



**Application Notes for a Bluesocket Wireless LAN Solution for branch and small offices with an Avaya Telephony Infrastructure and Avaya 3631 Wireless IP Telephone in a Converged VoIP and Data Network - Issue 1.0**

**Abstract**

These Application Notes describe a solution for supporting wireless voice traffic over an Avaya IP Telephony infrastructure using Bluesocket Wireless LAN Solution for branch and small offices consisting of the Bluesocket BSC-600 BlueSecure WLAN Controller managing multiple Bluesocket BlueSecure 1800 and 1540 Access Point. The Avaya 3631 Wireless IP Telephones gained network access through the BlueSecure Access Points and register with Avaya Communication Manager. Emphasis of the testing was placed on verifying prioritization of VoIP traffic on calls associated with the Avaya 3631 Wireless IP Telephones.

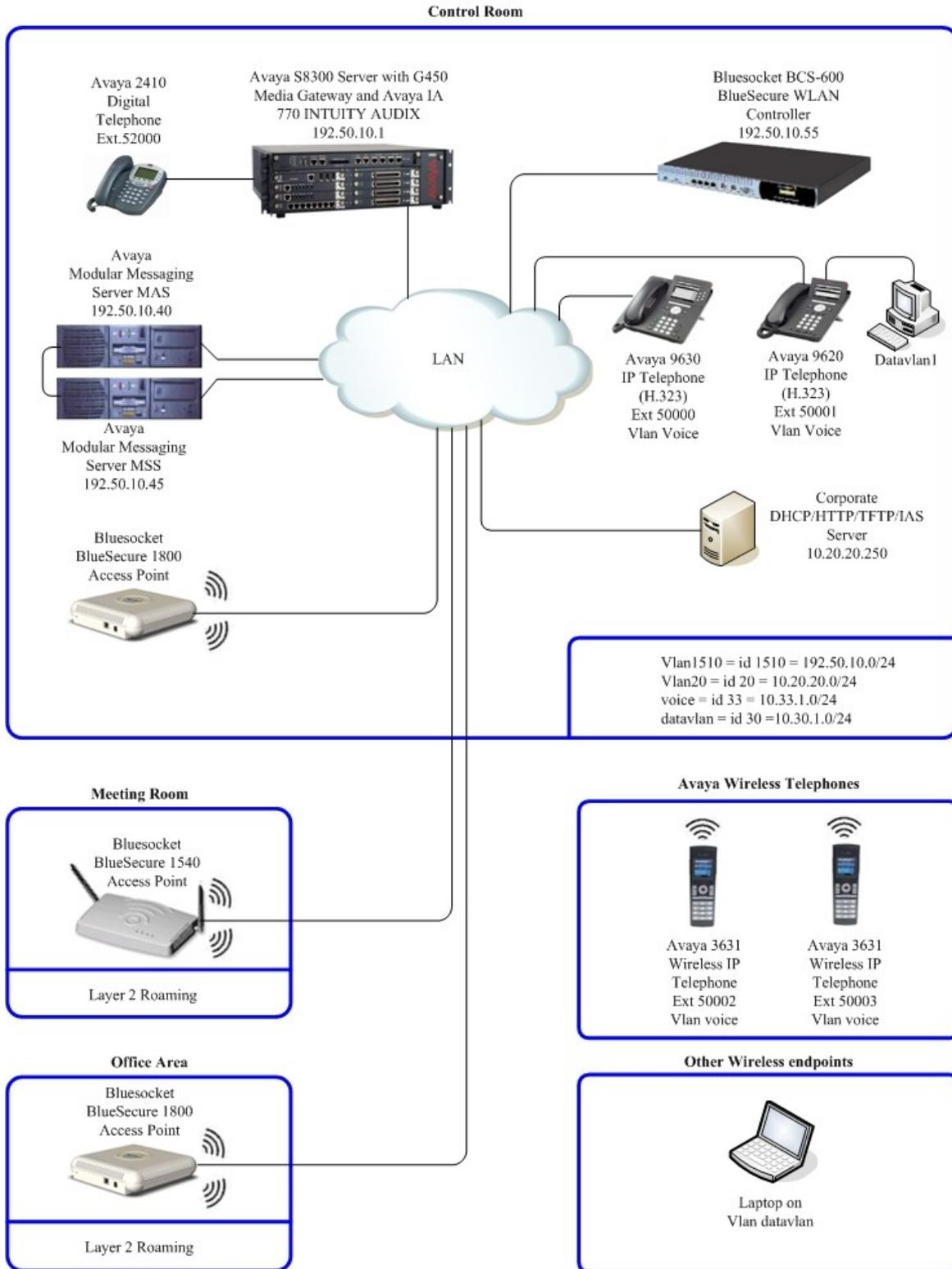
Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

These Application Notes describe a solution for supporting wireless voice traffic in an Avaya IP Telephony infrastructure using the Bluesocket Wireless LAN Solution consisting of the Bluesocket BSC-600 BlueSecure WLAN Controller (BSC) managing multiple Bluesocket BlueSecure 1800 and 1540 Access Point. The Bluesocket APs running in Edge-to-Edge mode allowed the Avaya 3631 Wireless IP Telephones to connect the LAN network to register with Avaya Communication Manager. Bluesocket's Edge-to-Edge mode allows wireless endpoints to directly talk between the Access Points limiting the network traffic to and from the controller. Emphasis of the testing was placed on verifying prioritization of VoIP traffic using Wi-Fi Multimedia (WMM) on calls associated with the Avaya wireless IP telephones.

## 1.1. Network Diagram

The network diagram shown in **Figure 1** illustrates the environment used for compliance testing. The network consists of Avaya Communication Manager running on an Avaya S8300 Server with an Avaya G450 Media Gateway, two Avaya 3631 Wireless IP Telephones, one Avaya one-X 9630 Deskphone Edition IP Telephone, one Avaya one-X 9620 Deskphone Edition IP Telephone, one Avaya 2410 digital telephone, one Avaya Modular Messaging Server MAS, one Avaya Modular Messaging Server MSS, one Bluesocket BSC-600 BlueSecure WLAN Controller, two Bluesocket BlueSecure 1800 Access Point, one Bluesocket BlueSecure 1540 Access Point. One computer is present in the network providing network services such as DHCP, TFTP and HTTP.



**Figure 1: Avaya and Bluesocket Wireless LAN Configuration**

## 2. Equipment and Software Validated

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

Equipment	Software/Firmware
<b>Avaya PBX Products</b>	
Avaya S8300 Server running Avaya Communication Manager	Avaya Communication Manager 5.1 - R015x.01.1.415.1
Avaya G450 Media Gateway MGP MM712 DCP Media Module	28.22.0 HW09
<b>Avaya Messaging (Voice Mail) Products</b>	
Avaya Modular Messaging - Messaging Application Server (MAS)	4.0
Avaya Modular Messaging - Message Storage Server (MSS)	4.0
Avaya IA 770 INTUITY AUDIX	5.1
<b>Avaya Telephony Sets</b>	
Avaya 3631 Wireless Telephone	1.5.3
Avaya 9600 Series IP Telephones	Avaya one-X Deskphone Edition 2.0
Avaya 2410 Digital Telephone	5.0
<b>Bluesocket Products</b>	
Bluesocket BSC-600 BlueSecure WLAN Controller	6.4.0-14
Bluesocket BlueSecure 1800 Access Point	6.4.0-14
Bluesocket BlueSecure 1540 Access Point	6.4.0-14
<b>MS Products</b>	
Microsoft Windows 2003 Server	File/DHCP Service

### 3. Configure Avaya Communication Manager

This section shows the necessary steps in configuring Avaya Communication Manager. For detailed information on the installation, maintenance, and configuration of Avaya Communication Manager, please refer to **Section 10 [1]**.

All of the telephones configured in the sample network in **Figure 1** were administered as H.323 stations in Avaya Communication Manager. The Avaya 3631 Wireless IP Telephone should use **Type 4620** as its station **Type** as in the example below. For complete references on how to administer these types of stations please refer to **Section 10 [1]** and **[2]**.

```
change station 50002                                     Page 1 of 5
                                                         STATION
Extension: 50002                                         Lock Messages? n          BCC: 0
  Type: 4620                                             Security Code: 123456    TN: 1
  Port: S00000                                          Coverage Path 1: 1      COR: 1
  Name: 3631-323                                       Coverage Path 2:        COS: 1
                                                         Hunt-to Station:
STATION OPTIONS
    Loss Group: 19                                       Time of Day Lock Table:
    Speakerphone: 2-way                                  Personalized Ringing Pattern: 1
    Display Language: english                            Message Lamp Ext: 50000
Survivable GK Node Name:                                Mute Button Enabled? y
    Survivable COR: internal                             Button Modules: 0
    Survivable Trunk Dest? y                             Media Complex Ext:
                                                         IP SoftPhone? y
                                                         IP Video Softphone? n
                                                         Customizable Labels? y
```

#### 3.1. Configure QoS on Avaya Communication Manager

IP networks were originally designed to carry data on a best-effort delivery basis, which meant that all traffic had equal priority and an equal chance of being delivered in a timely manner. As a result, all traffic had an equal chance of being dropped when congestion occurred. To carry voice, Quality of Service (QoS) has to be implemented throughout the network.

In order to achieve good voice quality, the VoIP traffic must be classified. The Avaya S8300 Server, Avaya G700 Media Gateway and Avaya IP Telephones support both Layer 2 802.1P/Q priority and Layer 3 Differentiated Services (DiffServ).

All network components are in network region 1 for this sample configuration. The DiffServ and 802.1p/Q values configured here will be downloaded to the Avaya IP Telephones via Avaya Communication Manager.

Except where stated the parameters in all steps are the default settings and are supplied for reference.

For this example configuration, the DIFFSERV/TOS PARAMETERS and 802.1P/Q PARAMETERS were set to 48 and 6. From the SAT prompt in Avaya Communication Manager, use the **change ip-network-region 1** to change the values.

