



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 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 multiple Ruckus ZoneDirector 1000 controllers 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. 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. 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 running on an Avaya S8300 Server with an Avaya G700 Media Gateway, 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 Avaya 2410 digital 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.

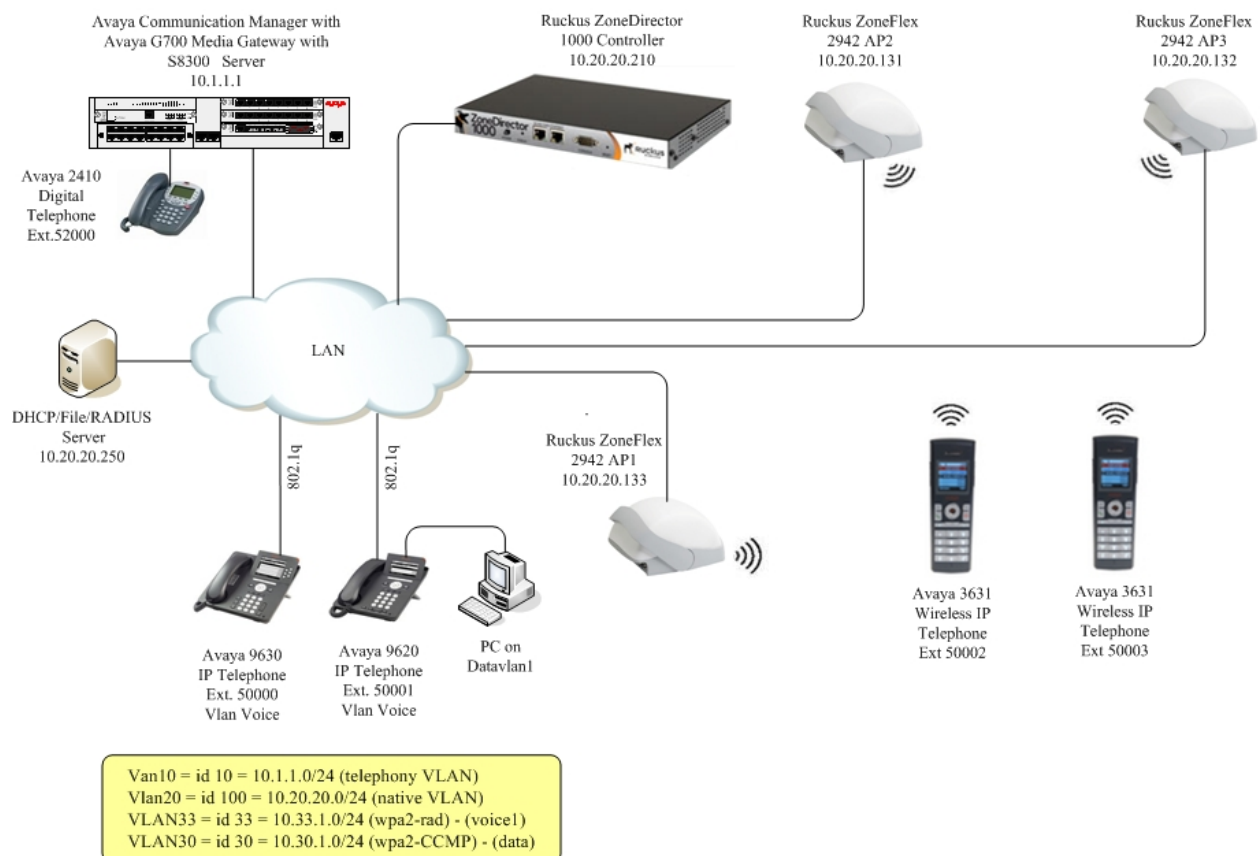


Figure 1: Avaya and Ruckus Wireless LAN Configuration

2. Equipment and Software Validated

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

Hardware Component	Software/Firmware
Avaya S8300 Server	Avaya Communication Manager 5.0 - R015x.00.0.825.4
Avaya G700 Media Gateway MGP MM712 DCP Media Module	26.31.0 HW05 / FW08
Avaya 3631 Wireless Telephone	1.5.3
Avaya Modular Messaging - Messaging Application Server (MAS)	3.1
Avaya Modular Messaging - Message Storage Server (MSS)	3.1
Avaya IA 770 INTUITY AUDIX	5.0
Avaya 9600 Series IP Telephones	Avaya one-X Deskphone Edition 2.0 (H.323)
Avaya 2410 Digital Telephone	5.0
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. 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 **Section 10 [1]**.

