Avaya Solution & Interoperability Test Lab

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.

©2009 Avaya Inc. All Rights Reserved.

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.

©2009 Avaya Inc. All Rights Reserved.

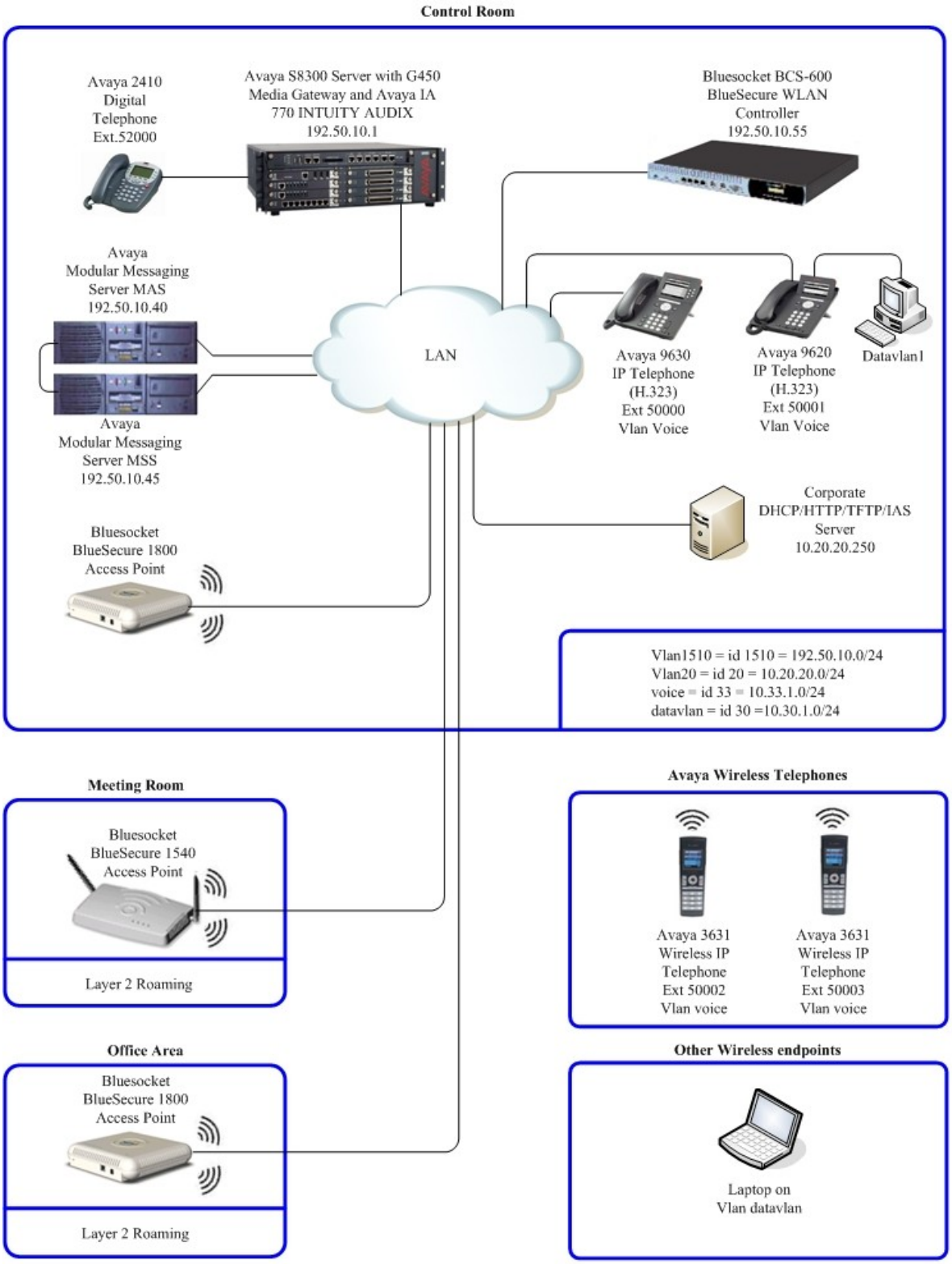


Figure 1: Avaya and Bluesocket Wireless LAN Configuration

©2009 Avaya Inc. All Rights Reserved.

2. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya PBX Products	
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
Avaya Messaging (Voice Mail) Products	
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
Avaya Telephony Sets	
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
Bluesocket Products	
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
MS Products	
Microsoft Windows 2003 Server	File/DHCP Service

©2009 Avaya Inc. All Rights Reserved.

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
                                          Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                               Message Lamp Ext: 50000
           Speakerphone: 2-way              Mute Button Enabled? y
        Display Language: english              Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal           Media Complex Ext:
   Survivable Trunk Dest? y                        IP SoftPhone? y

                                             IP Video Softphone? n


                                        Customizable Labels? y
```

3.1. Configure QoS on Avaya Communication Manager

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

©2009 Avaya Inc. All Rights Reserved.

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
```


©2009 Avaya Inc. All Rights Reserved.

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**.**

©2009 Avaya Inc. All Rights Reserved.

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**].