- **Call Control PHB Value set to 48**
- **Audio PHB Value set to 48**
- **Call Control 802.1p set to 6**
- **Audio 802.1p priority set to 6**

```
change ip-network-region 1                                     Page 1 of 19
                                                           IP NETWORK REGION
  Region: 1
  Location:          Authoritative Domain: devcon.com
  Name:
  MEDIA PARAMETERS          Intra-region IP-IP Direct Audio: yes
    Codec Set: 1           Inter-region IP-IP Direct Audio: yes
    UDP Port Min: 2048      IP Audio Hairpinning? y
    UDP Port Max: 3027
  DIFFSERV/TOS PARAMETERS          RTCP Reporting Enabled? y
  Call Control PHB Value: 48      RTCP MONITOR SERVER PARAMETERS
    Audio PHB Value: 48          Use Default Server Parameters? y
    Video PHB Value: 26
  802.1P/Q PARAMETERS
  Call Control 802.1p Priority: 6
    Audio 802.1p Priority: 6
    Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
  H.323 IP ENDPOINTS          RSVP Enabled? n
  H.323 Link Bounce Recovery? y
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
  Keep-Alive Count: 5
```

## 4. Configure the Bluesocket Wireless Equipment

The following steps detail the configuration for the Bluesocket Wireless Solution used for the compliance testing.

Except where stated the parameters in all steps are the default settings and are supplied for reference.

### 4.1. Configure Bluesocket BSC-600 Controller

The initial configuration on the Bluesocket BSC-600 Controller was administered via the command line interface over a console connection.

Configure Bluesocket BSC-600 Controller as depicted in **Figure 1**.

To perform the initial configuration on the Bluesocket BSC-600 controller, setup a serial connection from a PC. Setup a terminal session with the following parameters:

**Bits per second** “9600”  
**Data Bits** “8”  
**Parity** “None”  
**Stop bits** “1”  
**Flow control** “None”

Log in to the Bluesocket BSC-600 Controller using default credentials which can be obtained from the Bluesocket BSC-600 Controller documentation.

After the login, the **BlueSecure Controller Troubleshooting Menu** will appear, type the following command to change the IP address of the protected interface.

- **i 10.20.20.55 255.255.255.0 10.20.20.1**

The following dialogue will appear:

Upon restart, Controller will have a protected IP address of 10.20.20.55, netmask 255.255.255.0, and default gateway 10.20.20.1

To return to the menu, press Enter/Return.

Press **Enter/Return** to get back the **BlueSecure Controller Troubleshooting Menu**.

Boot the Bluesocket BSC-600 Controller:

- From the **Controller Troubleshooting Menu** type **4** then **enter**. The Controller will reboot.

## 4.2. Create VLANs for voice and data

The remainder configuration on the Bluesocket BSC-600 Controller was administered via the Web configuration tool. Except where stated the parameters in all steps are the default settings and are supplied for reference.

From a PC on the 10.20.20.0 network, open a web-browser and input that IP address into the URL address of: <http://10.20.20.55/admin.pl>, login using appropriate login credentials. A prompt will appear to change the password (Not shown).

Input the appropriate login credentials, which can be obtained by reading the Bluesocket document found in **Section 10 [9]**.

bluesocket 

© 2008 Bluesocket, Inc. All rights reserved globally

### BlueSecure Controller Admin Login

**Administrator Username**

**Password**

[Change password?](#)

Did you get an [SSL warning?](#)

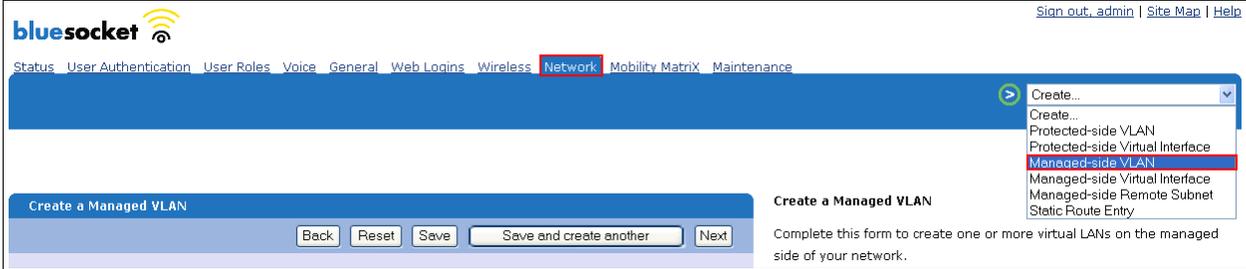
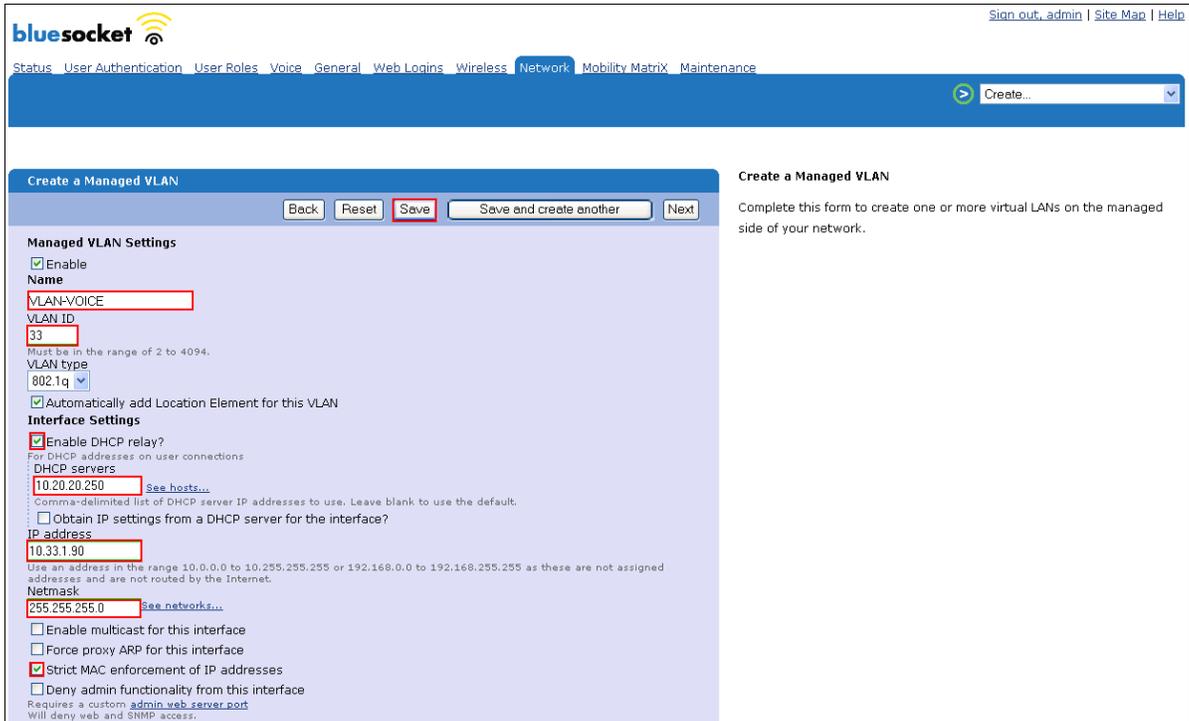
Were you looking for the [User Login?](#)

### 4.3. Create the voice and data VLAN's

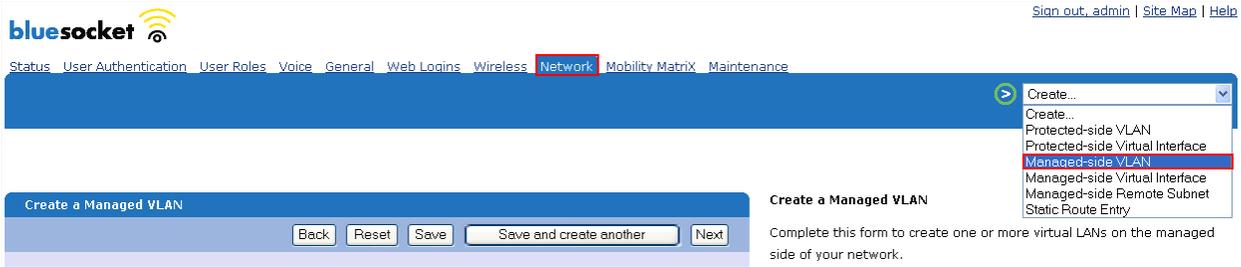
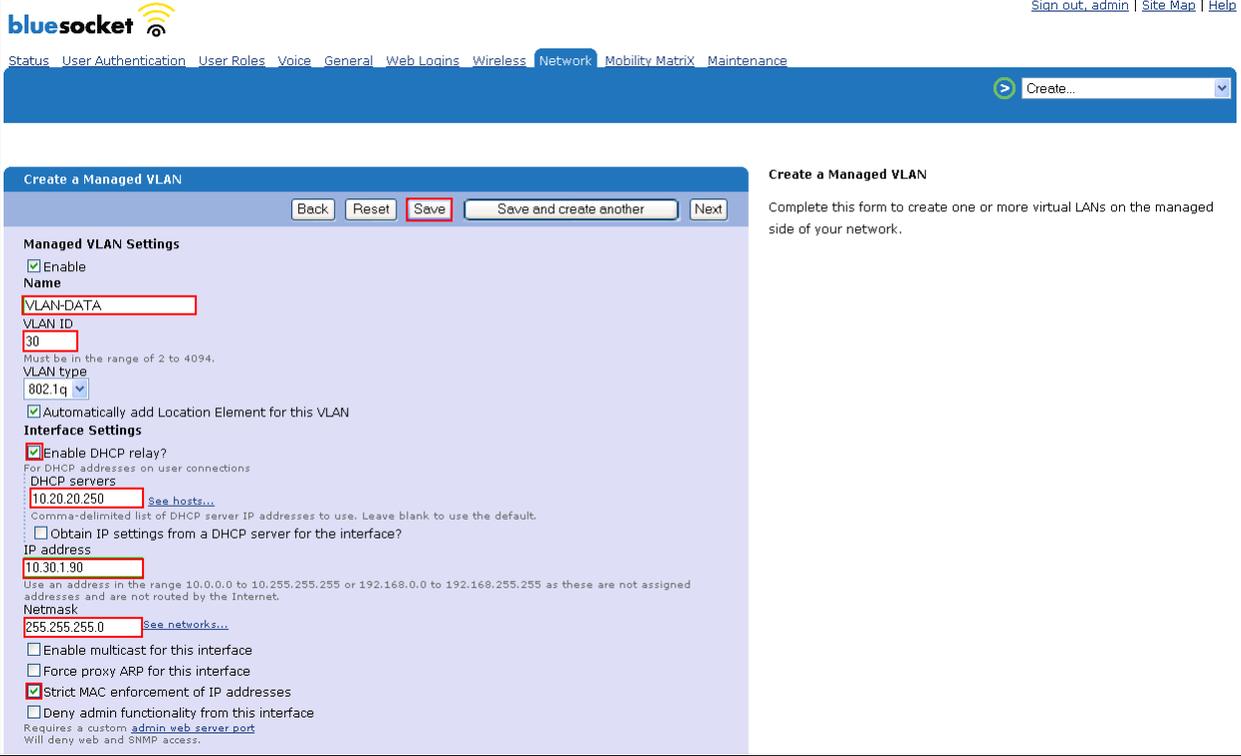
Create two VLANs, one for **voice** and one for **data** with a tags of **33** and **30**, respectively.

