



## **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.

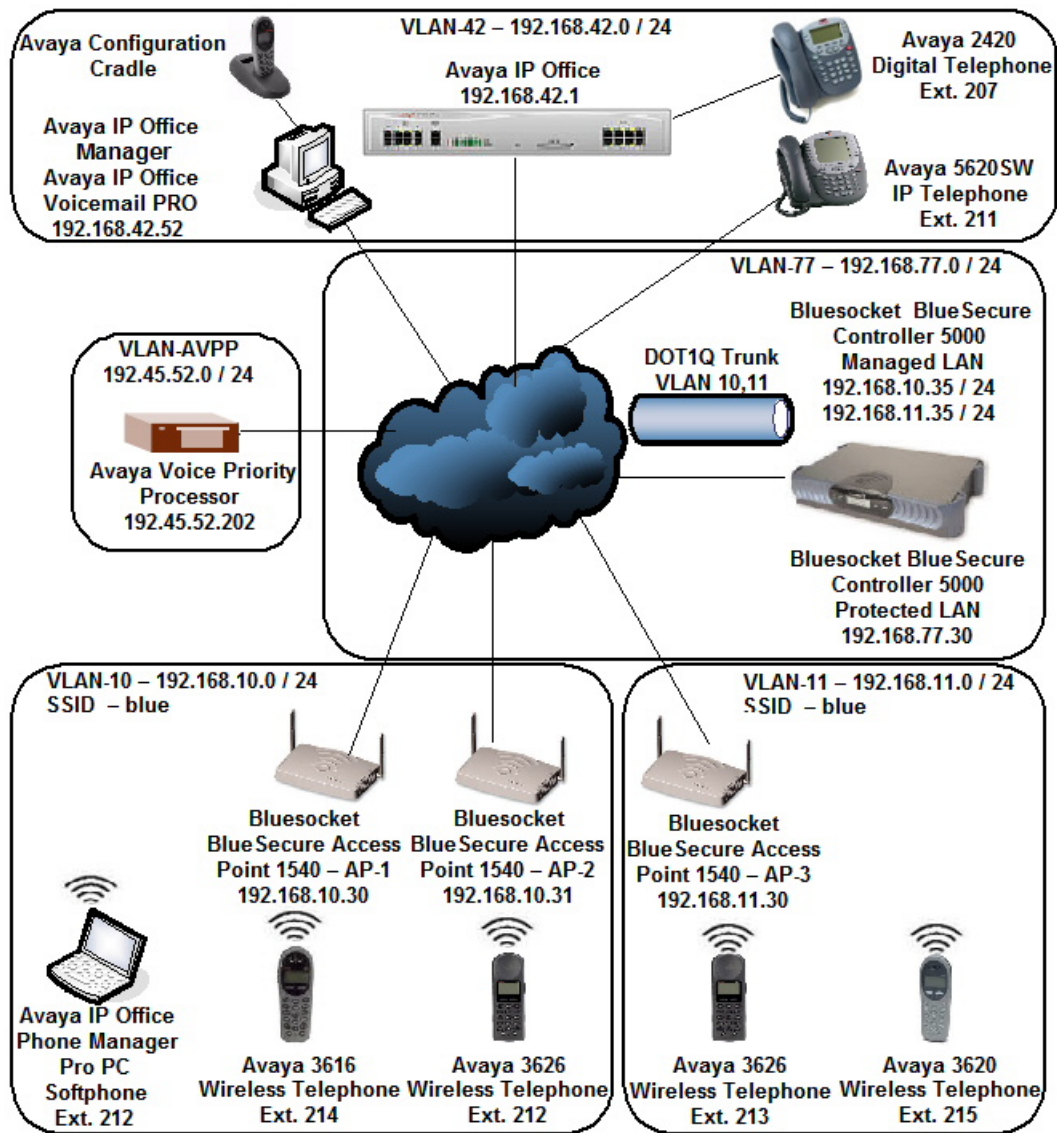
The Bluesocket Total Wireless LAN Solution is comprised of a controller and access points. Bluesocket BlueSecure controllers provide reliable, policy-based wireless LAN (WLAN) security, stateful firewalling, Quality of Server/Class of Service (QoS/CoS), Layer 3 intrusion detection, and dynamic RF management. 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 omni-directional 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