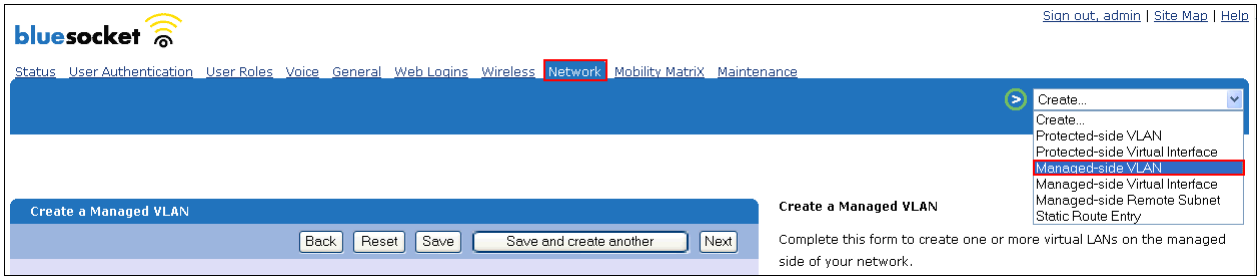
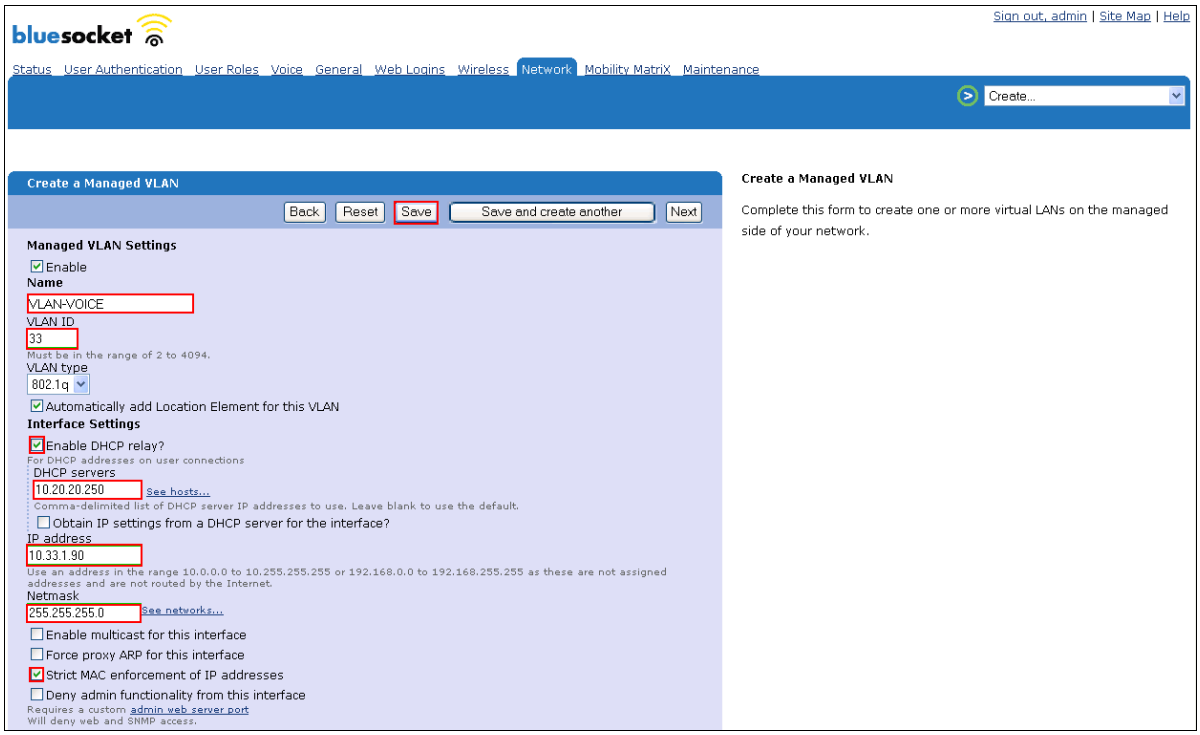
©2009 Avaya Inc. All Rights Reserved.

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.

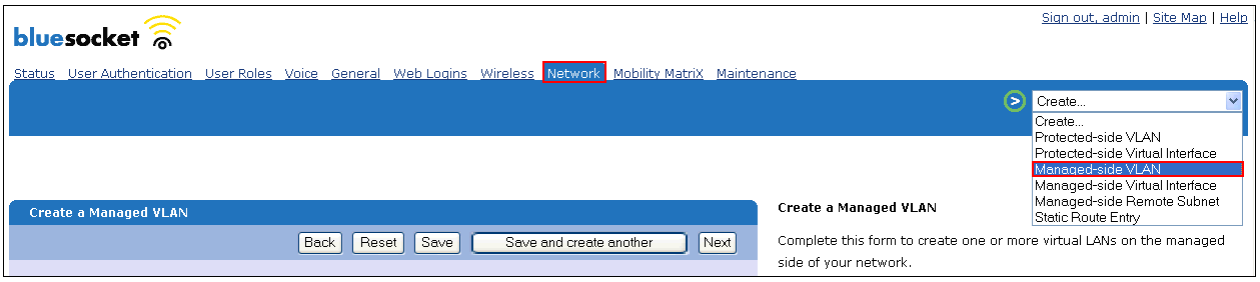
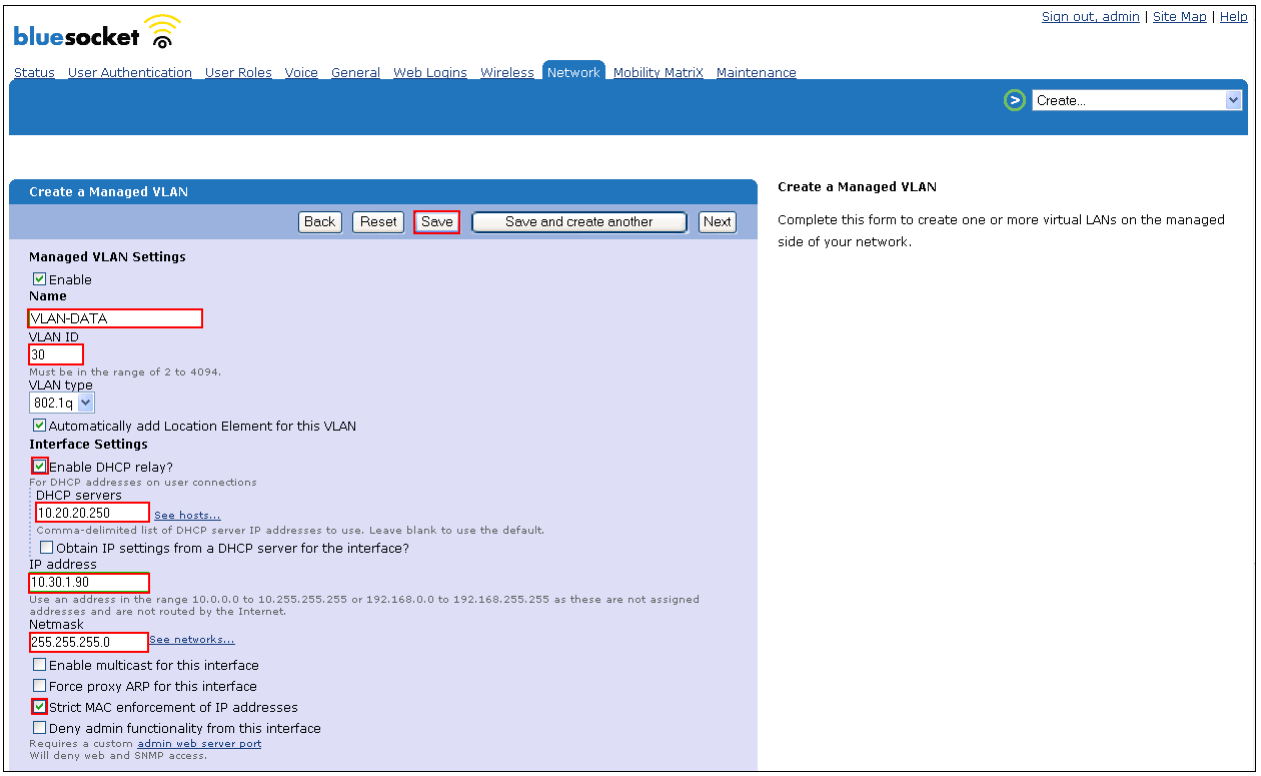
For the compliance testing, a centralized corporate DHCP server was put in place to handle both the wired and wireless subnets requests.

