

Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the Bluesocket Total Wireless LAN Solution with Avaya IP Office and Avaya 3600 Series Wireless Telephones - Issue 1.0

Abstract

These Application Notes describe the configuration process for enabling interoperability between the Bluesocket Total Wireless LAN Solution with Avaya IP Office and Avaya 3600 Series Wireless Telephones. Information in these Application Notes has been obtained through Developer*Connection* compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

Integrating wireless telephony requires interoperability between the wireless telephony products and the wireless networking infrastructure. The ability to overlay wireless telephony upon an existing wireless network or at an initial deployment of a wireless network is crucial for wireless hardware manufacturers.

These Application Notes describe the configuration process necessary to provide interoperability of Avaya IP Office and Avaya 3600 Series Wireless Telephones with the Bluesocket Total Wireless LAN Solution.

The Bluesocket Total Wireless LAN Solution is comprised of a controller and access points. Bluesocket BlueSecure controllers provide reliable, policy-based wireless LAN (WLAN) security, stateful firewalling, Quality of Server/Class of Service (QoS/CoS), Layer 3 intrusion detection, and dynamic RF management. BlueSecure access points work in conjunction with BlueSecure controllers for enterprise WLAN deployments. The BlueSecure access points (AP) include dual radios supporting 802.11 a/b/g in a plenum-rated housing with fixed omnidirectional antennas (model AP-1500) and optional external antennas (model AP-1540).

1.1. Network Diagram

The network diagram shown in **Figure 1** illustrates the testing environment used for compliance testing. The network consists of an Avaya IP Office, an Avaya Voice Priority Processor (AVPP), three different models of wireless IP telephones, a digital telephone, an IP telephone and the wireless network infrastructure, which is described below.

The wired telephones include an Avaya 5620SW IP Telephone and an Avaya 2420 Digital Telephone. The wireless IP telephones include the Avaya 3616, the Avaya 3620 and the Avaya 3626 Wireless Telephones. An Avaya Voice Priority Processor is attached to the wired portion of the network. AVPP marks the voice traffic from the Avaya 3600 Series Wireless Telephones with QoS parameters. A wireless laptop running Avaya IP Office Phone Manager Pro PC Softphone is also connected to the network.

The wireless network is provided by the Bluesocket Total Wireless LAN Solution, which is comprised of a single Bluesocket BlueSecure Controller 5000 (BSC 5000) and three Bluesocket BlueSecure Access Point 1540 (BSAP 1540).

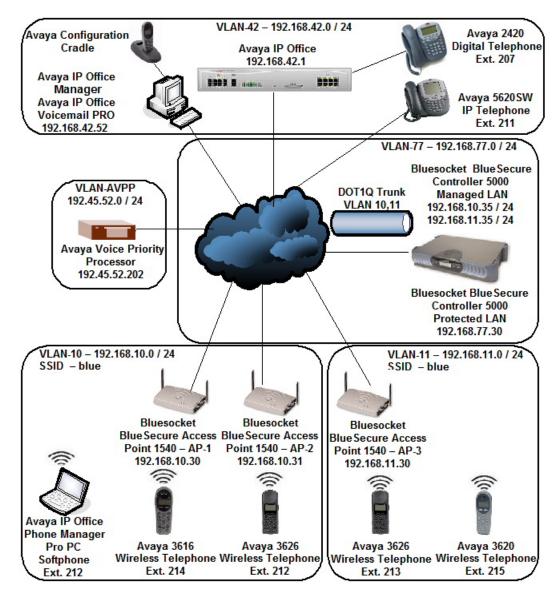


Figure 1: Sample Network for Bluesocket Total Wireless LAN Solution

2. Equipment and Software Validated

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

Equipment	Software
Avaya IP Office	4.0.5
Avaya IP Office Manager	6.0.5.0
Avaya IP Office Phone Manager Pro PC Softphone	4.0.15
Avaya IP Office Voicemail Pro	4.0.15
Avaya 2420 Digital Telephone	N/A
Avaya 5620SW IP Telephone	2.3
Avaya 3616 Wireless Telephone	96.048
Avaya 3620 Wireless Telephone	96.048
Avaya 3626 Wireless Telephone	96.048
Avaya Voice Priority Processor	174.028
Avaya Configuration Cradle	2.11.03
Bluesocket BlueSecure Controller 5000 – BSC 5000	5.3.1.11
Bluesocket BlueSecure Access Point 1540 – BSAP 1540	5.3.1-1

3. Configure Avaya IP Office

All of the telephones configured in the sample network in **Figure 1** were administered as VoIP extensions in Avaya IP Office except for the digital telephone which was administered as a digital extension. For complete references on how to administer these types of stations please refer to **Section 11** [1] and [2].

4. Configure Avaya 3600 Series Wireless Telephones

The Avaya 3600 Series Wireless Telephones provide two methods for configuration. The telephones can be configured manually using the keypad on the telephone or the telephones can be configured using the Avaya Configuration Cradle. The Avaya Configuration Cradle is a device that connects to a computer via a serial cable. The Avaya Configuration Cradle has slots where the Avaya 3600 Series Wireless Telephones can be placed for configuration. An additional piece of software is needed on the computer to which the Avaya Configuration Cradle is attached. For complete details about the Avaya Configuration Cradle refer to **Section 11** [4].

The Avaya Configuration Cradle application is started by double clicking the application icon once the software has been installed. Once the application is started, the **Config Cradle** page is shown (see **Step 1**).

1. From the Config Cradle page, configure the Avaya 3600 Series Wireless Telephon with the parameters below. Once all the configuration data has been set, click the button and then click the Write Phone button. The ESS ID: Static Entry field must	\Rightarrow				
	St				
match the SSID field configured on the BSC 5000 in Section 6, Step 18. The Secur	rity				
field must match the Authentication Type field configured on the BSC 5000 in Se	ection				
6, Step 18. Repeat this process for each telephone and modify the Call Server Externation	ension				
field to reflect the extension being provisioned. Three different security schemas we	ere				
tested: "None", "WEP" and "WPA-PSK". For details about configuring these optio	ons,				
refer to Section 11 [4].					
Call Server Extension "212"					
Call Server Password "1234"					
IP address "Use DHCP"					
ESS ID "Static entry"					
ESS ID : Static Entry "blue"					
Security "None"					
Config Cradle Ele Settings Vew Help					
System System Open Save Syst Gip Ust Syst Gip Ust Read Phone Serial 660311849 Active					
Group group1 Deen. Save Copy Wite Phone MAC 00:907a:04:c229 Wite	Group group1 Dpen Save Copy Wite Phone MAC 00:90.7a:04:c2:23 Read Write				
User sal Open Save settings Stop Ver 96.048 Error					
C C C C License Key 09 > 96.036					
C C C Cal Server Extension 212 Next. 212					
C C C Call Server IP					
C C C Cal Server Password 1234 1234					
C C C IP Office Flag					
C C C IP address Use DHCP Use DHCP C C C Static IP : Phone IP Negt					
C C G Static IP : Default Gateway					
C C G Static IP: Subnet mark					
C C C AVPP IP Address	C C C AVPP IP Address				
C C C OAI IP Address	C C C OAI On / Off Disable OAI				
C C C Syslog mode None None	C C G Syslog mode None None				
C C C Syslog IP Address					
C C G ESS ID Static entry ▼ Static entry ■					
C C G Security None V None					
C C C WEP Authentication					
C C C WEP: Default Key					
C C G WEP: Key Length					
Ready					