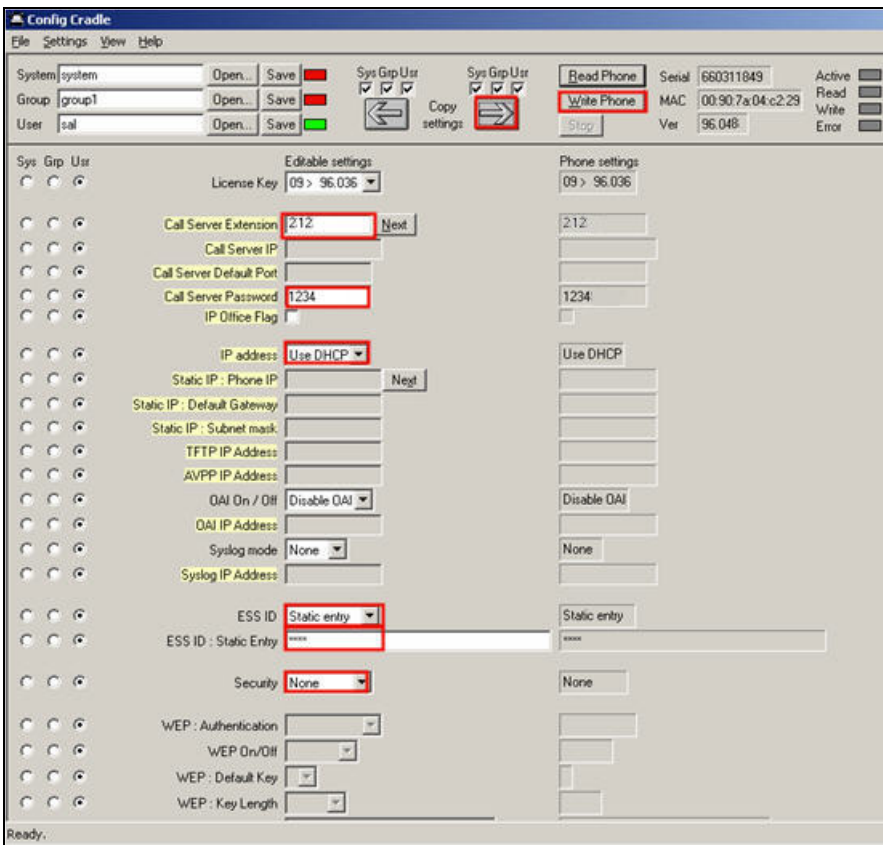
### 3. Configure Avaya IP Office


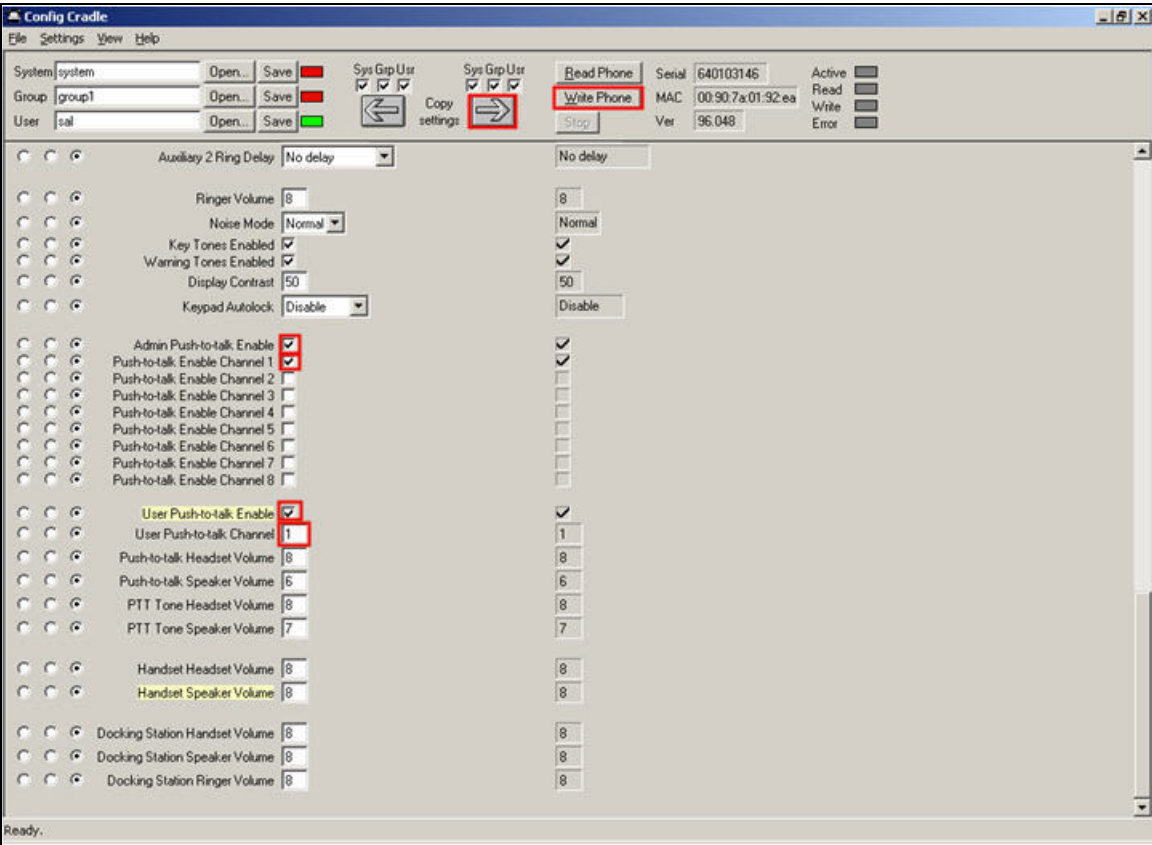
All of the telephones configured in the sample network in **Figure 1** were administered as VoIP extensions in Avaya IP Office except for the digital telephone which was administered as a digital extension. For complete references on how to administer these types of stations please refer to **Section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

Step	Description
1.	<p>From the <b>Config Cradle</b> page, configure the Avaya 3600 Series Wireless Telephones with the parameters below. Once all the configuration data has been set, click the  button and then click the <b>Write Phone</b> button. The <b>ESS ID: Static Entry</b> field must match the <b>SSID</b> field configured on the BSC 5000 in <b>Section 6, Step 18</b>. The <b>Security</b> field must match the <b>Authentication Type</b> field configured on the BSC 5000 in <b>Section 6, Step 18</b>. Repeat this process for each telephone and modify the <b>Call Server Extension</b> field to reflect the extension being provisioned. Three different security schemas were tested: “None”, “WEP” and “WPA-PSK”. For details about configuring these options, refer to <b>Section 11 [4]</b>.</p> <p> <b>Call Server Extension</b> “212”  <b>Call Server Password</b> “1234”  <b>IP address</b> “Use DHCP”  <b>ESS ID</b> “Static entry”  <b>ESS ID : Static Entry</b> “blue”  <b>Security</b> “None” </p> 

Step	Description
2.	<p>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 <b>Admin Push-to-talk Enable</b> and <b>User Push-to-talk Enable</b> have been checked. Ensure that the check-box labeled <b>Push-to-talk Enable Channel 1</b> has been checked. Input “1” in the <b>User Push-to-talk Channel</b> field. This value must be configured on the 3626 Wireless Telephones using the feature. Once the parameters for “Push-to-talk” have been configured, click the  button and then click the <b>Write Phone</b> button to save the configuration to the telephone.</p> 

## 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.

<b>Terminal Type</b>	“VT-100”
<b>Bits per second</b>	“9600”
<b>Data bits</b>	“8”
<b>Parity</b>	“None”
<b>Stop bits</b>	“1”
<b>Flow control</b>	“None”

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

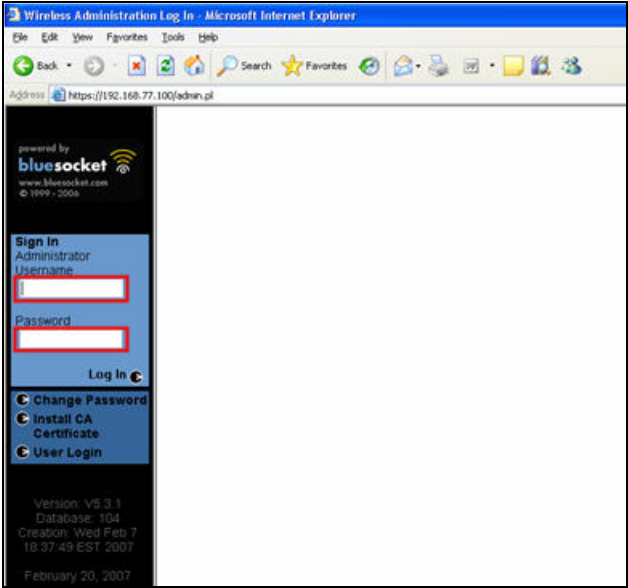


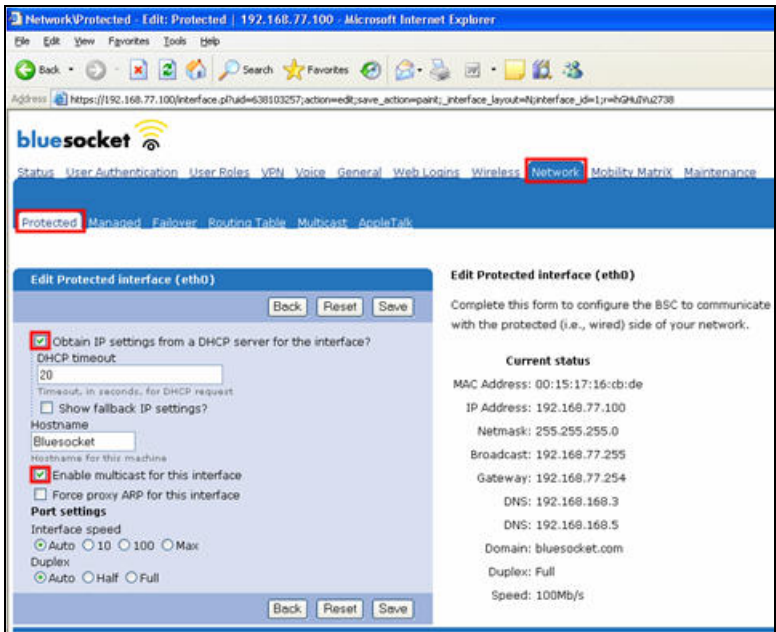
Step	Description
2.	<p data-bbox="280 237 1424 342">From the <b>Network Configuration</b> screen navigate using the up/down arrow keys and input the following information. Press <b>ESC</b> when all the configuration information has been set.</p> <div data-bbox="375 380 865 489"> <p><b>IP Address</b>                “192.45.52.202”</p> <p><b>Subnet Mask</b>            “255.255.255.0”</p> <p><b>Default Gateway</b>       “192.45.52.1”</p> </div> <div data-bbox="284 527 1417 1052" style="border: 1px solid black; padding: 10px;"> <pre data-bbox="297 531 1404 1035"> Network Configuration Hostname: [AVPPTR6], Address: 0.0.0.0  Ethernet Address (fixed):    00:90:7A:00:00:06 <b>IP Address:</b>                <b>192.45.52.202</b> Hostname:                   AVPPTR6 <b>Subnet Mask:</b>               <b>255.255.255.0</b> <b>Default Gateway:</b>          <b>192.45.52.1</b> SVP-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 </pre> </div>