4.3.1. Create and configure the voice VLAN

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

©2009 Avaya Inc. All Rights Reserved.

4.3.2. Create and configure the data VLAN

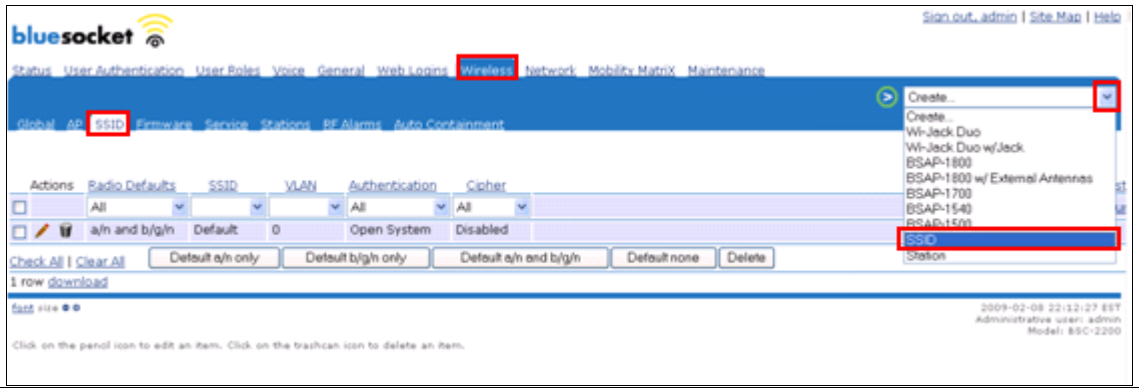
Step	Description
1.	Select **Network** , use the pull down arrow and select **Managed-side VLAN**. 
2.	The **Create a Managed VLAN** window will appear. From the **Create a Managed VLAN** window, enter the VLAN **Name** and **VLAND ID**. Check the box next to **Enable DHCP relay?** and enter the IP address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

©2009 Avaya Inc. All Rights Reserved.

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

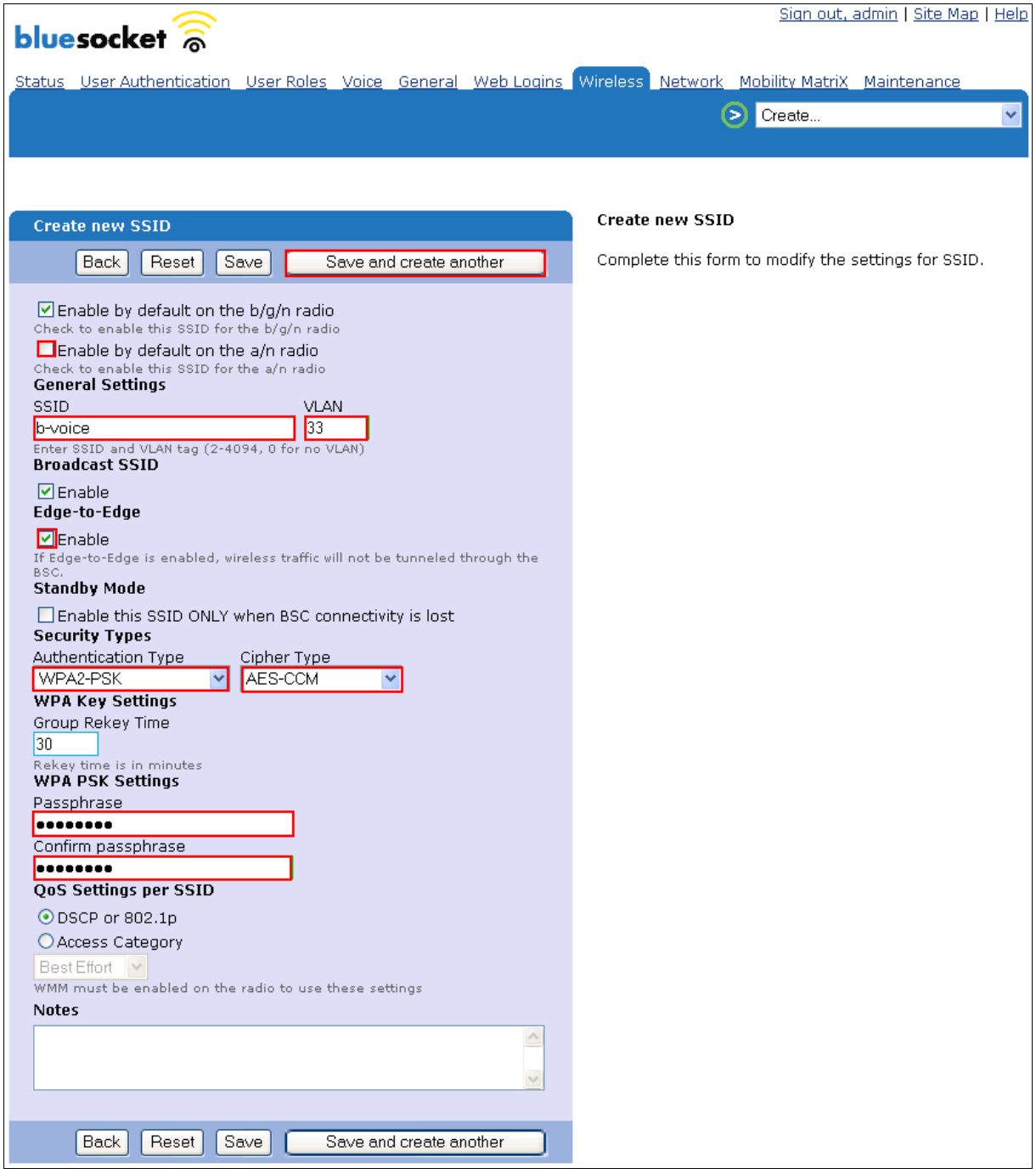
Create SSIDs for the voice and data networks. Three different security schemas were tested: Clear, WEP-128 and WPA2. Clear and WEP SSIDs will not be covered in these Application Notes. Refer to **Section 10** [**9**] for additional information about Authentication and Cipher types supported by the Bluesocket 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.	Navigate to the SSID web page by clicking **Wireless** then **SSID**. Using the pull down menu select "**SSID**". 