Step	Description			
2.	The Avaya 3626 Wireless Telephones sup	The Avaya 3626 Wireless Telephones support the "Push-to-talk" feature. This feature		
	requires additional configuration which is shown below. Ensure that the check-boxes			
	labeled Admin Push-to-talk Enable and User Push-to-talk Enable have been checked.			
	Ensure that the check-box labeled Push-t	o-talk Enable Channel 1 has been checked.		
		nel field. This value must be configured on the		
	1	ire. Once the parameters for "Push-to-talk" have		
		-		
		I then click the Write Phone button to save the		
	configuration to the telephone.			
	Config Cradle Elle Settings Yew Help	_16 ×		
	System System Open. Save System System System V V V	Bead Phone Serial 640103146 Active		
	uroup igroup Upen. save	Wite Phone MAC 00:90:7a:01:92:ea Read Write		
		<u>Stop</u> Ver 96.048 Error No delaw		
	C C Auzdiany 2 Ring Delay No delay	No delay		
	C C Ringer Volume 8 C C C Noise Mode Normal V	8 Normal		
	C C C Key Tones Enabled 🔽	2		
	C C C Warning Tones Enabled C C C Display Contrast 50	50		
	C C C Keypad Autolock Disable	Disable		
	C C @ Admin Push-to-talk Enable 🗹	2		
	C C € Push-to-talk Enable Channel 1 C C € Push-to-talk Enable Channel 2			
	C C Push-to-talk Enable Channel 3 T C C Push-to-talk Enable Channel 4 T	F		
	C C Push-to-talk Enable Channel 5	Ē		
	C C C Push-to-talk Enable Channel 6 C C Push-to-talk Enable Channel 7 C C Push-to-talk Enable Channel 7	F		
		2		
	C C C User Push-to-tak Enable Z C C C User Push-to-tak Channel 1	1		
	C C Push-to-talk Headset Volume 8	8		
	C C Puth-to-talk Speaker Volume 6	6		
	C C PTT Tone Headset Volume 8 C C PTT Tone Speaker Volume 7	8 7		
	C C G Handset Headset Volume 8 C C G Handset Speaker Volume 8	8		
	C C Docking Station Handset Volume 8 C C C Docking Station Speaker Volume 8	8 8		
	C C Docking Station Speaker Volume 18	8		
	Ready.			
L				

5. Configure Avaya Voice Priority Processor

The Avaya Voice Priority Processor is a device that marks the voice traffic from the Avaya 3600 Series Wireless Telephones with QoS parameters.

The initial configuration of the AVPP is administered through a console/serial cable connection directly to the AVPP. Using a DB-9 female, null-modem cable, connect the AVPP to the serial port of a terminal or PC. Using a terminal emulation program (such as HyperTerminal) initiate a session with the following parameters.

Terminal Type	"VT-100"
Bits per second	"9600"
Data bits	''8''
Parity	"None"
Stop bits	"1"
Flow control	"None"

Step	Description		
1.	Input the appropriate login credentials which can be found in the AVPP support documentation in Section 11 [3]. Once connected, navigate to Network Configuration by using the up/down arrow keys and press the Enter button.		
	NetLink SVP-II System Hostname: [AVPPTR6], Address: 0.0.0.0		
		System Status SVP-II Configuration Network Configuration Change Password Exit	
	Enter=Select	ESC=Exit Use Arrow Keys to Move Curso	or

Step	Description		
2.	From the Network Configuration screen navigate using the up/down arrow keys and		
	input the following information. Press ESC when all the configuration information has		
	been set.		
	IP Address "192.45.52.202"		
	Subnet Mask "255.255.25.0"		
	Default Gateway "192.45.52.1"		
	Network Configuration		
	Hostname: [AVPPTR6], Address: 0.0.0.0		
	Ethernet Address (fixed): 00:90:7A:00:00:06		
	IP Address: 192.45.52.202		
	Hostname: AVPPTR6		
	Subnet Mask: 255.255.255.0		
	Default Gateway:192.45.52.1SVP-II TFTP Download Master:NONE		
	Primary DNS Server: NONE		
	Secondary DNS Server: NONE		
	DNS Domain: NONE		
	WINS Server: NONE		
	Workgroup: WORKGROUP		
	Syslog Server: NONE		
	Disable Telnet service: N		
	Maintenance Lock: N		
	Enter=Change S=SendAll ESC=Exit Use Arrow Keys to Move Cursor		

6. Configure Bluesocket BlueSecure Controller 5000

To perform the initial configuration on the BSC 5000, plug the Protected port on the BSC 5000 into a DHCP enabled port on the network. Monitor the DHCP server logs and find the IP address that was provided to the BSC 5000. If a DHCP server is not available on the network, the Protected port on the BSC 5000 defaults to the IP address of 192.168.130.1. Note that the IP address is also displayed on the front panel of the BSC 5000.

A command line interface (CLI) is not available on the BSC 5000. The configuration is made via a web-browser. In the sample configuration, the BSC 5000 received a DHCP IP address of 192.168.77.100. Open a web-browser and input the IP address into the URL address field and specify the admin.pl page (<u>http://192.168.77.100/admin.pl</u>). Once connected to the BSC 5000, the IP address will be reconfigured to 192.168.77.30 as shown in **Figure 1**.

Step	Description
Step 1.	Login to the BSC 5000 by providing the appropriate login credentials, available in the Bluesocket document found in Section 11 [5]. Once connected and logged in to the BSC 5000 the user can administer the wired and wireless configuration.
	Certificate C User Login Version V5 3.1 Database: 104

Step	Description				
2.	To configure the BSC 5000 Protected port to use a static IP address, navigate to the Edit Protected Interface page by clicking Network and then Protected . Uncheck the check-				
	box labeled Obtain IP settings from a DHCP s	net Explorer mt_interface_layout=Hphterface_ld=1;r=hQHL01u2708			

Step	Description	
3.	Once the check-box labeled Obtain IP Settings from a interface? has been unchecked, the user is presented we configure the IP address and other parameters. To support supported on the Avaya 3626 Wireless Telephones, mai Enable multicast for this interface has been checked. information has been set, click Save . In the sample network for the following:	ith the following screen to ort the "Push-to-talk" feature ke sure that the check-box labeled Once all the configuration
	IP Address "192.168.77.30" Netmask "255.255.255.0" Gateway "192.168.77.254" Primary DNS "192.168.77.50" Hostname "Bluesocket" Interface Speed "100" Duplex "Full"	
	Network/Urotected - Edit: Protected 1927.168.77.100 - Microsoft Internet Explorer Be Edit: Yew Fyrontes: Tools table Beach : D : Reference to table to tab	
	Back Reset Seve Complete this with the profile of the interface? Current of the interface? Curre	is form to configure the BSC to communicate tected (i.e., wired) side of your network. rrent status s: 00:15:17:16:cb:de s: 192.168.77.100 k: 255.255.255.0 t: 192.168.77.255 y: 192.168.77.254 S: 192.168.168.3 S: 192.168.168.5 n: bluesocket.com
	Force prove APP for this interface Port settings Interface speed Auto 0 10 10 100 Max Duplex Auto 0 Hair for full Back Reset Seve	