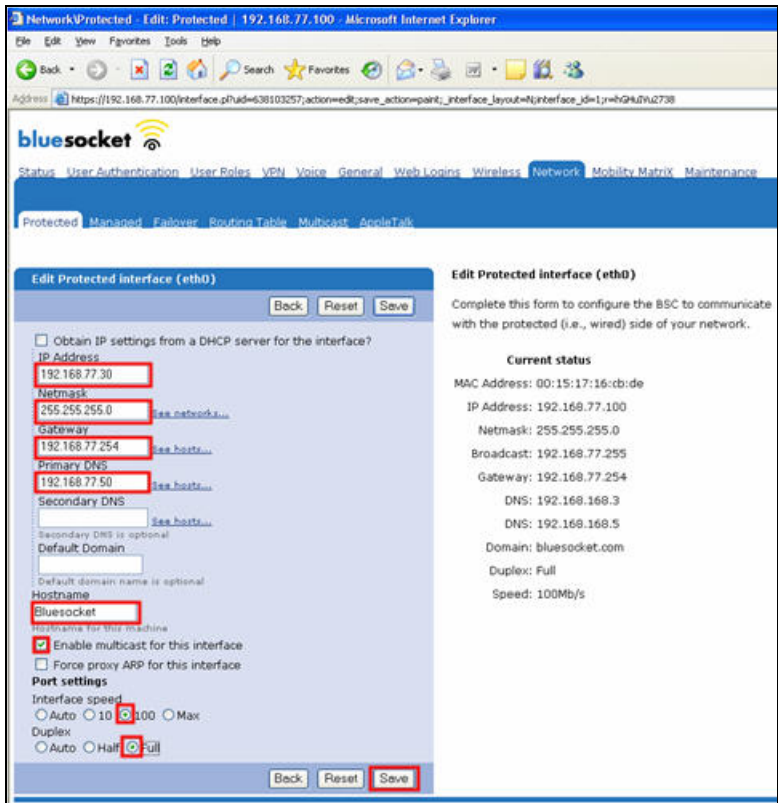
## 6. Configure Bluesocket BlueSecure Controller 5000

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 (<http://192.168.77.100/admin.pl>). Once connected to the BSC 5000, the IP address will be reconfigured to 192.168.77.30 as shown in **Figure 1**.

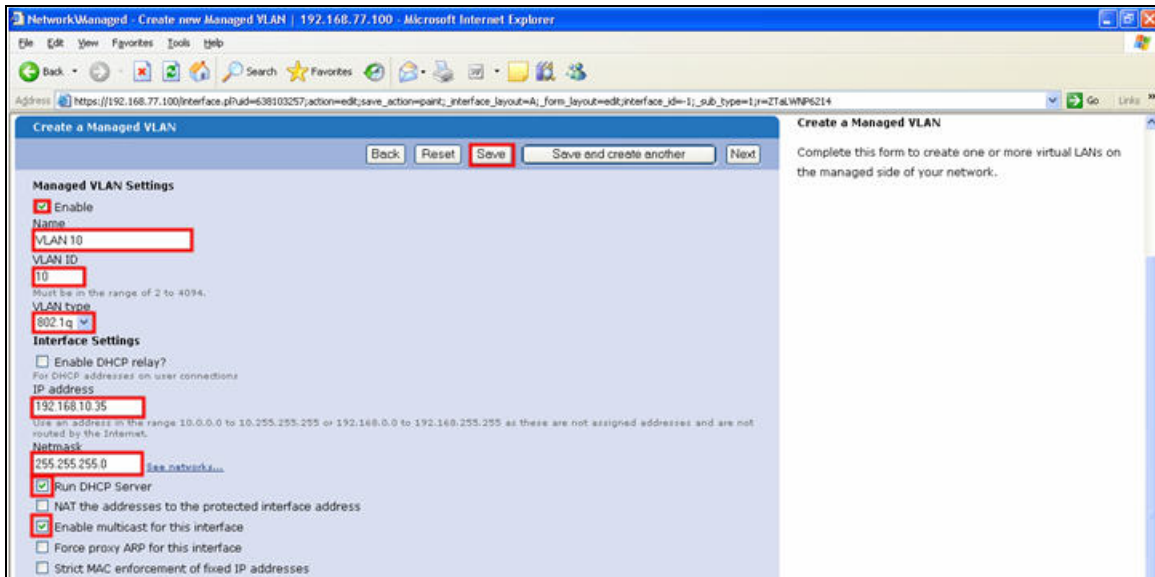
Step	Description
1.	<p>Login to the BSC 5000 by providing the appropriate login credentials, available in the Bluesocket document found in <b>Section 11 [5]</b>. Once connected and logged in to the BSC 5000 the user can administer the wired and wireless configuration.</p> 


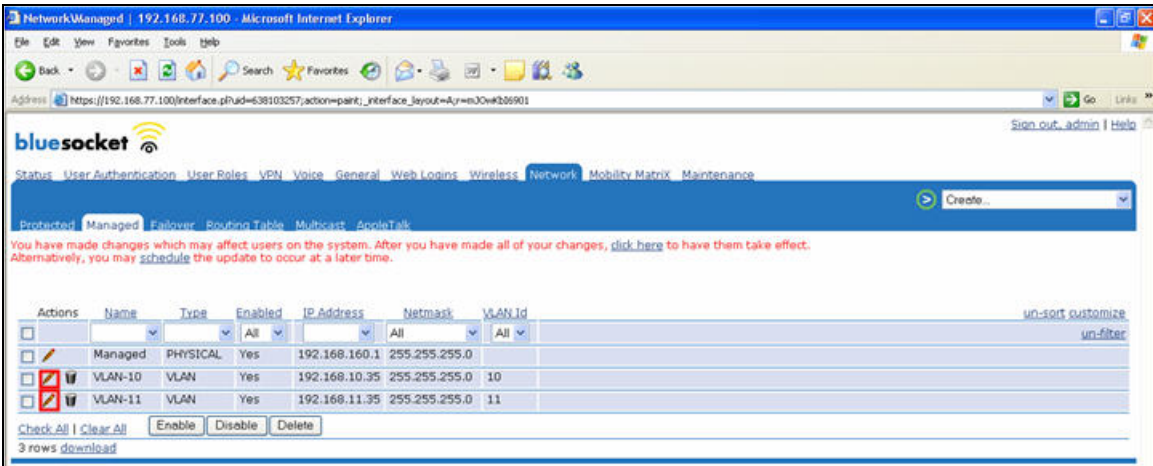
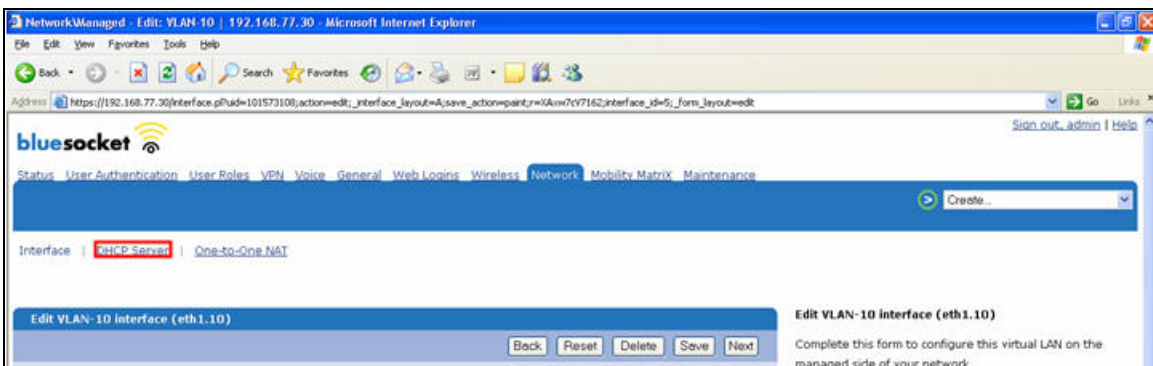
Step	Description
2.	<p>To configure the BSC 5000 Protected port to use a static IP address, navigate to the <b>Edit Protected Interface</b> page by clicking <b>Network</b> and then <b>Protected</b>. Uncheck the checkbox labeled <b>Obtain IP settings from a DHCP server for the interface?</b>.</p> 