For the compliance testing, a centralized corporate DHCP server was put in place to handle both the wired and wireless subnets requests.

#### 4.3.1. Create and configure the voice VLAN

Step	Description
1.	<p>Select <b>Network</b>, use the pull down arrow and select <b>Managed-side VLAN</b>.</p>  <p>The screenshot shows the Bluesocket network management interface. The 'Network' menu is open, and 'Managed-side VLAN' is highlighted. Below the menu, the 'Create a Managed VLAN' form is visible with buttons for 'Back', 'Reset', 'Save', 'Save and create another', and 'Next'.</p>
2.	<p>The <b>Create a Managed VLAN</b> window will appear. From the <b>Create a Managed VLAN</b> window, enter the <b>VLAN Name</b> and <b>VLAN ID</b>. Check the box next to <b>Enable DHCP relay?</b> and enter the IP address in the <b>DHCP servers</b>. Enter a unique <b>IP address</b>, and <b>Netmask</b> of the voice VLAN, check the box next to <b>Strict MAC enforcement of IP addresses</b>, and click <b>Save</b> to continue.</p>  <p>The screenshot shows the 'Create a Managed VLAN' configuration form. The 'Managed VLAN Settings' section has 'Enable' checked. The 'Name' field contains 'VLAN-VOICE' and the 'VLAN ID' field contains '33'. The 'Interface Settings' section has 'Enable DHCP relay?' checked, 'DHCP servers' set to '10.20.20.250', 'IP address' set to '10.33.1.90', and 'Netmask' set to '255.255.255.0'. 'Strict MAC enforcement of IP addresses' is also checked. The 'Save' button is highlighted.</p>

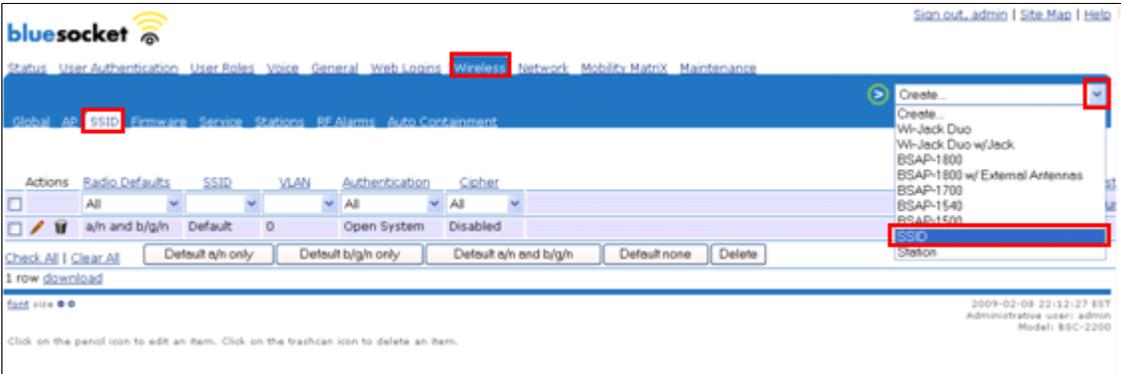
### 4.3.2. Create and configure the data VLAN

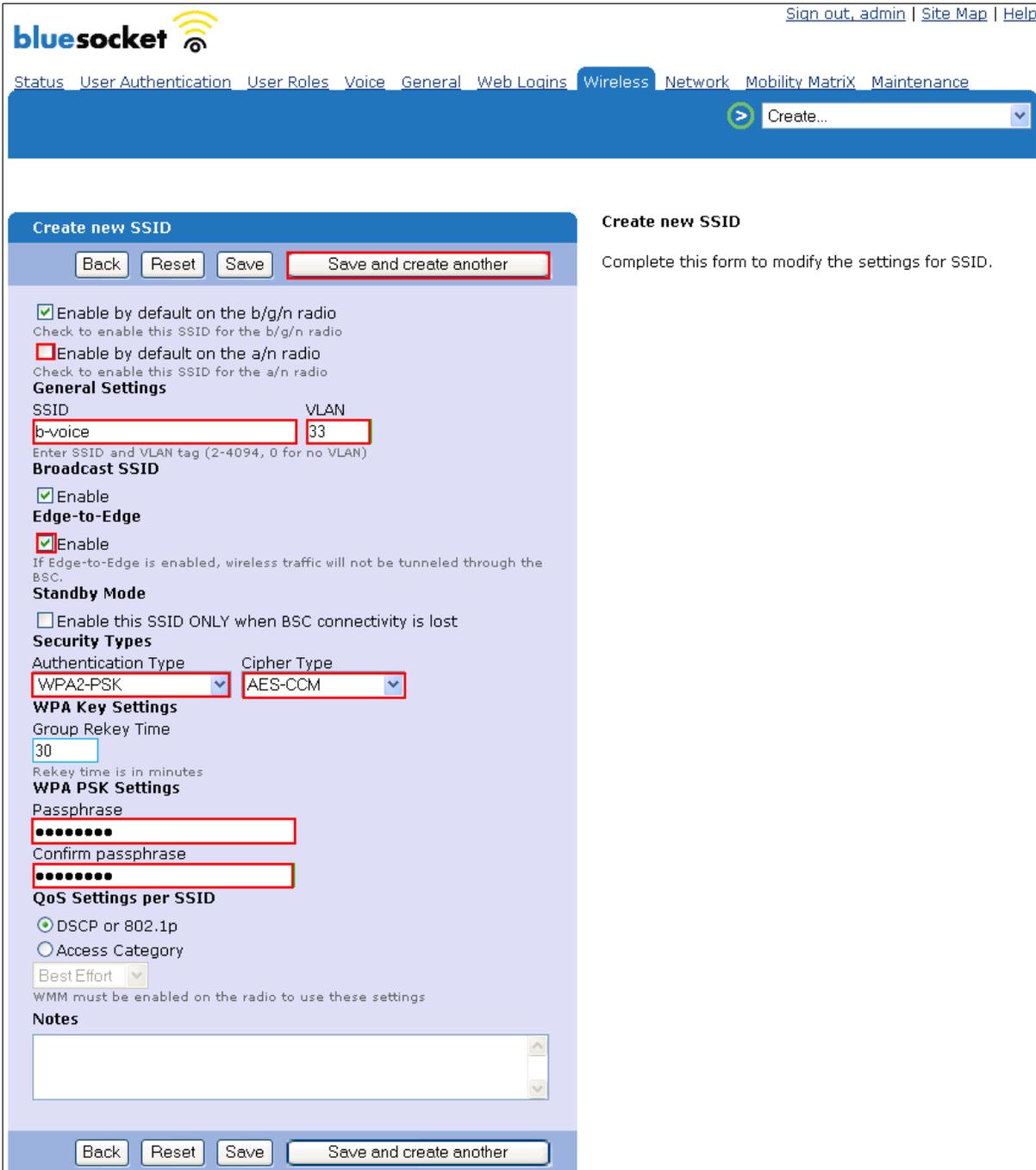
Step	Description
1.	<p>Select <b>Network</b> , use the pull down arrow and select <b>Managed-side VLAN</b>.</p> 
2.	<p>The <b>Create a Managed VLAN</b> window will appear. From the <b>Create a Managed VLAN</b> window, enter the <b>VLAN Name</b> and <b>VLAN ID</b>. Check the box next to <b>Enable DHCP relay?</b> and enter the IP address in the <b>DHCP servers</b>. Enter a unique <b>IP address</b>, and <b>Netmask</b> of the data VLAN, check the box next to <b>Strict MAC enforcement of IP addresses</b>, and click <b>Save</b> to continue.</p> 