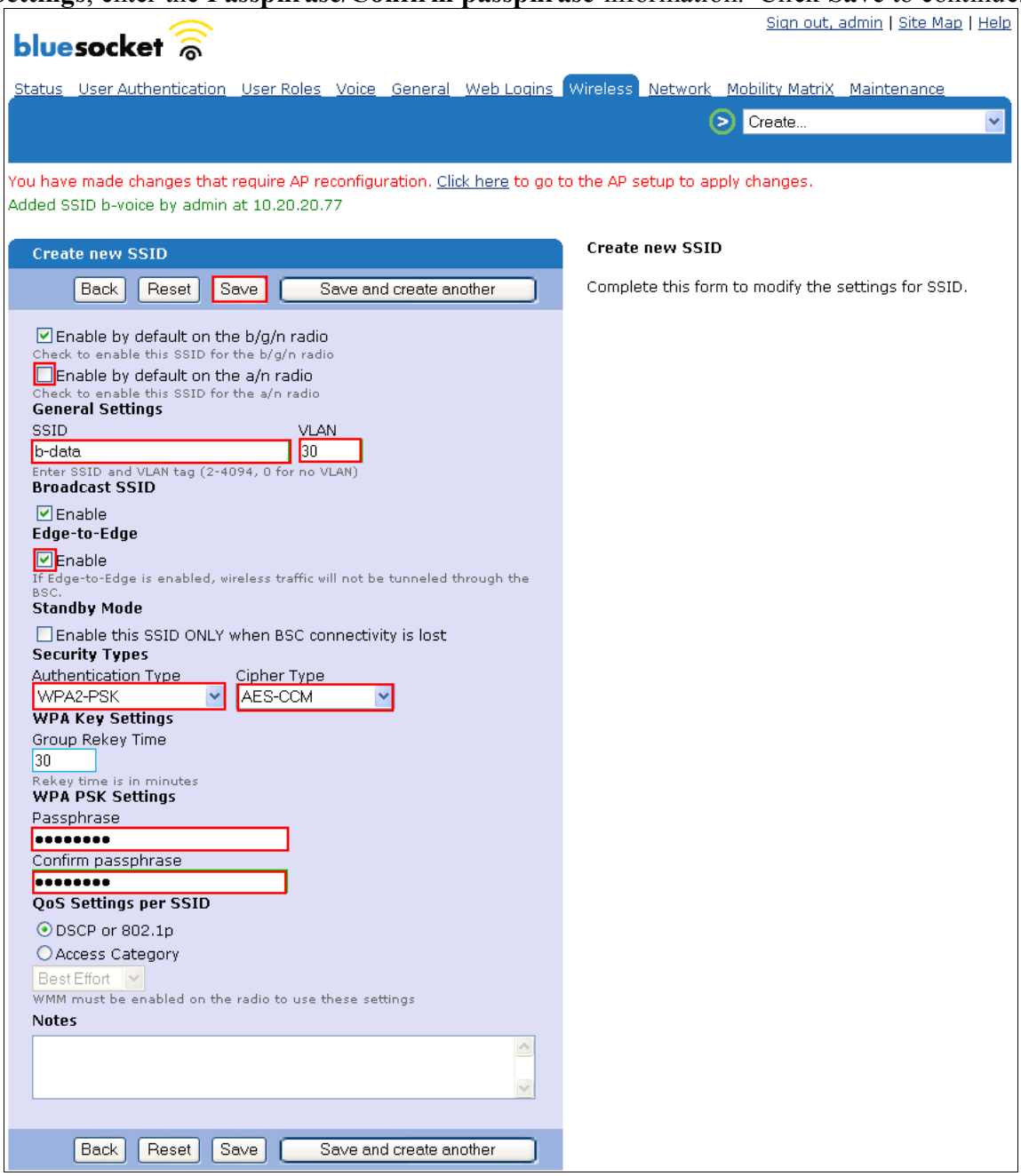
©2009 Avaya Inc. All Rights Reserved.

Step	Description
2.	Uncheck the **Enable by default on the a/n radio** box, configure the **SSID** name and **VLAN**. Under **Edge-to-Edge**, check the **Enable** box. Using the pull down menus, set the **Authentication Type** to **WPA2-PSK** and **Cipher Type** to **AES-CCM**. Under **WPA PSK Settings**, enter the **Passphrase/Confirm passphrase** information. Click **Save and create another** to continue.



©2009 Avaya Inc. All Rights Reserved.

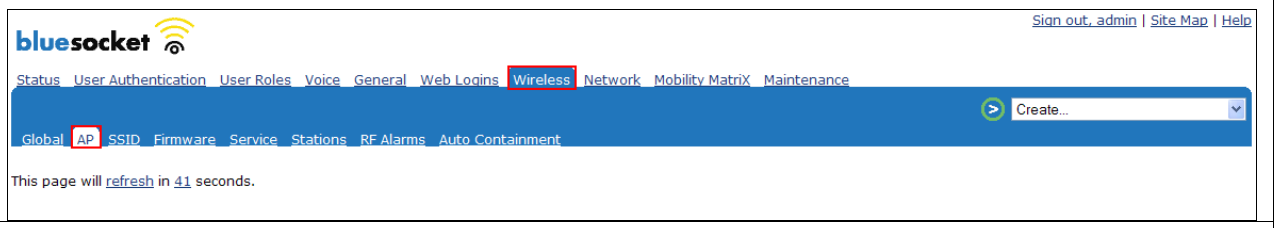
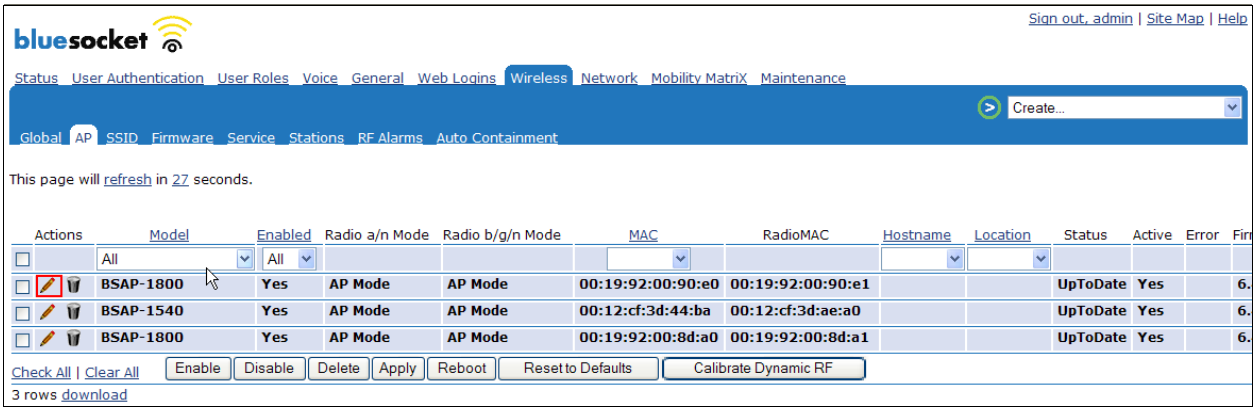
Step	Description
3.	Uncheck the **Enable by default on the a/n radio** box, configure the **SSID** name and **VLAN**. Under **Edge-toEdge**, check the **Enable** box. Using the pull down menus, set the **Authentication Type** to **WPA2-PSK** and **Cipher Type** to **AES-CCM**. Under **WPA PSK Settings**, enter the **Passphrase/Confirm passphrase** information. Click **Save** to continue.