Step	Description
3.	<p>Once the check-box labeled <b>Obtain IP Settings from a DHCP server for this interface?</b> has been unchecked, the user is presented with the following screen to configure the IP address and other parameters. To support the “Push-to-talk” feature supported on the Avaya 3626 Wireless Telephones, make sure that the check-box labeled <b>Enable multicast for this interface</b> has been checked. Once all the configuration information has been set, click <b>Save</b>. In the sample network the BSC 5000 was configured for the following:</p> <p> <b>IP Address</b> “192.168.77.30”  <b>Netmask</b> “255.255.255.0”  <b>Gateway</b> “192.168.77.254”  <b>Primary DNS</b> “192.168.77.50”  <b>Hostname</b> “Bluesocket”  <b>Interface Speed</b> “100”  <b>Duplex</b> “Full” </p> 

Step	Description
4.	<p>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.</p>
5.	<p>To configure the BSC 5000 Managed port, click <b>Network</b> and then <b>Managed</b>. Use the pull down arrow and select <b>Managed-side VLAN</b>. This will bring up a new page where the VLAN information can be configured.</p>

Step	Description															
6.	<p>From the <b>Create a Managed VLAN</b> page, check the <b>Enable</b>, <b>Run DHCP Server</b>, and <b>Enable multicast for this interface</b> check-boxes. The <b>Enable multicast for this interface</b> check-box needs to be checked in order to support the Avaya 3626 Wireless Telephone “Push-to-talk” feature. In the sample network the BSC 5000 was the DHCP server and two VLANs were created with the configuration parameters listed below. Once all the configuration information has been set, click <b>Save</b>. Repeat <b>Step 5-6</b> for each VLAN.</p> <table><tr><td><b>Name</b></td><td>“VLAN 10”</td><td>“VLAN 11”</td></tr><tr><td><b>Tag</b></td><td>“10”</td><td>“11”</td></tr><tr><td><b>Type</b></td><td>“802.1q”</td><td>“802.1q”</td></tr><tr><td><b>IP address</b></td><td>“192.168.10.35”</td><td>“192.168.11.35”</td></tr><tr><td><b>Netmask</b></td><td>“255.255.255.0”</td><td>“255.255.255.0”</td></tr></table>	<b>Name</b>	“VLAN 10”	“VLAN 11”	<b>Tag</b>	“10”	“11”	<b>Type</b>	“802.1q”	“802.1q”	<b>IP address</b>	“192.168.10.35”	“192.168.11.35”	<b>Netmask</b>	“255.255.255.0”	“255.255.255.0”
<b>Name</b>	“VLAN 10”	“VLAN 11”														
<b>Tag</b>	“10”	“11”														
<b>Type</b>	“802.1q”	“802.1q”														
<b>IP address</b>	“192.168.10.35”	“192.168.11.35”														
<b>Netmask</b>	“255.255.255.0”	“255.255.255.0”														

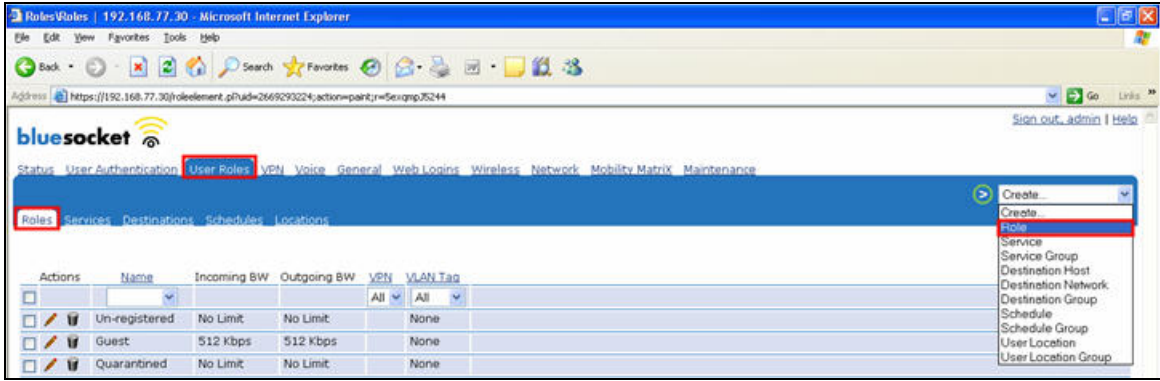


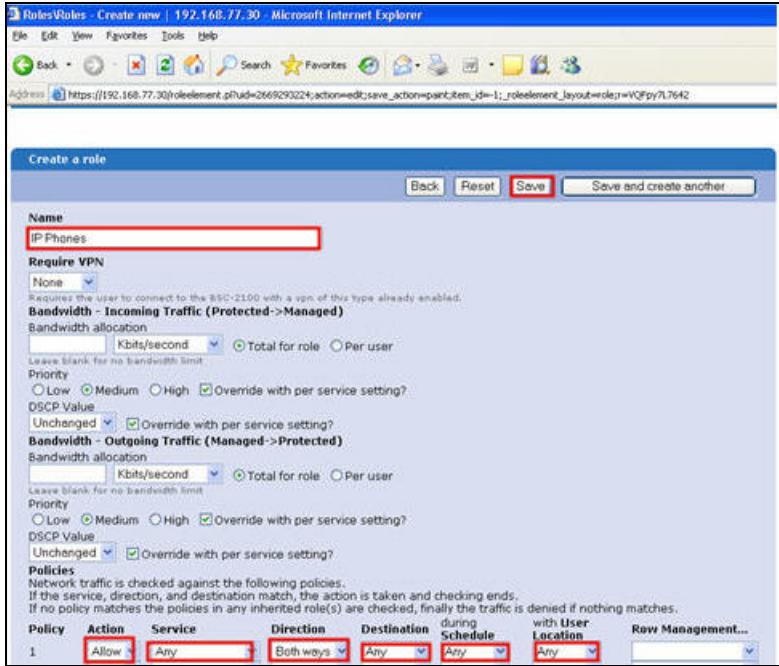
Step	Description
7.	<p>Navigate to the <b>Managed</b> page by clicking <b>Network</b> and then <b>Managed</b>. This page now shows the VLAN information. Click the  icon for one of the listed VLANs to configure the DHCP server settings for that VLAN.</p> 
8.	<p>Navigate to the <b>DHCP Server</b> page from the <b>Edit VLAN</b> page by clicking <b>DHCP Server</b>.</p> 