The Avaya 9600 Series IP 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 **Type 4620** as their station **Type** as in the example below. For complete references on how to administer these types of stations please refer to **Section 10 [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 2 802.1p/Q priority and Layer 3 Differentiated Services (DiffServ).

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, respectively. 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 Priority** 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

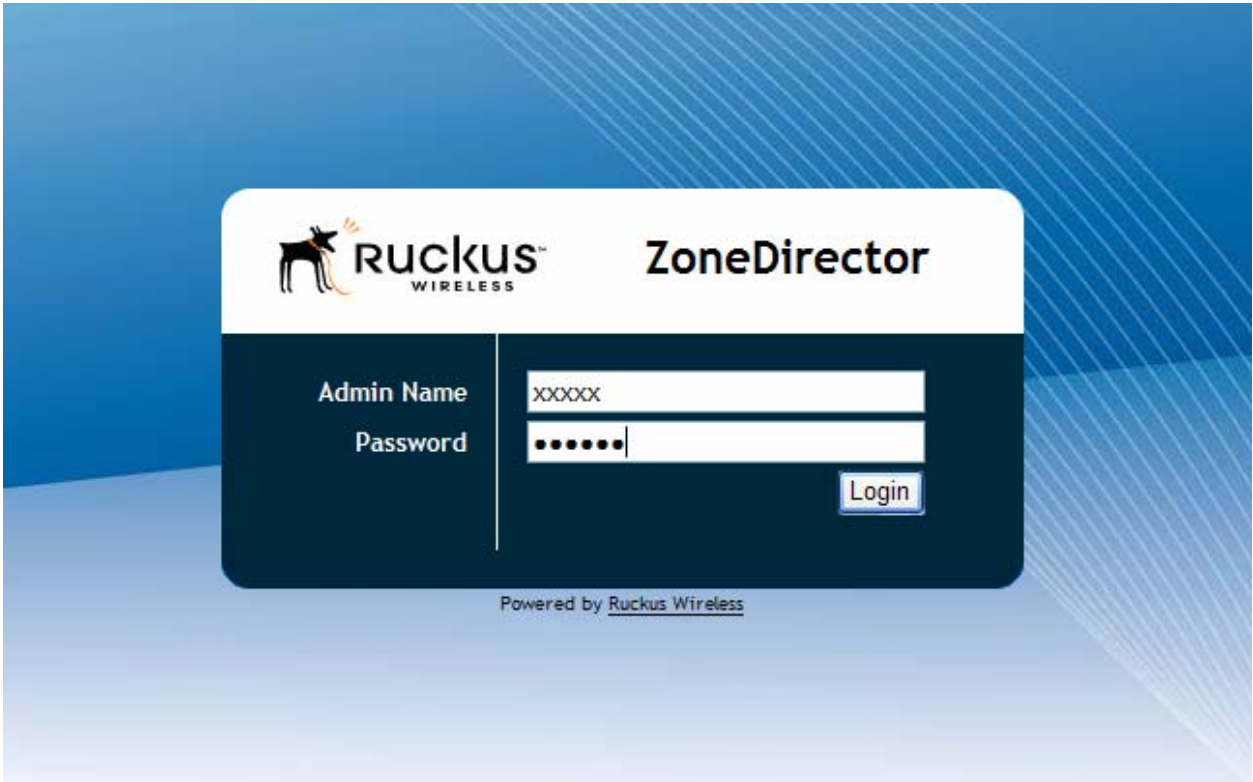
```

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

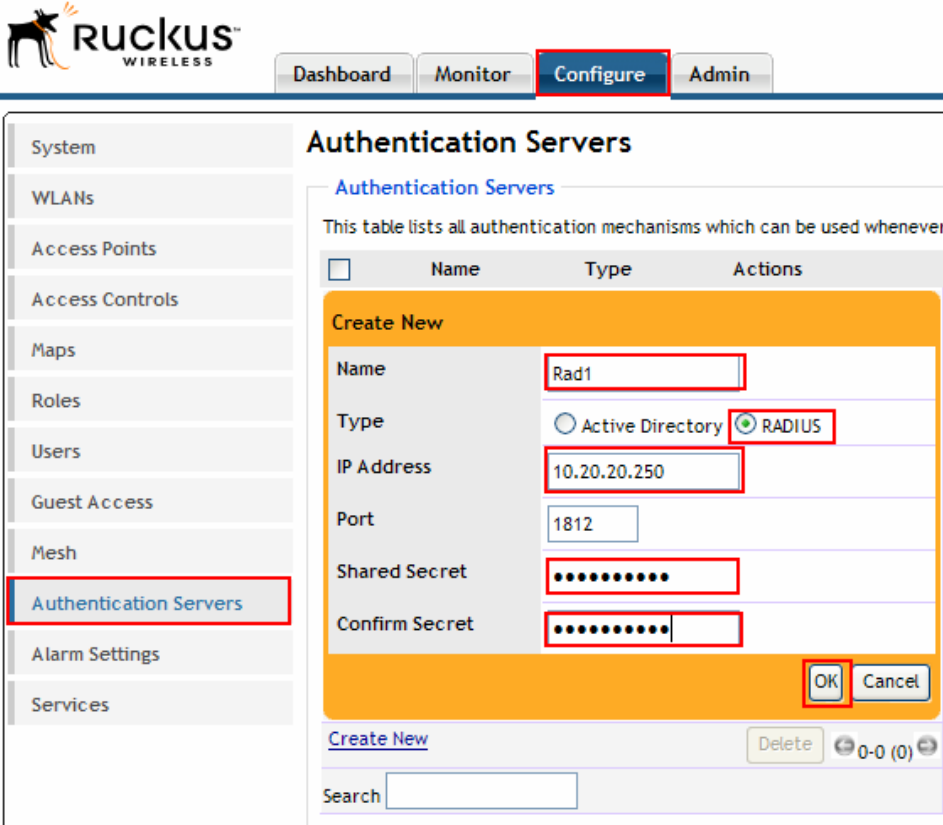
The following steps detail the initial configuration for the Ruckus Mobility Solution used for the compliance testing.

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

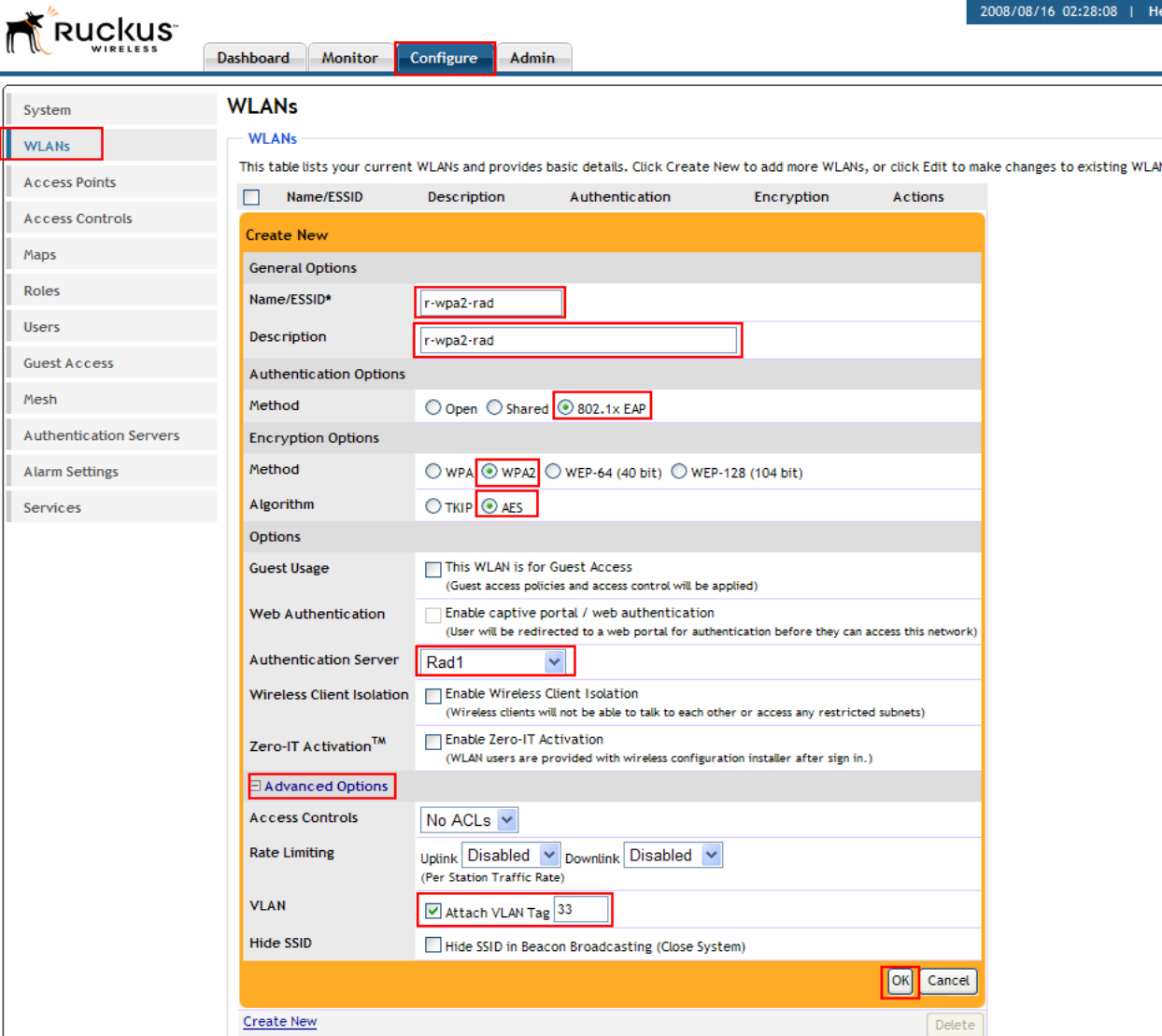
Step	
	<p>1. Configure the Ruckus ZoneDirector 1000 using the built-in web-based Management Tool. Access this tool by establishing a web browser connection to the Ruckus ZoneDirector 1000 controller. It is assumed that basic IP information has been completed on the Ruckus ZoneDirector 1000 controller. Refer to Section 10 [9].</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	