©2009 Avaya Inc. All Rights Reserved.

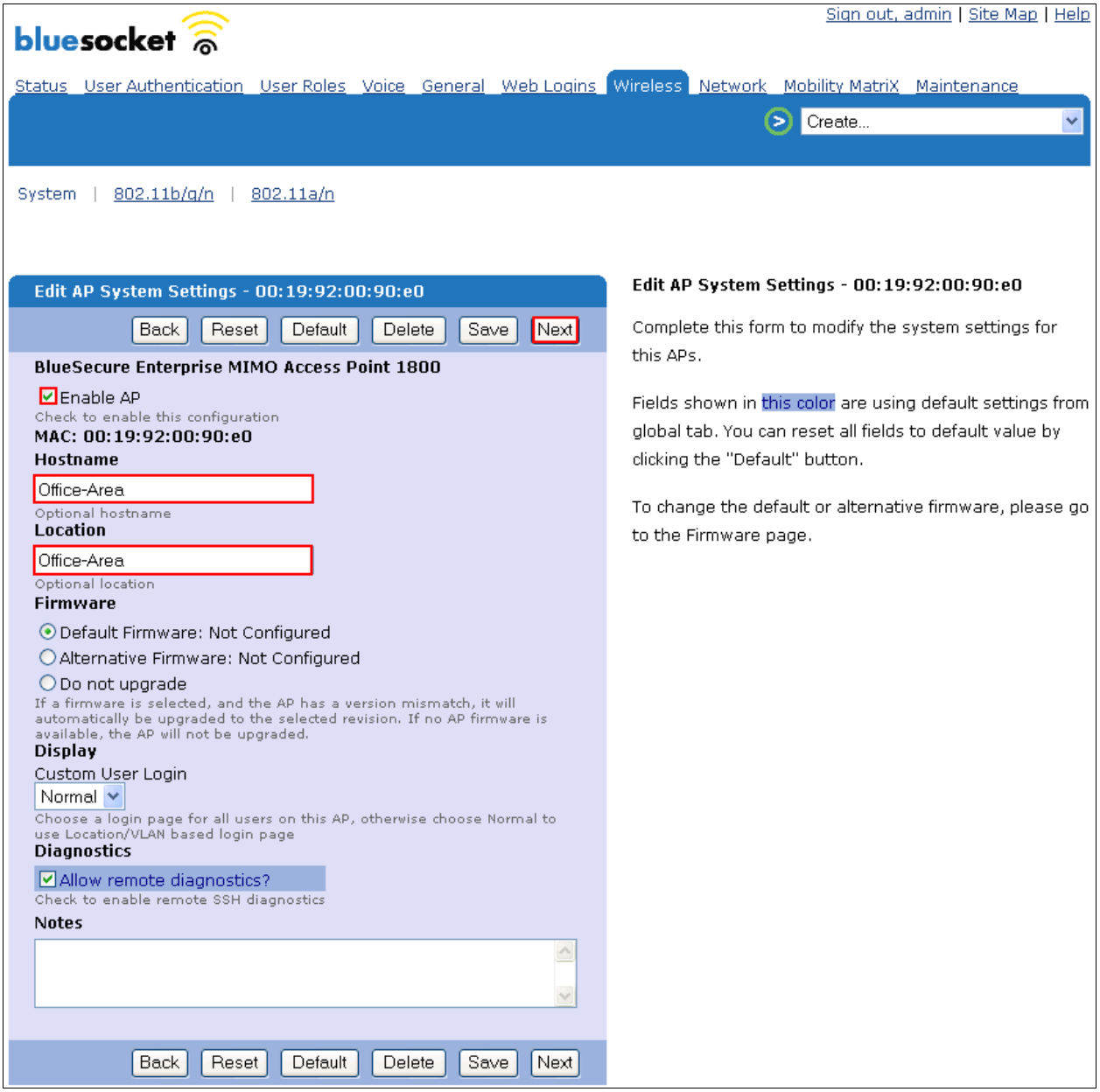
4.5. Configure Bluesocket BlueSecure Access Points

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.	Navigate to the AP web page by clicking **Wireless** and then **AP**. 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. 
2.	Following APs are discovered by the BSC-600. Click the icon under the **Actions** column to edit the configuration information for the newly discovered access points. 