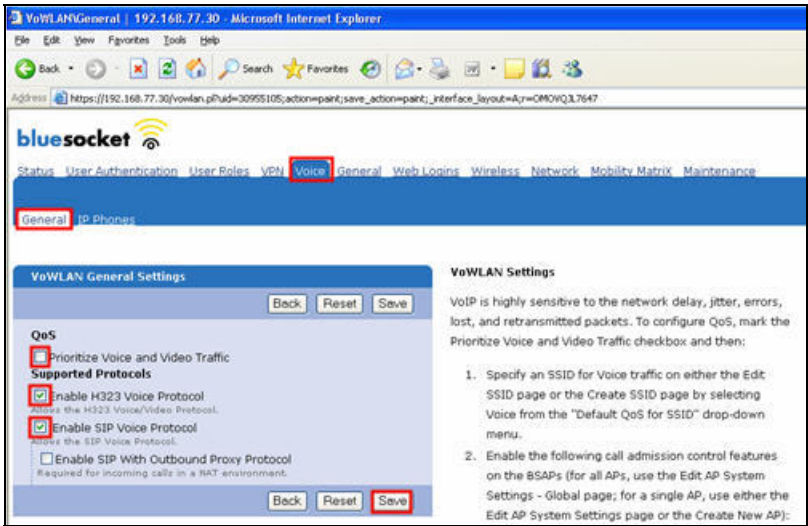


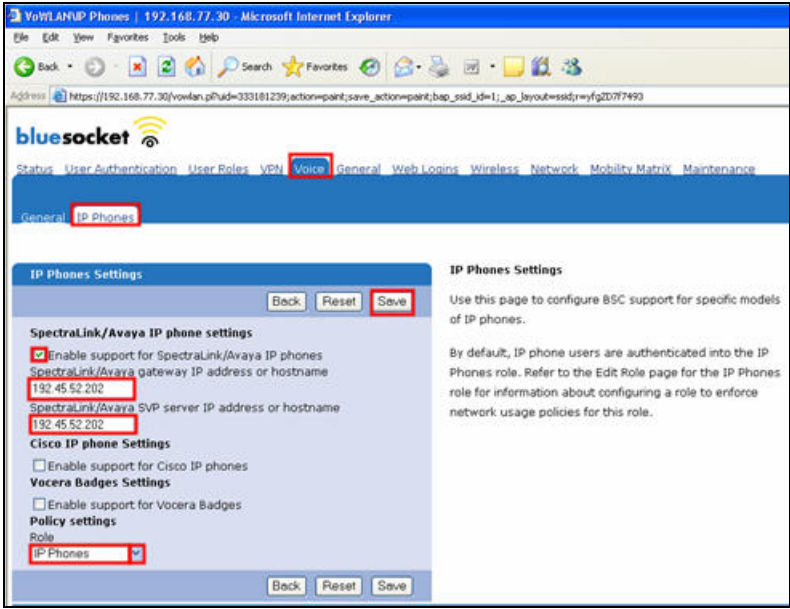
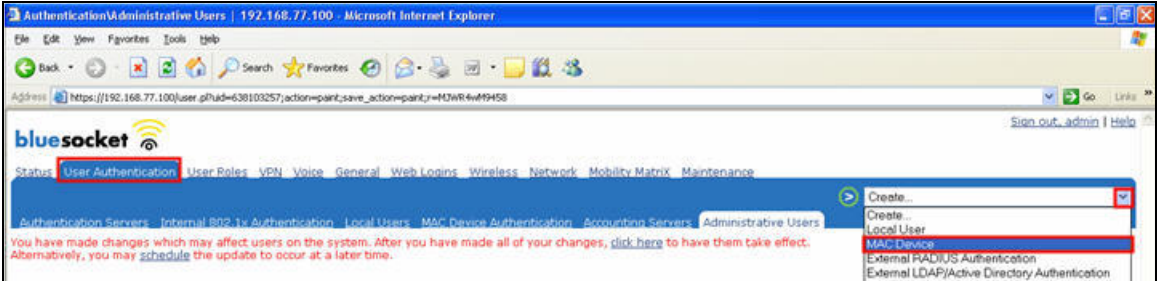
Step	Description									
9.	<p>From the <b>DHCP Server</b> page configure the <b>First IP address</b> and <b>Last IP address</b> fields that will be used to dynamically assign IP addresses to the wireless devices. The values used for the DHCP parameters for this sample network are listed below.</p> <table><tr><td>Name</td><td>VLAN 10</td><td>VLAN 11</td></tr><tr><td><b>First IP address</b></td><td>“192.168.10.150”</td><td>“192.168.11.150”</td></tr><tr><td><b>Last IP address</b></td><td>“192.168.10.175”</td><td>“192.168.11.175”</td></tr></table> <p>Using the scroll bar on the right side of the screen, scroll down to the <b>Advanced DHCP Custom Options</b> section. Two options are needed so that the Avaya 3600 Series Wireless Telephones can successfully register with Avaya IP Office. DHCP Option 176 provides the IP address of the Avaya IP Office system via the <b>MCIPADD</b> parameter and the port to be used for communication via the <b>MCPOR</b> parameter. In the sample network the value for Option 176 was set to “MCIPADD=192.168.42.1;MCPOR=1719”. Option 151 provides the IP address of the Avaya Voice Priority Processor and was set to “192.45.52.202” in the sample network. Once all the information has been set, click <b>Save</b>.</p> <p>Repeat <b>Steps 7-9</b> for each VLAN.</p>	Name	VLAN 10	VLAN 11	<b>First IP address</b>	“192.168.10.150”	“192.168.11.150”	<b>Last IP address</b>	“192.168.10.175”	“192.168.11.175”
Name	VLAN 10	VLAN 11								
<b>First IP address</b>	“192.168.10.150”	“192.168.11.150”								
<b>Last IP address</b>	“192.168.10.175”	“192.168.11.175”								