1.	<p>Navigate to Configure → Authentication Servers, select Create New 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 and 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 drop-down list 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>  <p>The screenshot shows the Ruckus Wireless configuration interface. The 'Configure' tab is selected, and the 'WLANs' section is active. The 'Create New' form is displayed, showing the following configuration details:</p> <ul style="list-style-type: none"> General Options: Name/ESSID* is 'r-wpa2-rad', Description is 'r-wpa2-rad'. Authentication Options: Method is '802.1x EAP'. Encryption Options: Method is 'WPA2', Algorithm is 'AES'. Options: Guest Usage, Web Authentication, and Zero-IT Activation are all disabled. Advanced Options: Authentication Server is 'Rad1', Access Controls are 'No ACLs', Rate Limiting is 'Disabled', and the 'Attach VLAN Tag' checkbox is checked with a value of '33'. <p>The 'OK' button is highlighted at the bottom right of the form.</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>

The screenshot shows the Ruckus Wireless configuration interface. The 'WLANs' tab is selected in the left sidebar. The 'Create New' form is displayed, with the following fields and values:

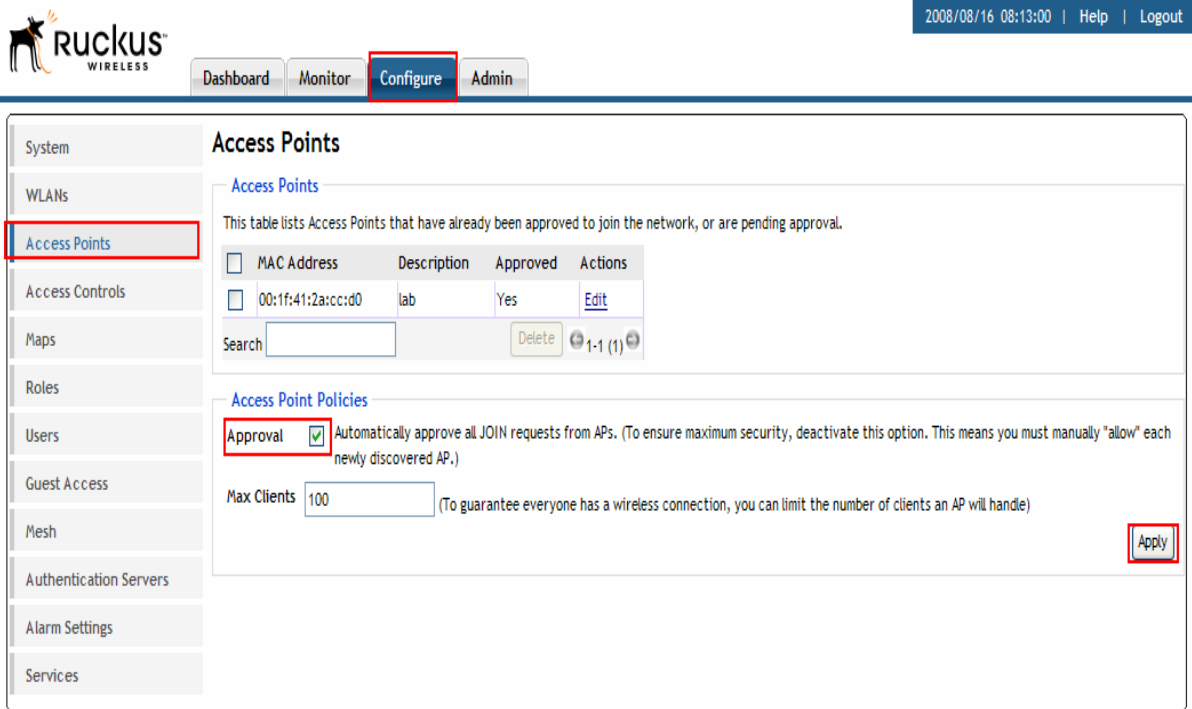
- Name/ESSID*:** r-wpa2
- Description:** r-wpa2
- Authentication Options:** Method: Open (selected), Shared, 802.1x EAP
- Encryption Options:** Method: WPA2 (selected), WPA, WEP-64 (40 bit), WEP-128 (104 bit), None; Algorithm: AES (selected), TKIP