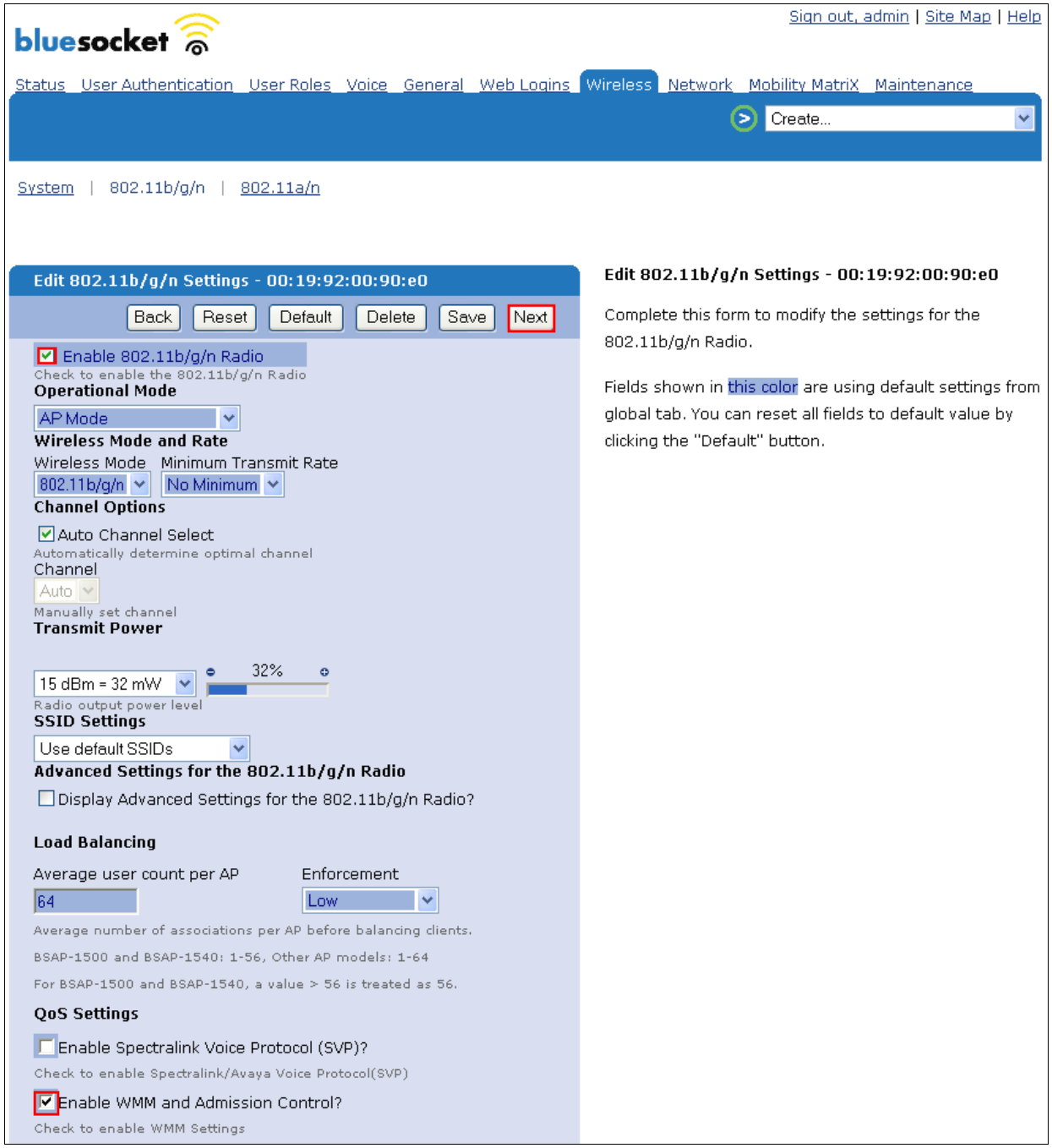
©2009 Avaya Inc. All Rights Reserved.

Step	Description
3.	Ensure that the check box labeled **Enable AP** is checked and populate the **Hostname** and **Location** fields. These are not required parameters but help identify hostname and location at a glance. Click **Next** to go to the **802.11b/g/n** screen.

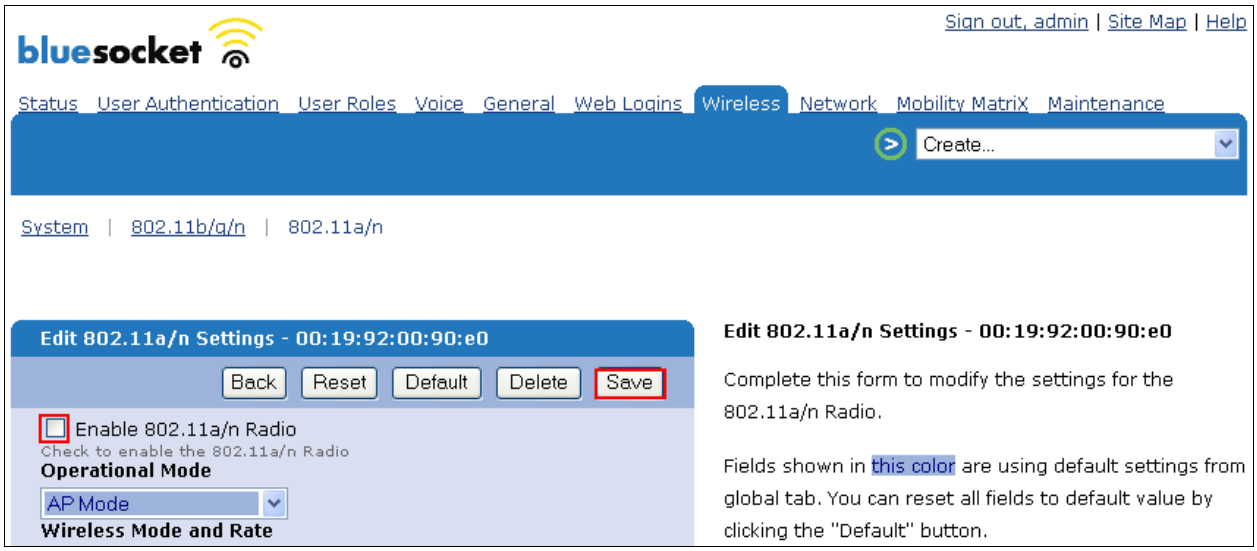


©2009 Avaya Inc. All Rights Reserved.

Step	Description
4.	Ensure that the check boxes labeled **Enable 802.11b/g/n Radio** and **Enable WMM and Admission Control?** are checked. Click **Next** to go to the **802.11a/n** screen.



©2009 Avaya Inc. All Rights Reserved.

Step	Description
5.	Uncheck the box labeled **Enable 802.11a/n Radio.** Click **Save** to continue. 
6.	The process for adding additional access points is the same. In the sample network a total of three access points were used. Repeat **Section 4.5**, **Steps 1-5** to create the Access Points for the **Control Room** and **Meeting Room**.

©2009 Avaya Inc. All Rights Reserved.

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

©2009 Avaya Inc. All Rights Reserved.

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.	Add the following information to the 46xxsettings file: Clear Configuration **SET WTPROF1 "b-voice"** **SET WTSSIDP1 "b-voice "** **SET DNSSRVRP1 "10.20.20.250"** **SET DOMAIN "dev4.com"** WEP Configuration **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 WPA2-PSK Configuration **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.

©2009 Avaya Inc. All Rights Reserved.

