tested: Clear, WEP-128, WPA2-CCMP and WPA2-CCMP with 802.1X on the Avaya 3631 Wireless IP Telephones. Clear and WEP ESSIDs will not be covered in these Application Notes.

4.3. Create the voice ESSID with wpa2 and 802.

Step	
1.	<p>Navigate to Configure → WLANs, select Create New under General Options enter the Name/ESSID* and Description of the ESSID, e.g., r-wpa2-rad. Under Authentication Options, select the 802.1x EAP check box. Under Encryption Options, select the WPA2 and AES check boxes. Click the Authentication Server pull down window and select Rad1. Click the check box next to Advanced Options, Click the check box for Attach VLAN Tag and enter the VLAN ID for the wireless voice network, e.g., 33. Select OK to continue.</p> 

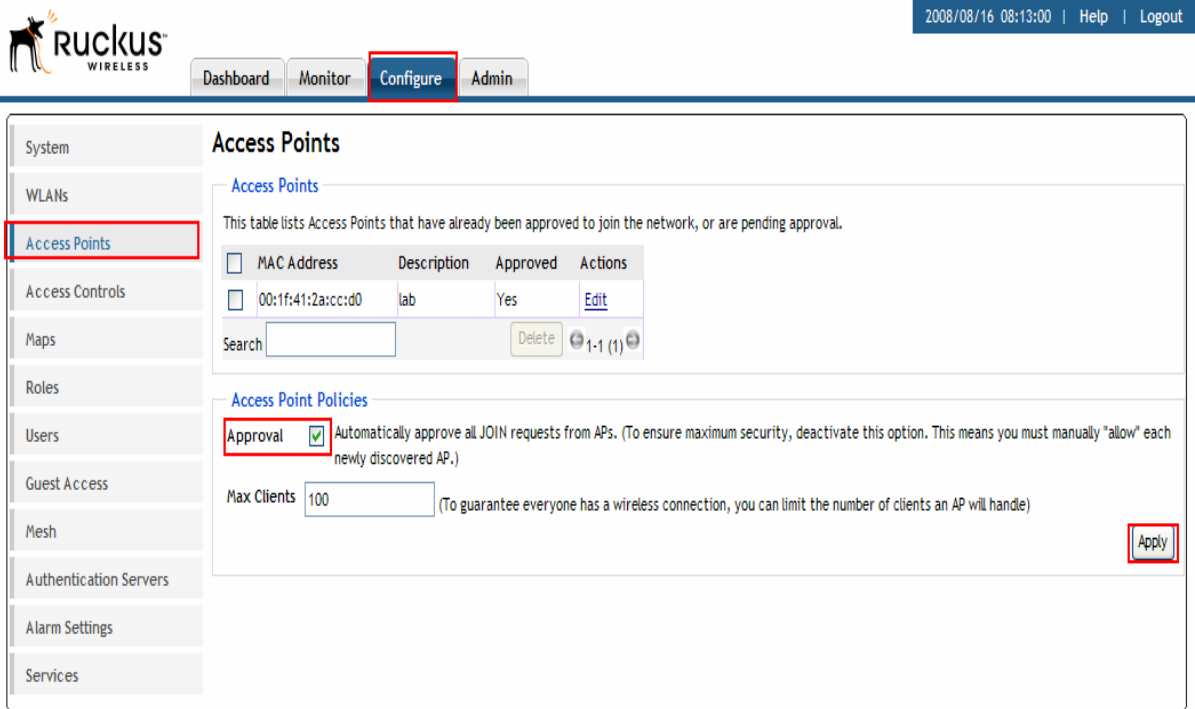
4.4. Create the data ESSID with wpa2

Step	
1.	<p>Navigate to Configure → WLANs, select Create New under General Options enter the Name/ESSID* and Description of the ESSID, e.g., r-wpa2. Under Encryption Options, select the WPA2 and AES check boxes and enter the Passphrase*. Click the check box next to Advanced Options, Click the check box for Attach VLAN Tag and enter the VLAN ID for the wireless data network, e.g., 30. Select OK to continue.</p> 

4.5. Configure the Ruckus ZoneFlex 2942 Access Points

For compliance testing the ZoneFlexAP Access Points were on the same node as the ZoneDirector and were able to be discovered by ZoneDirector as well as obtain an IP address from the DHCP server. The ZoneFlexAP Access Points can be on a different node than the ZoneDirector, but this will not be documented in these Application Notes.