Step	Description					
4.	The user may be presented with a screen that indicates the changes made to the system are					
	not active until they are made active. Since additional changes will be made, the					
	configuration process can continue before activating all the changes.					
	Network/Protected - Edit: Protected 192.168.77.100 - Alicrosoft Internet Explorer					
	Bie Edit Yew Favorites Iools Holp Carlot + Carlot Restrict And Sector And Se					
	Software Share and Share a					
	Status User Authentication User Roles VPN Voice General Web Logins Wireless (Network) Mobility Matrix Maintenance					
	Serve over something of our roles and very one of the server courses were a source source restorance					
	Protected Managed Failover Routing Table Multicost AppleTals. You have made changes which may affect users on the system. After you have made all of your changes, <u>dick here</u> to have them take effect.					
	Abimatively, you may <u>schedule</u> the update to occur at a later time.					
5.	To configure the BSC 5000 Managed port, click Network and then Managed. Use the					
	pull down arrow and select Managed-side VLAN. This will bring up a new page where					
	the VLAN information can be configured.					
	🔹 Network/Wanaged 192.168.77.100 - Microsoft Internet Explorer 📰 💽 💽					
	Be Edit Yow Figurates Ious Bob Co Back • Co • R 2 Co Dearch 🛃 Favorites 🚱 Co • So 🖉 · 🕞 🏙 🎎					
	Address 🔕 https://192.166.77.100/kteface.phude-638101257;acton-park;see_acton-park;steface.jd=1;_steface.jsvad=Ay=80199/W7371					
	Sign Out, admin Helo Sign Out, admin Helo Sign Out, admin Helo Sign Out, admin Helo Catalogue Status User Authentication User Roles VEN Voice General Web Logins Wireless Network Mobility Matrix Maintenance					
Protected Managed Fallovar Bourna Table Multicast Angle Tail. Create. Protected ski You have made changes which may affect users on the system. After you have made all of your changes, dirk here to have them take effect. Protected-ski						
	You have made changes which may affect users on the system. After you have made all of your changes, disk here to have them take effect. Alternatively, you may <u>schedule</u> the update to occur at a later time. MonogudesicOVLAN ManagudesicOVLAN ManagudesicOVLAN					
	Actions Name Type Enabled IP Address Netmask VLAN Id Static Route Entry					

Step	Description			
6.	Enable multicas interface check- Telephone "Push server and two V	St for this interface che box needs to be checke a-to-talk" feature. In th LANs were created wi	eck-boxes. The Enab ed in order to support e sample network the th the configuration	e, Run DHCP Server, and ble multicast for this the Avaya 3626 Wireless e BSC 5000 was the DHCP parameters listed below. Once epeat Step 5-6 for each
	Name Tag Type IP address	"VLAN 10" "10" "802.1q" "192.168.10.35"	"VLAN 11" "11" "802.1q" "192.168.11.35"	
	Netmask	"255.255.255.0"	"255.255.255.0"	
	Address @ https://192.166.77.100/htterface Create a Managed VLAN Managed VLAN Settings @ Enable Name VLAN 10 VLAN 10 VLAN 10 Must be in the range of 2 to 4094. VLAN 10 Must be in the range of 2 to 4094. VLAN 10 Must be in the range of 2 to 4094. VLAN 10 Must be in the range of 2 to 4094. VLAN 10 Enable DHCP relay? For OfCP addresses on user connect IP address 192.168 10.35	Search Reportes Provide Interface address face	out=Ai, form, Jayout=edit, interface_id=-1;_oub_type=1;r=21	ALWHPS214 Create a Managed YLAN Complete this form to create one or more virtual LANs on the managed side of your network.

Step	Description			
7.	Navigate to the Managed page by clicking Network and then Managed. This page now			
	shows the VLAN information. Click the <i>icon</i> for one of the listed VLANs to configure the DHCP server settings for that VLAN.			
	NetworkWanaged 1922148.772100 - Microsoft Internet Explorer Be Edit Yom Figuretes Look type Bedit Yom Figuretes Look type Bedit + Be Edit Yom Figuretes Poly Figuretes Bedit + Be Edit Yom Figuretes Poly Figuretes Bedit + Be Edit Yom Figuretes Bedit Yom Figuretes Bedit + Be Edit Yom Figuretes Bedit Yom Figuretes Bedit Yom Figuretes Bedit + Be Edit Yom Figuretes Be Yom Figuretes Be Edit Yom Fig			
	Address 🔕 https://192.168.77.100/interface.plnud=638103257;adton=paint;_steeface_layout=Ay=ex0.0i+826501 👻 💆 🌜 Uris *			
	bluesocket 👼			
	Status User Authentication User Roles VPN Voice General Web Logins Wireless Notwork Mobility Matrix Maintenance			
	Protected Managed Failover Routing Table Multicast AppleTalk			
	You have made changes which may affect users on the system. After you have made all of your changes, <u>dick here</u> to have them take effect. Alternatively, you may <u>schedule</u> the update to occur at a later time.			
	Actions Name Type Enabled IP Address Netmask VLAN.1d un-sort customize			
	Managed PHYSICAL Yes 192.168.160.1 255.255.250 VLAN-10 VLAN Yes 192.168.10.35 255.255.250 10			
	VLAN-11 VLAN Yes 192.168.11.35 255.255.255.0 11			
	Check All I Clear All Enable Delete			
	3 rows download			
8.	Navigate to the DHCP Server page from the Edit VLAN page by clicking DHCP Server .			
	🗟 NetworkWanaged - Edit: YLAN 10 192.168.77.30 - Microsoft Internet Explorer			
	Bin Edit Yew Figuretes Iools Birb			
	③ Bad. • ② · ≥ ② ⑤ P Search ★ Ferrates ④ ② - ⇒ □ 1 3 3			
	Address 👔 https://192.168.77.30/interface.phud=101573108;action=edit;_piterface_layout=A;sere_action=parkt;=VAuvr70/7162;interface_jd=5;_form_jayout=edit 💌 🔂 60 Links ** blue socket Sign_outadmin 1 Heig			
	Status User Authentication User Roles VEN Voice General Web Logins Wireless Notwork Mobility Matrix Maintenance			
	Interface CHCP Server One-to-One NAT			
	Edit VLAN-10 interface (eth1.10) Edit VLAN-10 interface (eth1.10)			
	Back Reset Delete Save Next Complete this form to configure this virtual LAN on the managed side of your network.			