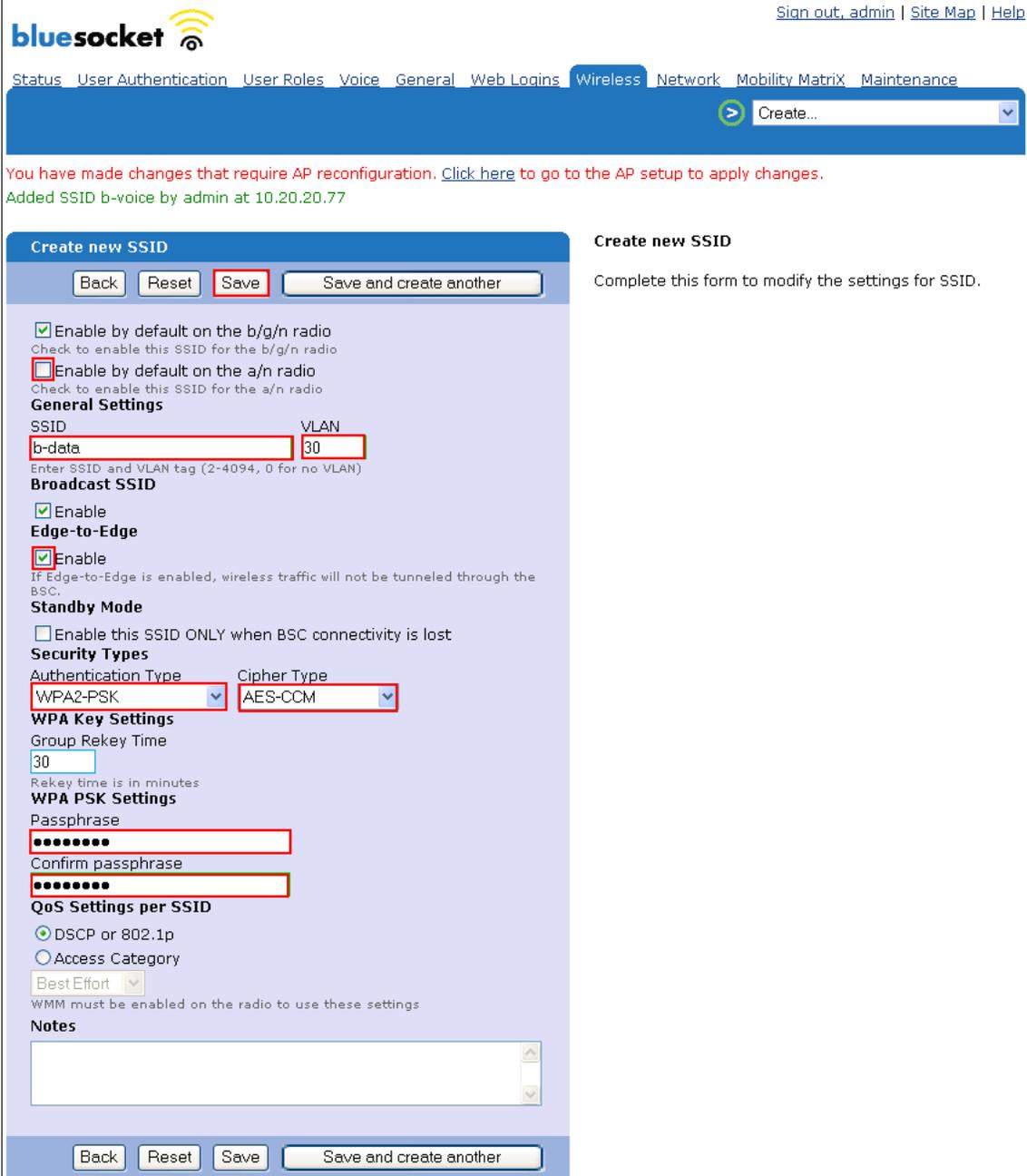
#### 4.4. Create and Configure the voice & data SSID's

Create SSIDs for the voice and data networks. Three different security schemas were tested: Clear, WEP-128 and WPA2. Clear and WEP SSIDs will not be covered in these Application Notes. Refer to **Section 10 [9]** for additional information about Authentication and Cipher types supported by the Bluesocket WAN Solution and their configuration parameters. Compliance testing covered only 802.11g.

Note: The parameters highlighted with the blue background are inherited configuration parameters from the Global AP settings web page. The default information was used.

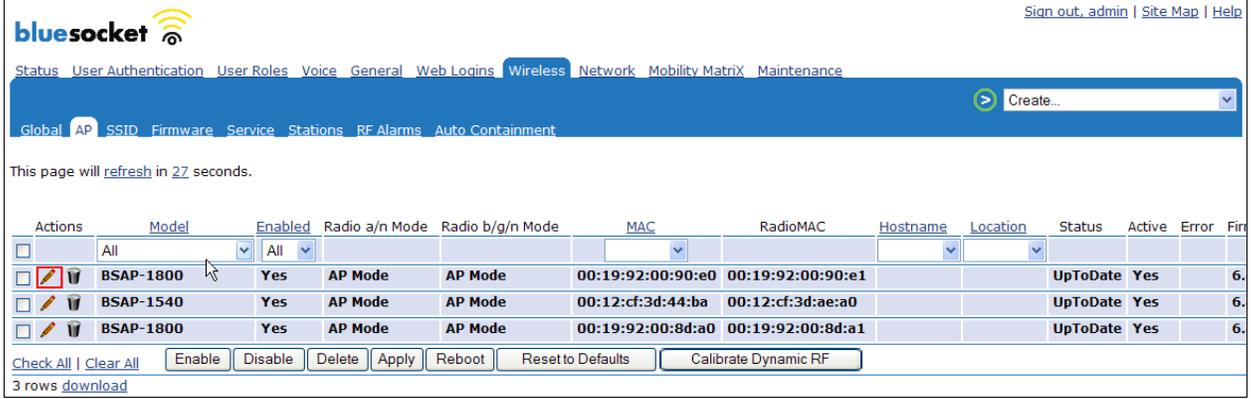
Step	Description
1.	<p>Navigate to the SSID web page by clicking <b>Wireless</b> then <b>SSID</b>. Using the pull down menu select “<b>SSID</b>”.</p>  <p>The screenshot shows the Bluesocket web interface. The top navigation bar includes 'Wireless' and 'SSID', both highlighted with red boxes. A dropdown menu is open, showing options like 'Create...', 'Wi-Jack Duo', and 'SSID', with 'SSID' highlighted in blue and a red box around it. The main content area shows a table with columns for 'Radio Defaults', 'SSID', 'VLAN', 'Authentication', and 'Cipher'. The 'SSID' column contains the value 'Default'. Below the table are buttons for 'Check All', 'Clear All', and 'Delete'. The footer shows the date '2009-02-08 22:12:27 EST' and the user 'Administrative user: admin'.</p>

Step	Description
2.	<p>Uncheck the <b>Enable by default on the a/n radio</b> box, configure the <b>SSID</b> name and <b>VLAN</b>. Under <b>Edge-to-Edge</b>, check the <b>Enable</b> box. Using the pull down menus, set the <b>Authentication Type</b> to <b>WPA2-PSK</b> and <b>Cipher Type</b> to <b>AES-CCM</b>. Under <b>WPA PSK Settings</b>, enter the <b>Passphrase/Confirm passphrase</b> information. Click <b>Save and create another</b> to continue.</p>  <p>The screenshot shows the 'Create new SSID' configuration page in the Bluesocket web interface. The page has a blue header with the Bluesocket logo and navigation links. Below the header is a breadcrumb trail: Status &gt; User Authentication &gt; User Roles &gt; Voice &gt; General &gt; Web Logins &gt; Wireless &gt; Network &gt; Mobility Matrix &gt; Maintenance. A 'Create...' button is visible in the top right. The main content area is titled 'Create new SSID' and contains several sections:     <ul style="list-style-type: none"> <li><b>General Settings:</b> Includes checkboxes for 'Enable by default on the b/g/n radio' (checked) and 'Enable by default on the a/n radio' (unchecked). Below are input fields for 'SSID' (containing 'b-voice') and 'VLAN' (containing '33').</li> <li><b>Broadcast SSID:</b> Includes a checked 'Enable' checkbox.</li> <li><b>Edge-to-Edge:</b> Includes a checked 'Enable' checkbox.</li> <li><b>Standby Mode:</b> Includes an unchecked 'Enable this SSID ONLY when BSC connectivity is lost' checkbox.</li> <li><b>Security Types:</b> Includes dropdown menus for 'Authentication Type' (set to 'WPA2-PSK') and 'Cipher Type' (set to 'AES-CCM').</li> <li><b>WPA Key Settings:</b> Includes a 'Group Rekey Time' input field set to '30'.</li> <li><b>WPA PSK Settings:</b> Includes 'Passphrase' and 'Confirm passphrase' input fields, both masked with dots.</li> <li><b>QoS Settings per SSID:</b> Includes radio buttons for 'DSCP or 802.1p' (selected) and 'Access Category', and a dropdown menu set to 'Best Effort'.</li> </ul>     At the bottom of the form are buttons for 'Back', 'Reset', 'Save', and 'Save and create another'.   </p>

