

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.

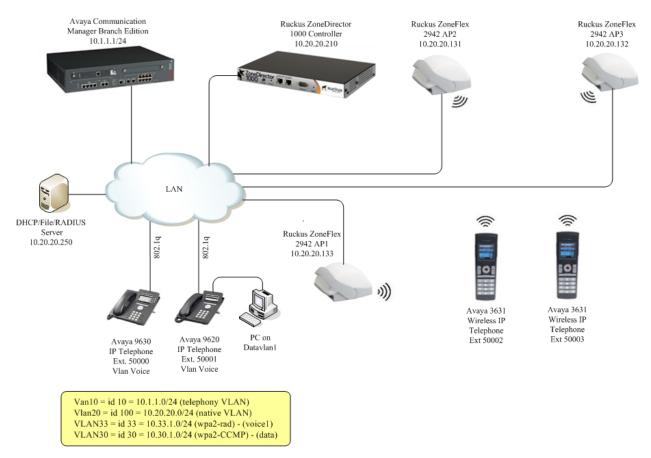


Figure 1: Avaya and Ruckus Wireless LAN Configuration

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	27.17.1
Avaya Communication Manager Branch Edition	1.2
AM110	
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
Where some windows 2005 Server	(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].

р	the values displayed b Name can be any desc the same information to code are numeric code	Jser frame by clicking Managed Object elow and then click Apply Changes. La priptive text that identifies this user. Nar that is entered in Native Name. Security that must match. Use the drop-down l	ast Name, First name and Nat ne (ASCII) may be populated y Code and Confirm Security ist for Extension and select an
	available extension. The tab to continue.	he remaining parameters were left to de	fault values. Click the Voicema Avaya Distributed Offi Local Mana ? Help © Logoff administra
	Home Managed Objects		Save Configuration
	Managed Objects Configuration Users Group Communication Call Handling Call Handling Call Automated Attendant Service Public Networking Call Resources Call System Parameters Platform	Edit User - (Ext.) Back to List Apply Changes General Voicemail Station Buttons Groups Last Name Extension Lest7 First name avaya Native Name Avaya test6 Name (ASCII) Avaya test6	Preferred Language English V IM Handle Authorization Code
	Maintenance & Monitoring Favorites Search		

ер	Description	
	Mailbox and select Lo	nail tab by clicking Voicemail. Click the drop-down list for Personal cal Mailbox. Under Local Mailbox Parameters, click the drop-down I select Regular. Check the Allow Password Change check box. Click
	Αναγα	Avaya Distributed Office
	Distributed Office Local Manager	? Help 🛽 Logoff administrato
	Home	Save Configuration 🚦
	Managed Objects	Edit User - (Ext.)
	Configuration	
	Users	Back to List O Apply Changes
	Group Communication	General Voicemail Station Buttons Groups
	Call Handling	General Voicemail Station Buttons Groups
	Automated Attendant Service	Personal Mailbox Local Mailbox 🗸
	Public Networking	
	Resources	Local Mailbox Parameters
	System Parameters	Mailbox Type Regular 💙
	▶ 🚞 Platform	Outgoing Email Address *
		Allow Outcalling
		Allow Broadcasting
		Allow Password Change
		Allow Native TTY Support
		* Fax messages will be sent to this email address and also saved in the personal mailbox
	Maintenance & Monitoring	
	Favorites	
	Search	

)	Description		TT (1 1 1	
	9620-SIP . This release Type for the Avaya 36 the drop-down list for	e of Avaya Communica 531 Wireless Telephone	tion Manager Bra . Therefore, the 9 cal VoiceMail. Th	lown list for Set Type to select unch Edition has no specific Se 620-SIP Set Type was used. In the remaining parameters were
	AVAYA Distributed Office Local Manager			Avaya Distributed Off Local Mana ? Help © Logoff administra
	Home Managed Objects	Edit User - (Ext.)		Save Configuration
	Configuration Users Call Handling Call Handl	Back to List Apply Chan General Voicemail Station Butt Set Type 9620-SIP Port IP EC500 Cellular Number		Hot Line Abbreviated Dialing List Hot Line Target
	Maintenance & Monitoring Favorites Search	Audible Message Waiting Idle Appearance Preference	 □ Fax or Modem ✓ Call Waiting Indication □ Expansion Module 	 ✓ Restrict Last Appearance ✓ Specific line FACs allowed