	Description		
).	From the DHCP Serv	er page configure the First IP	address and Last IP address fields
	that will be used to dy	namically assign IP addresses	to the wireless devices. The values
	used for the DHCP par	rameters for this sample netwo	rk are listed below.
	1	1	
	Name	VLAN 10 VLA	AN 11
			2.168.11.150"
	Last IP address		2.168.11.175"
		192.108.10.175 19	2.108.11.175
	Using the seroll her or	the right side of the series of	well down to the Advanced DUCD
	-	-	eroll down to the Advanced DHCP
	_	-	that the Avaya 3600 Series Wireless
	1		Office. DHCP Option 176 provides
		•	MCIPADD parameter and the port
	to be used for commun	nication via the MCPORT par	ameter. In the sample network the
	value for Option 176 v	vas set to "MCIPADD=192.16	8.42.1;MCPORT=1719". Option 151
	provides the IP addres	s of the Avaya Voice Priority l	Processor and was set to
	-		information has been set, click Save.
	is is is 2.202 in the		
	Repeat Steps 7-9 for e	och VI AN	
	Repeat Steps 7-9 for e	ach VLAN.	
	NetworkWanaged - Edit: VLAN-10 192.168.7 Ele Edit Yew Figurites Tools Belp	7.30 - Microsoft Internet Explorer	2 S X
	🔇 Back - 🔘 · 💌 😰 🐔 🔎 Search 🥎	🔭 Favorites 🤣 🙆 - 🥁 🛍 - 🛄 🛍 🤹	
	Agdress () https://192.168.77.30/interface.phud=10157310	8;action=edit;save_action=paint;interface_id=5;_interface_layout=A;_form_layout=dhc	ody==aqh/(2)(2756) 🚽 🛃 Go Links 🦉
			ore managed side of the Heckfork.
	Address range to dynamically assign (Optiona First IP address Last IP address	0	ore managed side or ose network.
	First IP address Last IP address 192.168.10.150 192.168.10.175 Ise nate Leave blank to use the entire managed subnet		Note that to run the server, you must mark the Run DHCP Server checkbox and clear the Enable DHCP Relay checkbox
	First IP address Last IP address 192.168.10.150 192.168.10.175 Tax.natv Lawe Blank to use the entire managed subnet Address ranges to exclude (Optional) Exclude IP addresses that are reserved for particula	and and a second se	Note that to run the server, you must mark the Run DHCP
	First IP address Last IP address 192.168.10.150 192.168.10.175 Issentht Lave Dark to use the active moused subnet Address ranges to exclude (Optional) Evolution of the active moused for particular Industry mere value for angle address.	and and a second se	Note that to run the server, you must mark the Run DHCP Server checkbox and clear the Enable DHCP Relay checkbox
	First IP address Last IP address 19216810.150 19216810.150 19216810.150 Cases Each Source Marken managed Juback Address ranges to exclude (Optional) Exclude ID addresses that are resreved for particula Input only one value for single address. From To Row M	ethdus r devices.	Note that to run the server, you must mark the Run DHCP Server checkbox and clear the Enable DHCP Relay checkbox
	First: IP address 192.168.10.150 192.168.10.150 192.168.10.150 192.168.10.150 192.168.10.15 Cover Extra to varies water managed subnet Address ranges to exclude (Optional) Exclude ID addresse Anta are reserved for particular Prom To Row M Netbios name server See hats	edia r devices. anogement	Note that to run the server, you must mark the Run DHCP Server checkbox and clear the Enable DHCP Relay checkbox
	First: IP address 192.168.10.150 192.168.10.150 192.168.10.150 192.168.10.150 192.168.10.15 Cover Extra to varies water managed subnet Address ranges to exclude (Optional) Exclude ID addresse Anta are reserved for particular Prom To Row M Netbios name server See hats	ethdus r devices.	Note that to run the server, you must mark the Run DHCP Server checkbox and clear the Enable DHCP Relay checkbox
	First: IP address 192:168:10:150 192:168:10:150 192:168:10:150 192:168:10:150 192:168:10:15 Address tampes to exclude (Optional) Exclude ID addresses that are resreved for particul Input only one value for single address. From Netbios name server Sec. hosts Enter the IP address of the Windows Intermet Nemo	edia r devices. anogement	Note that to run the server, you must mark the Run DHCP Server checkbox and clear the Enable DHCP Relay checkbox
	First: IP address Last IP address 192:168:10:150 192:168:10:175 Lase Bank to use the when managed Jubnet. Address ranges to exclude (Optional) Richold ID address that are resreved for particular Prom Row M Netbios name server Inter her IP address. Inter the IP address of the Windexs: Internet Name DHCP Lease Options	edia r devices. anogement	Note that to run the server, you must mark the Run DHCP Server checkbox and clear the Enable DHCP Relay checkbox
	First: IP address Last IP address 192 168 10.150 192 168 10.157 Lawe Network 192 168 10.157	edia r devices. anogement	Note that to run the server, you must mark the Run DHCP Server checkbox and clear the Enable DHCP Relay checkbox
	First: IP address Last IP address 192.168.10.150 192.168.10.175 Leave Earch to use the softer managed subnet. Address ranges to exclude (Optional) Exclude ID address Atha are rereved for particule Prom To Row M Netbios name server Stachold P. Address of the Window: Intervet Hemo DHCP Lease Options ONS domain name The domain name assigned to ungualified name: Primary DNS Secondary DIS Secondary DIS	edia r devices. anogement	Note that to run the server, you must mark the Run DHCP Server checkbox and clear the Enable DHCP Relay checkbox
	First: IP address Last IP address 192.168.10.150 192.168.10.175 Lase Earch to use the softer managed subnet. Address ranges to exclude (Optional) Exclude ID address that are rereved for particult Prom To Row M Netbios name server Stabular Exclude ID address of the Window: Enternet New DHCP Lease Options ONS domain name The domain name assigned to unpaulified names Primary DNS Secondary DNS Secondary DNS Secondary DNS Secondary DNS Secondary DNS Secondary DNS Default lease Dofault lease	edia r devices. anogement	Note that to run the server, you must mark the Run DHCP Server checkbox and clear the Enable DHCP Relay checkbox
	First: IP address Last IP address 192:168:10:150 192:168:10:175 Lawse Elank to use therefore managed subnet. Address ranges to exclude (Optional) Bichode ID addresses that are rearveed for particular Prom To Row M Netbios name server Ses.holts The domain name DHCP Lease Options DNS domain name The domain name assigned to unqualified names Primary DNS See.holts Lawse Blank to use the system dafaults Secondary DNS Secondary DNS Secondary DNS Directual lease 7200 Default lease time in second	edia r devices. anogement	Note that to run the server, you must mark the Run DHCP Server checkbox and clear the Enable DHCP Relay checkbox
	First: IP address Last IP address 192:168:10:150 192:168:10:157 Lases Elank to use the whom managed subnet. Address ranges to exclude (Optional) Richold IP addresses that are reserved for particular Input only size value for single address. Prom To Robits name server Interview Interview Interview Interview Robits name server Interview Interview DHCP Lease Options DVIS domain name The domain name The domain name The domain to the spream defaulte Secondary DNS Secondary DNS Secondary DNS Particlesse 7200	edia r devices. anogement	Note that to run the server, you must mark the Run DHCP Server checkbox and clear the Enable DHCP Relay checkbox
	First: IP address Last IP address 192:168:10:150 192:168:10:157 Lases Elank to use the whom managed subnet. Address ranges to exclude (Optional) Richold IP addresses that are reserved for particular India only and value for single address. Prom To Robits name server Stabular Inter the 1P address of the Windex: Internet Name DHCP Lease Options ONS domain name The domain name The domain name The domain name The domain name ONS domain name ONS domain name Ons that, to use the system defaults Secondary DNS Secondary DNS Secondary DNS Cafsult lease 7200 Maximum lease 7200	edia r devices. anogement	Note that to run the server, you must mark the Run DHCP Server checkbox and clear the Enable DHCP Relay checkbox