5.2. Downloading 46xxsettings File via USB Cable

Step	**Description** Configuring 46xxsettings file
1.	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. Use the following procedure to download the 46xxsettings.txt file to the phone via a USB cable: 1. On the Avaya 3631 Wireless IP Telephone, access the **Advanced Settings** menu, select the **Admin access mode** and specify the **Admin password**. 2. From the **Advanced** menu, select the **Service** sub-menu. 3. From the **Service** menu, select **Backup & Restore over USB**. 4. From the **Backup & Restore …** menu, select **Download settings file.** • The "Starting USB driver …" status message is displayed 5. When prompted, insert (or remove and re-insert) the USB cable into its connector on the bottom of the phone. • A confirmation window appears, with instructions on copying files. 6. From the Windows PC, drag and drop the **46xxsettings.txt** file onto the USB drive folder associated with the phone. 7. Once the file has been copied to the USB drive, return to the phone and select the **Done** softkey. • The phone displays a "Downloading file…" status message 8. When the phone displays a "Completed" message, press the **Back** softkey. • The phone displays a Confirmation window for restarting the phone.

©2009 Avaya Inc. All Rights Reserved.

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 Egde-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).

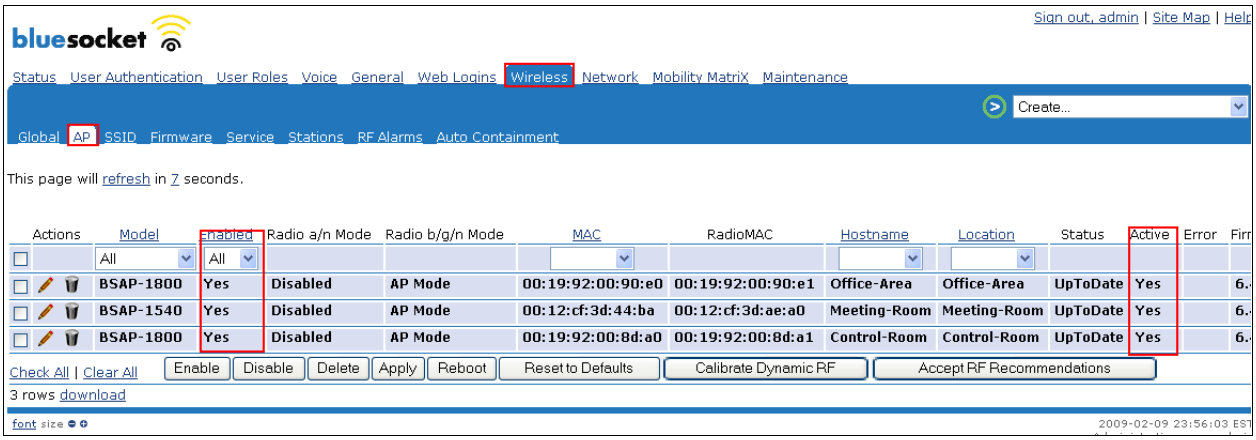
The telephony features verified to operate correctly included attended/unattended transfer, conference call participation, conference call add/drop, multiple call appearances, caller ID operation, call forwarding unconditional, call forwarding on busy, call Park, call pick-up, bridged call appearances,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

©2009 Avaya Inc. All Rights Reserved.

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.**



©2009 Avaya Inc. All Rights Reserved.

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.

©2009 Avaya Inc. All Rights Reserved.

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.

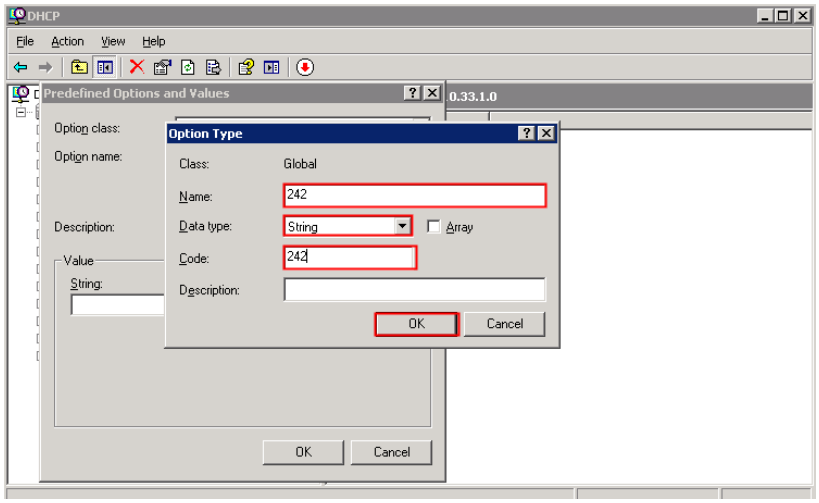
[9] BlueSecure™ Controller Setup and Administration Guide, January 2007, Part Number 870-202TT-M00

©2009 Avaya Inc. All Rights Reserved.

Appendix A:

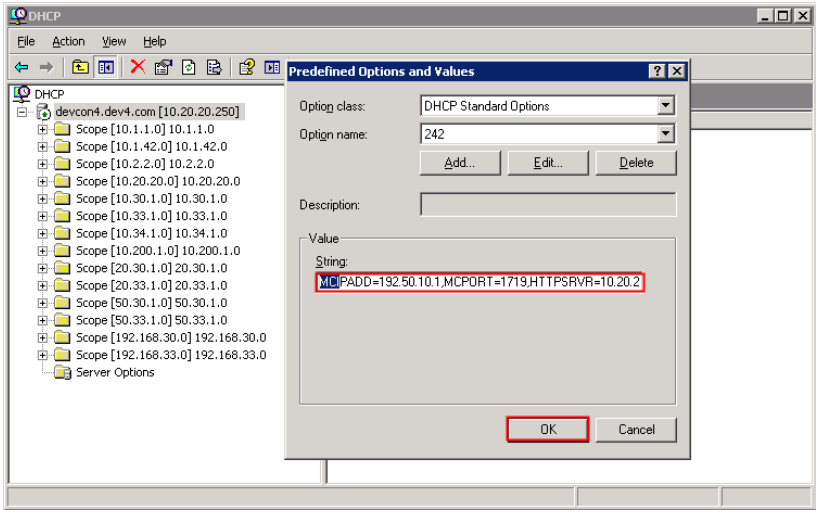
This section describes how to configure the Vendor Class Identifier Code (option 242) on a Microsoft Windows-based DHCP server.

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



©2009 Avaya Inc. All Rights Reserved.

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.

