AVAYA

Avaya Solution & Interoperability Test Lab

Application Notes for Colubris Networks Wireless LAN Solution with Avaya IP Office and Avaya Wireless IP Telephones 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 Colubris Intelligent Mobility Solution. The solution consists of the Colubris Networks MultiService Controller 5000 Series managing multiple Colubris Networks MultiService Access Points 300 Series (MAP-330s). Avaya Wireless IP Telephones gained network access through the Colubris MAP-330s and registered with Avaya IP Office. The Avaya Voice Priority Processor (AVPP) was used to support SpectraLink Voice Priority (SVP) on the Avaya Wireless IP Telephones. Emphasis of the testing was placed on verifying prioritization of VoIP traffic on calls associated with the Avaya 3600 Series Wireless IP Telephones.

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

TMA; Reviewed:
SPOC 2/13/2008
Solution & Interoperability Test Lab Application Notes
©2008 Avaya Inc. All Rights Reserved.
1 of 29
Colubris-IPO

1. Introduction

These Application Notes describe a solution for supporting wireless voice traffic over an Avaya IP Telephony infrastructure using Colubris Networks MultiService Controller 5000 Series (MSC) managing multiple Colubris Networks MultiService Access Points 300 Series (MAP-330s). The Colubris MSC-5100 controller and the Colubris MAP-330s were used for testing. The Colubris MAP-330s connected the Avaya 3600 Series Wireless IP Telephones to the wired network and allowed them to register with Avaya IP Office. Emphasis of the testing was placed on verifying prioritization of VoIP traffic on calls associated with the Avaya wireless IP telephones.

1.1. Avaya 3641 Wireless IP Telephone-

The Avaya 3641 IP Wireless Telephone is an 802.11b/g/a wireless telephone that works with industry-standard, enterprise-grade wireless LANs.

1.2. Avaya 3645 Wireless IP Telephone

The Avaya 3645 IP Wireless Telephone is an 802.11b/g/a wireless telephone that works with industry-standard, enterprise-grade wireless LANs and features push-to-talk (PTT).

1.3. Avaya 3616 Wireless IP Telephone

The Avaya 3616 IP Wireless Telephone is an 802.11b wireless telephone that works with industry-standard, enterprise-grade wireless LANs.

This Application Notes assumes the Avaya 3600 series wireless telephones were configured prior to testing.

1.4.   Colubris MultiService Controller 5000 Series

The Colubris MSC-5100 centrally manage the configuration and operation of a network of Colubris MAP-330s, provisioning a broad range of identity and roles-based services to ensure consistent QoS and security to clients that use and roam across the network. An integral component of the Colubris Intelligent Mobility Solution, the Colubris MSC-5100 pushes QoS and security policies to Colubris MAP-330s at the network edge, where traffic is forwarded directly from source to destination. This architecture reduces the amount of wireless traffic on the LAN backbone, when compared with other wireless LAN solutions, and enables scalability and migration to high-capacity 802.11n networks.

1.5. Colubris MultiService Access Points 300 Series

Colubris MAP-330s bring intelligence to the network edge, providing scalable, seamless wireless. Colubris' enterprise-grade feature set includes dispensing multiple network services, enforcing security and delivering client access. An integral component of the Colubris Intelligent Mobility Solution, Colubris MAP-330s support a plug-and-play automatic configuration and ongoing central control by Colubris MSC-5100 to simplify WLAN deployment.

For the compliance testing the DHCP server function on Avaya IP Office was disabled and instead a centralized corporate DHCP server was put in place to handle both the corporate and remote sites. To better manage the different traffic types at each site, the voice and data traffic were separated onto different VLANs.