	First: IP address Last IP address 192.168.10.150 192.168.10.157 Lases Elank to use the softer managed subnet. Address ranges to exclude (Optional) Dickode ID address at that are reared to for particular Dick only one value for single address. From To Row M Netbios name server Stackode Status Tenter the ID address of the Windows: Internet Name DHCP Less Options ONS domain name The domain name assigned to unpaulified names Primary DNS Secondary DNS Secondary DNS Default lease Dofault lease 7200 Maximum lease time in seconds Darkel elased Orase Difference Disabled of Dispanic CHS update scheme	edia r devices. anogement	Note that to run the server, you must mark the Run DHCP Server checkbox and clear the Enable DHCP Relay checkbox
	First: IP address Last IP address 192.168.10.150 192.168.10.175 Lases Earlies to use the softer managed pubmet. Address ranges to exclude (Optional) Dickobel IP address at that are reareed address. Prom To Row M Index only one value for single address. Prom To Row M Index only one value for single address. Prom To Row M Index only one value for single address. Netbios name server Iss.batts ONS domain name The domain name	edia r devices. anogement	Note that to run the server, you must mark the Run DHCP Server checkbox and clear the Enable DHCP Relay checkbox
	First: IP address Last IP address 192.168.10.150 192.168.10.157 Lases Elank to use the softer managed subnet. Address ranges to exclude (Optional) Dickode ID address at that are reared to for particular Dick only one value for single address. From To Row M Netbios name server Stackode Status Tenter the ID address of the Windows: Internet Name DHCP Less Options ONS domain name The domain name assigned to unpaulified names Primary DNS Secondary DNS Secondary DNS Default lease Dofault lease 7200 Maximum lease time in seconds Darkel elased Orase Difference Disabled of Dispanic CHS update scheme	edia r devices. anogement	Note that to run the server, you must mark the Run DHCP Server checkbox and clear the Enable DHCP Relay checkbox
	First: IP address Last IP address 192:168:10.150 192:168:10.175 Lases Elank to use there managed subnet. Address ranges to exclude (Optional) Bichode ID addeesset that are reserved to for particular Doub only one value for single addeess. Prom To Rest Data are reserved in the Windows: Internet Neme DHCP Lease Options DNS domain name The domain name assigned to unqualified names Primary DNS See hosts Lease Blank to use the system defaults Secondary DNS Default lease 7200 Default lease Disabled M Drynamic DNS Calest in mark time in seconds Maximum lease 7200 Default lease Disabled M Drynamic DNS Cleade mark time in seconds Maximum lease 7200 Disabled M Option Name Option Name Option Name	edua. e devices. snagement v v v v v v v v v v v v v	Note that to run the server, you must mark the Run DHCP Server checkbox and clear the Enable DHCP Relay checkbox
	First: IP address 1.92.168.10.150 1.92.168.10.157 i.ex.netw Laxes Elank to use the short managed subnet: Address ranges to exclude (Optional) Exclude If optional) Exclude ID address: Interview address: Interview address: Prom To Row M Netbios name server Isk holds: Interview address: Interview Isk holds: Interview ONS domain name Interview ID address of the Windex: Intervet Name DHCP Lease Options ONS domain name The domain name Interview ID address of the Windex: Intervet Name DHCP Lease Options ONS domain name Charse Intervet ID address of the strengestified name: Primary DNS Exame Intervet ID Isk holds. Becontary DNS Isk holds. Cafsuit lease Isk holds. Option Isk holds. Despine ION Option	edua r devices. anagement y y service (WINS) rever (only used for Hicosoft Windows name revolution). The service (WINS) rever (only used for Hicosoft Windows name revolution).	Note that to run the server, you must mark the Run DHCP Server checkbox and clear the Enable DHCP Relay checkbox
	First: IP address Last IP address 192:168:10.150 192:168:10.175 Lases Elank to use there managed subnet. Address ranges to exclude (Optional) Bichode ID addeesset that are reserved to for particular Doub only one value for single addeess. Prom To Rest Data are reserved in the Windows: Internet Neme DHCP Lease Options DNS domain name The domain name assigned to unqualified names Primary DNS See hosts Lease Blank to use the system defaults Secondary DNS Default lease 7200 Default lease Disabled M Drynamic DNS Calest in mark time in seconds Maximum lease 7200 Default lease Disabled M Drynamic DNS Cleade mark time in seconds Maximum lease 7200 Disabled M Option Name Option Name Option Name	eduu. r devices. snagement v v v s Bervice (WINS) rerver (only used for Microsoft Windows name resolution). S Bervice (WINS) rerver (only used for Microsoft Windows name resolution). Data Type Value Row Management Data String v MicroADO-192.16 v P-Address v 192.45.52.202 v	Note that to run the server, you must mark the Run DHCP Server checkbox and clear the Enable DHCP Relay checkbox
	First: IP address Last IP address 192:168:10.150 192:168:10.175 Lases Elank to use there managed subnet. Address ranges to exclude (Optional) Bichode ID addeesset that are reserved to for particular Doub only one value for single addeess. Prom To Rest Data are reserved in the Windows: Internet Neme DHCP Lease Options DNS domain name The domain name assigned to unqualified names Primary DNS See hosts Lease Blank to use the system defaults Secondary DNS Default lease 7200 Default lease Disabled M Drynamic DNS Calest in mark time in seconds Maximum lease 7200 Default lease Disabled M Drynamic DNS Cleade mark time in seconds Maximum lease 7200 Disabled M Option Name Option Name Option Name	edua. r devices. angement v v sg Bereits (WINE) server (only used for Microsoft Windows name resolution). g Bereits (WINE) server (only used for Microsoft Windows name resolution). Data Type Value Row Management. Dota String V MicroADD-192 16 V IP Address V 192 45 52 22 V	Note that to run the server, you must mark the Run DHCP Server checkbox and clear the Enable DHCP Relay checkbox
	First: IP address Last IP address 192:168:10.150 192:168:10.175 Lases Elank to use there managed subnet. Address ranges to exclude (Optional) Bichode ID addeesset that are reserved to for particular Doub only one value for single addeess. Prom To Rest Data are reserved in the Windows: Internet Neme DHCP Lease Options DNS domain name The domain name assigned to unqualified names Primary DNS See hosts Lease Blank to use the system defaults Secondary DNS Default lease 7200 Default lease Disabled M Drynamic DNS Calest in mark time in seconds Maximum lease 7200 Default lease Disabled M Drynamic DNS Cleade mark time in seconds Maximum lease 7200 Disabled M Option Name Option Name Option Name	edului r devices. snagement v v v s Bereica (WINS) rerver (only used for Microsoft Windows name resolution). S Bereica (WINS) rerver (only used for Microsoft Windows name resolution). Data Type Value Row Management Data String v MicroADO-192.16 v P Address v 192.45.52.202 v P Address v v	Note that to run the server, you must mark the Run DHCP Server checkbox and clear the Enable DHCP Relay checkbox on the Edit Managed Interface page.
	First: IP address Last IP address 192:168:10.150 192:168:10.175 Lases Elank to use there managed subnet. Address ranges to exclude (Optional) Bichole ID addresses that are resreved to for particular Doub only one value for single address. Prom To Rest Data are resreved to the Windows: Internet Neme DHCP Lease Options DNS domain name The domain name assigned to unqualified names Primary DNS See hosts Lease Blank to use the system defaults Secondary DNS Default lease 7200 Default lease Disabled M Drynamic DNS Calest in mark time in seconds Maximum lease 7200 Default lease Disabled M Disabled M Organic DHC Rest otherme Calest may receive different adverses Advanced DHCP Custom Options Option Yate	edului r devices. snagement v v v s Bereica (WINS) rerver (only used for Microsoft Windows name resolution). S Bereica (WINS) rerver (only used for Microsoft Windows name resolution). Data Type Value Row Management Data String v MicroADO-192.16 v P Address v 192.45.52.202 v P Address v v	Note that to run the server, you must mark the Run DHCP Server checkbox and clear the Enable DHCP Relay checkbox on the Edit Managed Interface page.