Step	Description Navigate to the Button	s tab by clicking Buttons . Use the drop-d	lown list for Button Assignme r
	Apply Changes and the indicating the system i	ppearance . The remaining parameters we len click Save Configuration . Note the us s busy if Save Configuration is clicked in s, simply click Save Configuration after	ser may receive a message mmediately after Apply
	8	each Avaya 3631 Wireless Telephone. C	
	Αναγα		Avaya Distributed Office Local Manager
	Distributed Office Local Manager		? Help 🛛 Logoff administrator
	Managed Objects 💿 Configuration Users Group Communication Call Handling Call Handling Cal	Edit User - (Ext.) Back to List Apply Changes General Voicemail Station Buttons Groups Button Assignment 1. Call Appearance 2. Call Appearance 4. C	
	Maintenance & Monitoring Favorites Search	Additional Parameters (if required) Ring Type: Normal Ringing	

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	
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] .
	 Start the Management Tool as follows: Start your web browser and enter https://10.20.20.31 Press Enter. Less in to the Dashee Zana Director 1000 controllar using default and braticle achiele and in the second start of the product of the second start of the sec
	 Log in to the Ruckus ZoneDirector 1000 controller using default credentials which can be obtained from the Ruckus ZoneDirector 1000 controller documentation.
	Ruckus ZoneDirector
	Admin Name Password Login
	Powered by <u>Ruckus Wireless</u>

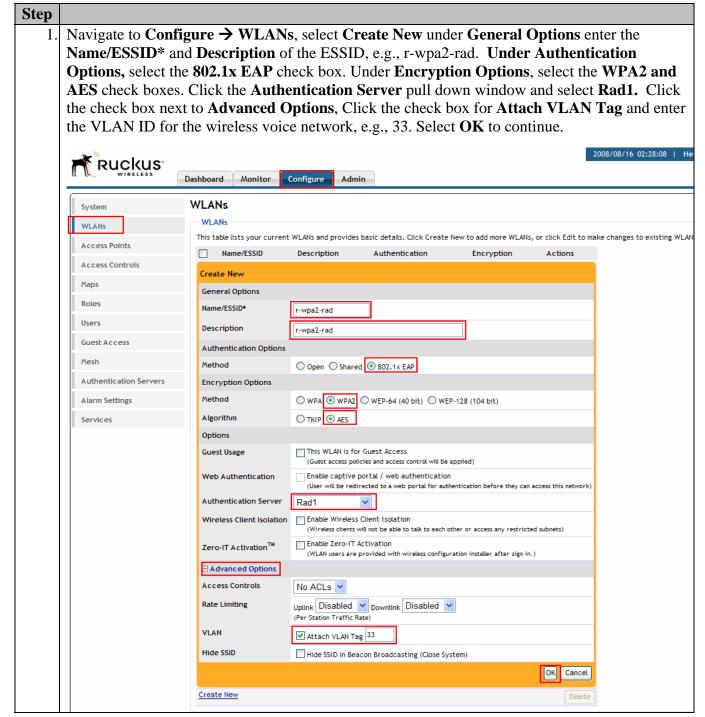
4.2. Configure Authentication Server entry (Radius)