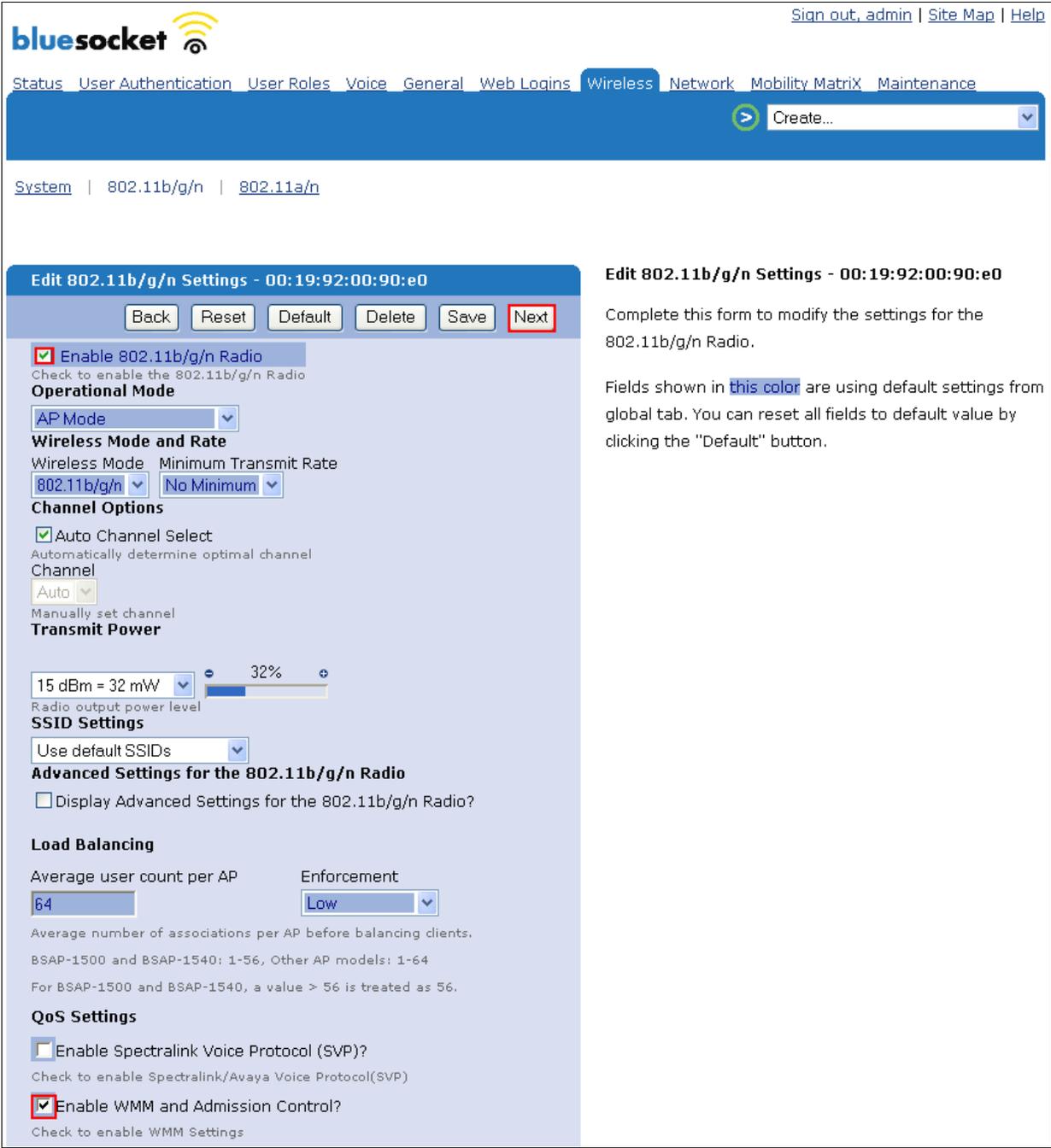
Step	Description
3.	<p>Uncheck the <b>Enable by default on the a/n radio</b> box, configure the <b>SSID</b> name and <b>VLAN</b>. Under <b>Edge-toEdge</b>, check the <b>Enable</b> box. Using the pull down menus, set the <b>Authentication Type</b> to <b>WPA2-PSK</b> and <b>Cipher Type</b> to <b>AES-CCM</b>. Under <b>WPA PSK Settings</b>, enter the <b>Passphrase/Confirm passphrase</b> information. Click <b>Save</b> to continue.</p>  <p>The screenshot shows the Bluesocket web interface for creating a new SSID. The page title is "Create new SSID". At the top, there are navigation links: Status, User Authentication, User Roles, Voice, General, Web Logins, Wireless, Network, Mobility Matrix, and Maintenance. A "Create..." button is visible in the top right. A red message states: "You have made changes that require AP reconfiguration. Click here to go to the AP setup to apply changes." Below this, a green message says: "Added SSID b-voice by admin at 10.20.20.77". The main form area is titled "Create new SSID" and contains several sections: <ul style="list-style-type: none"> <li><b>Enable by default on the b/g/n radio</b>: <input checked="" type="checkbox"/> (checked)</li> <li><b>Enable by default on the a/n radio</b>: <input type="checkbox"/> (unchecked)</li> <li><b>General Settings</b>: SSID field contains "b-data", VLAN field contains "30".</li> <li><b>Broadcast SSID</b>: <input checked="" type="checkbox"/> (checked)</li> <li><b>Edge-to-Edge</b>: <input checked="" type="checkbox"/> (checked)</li> <li><b>Standby Mode</b>: <input type="checkbox"/> (unchecked)</li> <li><b>Security Types</b>: Authentication Type is "WPA2-PSK", Cipher Type is "AES-CCM".</li> <li><b>WPA Key Settings</b>: Group Rekey Time is "30".</li> <li><b>WPA PSK Settings</b>: Passphrase and Confirm passphrase fields are filled with masked characters.</li> <li><b>QoS Settings per SSID</b>: DSCP or 802.1p is selected, Access Category is "Best Effort".</li> </ul> At the bottom of the form, there are buttons for "Back", "Reset", "Save" (highlighted with a red box), and "Save and create another".</p>

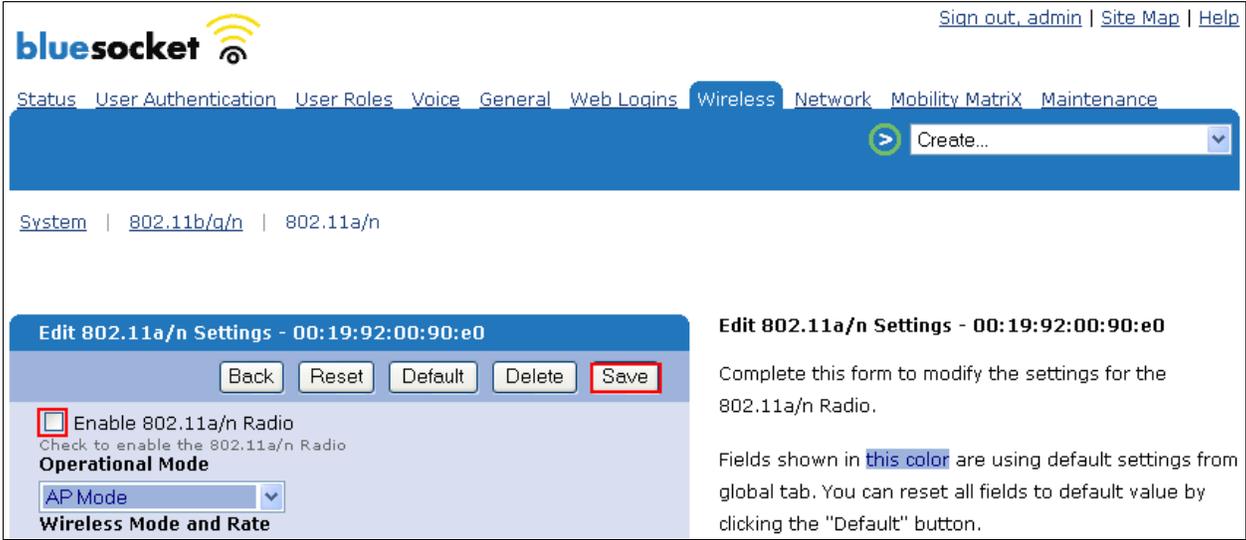
## 4.5. Configure Bluesocket BlueSecure Access Points

In the configuration that was compliance tested, the Bluesocket BlueSecure Access Points acquired an IP address and the BSC information from the corporate DHCP server (**Figure 1**). A required Vendor Class entry must be created on the DHCP server for the BSC information to be handed out. Creation of the Vender Class is covered in **Appendix B**.

Step	Description																																																				
1.	<p>Navigate to the AP web page by clicking <b>Wireless</b> and then <b>AP</b>. The AP web page lists the access points BSC-600 has discovered. To this point, no Access Points have been connected to the network, therefore no access points have been discovered. Plug all three Access Points into the same subnet that the BSC-600 is on. Wait for all three APs to be discovered.</p>  <p>The screenshot shows the Bluesocket web interface. The 'Wireless' menu is highlighted in red, and the 'AP' sub-menu is also highlighted in red. The page title is 'Global AP SSID Firmware Service Stations RF Alarms Auto Containment'. A 'Create...' button is visible in the top right. A refresh timer indicates the page will refresh in 41 seconds.</p>																																																				
2.	<p>Following APs are discovered by the BSC-600. Click the icon under the <b>Actions</b> column to edit the configuration information for the newly discovered access points.</p>  <p>The screenshot shows the Bluesocket web interface with a table of discovered access points. The 'Wireless' menu is highlighted. The table has columns for Actions, Model, Enabled, Radio a/n Mode, Radio b/g/n Mode, MAC, RadioMAC, Hostname, Location, Status, Active, and Error. Three rows of data are shown, all with 'UpToDate' status and 'Yes' active. Below the table are buttons for 'Check All', 'Clear All', 'Enable', 'Disable', 'Delete', 'Apply', 'Reboot', 'Reset to Defaults', and 'Calibrate Dynamic RF'. A refresh timer indicates the page will refresh in 27 seconds.</p> <table border="1"> <thead> <tr> <th>Actions</th> <th>Model</th> <th>Enabled</th> <th>Radio a/n Mode</th> <th>Radio b/g/n Mode</th> <th>MAC</th> <th>RadioMAC</th> <th>Hostname</th> <th>Location</th> <th>Status</th> <th>Active</th> <th>Error</th> <th>Fin</th> </tr> </thead> <tbody> <tr> <td> </td> <td>BSAP-1800</td> <td>Yes</td> <td>AP Mode</td> <td>AP Mode</td> <td>00:19:92:00:90:e0</td> <td>00:19:92:00:90:e1</td> <td></td> <td></td> <td>UpToDate</td> <td>Yes</td> <td></td> <td>6.</td> </tr> <tr> <td> </td> <td>BSAP-1540</td> <td>Yes</td> <td>AP Mode</td> <td>AP Mode</td> <td>00:12:cf:3d:44:ba</td> <td>00:12:cf:3d:ae:a0</td> <td></td> <td></td> <td>UpToDate</td> <td>Yes</td> <td></td> <td>6.</td> </tr> <tr> <td> </td> <td>BSAP-1800</td> <td>Yes</td> <td>AP Mode</td> <td>AP Mode</td> <td>00:19:92:00:8d:a0</td> <td>00:19:92:00:8d:a1</td> <td></td> <td></td> <td>UpToDate</td> <td>Yes</td> <td></td> <td>6.</td> </tr> </tbody> </table>	Actions	Model	Enabled	Radio a/n Mode	Radio b/g/n Mode	MAC	RadioMAC	Hostname	Location	Status	Active	Error	Fin		BSAP-1800	Yes	AP Mode	AP Mode	00:19:92:00:90:e0	00:19:92:00:90:e1			UpToDate	Yes		6.		BSAP-1540	Yes	AP Mode	AP Mode	00:12:cf:3d:44:ba	00:12:cf:3d:ae:a0			UpToDate	Yes		6.		BSAP-1800	Yes	AP Mode	AP Mode	00:19:92:00:8d:a0	00:19:92:00:8d:a1			UpToDate	Yes		6.
Actions	Model	Enabled	Radio a/n Mode	Radio b/g/n Mode	MAC	RadioMAC	Hostname	Location	Status	Active	Error	Fin																																									
	BSAP-1800	Yes	AP Mode	AP Mode	00:19:92:00:90:e0	00:19:92:00:90:e1			UpToDate	Yes		6.																																									
	BSAP-1540	Yes	AP Mode	AP Mode	00:12:cf:3d:44:ba	00:12:cf:3d:ae:a0			UpToDate	Yes		6.																																									
	BSAP-1800	Yes	AP Mode	AP Mode	00:19:92:00:8d:a0	00:19:92:00:8d:a1			UpToDate	Yes		6.																																									