Solution & Interoperability Test Lab Application Notes ©2007 Avaya Inc. All Rights Reserved.

Step	Description		
10.	Navigate to the Roles page by clicking User Roles and then Roles . connects to the BSC 5000 must have a role. Roles are used to place limits or schedules on the devices. Using the pull down arrow, selec	bandwidth/session	
	down menu.		
	Robes Roles 192.168.77.30 - Microsoft Internet Explorer		
	Ele Edit Yew Figurates Icols Help	At	
	🔇 bad. + 🐑 - 🖹 😫 🐔 🔎 Seech 📌 Ferrets 🔗 🔗 + 🌺 🖻 + 📃 🏭 35		
	Agdross 🔞 https://192.168.77.30/noiselement.pl?uid=2669293224;action=paint;r=5ex.gnp;75244	🛩 🛃 Go Livis 🎽	
	blue socket	Sion out, admin Helo 🗅	
	Roles Services Destinations Schedules Locations	Create V Create	
	Actions Name Incoming BW Outgoing BW VEN VIAN Tag	Service Service Group Destination Network	
		Destination Group	
	Virregistered No Limit No Limit None	Schedule Schedule Group	
		Schedule	

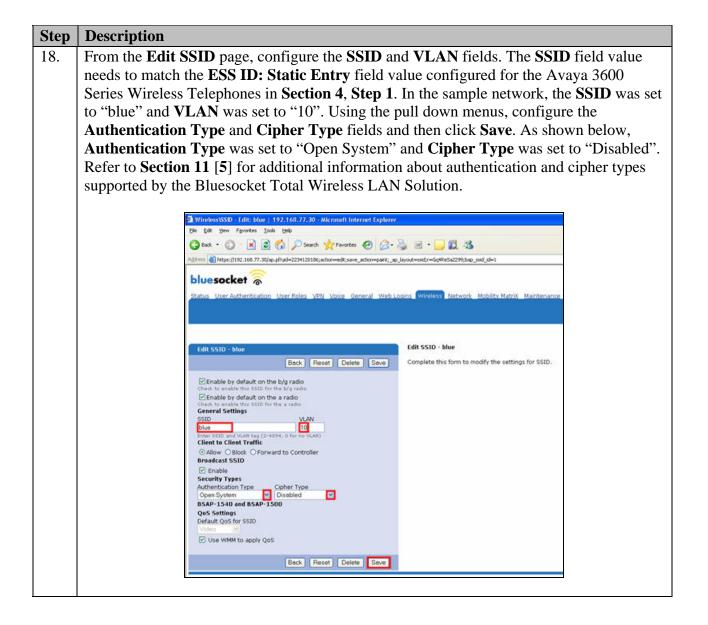
Step	Description		
11.	for the Avaya 360 Desktop Edition a background data c for the roles are lis From the Create a	0 Series Wireless Tel nd Avaya IP Softpho lients to verify QoS f sted below. a role page, input the	oles were created. One role was called IP Phones lephones and laptops running Avaya one-X ne. The other role was called Data Clients for for the voice traffic. The configuration parameters parameters shown below. Once all the settings rocess for configuring the Data Clients role.
	Ele 6	Woles Create new 197.168.77.30 Microso & Yew Fgwartes Iools Help	
	National Section 1997	Attps://192.166.77.30/ndeviewent.ghud=2666273224; ate a role ate a	e OPer user service setting? ng? ted) e OPer user service setting? ng? service setting? ng? service setting? ng? setting: and checking ends, setting with User Box Management an Destination Schedul Location Row Management

Step	Description	
12.	Navigate to the VoWLAN General Settings p. Uncheck the check-box labeled Prioritize Voic enables the rewrite feature where the BSC 5000 wireless devices. Check the check-boxes labele Enable SIP Voice Protocol and then click Sav	ce and Video Traffic . This check-box) will modify the QoS values set by the d Enable H323 Voice Protocol and
	VoWLANGeneral 192.168.77.30 - Microsoft Internet Explorer	
	Bie Edit Yew Favorites Iools Belo Co Back - Co - R 2 Co Search 👷 Favorites 🕢 📿 -	
	Address Thetes: (/192.168.77.30/vowlan.phude=30955105;action=park;save_action=park;	
	Status User Authentication User Roles VPN Voice General Web L	osins Wireless Network Mobility Matrix Meintenanse
	VoWLAN General Settings	VoWLAN Settings
	Back Reset Seve QoS Prioritize Voice and Video Traffic Supported Protocols Young the H023 Voice Protocol Write the BIP Voice Protocol Write BIP Voice Protocol Write BIP Voice Protocol Required for incoming calls in a HAT environment. Back Reset	 VolP is highly sensitive to the network delay, jitter, errors, lost, and retransmitted packets. To configure QoS, mark the Prioritize Voice and Video Traffic checkbox and then: 1. Specify an SSID for Voice traffic on either the Edit SSID page or the Create SSID page by selecting Voice from the "Default QoS for SSID" drop down menu. 2. Enable the following call admission control features on the ESAPs (for all APs, use the Edit AP System Settings - Global page; for a single AP, use either the Edit AP System Settings page or the Create New AP);