Configure the ZoneDirector to automatically approve the ZoneFlexAP Access Points.

Step	
1.	<p>Navigate to Configure → Access Points and select the Approval check box. Select Apply to continue.</p> 

4.6. Configure QoS Policy

This must be configured on each AP used.

Step	
1.	<p data-bbox="285 428 1419 491">Using SSH, log onto the Ruckus ZoneFlex 2942 Access Point 1 using default credentials which can be obtained from the Ruckus ZoneFlex 2942 Access Point documentation.</p> <div data-bbox="285 531 1464 898"><pre data-bbox="298 537 1333 821">login as: admin Please login: admin password : Copyright(C) 2005-2007 Ruckus Wireless, Inc. All Rights Reserved. Warning: AP is in ZoneDirector-Managed mode Current or latest Ruckus ZoneDirector: 10.20.20.210 / 00:1d:2e:16:b1:90 Any configuration changes made in CLI may conflict with the ZoneDirector's management and will cause undefined results. rkscli:</pre></div>
Step	
2.	<p data-bbox="285 1064 634 1096">Set the holdingtime option</p> <div data-bbox="285 1136 1464 1421"><pre data-bbox="298 1163 873 1184">rkscli: set mq holdingtime 2000 2000 10000 40</pre></div>

5. Configure Avaya 3631 Wireless IP Telephone

For complete details on all the supported features on the Avaya 3631 Wireless IP Telephone refer **Section 10 [3]**.

6. Interoperability Compliance Testing

Interoperability compliance testing covered feature functionality, serviceability, and Quality of Service testing. Feature functionality testing verified the ability of the Ruckus Wireless Solution to provide network access to the Avaya 3600 Series Wireless IP Telephones. The emphasis of testing was on the QoS implementation, roaming, RADIUS authentication, WPA2 Enterprise and 802.1x encryption methods.

6.1. General Test Approach

The general test approach was to register the Avaya 3600 Series Wireless IP Telephones with Avaya Communication Manager Branch Edition through the Ruckus Wireless 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 Ruckus Wireless Solution was verified to maintain voice calls while dropping the low priority traffic. Network level tests included verifying roaming from one access point to another and validating Quality of Service for voice traffic.

6.2. Test Results

The Avaya 3600 Series Wireless IP Telephones were verified to successfully register with Avaya Communication Manager Branch Edition through the Ruckus Wireless Solution and passed all test cases for registration, QoS and Roaming.

Four different security schemas were tested: Clear, WEP-128, WPA2-PSK TKIP and WPA2-CCMP-802.1x on the Avaya 3631 Wireless IP Telephones. 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 Branch Edition (while in a conference call). Calls were maintained for durations over one minute without degradation of 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 call pick-up, bridged call appearances, voicemail, Message Waiting Indicator (MWI) and hold and return from hold.

7. 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 a call between two Avaya 3600 Series Wireless IP Telephones and verify good voice quality in both directions.
- Check that the Avaya 3600 Series Wireless IP Telephones have successfully registered with Avaya Communication Manager Branch Edition by typing the **list registered-ip-station** command on the SAT in Avaya Communication Manager Branch Edition.

8. Support

Technical support for Ruckus Wireless can be obtained through the following:

- **Email:** <mailto:support@ruckuswireless.com>

9. Conclusion

These Application Notes illustrate the procedures necessary for configuring the Ruckus Wireless ZoneDirector 1000 and ZoneFlex 2942 Access Points to support the Avaya 3631 IP Wireless Telephones and Avaya Communication Manager Branch Edition. The Ruckus ZoneDirector 1000 controller and Ruckus ZoneFlex 2942 Access Point were successfully compliance-tested in a converged voice and data network configuration. The Ruckus ZoneDirector 1000 controller and Ruckus ZoneDirector 1000 controller were able to support 802.11 b/g radio, roaming, VLAN Tagging, QoS, and 802.1x authentication.

10. Additional References

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

- [1] *Avaya Communication Manager Branch Edition i120 Installation Quick Start*, May 2007 Issue 1, Document Number 03-602289
- [2] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide*
- [3] *Avaya 3631 Wireless Telephone Administrator Guide*, March 2007, Issue 2, Document Number 16-602203

The following product documentation is provided by Ruckus. For additional product and company information, visit <http://www.ruckuswireless.com>.

- [4] *Ruckus RFS Series Wireless LAN Switches WiNG System Reference Guide*

©2008 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.