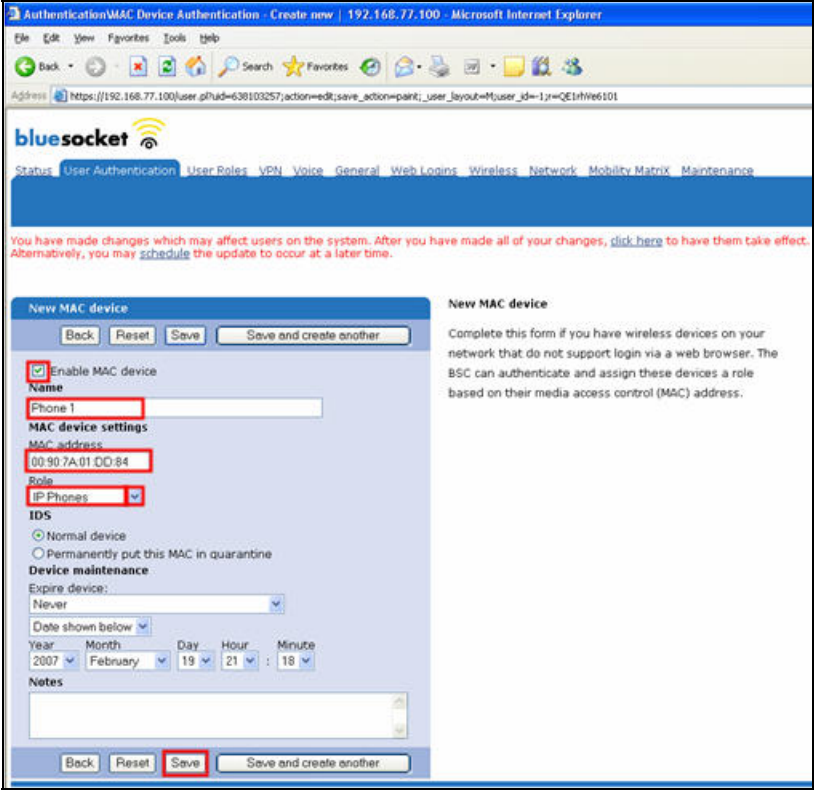


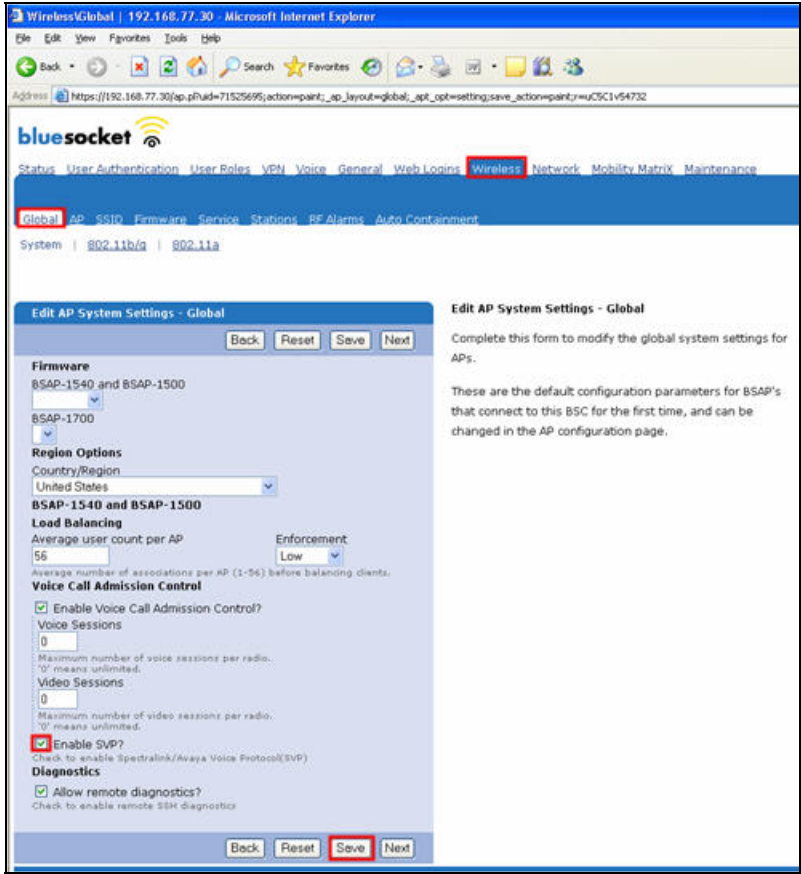
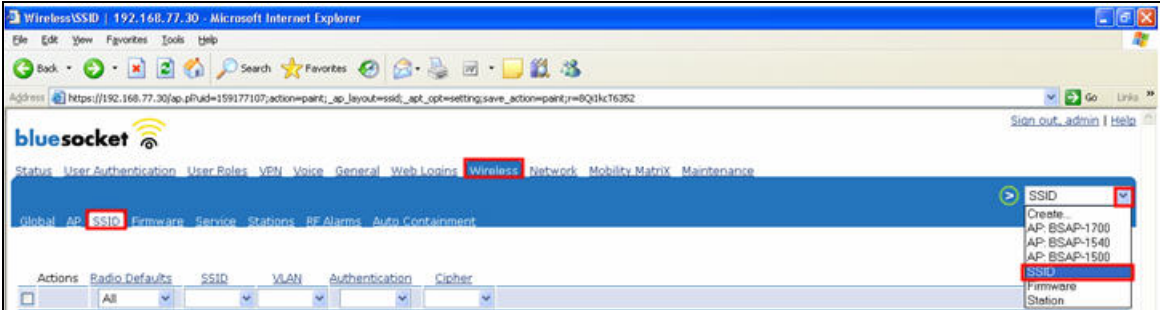
Step	Description
10.	<p>Navigate to the <b>Roles</b> page by clicking <b>User Roles</b> and then <b>Roles</b>. Every device that connects to the BSC 5000 must have a role. Roles are used to place bandwidth/session limits or schedules on the devices. Using the pull down arrow, select <b>Role</b> from the drop down menu.</p> 

Step	Description																					
11.	<p>In the sample network two additional roles were created. One role was called <b>IP Phones</b> for the Avaya 3600 Series Wireless Telephones and laptops running Avaya one-X Desktop Edition and Avaya IP Softphone. The other role was called <b>Data Clients</b> for background data clients to verify QoS for the voice traffic. The configuration parameters for the roles are listed below.</p> <p>From the <b>Create a role</b> page, input the parameters shown below. Once all the settings have been set, click <b>Save</b>. Repeat the process for configuring the <b>Data Clients</b> role.</p> <table><tr><td><b>Name</b></td><td>“IP Phones”</td><td>“Data Clients”</td></tr><tr><td><b>Action</b></td><td>“Allow”</td><td>“Allow”</td></tr><tr><td><b>Service</b></td><td>“Any”</td><td>“Any”</td></tr><tr><td><b>Direction</b></td><td>“Both ways”</td><td>“Both ways”</td></tr><tr><td><b>Destination</b></td><td>“Any”</td><td>“Any”</td></tr><tr><td><b>Schedule</b></td><td>“Any”</td><td>“Any”</td></tr><tr><td><b>User Location</b></td><td>“Any”</td><td>“Any”</td></tr></table> 	<b>Name</b>	“IP Phones”	“Data Clients”	<b>Action</b>	“Allow”	“Allow”	<b>Service</b>	“Any”	“Any”	<b>Direction</b>	“Both ways”	“Both ways”	<b>Destination</b>	“Any”	“Any”	<b>Schedule</b>	“Any”	“Any”	<b>User Location</b>	“Any”	“Any”
<b>Name</b>	“IP Phones”	“Data Clients”																				
<b>Action</b>	“Allow”	“Allow”																				
<b>Service</b>	“Any”	“Any”																				
<b>Direction</b>	“Both ways”	“Both ways”																				
<b>Destination</b>	“Any”	“Any”																				
<b>Schedule</b>	“Any”	“Any”																				
<b>User Location</b>	“Any”	“Any”																				

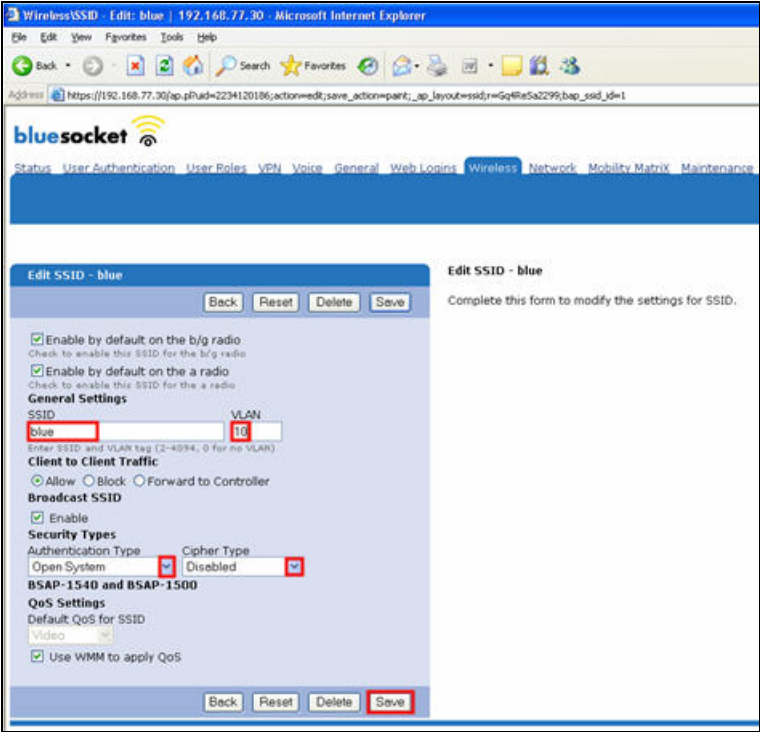
Step	Description
12.	<p>Navigate to the <b>VoWLAN General Settings</b> page by clicking <b>Voice</b> and then <b>General</b>. Uncheck the check-box labeled <b>Prioritize Voice and Video Traffic</b>. This check-box enables the rewrite feature where the BSC 5000 will modify the QoS values set by the wireless devices. Check the check-boxes labeled <b>Enable H323 Voice Protocol</b> and <b>Enable SIP Voice Protocol</b> and then click <b>Save</b>.</p> 