Step	Description
3.	<p>Ensure that the check box labeled <b>Enable AP</b> is checked and populate the <b>Hostname</b> and <b>Location</b> fields. These are not required parameters but help identify hostname and location at a glance. Click <b>Next</b> to go to the <b>802.11b/g/n</b> screen.</p> <div data-bbox="277 380 1523 1612"> </div>

Step	Description
4.	<p data-bbox="277 239 1409 306">Ensure that the check boxes labeled <b>Enable 802.11b/g/n Radio</b> and <b>Enable WMM and Admission Control?</b> are checked. Click <b>Next</b> to go to the <b>802.11a/n</b> screen.</p> <div data-bbox="285 342 1515 1686">  <p>The screenshot shows the Bluesocket web interface. At the top, there is a navigation menu with options: Status, User Authentication, User Roles, Voice, General, Web Logins, <b>Wireless</b>, Network, Mobility Matrix, and Maintenance. Below the menu is a blue bar with a 'Create...' button. The main content area is titled 'Edit 802.11b/g/n Settings - 00:19:92:00:90:e0'. It features several sections: <ul style="list-style-type: none"> <li><b>Operational Mode:</b> Includes a checked checkbox for 'Enable 802.11b/g/n Radio', a dropdown for 'AP Mode', and a section for 'Wireless Mode and Rate' with dropdowns for '802.11b/g/n' and 'No Minimum'.</li> <li><b>Channel Options:</b> Includes a checked checkbox for 'Auto Channel Select' and a dropdown for 'Channel' set to 'Auto'.</li> <li><b>Transmit Power:</b> Shows a slider set to '15 dBm = 32 mW' (32%) and a 'Radio output power level' label.</li> <li><b>SSID Settings:</b> Includes a dropdown for 'Use default SSIDs'.</li> <li><b>Advanced Settings for the 802.11b/g/n Radio:</b> Includes an unchecked checkbox for 'Display Advanced Settings for the 802.11b/g/n Radio?'.</li> <li><b>Load Balancing:</b> Includes a text input for 'Average user count per AP' set to '64' and a dropdown for 'Enforcement' set to 'Low'.</li> <li><b>QoS Settings:</b> Includes an unchecked checkbox for 'Enable Spectralink Voice Protocol (SVP)?' and a checked checkbox for 'Enable WMM and Admission Control?'.</li> </ul> At the top of the settings form, there are buttons for 'Back', 'Reset', 'Default', 'Delete', 'Save', and 'Next'. The 'Next' button is highlighted with a red box. </p> </div> <p data-bbox="987 653 1461 674"><b>Edit 802.11b/g/n Settings - 00:19:92:00:90:e0</b></p> <p data-bbox="987 699 1437 751">Complete this form to modify the settings for the 802.11b/g/n Radio.</p> <p data-bbox="987 783 1510 867">Fields shown in <b>this color</b> are using default settings from global tab. You can reset all fields to default value by clicking the "Default" button.</p>

Step	Description
5.	<p>Uncheck the box labeled <b>Enable 802.11a/n Radio</b>. Click <b>Save</b> to continue.</p>  <p>The screenshot shows the Bluesocket management interface. At the top, there are navigation links: <a href="#">Sign out, admin</a>, <a href="#">Site Map</a>, and <a href="#">Help</a>. Below the navigation is a menu with options: <a href="#">Status</a>, <a href="#">User Authentication</a>, <a href="#">User Roles</a>, <a href="#">Voice</a>, <a href="#">General</a>, <a href="#">Web Logins</a>, <a href="#">Wireless</a> (selected), <a href="#">Network</a>, <a href="#">Mobility Matrix</a>, and <a href="#">Maintenance</a>. A blue bar contains a 'Create...' button. Below this, there are links for <a href="#">System</a>, <a href="#">802.11b/g/n</a>, and <a href="#">802.11a/n</a>. The main content area is titled 'Edit 802.11a/n Settings - 00:19:92:00:90:e0'. It features buttons for 'Back', 'Reset', 'Default', 'Delete', and 'Save' (highlighted with a red box). A checkbox labeled 'Enable 802.11a/n Radio' is unchecked and highlighted with a red box. Below it, the text says 'Check to enable the 802.11a/n Radio'. The 'Operational Mode' is set to 'AP Mode'. The 'Wireless Mode and Rate' section is visible below. To the right of the form, there is explanatory text: 'Complete this form to modify the settings for the 802.11a/n Radio. 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.'</p>
6.	<p>The process for adding additional access points is the same. In the sample network a total of three access points were used. Repeat <b>Section 4.5, Steps 1-5</b> to create the Access Points for the <b>Control Room</b> and <b>Meeting Room</b>.</p>

## 5. Configure Avaya 3631 Wireless IP Telephone

The following steps detail the configuration process for the Avaya 3631 Wireless IP Telephone. For complete details on all the supported features on the Avaya 3631 Wireless IP Telephone refer **Section 10 [5]**.



### 5.1. 46xxsettings File Options

The 46xxsettings.txt file is used to specify certain system parameters. It is used by all Avaya 4600 and 9600 IP & SIP Telephones. The 46xxsettings.txt file can be delivered to the Avaya 3631 Wireless IP Telephone through either of the following two methods:

- Automatically over-the-air from an HTTP server. The file is delivered whenever the Avaya 3631 Wireless IP Telephone is restarted.
- Manually via a USB cable connected between the Avaya 3631 Wireless IP Telephone and a PC

For this compliance test, the 46xxsetting file was delivered manually via a USB cable connected between the Avaya 3631 Wireless IP Telephone and a PC. For more information on configuring 46xxsetting options refer to **Section 10 [5]**.

Add **ONE** of the following attributes to the 46xxsettings file. For this example, **WPA2-PSK Configuration** was used to match what was configured for Authentication in **Section 4.4, Step 2**.

Step	Description Configuring 46xxsettings file
1.	<p>Add the following information to the 46xxsettings file:</p> <p>Clear Configuration</p> <pre>SET WTPROF1 "b-voice" SET WTSSIDP1 "b-voice " SET DNSSRVRP1 "10.20.20.250" SET DOMAIN "dev4.com"</pre> <p>WEP Configuration</p> <pre>SET WTPROF1 " b-voice " SET WTSSIDP1 " b-voice " SET WTSECP1 "1" SET ENCRYPTP1 "2" SET DNSSRVRP1 "10.20.20.250" SET DOMAIN "dev4.com" SET WTKEYP1 "1234567890123" ← Use this setting for testing only. Manually enter the key into the phone</pre> <p>WPA2-PSK Configuration</p> <pre>SET WTPROF1 " b-voice " SET WTSSIDP1 " b-voice " SET DNSSRVRP1 "10.20.20.250" SET DOMAIN "dev4.com" SET WTSECP1 "2" SET ENCRYPTP1 "3" SET WTKEYP1 "XXXXXX" ← This setting is for testing only,. Use to passphrase information from Section 4.4, Step 2. Manually enter the key into the phone.</pre>

## 5.2. Downloading 46xxsettings File via USB Cable

Step	Description
1.	<p>Configuring 46xxsettings file</p> <p>Only a Samsung cable with an 18-pin connector can be used to support USB operations on the Avaya 3631 Wireless IP Telephone. This cable is orderable through Avaya. This cable works with the standard Windows USB driver; it is not necessary to install a special USB driver to use this cable.</p> <p>Use the following procedure to download the 46xxsettings.txt file to the phone via a USB cable:</p> <ol style="list-style-type: none"><li>1. On the Avaya 3631 Wireless IP Telephone, access the <b>Advanced Settings</b> menu, select the <b>Admin access mode</b> and specify the <b>Admin password</b>.</li><li>2. From the <b>Advanced</b> menu, select the <b>Service</b> sub-menu.</li><li>3. From the <b>Service</b> menu, select <b>Backup &amp; Restore over USB</b>.</li><li>4. From the <b>Backup &amp; Restore ...</b> menu, select <b>Download settings file</b>.<ul style="list-style-type: none"><li>• The “Starting USB driver ...” status message is displayed</li></ul></li><li>5. When prompted, insert (or remove and re-insert) the USB cable into its connector on the bottom of the phone.<ul style="list-style-type: none"><li>• A confirmation window appears, with instructions on copying files.</li></ul></li><li>6. From the Windows PC, drag and drop the <b>46xxsettings.txt</b> file onto the USB drive folder associated with the phone.</li><li>7. Once the file has been copied to the USB drive, return to the phone and select the <b>Done</b> softkey.<ul style="list-style-type: none"><li>• The phone displays a “Downloading file...” status message</li></ul></li><li>8. When the phone displays a “Completed” message, press the <b>Back</b> softkey.<ul style="list-style-type: none"><li>• The phone displays a Confirmation window for restarting the phone.</li></ul></li></ol>

### 5.3. Configure DHCP

The Avaya 3631 Wireless IP Telephone supports DHCP for IP address assignment and configuration of other telephone parameters. The Avaya 3631 Wireless IP Telephone supports Site-Specific Option Numbers (SSON) 242 and 176. The default is 242. Note that this parameter can be changed only through the phone's menu interface. A required Vendor Class entry must be created on the DHCP server for the 46xxsettings information to be handed down to the Avaya 3631. Creation of the Vendor Class is covered in **Appendix A**.