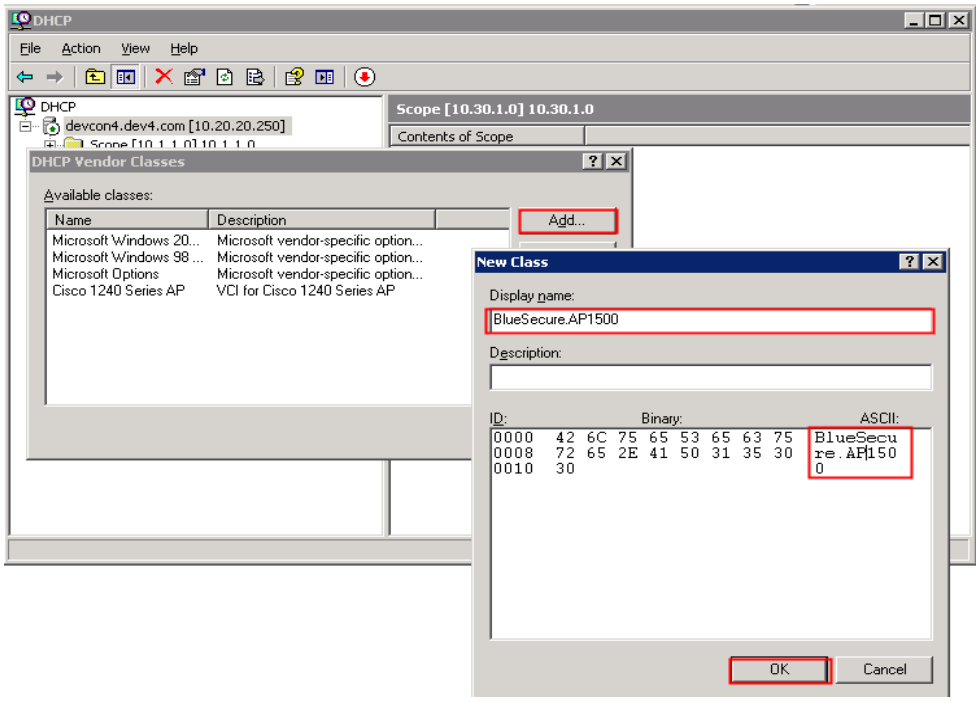
A. Define the Vendor Class.

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).



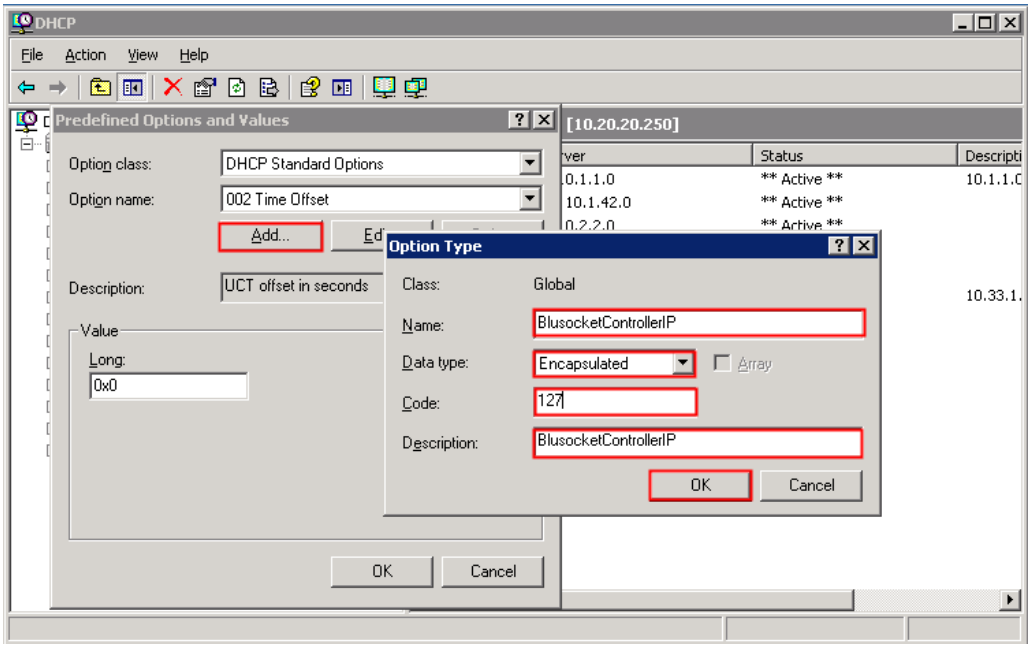
©2009 Avaya Inc. All Rights Reserved.

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.



©2009 Avaya Inc. All Rights Reserved.

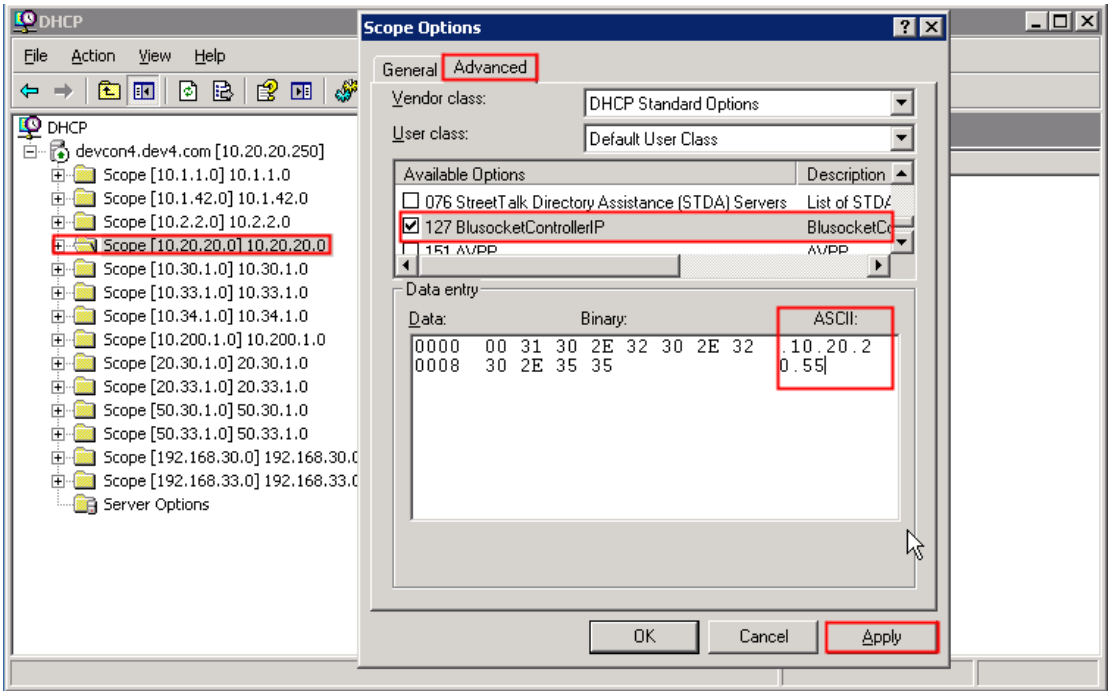
c. Configure the Option for the AP DHCP scope.

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.

©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.