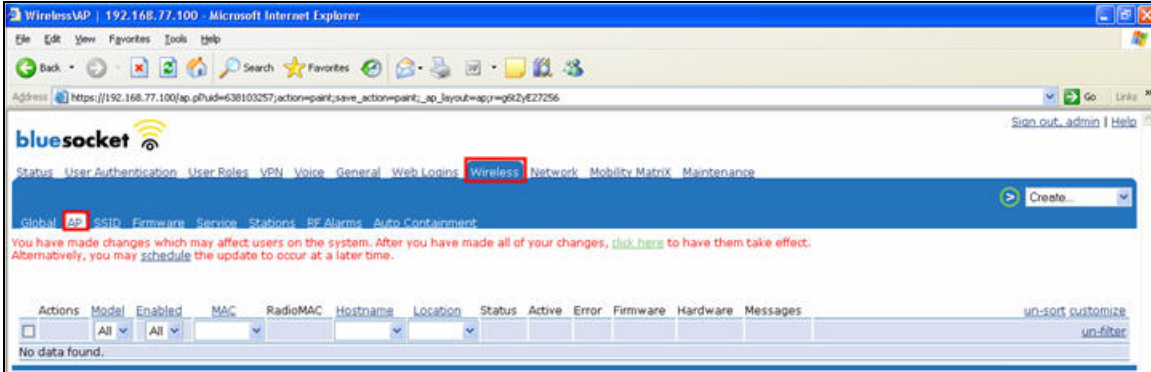

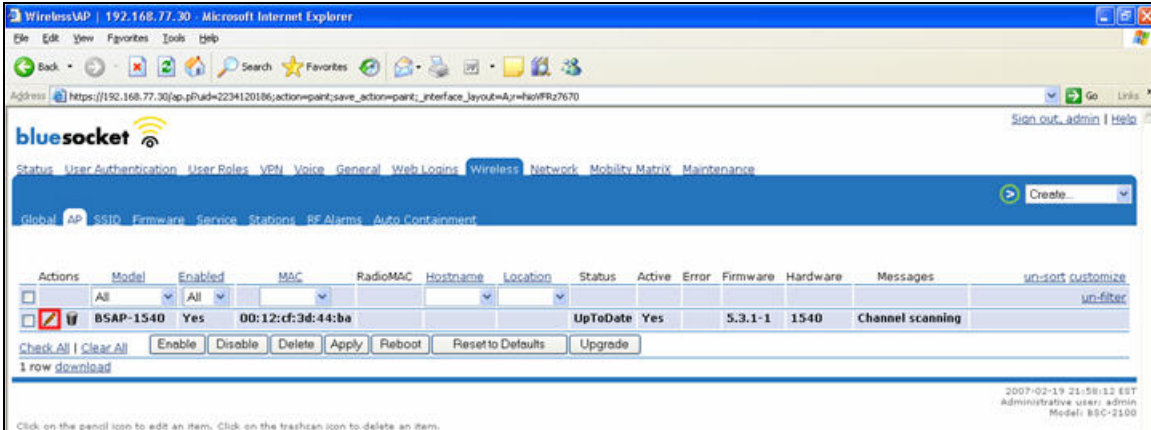
Step	Description
13.	<p>Navigate to the <b>IP Phones Settings</b> page by clicking <b>IP Phones</b>. Check the check-box labeled <b>Enable support for SpectraLink/Avaya IP phones</b>. Configure the IP address of the Avaya Voice Priority Processor (see <b>Figure 1</b>). Using the pull down menu under <b>Role</b>, select <b>IP Phones</b>. Click <b>Save</b>.</p> <p><b>SpectraLink/Avaya gateway IP address or hostname</b> “192.45.52.202”  <b>SpectraLink/Avaya SVP server IP address or hostname</b> “192.45.52.202”</p> 
14.	<p>Navigate to the <b>User Authentication</b> page by clicking <b>User Authentication</b>. 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 <b>MAC Device</b>.</p> 

Step	Description
15.	<p>From the <b>New MAC Device</b> page check the check-box labeled <b>Enable MAC device</b>. Configure the <b>Name</b> and <b>MAC address</b> fields. Note that the MAC address format uses the colon as the delimiter XX:XX:XX:XX:XX:XX. For information on obtaining the MAC address of the Avaya 3600 Series Wireless Telephones, please refer to <b>Section 11 [3]</b>. Use the pull down arrow for <b>Role</b> and select <b>IP Phones</b>. Click <b>Save</b>. Every device that connects to the BSC 5000 needs a MAC rule allowing access to the system. Repeat this step for each wireless device that connects to the network.</p> 

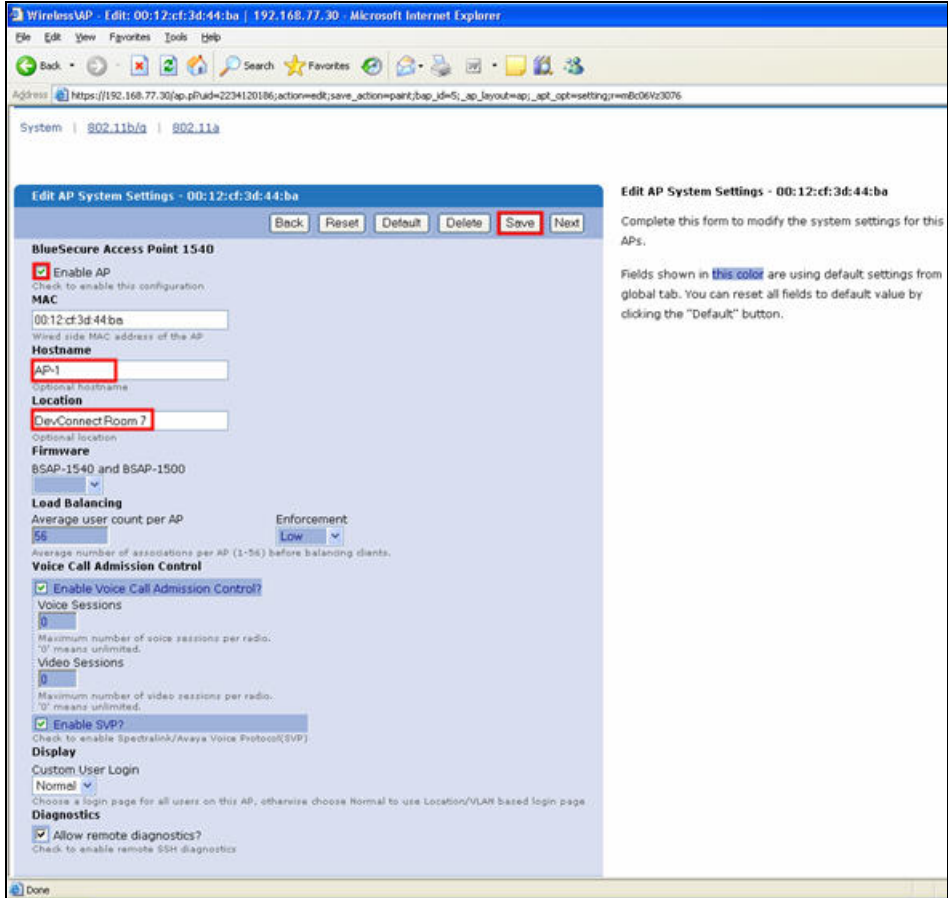
Step	Description
16.	<p>Navigate to the <b>Edit AP System Settings – Global</b> page by clicking <b>Wireless</b> and then <b>Global</b>. Each AP will inherit these global parameters. However, these global settings can be overwritten for an individual AP using the <b>Edit AP System Settings</b> page (see <b>Step 21</b>). Ensure that the check-box labeled <b>Enable SVP?</b> is checked. Click <b>Save</b>.</p> 
17.	<p>Navigate to the <b>SSID</b> page by clicking <b>Wireless</b> and then <b>SSID</b>. Using the pull down menu select <b>SSID</b>.</p> 