## 6. Interoperability Compliance Testing

Interoperability compliance testing covered feature functionality, serviceability, and Quality of Service testing. Feature functionality testing verified the ability of the Bluesocket Wireless LAN Solution to provide network access to the Avaya Wireless IP Telephones. Emphasis of the testing was placed on verifying prioritization of VoIP traffic using WMM Quality of Service on calls associated with the Avaya Wireless IP Telephones.

### 6.1. General Test Approach

The general test approach was to register the Avaya 3631 Wireless IP Telephone with Avaya Communication Manager through the Bluesocket Wireless LAN Solution. Calls were made between both wired and wireless telephones and specific calling features were exercised. To validate WMM Quality of Service, low priority background traffic was injected into the network and the Bluesocket Wireless LAN Solution was verified to maintain voice calls while dropping the lower priority traffic. Network level tests included verifying Layer 2 Edge-to-Edge roaming from one access point to another and validating Quality of Service for voice traffic.

### 6.2. Test Results

The Avaya 3631 Wireless IP Telephone with Avaya Communication Manager utilizing Bluesocket Wireless LAN Solution passed all test cases. The Avaya 3631 Wireless IP Telephone was verified to successfully register with Avaya Communication Manager through the Bluesocket Wireless LAN Solution. The compliance testing also verified WMM Quality of Service for voice traffic while low priority background traffic was competing for bandwidth. The Avaya 3631 Wireless IP Telephone was verified to roam successfully between the Edge-to-Edge access points while maintaining voice calls.

Three different security schemas were tested: Clear, WEP-128 and WPA2 as well as two codecs, G.711MU and G.729AB. Telephone calls were verified to operate correctly with the media path direct between the telephones (shuffling enabled) and with the media path centralized through Avaya Communication Manager (shuffling disabled).

The telephony features verified to operate correctly included attended/unattended transfer, conference call participation, conference call add/drop, multiple call appearances, caller ID operation, call forwarding unconditional, call forwarding on busy, call Park, call pick-up, bridged call appearances, voicemail using Avaya Modular Messaging and Avaya IA770 INTUITY AUDIX, Message Waiting Indicator (MWI), and hold and return from hold.

## 7. Verification Steps

This section provides the verification steps that may be performed to verify that the wireless IP endpoints have connectivity to the network and that good voice quality is being provided on wireless calls.

- Place calls from the Avaya 3631 Wireless IP Telephone and verify two-way audio.
- Ensure that the **SSID** field value configured in **Section 4.4, Step 2** on the Bluesocket BSC-600 Controller matches the **SSID** field value on the Avaya 3631 Wireless IP Telephone.
- Check that the Avaya 3631 Wireless IP Telephones have successfully registered with Avaya Communication Manager by typing the **list registered-station** command on the SAT in Avaya Communication Manager.
- Place a call between two Avaya 3631 Wireless IP Telephones and verify good voice quality in both directions.
- Verify that the Bluesocket APs are recognized by the Bluesocket BSC-600 Controller and that they are active. Click **Wireless** → **AP**.

The screenshot shows the Bluesocket web interface. The 'Wireless' menu item is highlighted in red. Below it, the 'AP' menu item is also highlighted in red. A table displays the configuration for three APs:

Actions	Model	enabled	Radio a/n Mode	Radio b/g/n Mode	MAC	RadioMAC	Hostname	Location	Status	Active	Error	Firm
<input type="checkbox"/>	All	All										
<input type="checkbox"/>	BSAP-1800	Yes	Disabled	AP Mode	00:19:92:00:90:e0	00:19:92:00:90:e1	Office-Area	Office-Area	UpToDate	Yes		6.
<input type="checkbox"/>	BSAP-1540	Yes	Disabled	AP Mode	00:12:cf:3d:44:ba	00:12:cf:3d:ae:a0	Meeting-Room	Meeting-Room	UpToDate	Yes		6.
<input type="checkbox"/>	BSAP-1800	Yes	Disabled	AP Mode	00:19:92:00:8d:a0	00:19:92:00:8d:a1	Control-Room	Control-Room	UpToDate	Yes		6.

Below the table, there are buttons for 'Check All', 'Clear All', 'Enable', 'Disable', 'Delete', 'Apply', 'Reboot', 'Reset to Defaults', 'Calibrate Dynamic RF', and 'Accept RF Recommendations'. The 'Active' column in the table is highlighted with a red box.

## 8. 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>

## 9. Conclusion

These Application Notes illustrate the procedures necessary for configuring Bluesocket Wireless LAN equipment to support the Avaya 3631 IP Wireless Telephones and Avaya Communication Manager. The Bluesocket BSC-600 BlueSecure WLAN Controller, as well as the Bluesocket BlueSecure 1800 and 1540 Access Point were successfully compliance-tested in a converged voice and data network configuration. The Bluesocket BSC-600 BlueSecure WLAN Controller, and Bluesocket BlueSecure 1800 and 1540 Access Point were able to support 802.11 g radio, Layer 2 roaming, VLAN Tagging, QoS, WEP and WPA2-PSK Encryption.

## 10. Additional References

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

- [1] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 3.1, February 2007
- [2] *Avaya Communication Manager Advanced Administration Quick Reference*, Doc # 03-300364
- [3] *Administration for Network Connectivity for Avaya Communication Manager*, Doc # 555-233-504
- [4] *Avaya IP Telephony Implementation Guide*, May 1, 2006
- [5] *Avaya 3631 Wireless Telephone Administrator Guide*, March 2007, Issue 2, Document Number 16-602203
- [6] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 2.0*, Document Number 16-300698.
- [7] *Messaging Application Server (MAS) Administration Guide*, Release 3.1, February 2007.
- [8] *Avaya IA 770 INTUITY AUDIX Messaging Application Release 5.0 Administering. Communication Manager Servers to Work with IA 770* November 2007.

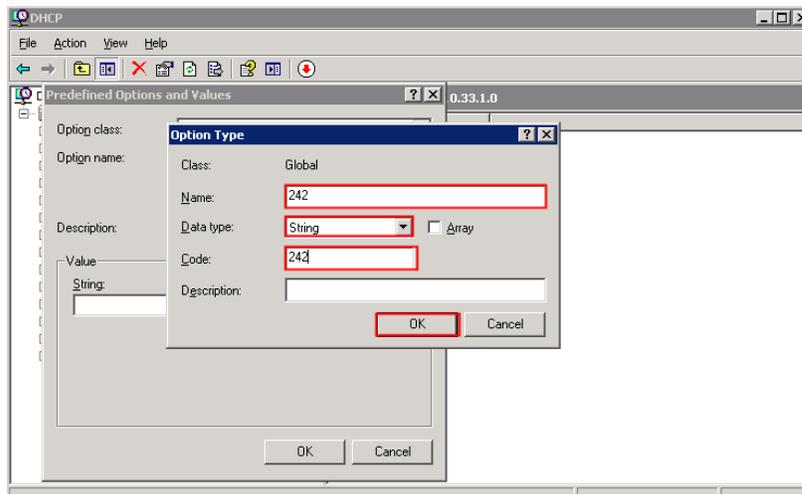
The following product documentation is provided by Bluesocket. Bluesocket documentation can be found at <http://support.bluesocket.com>.

- [9] *BlueSecure™ Controller Setup and Administration Guide*, January 2007, Part Number 870-202TT-M00

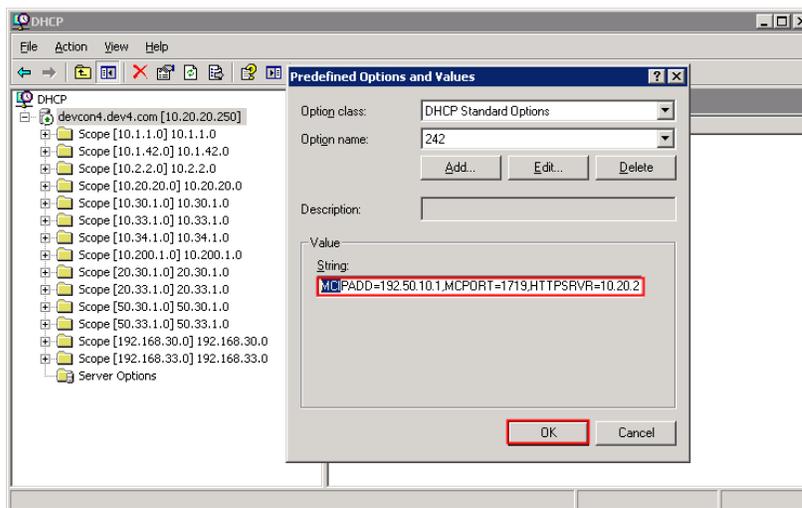
## Appendix A:

This section describes how to configure the Vendor Class Identifier Code (option 242) on a Microsoft Windows-based DHCP server.