Step	Description
13.	Navigate to the IP Phones Settings page by clicking IP Phones . Check the check-box labeled Enable support for SpectraLink/Avaya IP phones . Configure the IP address of the Avaya Voice Priority Processor (see Figure 1). Using the pull down menu under Role , select IP Phones . Click Save . SpectraLink/Avaya gateway IP address or hostname "192.45.52.202"
	SpectraLink/Avaya SVP server IP address or hostname "192.45.52.202"
	IP Phones IP Phones Settings IP Phones Settings Back Reset Spectralink/Avaya IP phones settings Inable support for Spectralink/Avaya IP phones Spectralink/Avaya Gateway IP address or hostname 192.45 52 202 Spectralink/Avaya SVP server IP address or hostname 192.45 52 202 Spectralink/Avaya SVP server IP address or hostname 192.45 52 202 Cisco IP phone Settings Cisco IP phones Policy settings Pole Pole Pole Bock Reset Bock Reset
14.	Navigate to the User Authentication page by clicking User Authentication. Each device that connects to the BSC 5000 requires authentication. In the sample network, MAC address authentication was used. Using the pull down arrow select MAC Device.
	Address & https://t52.166.77.100/Lear ghude-638100257/action-park/seve_action-park/seve/1458

Step	Description	
15.	From the New MAC Device page check the che Configure the Name and MAC address fields. I	
	the colon as the delimiter XX:XX:XX:XX:XX:XX:XX	XX. For information on obtaining the
	MAC address of the Avaya 3600 Series Wireles	s Telephones, please refer to Section 11
	[3]. Use the pull down arrow for Role and select	t IP Phones. Click Save. Every device
	that connects to the BSC 5000 needs a MAC rul	e allowing access to the system. Repeat
	this step for each wireless device that connects to	to the network.
	Authentication/MAC Device Authentication - Create new 192.168.77.100 - Ele Ede Yew Favores Tools theb	- Microsoft Internet Explorer
	3 Back - 3 - 🗷 🖉 🐔 🔎 Search 👷 Pavortes 🔗 🍰 - 🍇	🖕 🖻 • 🔜 🏭 🥸
	Address () https://192.168.77.100/user.phud=638103257;adion=edk;save_edion=paint;_user	r_Jayout=M(user_jd=-1)r=QE1rNVe6101
	bluesocket	
	Status User Authentication User Roles VPN Voice General Web Login	ins Wireless Network Mobility Matrix Maintenance
	You have made changes which may affect users on the system. After you have Alternatively, you may <u>schedule</u> the update to occur at a later time.	ive made all of your changes, <u>dirk here</u> to have them take effect.
	New Service	New MAC device Complete this form if you have wireless devices on your
		network that do not support login via a web browser. The
		BSC can authenticate and assign these devices a role based on their media access control (MAC) address.
	MAC device settings	
	MAC address 00:90 7A:01 DD:84	
	Bole IP Phones	
	⊙ Normal device	
	O Permanently put this MAC in guarantine Device maintenance	
	Expire device: Never	
	Dote shown below M Year Month Day Hour Minute	
	2007 V February V 19 V 21 V : 18 V Notes	
	2	
	Back Reset Save Save and create another	
	Back Heser Save and Credie enother	

Step	Description
16.	Navigate to the Edit AP System Settings – Global page by clicking Wireless and then Global . Each AP will inherit these global parameters. However, these global settings can be overwritten for an individual AP using the Edit AP System Settings page (see Step 21). Ensure that the check-box labeled Enable SVP? is checked. Click Save .
	Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Strice Str
17.	Navigate to the SSID page by clicking Wireless and then SSID. Using the pull down menu select SSID. WirelessSSD 192.16E.77.30 - Microsoft Internet Explorer Book - O - N O - South -
	Artions Radio Defaults SSID VIAN Authentication Cipher Station All V V V V Stations Station Station



Step	Description
19.	Navigate to the AP page by clicking Wireless and then AP . The AP page lists the access
	points the BSC 5000 has found. In the sample network, no access points were connected
	to the network. Therefore, no access points are shown.
	Wirelesskip 192.168.77.100 - Microsoft Internet Explorer Ele Ede Verv Favores Tools tieb
	G bat. • () · x () () South ☆ Favories () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () · 2 () () () · 2 () () () () () () () () () () () () ()
	Address 🔕 https://192.168.77.100/ap.p?ud=638103257;action=parit_save_action=parit_ap_layout=apy=g62/627256
	bluesocket
	Status User Authentication User Roles VPN Voice General Web Logins Wireless Network Mobility Matrix Maintenance
	Global 🗗 SSID. Firmware Service. Stations RF Alarms Auto Containment
	You have made changes which may affect users on the system. After you have made all of your changes, <u>dick here</u> to have them take effect. Alternatively, you may schedule the update to occur at a later time.
	Actions Model Enabled MAC RadioMAC Hostname Location Status Active Error Firmware Hardware Messages un-sort customize
	No data found.
20.	A Bluesocket BlueSecure Access Point 1540 was plugged into the network and
	configured to use VLAN 10. As shown below, the BSAP-1540 was recognized by the
	BSC 5000. Click the <i>licon</i> to edit the configuration information for the newly
	discovered access point.
	discovered access point.
	🕽 Wireless AAP 192.168.77.30 - Microsoft Internet Explorer
	Be Edk Yew Figurites Look Heb
	Sion out, admin I Help
	Status User Authentrication User Roles VPN Voice General Web Logins Wireless Network Mobility Matrix Maintenance
	Create_
	Global AP SSID Firmware Service Stations RF Alarms Auto Containment
	Actions Model Enabled MAC RadioMAC Hostname Location Status Active Error Firmware Hardware Messages un-sort customize
	All V All V V V V
	Image: Same of the second se
	1 row download
	2007-02-19 21:51:12 617 Administrative users: Admin Model: BSC-2100 Click on the pencil icon to edit an item.
	Second and one preside near on each are fremily safety on the treatment out of device an identic