- Passphrase*:** test123123
- Options:** Guest Usage: This WLAN is for Guest Access (unchecked); Web Authentication: Enable captive portal / web authentication (unchecked); Authentication Server: Local Database; Wireless Client Isolation: Enable Wireless Client Isolation (unchecked); Zero-IT Activation™: Enable Zero-IT Activation (unchecked)
- Advanced Options:** Access Controls: No ACLs; Rate Limiting: Uplink: Disabled, Downlink: Disabled; VLAN: Attach VLAN Tag (checked), 30; Hide SSID: Hide SSID in Beacon Broadcasting (Close System) (unchecked)

The 'OK' button is highlighted in the bottom right corner of the form.

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>  <p>The screenshot shows the Ruckus ZoneDirector web interface. The top navigation bar includes 'Dashboard', 'Monitor', 'Configure' (highlighted), and 'Admin'. The left sidebar lists various system settings, with 'Access Points' highlighted. The main content area is titled 'Access Points' and contains a table of approved and pending APs. Below the table, the 'Access Point Policies' section is visible, where the 'Approval' checkbox is checked. The 'Max Clients' is set to 100. The 'Apply' button is highlighted in the bottom right corner.</p>

4.6. Configure QoS Policys

This must be configured on each AP used.

Step	
1.	<p>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> <pre>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>

Step	
2.	<p>Set the holdingtime option.</p> <pre>rkscli: set mq holdingtime 2000 2000 10000 40</pre>

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 [5]**.

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 at layer2 and layer3, 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 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 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. 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 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 by typing the **list registered-ip-station** command on the SAT in Avaya Communication Manager.

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. 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] *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
- [3] *Administration for Network Connectivity for Avaya Communication Manager*, Doc # 555-233-504
- [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 Release 2.0*, Document Number 16-300698.
- [7] *Messaging Application Server (MAS) Administration Guide*, Release 3.1, February 2007.
- [8] *Avaya IA 770 INTUITY AUDIX Messaging Application Release 5.0 Administering. Communication Manager Servers to Work with IA 770* November 2007.

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

- [9] *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.