1. On the DHCP server, open the **DHCP server administration** tool by clicking **Start → Administration Tools → DHCP**.
2. Right-click on the DHCP server name. Select **Set Predefined Options**.
3. In the **Predefined Options and Values** dialog box, click the **Add** button.
4. In the **Option Type** dialog box, enter the following information:
  - **Name = 242**
  - **Data type = String**
  - **Code = 242**
5. Click the **OK** button to save this information.



6. Add the following **String** under **Value** on the **Predefined Options and Values** dialog box:  
**MCIPADD=192.50.10.1,MCPORT=1719,HTTPSRVR=10.20.20.250**



## Appendix B Setting up a Microsoft DHCP Server to hand out Controller information

- A. Define the Vendor Class.
- B. Set the Predefined Option.
- C. Configure the Option for the AP DHCP scope.

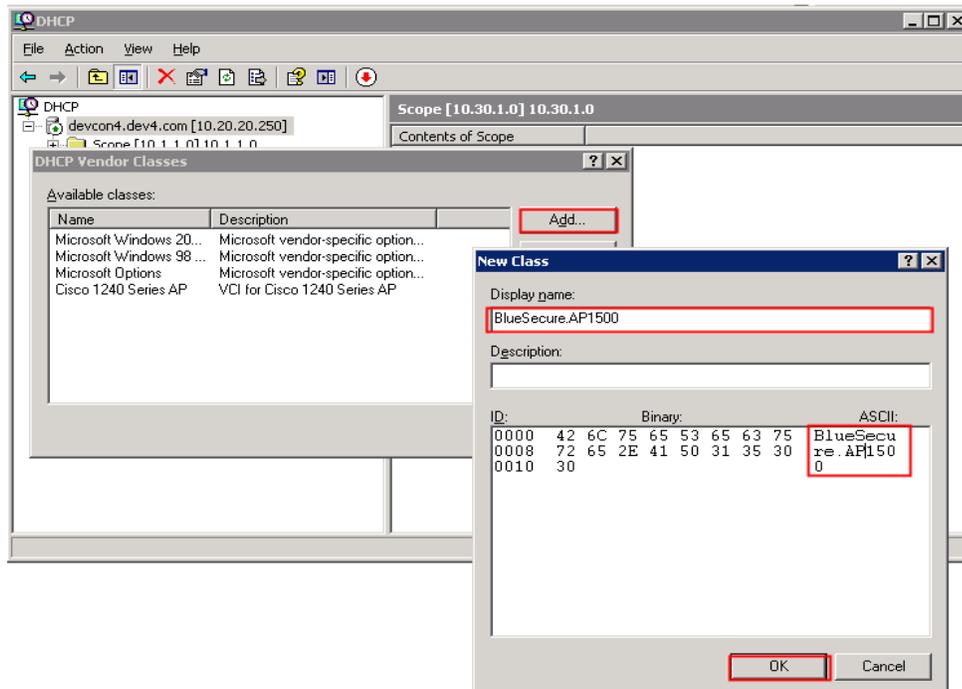
### A. Define the Vendor Class.

1. On the DHCP server, open the **DHCP server administration** tool by clicking **Start → Administration Tools → DHCP**.
2. Right-click on the DHCP server name, select **Define Vendor Classes**.
3. The **DHCP Vendor Classes** dialog box will appear, click the **Add** button.
4. In the **New Class** dialog box, enter the following information:

- **Display name = BlueSecure.AP1500**
- **ASCII = BlueSecure.AP1500**

Note: The ID and Binary information strings (Hexadecimal) will automatically be populated.

5. Click the **OK** button to save this information. Click **Close** to continue (Not shown).

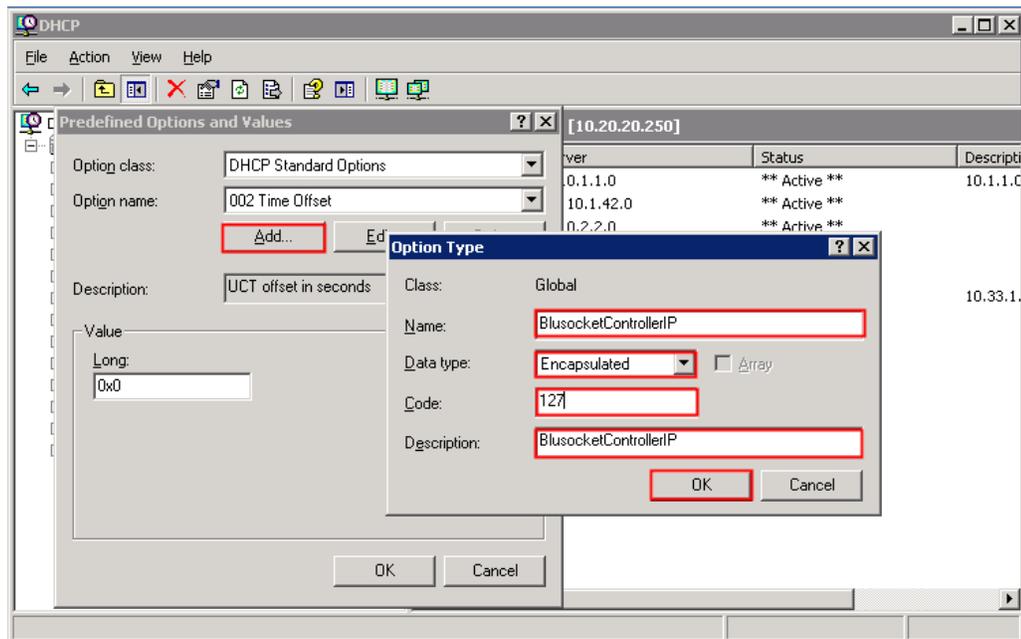


## B. Set the Predefined Option.

1. On the DHCP server, open the **DHCP server administration** tool by clicking **Start → Administration Tools → DHCP**.
2. Right-click on the DHCP server name, select. Select **Set Predefined Options**.
3. The **Predefined Options and Values** dialog box will appear, click the **Add** button.
4. In the **Option Type** dialog box, enter the following information:

- **Name = BluesocketControllerIP**
- **Data type = Encapsulated**
- **Code = 127**
- **Description = BluesocketControllerIP**

5. Click the **OK** button to save this information, and then click **OK** to continue.



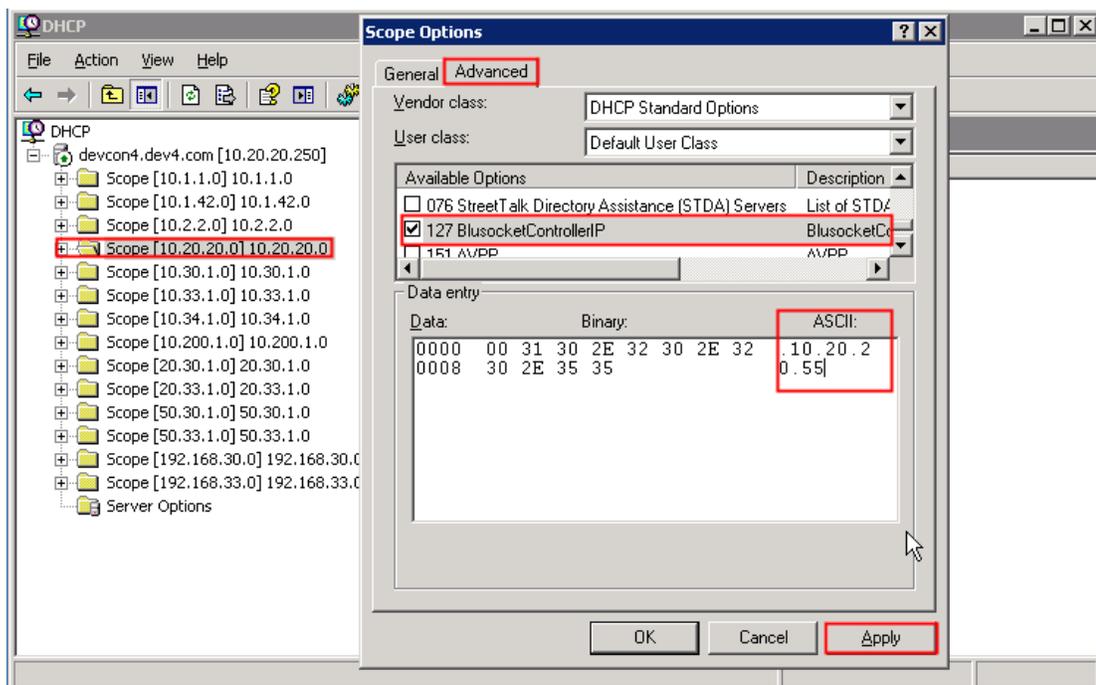
### c. Configure the Option for the AP DHCP scope.

1. On the DHCP server, open the **DHCP server administration** tool by clicking **Start → Administration Tools → DHCP**.
2. Locate the Address scope to be used, for the compliance testing **10.20.20.0** was used. Right click on **Scope Options** and right click on **Configure Options**. The Scope Options dialogue box appears, click the **Advance** tab, scroll down to **127** under **Available Options** and check it. Select **Set Predefined Options** (Not shown).
3. In the **Scope Options** dialog box, enter the following information:

- **ASCII = 10.20.20.55**

Note: The ID and Binary information strings (Hexadecimal) will automatically be populated:

5. Click the **Apply** button to save this information, and then click **OK** to continue.



---

**©2009 Avaya Inc. All Rights Reserved.**

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

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).