Step

Step							
1.	Name for the Authentie of the radius server. En continue.	cation Server. Sele ter the Shared Sec	n Servers , select Create New (not shown) and enter a ect the RADIUS check box and enter the IP Address cret and Confirm Secret information. Select OK to match the Radius server and be obtained from the				
		Dashboard Monitor	Configure				
	System	Authentication	Servers				
	WLANs	- Authentication Serv					
	Access Points	This table lists all authentication mechanisms which can be used whenever authentication is needed. Name Type Actions					
	Access Controls	Create New	Type Actions				
	Maps						
	Roles	Name	Rad1				
	Users	Туре	O Active Directory O RADIUS				
		IP Address	10.20.250				
	Guest Access	Port	1812				
	Mesh	Shared Secret	•••••				
	Authentication Servers	Confirm Secret					
	Alarm Settings						
	Services		OK Cancel				
		Create New	Delete 0-0 (0)				
		Search					

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.	Name/ESSID* select the WPA to Advanced O for the wireless	and Descripti 2 and AES ch ptions, Click t data network,	on of the leck boxe the check	ESSID, e.g s and enter box for At Select OK	g., r-wpa2. the Passp ttach VLA	. Under En ohrase*. Cl AN Tag and	Options enter the cryption Options, ick the check box next d enter the VLAN ID
	System	WLANs					
	WLANS	WLANs					
	Access Points						ake changes to existing WLANs.
	Access Controls	Name/ESSID	Description r-wpa2-rad	Authentication 802.1x EAP	Encryption WPA2	Actions Edit Clone	
	Maps	Create New					
	Roles	General Options					
	Users	Name/ESSID*	r-wpa2	7			
	Guest Access	Description	r-wpa2	╡───			
	Mesh	Authentication Options	· ·				
	Authentication Servers	Method	⊙ Open ◯ Share	ed 🔿 802.1x EAP			
	Alarm Settings	Encryption Options					
	Services	Method	🔿 WPA 💽 WPA2	🔿 WEP-64 (40 bit) 🔘	WEP-128 (104 bit) 🔘	None	
		Algorithm	◯ TKIP 💽 AES	<u>]</u>			
		Passphrase*	test123123				
		Options					
		Guest Usage	This WLAN is for (Guest access po	or Guest Access dicies and access control wil	ll be applied)		
		Web Authentication		portal / web authentica firected to a web portal for		ey can access this network)	
		Authentication Server	Local Database	3			
		Wireless Client Isolation		s Client Isolation will not be able to talk to ea	ach other or access any re	stricted subnets)	
		Zero-IT Activation TM	Enable Zero-IT				
		Advanced Options					
		Access Controls	No ACLs 🛩				
		Rate Limiting	Uplink Disabled (Per Station Traffic	Downlink Disabled	¥ t		
		VLAN	Attach VLAN T	ag 30			
		Hide SSID	Hide SSID in Be	acon Broadcasting (Close	e System)		
						OK Cancel	
l		Create New				Delete	

4.4. Create the data ESSID with wpa2

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.

	Dashboard Monitor Configure Admin
System	Access Points
WLANs Access Points	This table lists Access Points that have already been approved to join the network, or are pending approval.
Access Controls	Image: provide a construction Image: provide a construction 00:1f:41:2a:cc:d0 lab Yes Edit
Maps	Search Delete G 1-1 (1)
Roles Users Guest Access	Access Point Policies Approval Image: Automatically approve all JOIN requests from APs. (To ensure maximum security, deactivate this option. This means you must manually "a newly discovered AP.) Max Clients 100 (To guarantee everyone has a wireless connection, you can limit the number of clients an AP will handle)
Mesh	That Clients 100 (To guarantee everyone has a wireless connection, you can limit the number of clients an AP will handle)
Authentication Servers	
Alarm Settings	

Configure the ZoneDirector to automatically approve the ZoneFlexAP Access Points.

4.6. Configure QoS Policy

This must be configured on each AP used.

Step	
1.	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.
	login as: admin
	Please login: admin password :
	Copyright(C) 2005-2007 Ruckus Wireless, Inc. All Rights Reserved.
	<pre>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.</pre>
	rkscli:

Step	
2.	Set the holdingtime option
	rkscli: set mq holdingtime 2000 2000 10000 40

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 <u>http://support.avaya.com.</u>

- [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 <u>http://www.ruckuswireless.com.</u>

[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 TM 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 <u>devconnect@avaya.com</u>.