Step	Description	
21.	From the Edit AP page, ensure that the check-box laber optional fields, Hostname and Location , can also be c The parameters highlighted with the blue background be AP System Settings – Global page (see Step 16).	onfigured. Click Save.
	In the sample network a total of three access points were VLAN 10 and one access point was on VLAN 11. Report VLAN 10 and for the AP on VLAN 11.	-
	 Wirelesskip - Edit: 00:12:cf:3d:44:ba 192.168.77.30 - Microsoft Internet Explorer Edit Yew Favorites Tools Help Back - O - R 2 A Post Provides O - Post ProvidesO - Post ProvidesO - Post ProvidesO - Post ProvidesO - Post Pro	ng1+e8-061/2/2076
	System <u>802.11b/a</u> <u>802.11a</u> Edit AP System Settings - 00:12:cf:3d:44:ba	Edit AP System Settings - 00: 12:cf:3d:44:ba
	Back Reset Default Delete Save Next BlueSecure Access Point 1540 Image: Save and	Complete this form to modify the system settings for this APs. Fields shown in this color are using default settings from global tab. You can reset all fields to default value by clicking the "Default" button.
	Hostname AP-1 Optional Rostname Location Dev.Connect Room 7 Optional Rostno Firmware BSAP-1540 and BSAP-1500	
	Lead Balancing Average user count per AP Enforcement Low Average number of assestations per AP (1-54) befres balanding clants. Voice Call Admission Control? Voice Sessions 0	
	Maximum number of voice sessions per radio. 10 maans unimited. 10 Maximum number of video sessions per radio. 10 maans unimited. 11 maans unimited. 12 maans unimited. 13 maans unimited. 14 maans unimited. 15 maans unimited. 15 maans unimited. 16 maans unimited. 17 maans unimited. 18 maans unimited. 18 maans unimited. 19 maans unimited. 19 maans unimited. 19 maans unimited. 10 maans unim	
	Custom User Login Normal Choose a login page for all users on this AP, otherwise choose Normal to use Location/VLAN based login page Diagnostics Chock to enable remote SSH diagnostics	
	Done	

2	Description				
	Once all the access points have been configured, return to the AP page by clicking				
	Wireless and then AP. Check the check-box found under the Actions column. This will				
	check all of the check-boxes for the known access points. Click Apply to update the configuration for all of the access points.				
	Wireless WP 192.168.77.30 - Microsoft Internet Explorer				
	Ele Edit Yew Figurates Iools Help				
	\bigcirc Each \cdot \bigcirc \land \blacksquare \textcircled{O} \land Search \checkmark Feverates \textcircled{O} \bigcirc \bullet \bigcirc \textcircled{U} \checkmark \textcircled{U} \checkmark				
	légéreis 🗃 https://192.168.77.20/ap.phud=11398326;adtom=psint;_pp.jayout=ap;_ptopt=setting==#672dr/356				
	Status User Authentication User Roles VPN Voice General Web Logins Wireless Network Mobility Matrix Maintenance Screeke.				
	Actions Model Enabled MAC RadioMAC Hostname Location Status Active Error Firmware Hardware Messa				
	Image: Constraint of the state of				

7. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying interoperability of the Bluesocket Total Wireless LAN Solution with Avaya IP Office, Avaya 3600 Series Wireless Telephones, and Avaya IP Office Phone Manager Pro PC Softphone. Additional testing verified proper operation between the Avaya 3600 Series Wireless Telephones with the Avaya 5620SW IP Telephone and with the Avaya 2420 Digital Telephone. Network level tests included verifying seamless roaming from access point to access point and validating Quality of Service for voice calls in a congested network.

7.1. General Test Approach

The general test approach was to register the Avaya 3600 Series Wireless Telephones and Avaya IP Office Phone Manager Pro PC Softphone with Avaya IP Office through the Bluesocket Total Wireless LAN Solution. Calls were made between both wired and wireless telephony products and specific calling features were exercised. To validate Quality of Service, low priority background traffic was injected into the network and the Bluesocket Total Wireless LAN Solution was verified to maintain voice calls while dropping the low priority traffic.

7.2. Test Results

The Bluesocket Total Wireless LAN Solution passed all test cases. Telephony products were verified to successfully register with Avaya IP Office through the Bluesocket Total Wireless LAN Solution. The compliance testing also focused on verifying Quality of Service for voice traffic while low priority background traffic was competing for bandwidth. Avaya 3600 Series Wireless Telephones were verified to roam successfully between access points on the same network (Layer 2 roaming) and between access points on a different network (Layer 3 roaming) while maintaining voice calls. Three different encryptions schemas were tested: Clear Encryption, WEP-128 and WPA-PSK. Two codecs were used for testing: G7.11 and G.729. The Avaya 3626 Series Wireless Telephone "Push-to-talk" feature was verified to operate correctly. Telephone calls were verified to operate correctly with the media path direct between the telephones and with the media path centralized through the Avaya IP Office. Calls were maintained for durations over one minute without degradation to voice quality. The telephony features verified to operate correctly included attended/unattended transfer, conference call participation, conference call add/drop, multiple call appearances, caller ID operation, hold, return from hold, leaving voicemail and retrieving voicemail.

8. Verification Steps

- Ensure that the **SSID** has been properly configured; see **Section 4**, **Step 1**.
- Check Section 6, Step 15 and ensure that the MAC addresses of the wireless devices are correct.
- Verify that the User Authentication page shows that Enable MAC device is enabled; see Section 6, Step 15.
- Ensure that the **Call Server Extension** and **Call Server Password** fields are administered correctly; see **Section 4**, **Step 1**.
- Ensure that the Avaya Voice Priority Processor is available on the IP network and reachable from the subnets where the wireless telephones will be used. Issue an extended ping, or a sourced ping, from the VLAN 10 and/or VLAN 11 IP addresses on the Bluesocket BSC 5000.
- After making any changes to the Bluesocket controller or Bluesocket access points, ensure that the configuration changes have been applied; see Section 6, Step 20.
- Ensure that "multicast" is enabled on the Protected port and on each VLAN on the BSC 5000; see Section 6 Step 2, Step 3, and Step 5.
- Ensure that the configuration on the telephone is administered to support the "Push-to-talk" feature; see Section 4, Step 2.

Note: Only the Avaya 3626 Wireless Telephones support the "Push-to-talk" feature.

9. Support

Technical support for the Bluesocket Total Wireless LAN Solution can be obtained through the following:

- **Phone:** 1-781-328-0888
- Email: support@bluesocket.com
- Web: <u>http://www.bluesocket.com</u>

10. Conclusion

These Application Notes demonstrate how to build a sample VoIP enabled wireless network using the Bluesocket Total Wireless LAN Solution with two VLANs and Avaya 3600 Series Wireless Telephones including enabling the "Push-to-talk" feature for the Avaya 3626 Wireless Telephones.

11. Additional References

The documents referenced below were used for additional support and configuration information. The Avaya documentation was obtained from <u>http://support.avaya.com</u>. The Bluesocket documentation was obtained from <u>http://www.bluesocket.com</u> (access to Bluesocket documentation may require a support account).

- [1] Avaya IP Office 4.0 Installation Manual, January 2007, Issue 15e, Document Number 15-601042
- [2] Avaya IP Office 4.0 Manager:02. Configuration Settings, January 2007, Issue 19k
- [3] Avaya Voice Priority Processor for SRP Installation, Setup, and Administration, July 2005, Issue 1, Document Number 21-300637
- [4] Avaya Configuration Cradle/Avaya 3600 Series Wireless Telephones Administrator Guide, July 2005, Issue 1, Document Number 21-300630
- [5] *BlueSecure*[™] *Controller Setup and Administration Guide*, January 2007, Part Number 870-202TT-M00

©2007 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 Developer*Connection* Program at <u>devconnect@avaya.com</u>.