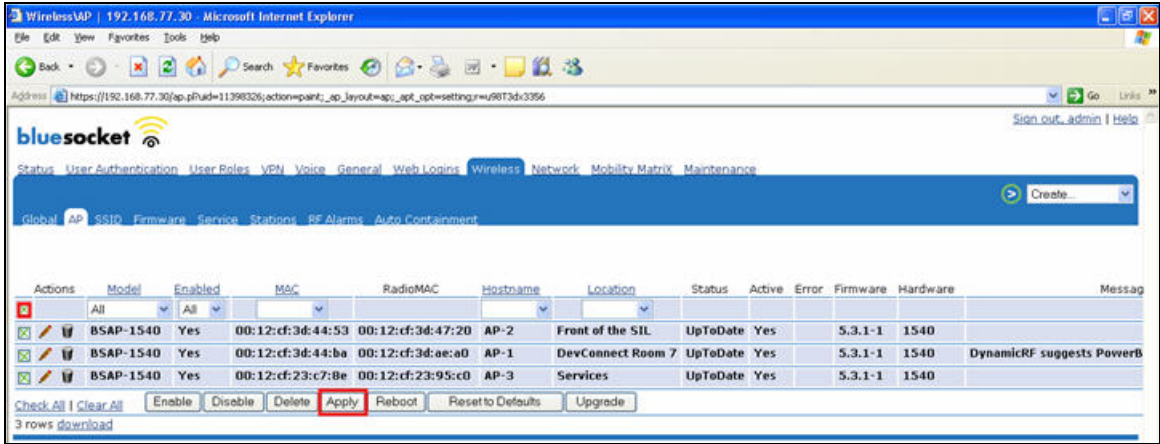


Step	Description
18.	<p>From the <b>Edit SSID</b> page, configure the <b>SSID</b> and <b>VLAN</b> fields. The <b>SSID</b> field value needs to match the <b>ESS ID: Static Entry</b> field value configured for the Avaya 3600 Series Wireless Telephones in <b>Section 4, Step 1</b>. In the sample network, the <b>SSID</b> was set to “blue” and <b>VLAN</b> was set to “10”. Using the pull down menus, configure the <b>Authentication Type</b> and <b>Cipher Type</b> fields and then click <b>Save</b>. As shown below, <b>Authentication Type</b> was set to “Open System” and <b>Cipher Type</b> was set to “Disabled”. Refer to <b>Section 11 [5]</b> for additional information about authentication and cipher types supported by the Bluesocket Total Wireless LAN Solution.</p>  <p>The screenshot shows a web browser window titled 'WirelessSSID - Edit: blue   192.168.77.30 - Microsoft Internet Explorer'. The address bar shows a URL from 192.168.77.30. The page has a blue header with the 'bluesocket' logo and navigation tabs: Status, User Authentication, User Roles, VPN, Voice, General, Web Logins, Wireless, Network, Mobility Matrix, and Maintenance. The 'Wireless' tab is selected. The main content area is titled 'Edit SSID - blue' and contains a form with the following sections: <ul style="list-style-type: none"> <li><b>General Settings:</b> Includes checkboxes for 'Enable by default on the b/g radio' and 'Enable by default on the a radio', both checked. Below are input fields for 'SSID' (containing 'blue') and 'VLAN' (containing '10').</li> <li><b>Client to Client Traffic:</b> Includes radio buttons for 'Allow' (selected), 'Block', and 'Forward to Controller'.</li> <li><b>Broadcast SSID:</b> Includes a checked checkbox for 'Enable'.</li> <li><b>Security Types:</b> Includes dropdown menus for 'Authentication Type' (set to 'Open System') and 'Cipher Type' (set to 'Disabled').</li> <li><b>BSAP-1540 and BSAP-1500:</b> A section header.</li> <li><b>QoS Settings:</b> Includes a dropdown for 'Default QoS for SSID' (set to 'Video') and a checked checkbox for 'Use WMM to apply QoS'.</li> </ul> At the bottom of the form are buttons for 'Back', 'Reset', 'Delete', and 'Save'. The 'Save' button is highlighted with a red box in the original image. </p>

Step	Description
19.	<p>Navigate to the <b>AP</b> page by clicking <b>Wireless</b> and then <b>AP</b>. The <b>AP</b> 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.</p>  <p>The screenshot shows the Bluesocket WirelessAP web interface in Microsoft Internet Explorer. The address bar shows the URL: https://192.168.77.100/ap.p?uid=638103257;action=point;save_action=point;_ap_layout=ap;wgs2yE27256. The 'Wireless' tab is selected in the top navigation bar. Below the navigation bar, there is a 'Global' tab and an 'AP' tab. The 'AP' tab is active, and it displays a table with columns: Actions, Model, Enabled, MAC, RadioMAC, Hostname, Location, Status, Active, Error, Firmware, Hardware, Messages. The table is empty, and a message at the bottom states 'No data found.'</p>
20.	<p>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  icon to edit the configuration information for the newly discovered access point.</p>  <p>The screenshot shows the Bluesocket WirelessAP web interface in Microsoft Internet Explorer. The address bar shows the URL: https://192.168.77.30/ap.p?uid=2234120186;action=point;save_action=point;interface_layout=AywhioVFRz7670. The 'Wireless' tab is selected in the top navigation bar. Below the navigation bar, there is a 'Global' tab and an 'AP' tab. The 'AP' tab is active, and it displays a table with columns: Actions, Model, Enabled, MAC, RadioMAC, Hostname, Location, Status, Active, Error, Firmware, Hardware, Messages. One access point is listed: BSAP-1540, Yes, 00:12:cf:3d:44:ba, UpToDate, Yes, 5.3.1-1, 1540, Channel scanning. A pencil icon is visible in the 'Actions' column for this access point. Below the table, there are buttons: Check All, Clear All, Enable, Disable, Delete, Apply, Reboot, Reset to Defaults, Upgrade. A message at the bottom states '1 row download'.</p>



Step	Description
21.	<p>From the <b>Edit AP</b> page, ensure that the check-box labeled <b>Enable AP</b> is checked. The optional fields, <b>Hostname</b> and <b>Location</b>, can also be configured. Click <b>Save</b>.</p> <p>The parameters highlighted with the blue background below are inherited from the <b>Edit AP System Settings – Global</b> page (see <b>Step 16</b>).</p> <p>In the sample network a total of three access points were used. Two access points were on VLAN 10 and one access point was on VLAN 11. Repeat this process for the second AP on VLAN 10 and for the AP on VLAN 11.</p> 

Step	Description
22	<p>Once all the access points have been configured, return to the <b>AP</b> page by clicking <b>Wireless</b> and then <b>AP</b>. Check the check-box found under the <b>Actions</b> column. This will check all of the check-boxes for the known access points. Click <b>Apply</b> to update the configuration for all of the access points.</p> 

## **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:** <http://www.bluesocket.com>

## 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 <http://support.avaya.com>. The Bluesocket documentation was obtained from <http://www.bluesocket.com> (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 ™ 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 DeveloperConnection Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).