1.6. Network Diagram

The network diagram shown in **Figure 1** illustrates the testing environment used for compliance testing. The network consisted of an Avaya IP Office 406v2, one PC running Avaya IP Office Manager, two Avaya 3645 Wireless IP Telephones, one Avaya 3641 Wireless IP Telephone, one Avaya 3616 Wireless IP Telephone, one Avaya 5610SW IP Telephone, one Avaya 5620SW IP Telephone one Colubris MSC-5100 and three Colubris MAP-330s. One computer was

present in the network providing network services such as DHCP, TFTP and HTTP.
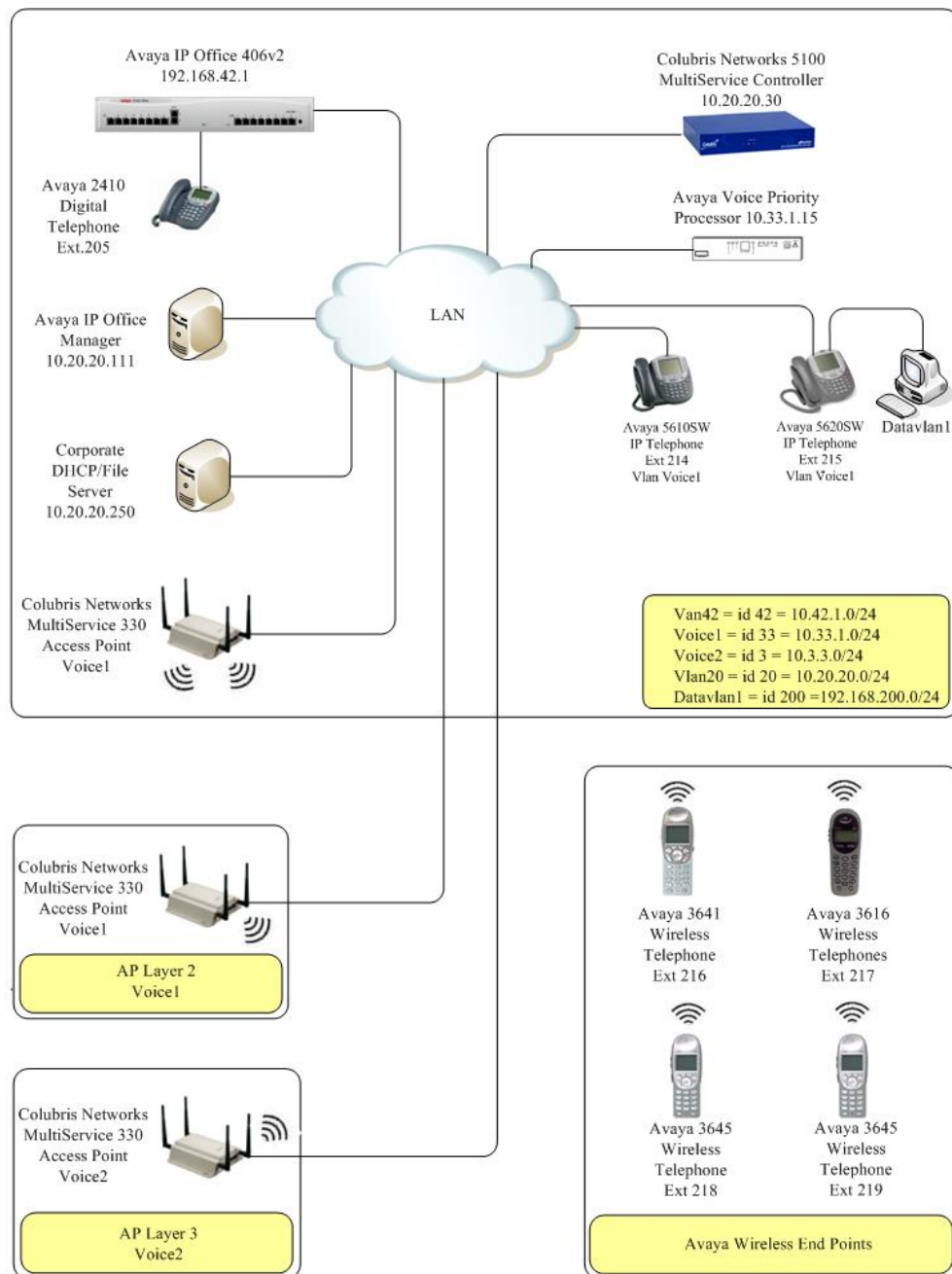
Figure 1: Avaya and Colubris Networks Wireless LAN Configuration

2. Equipment and Software Validated

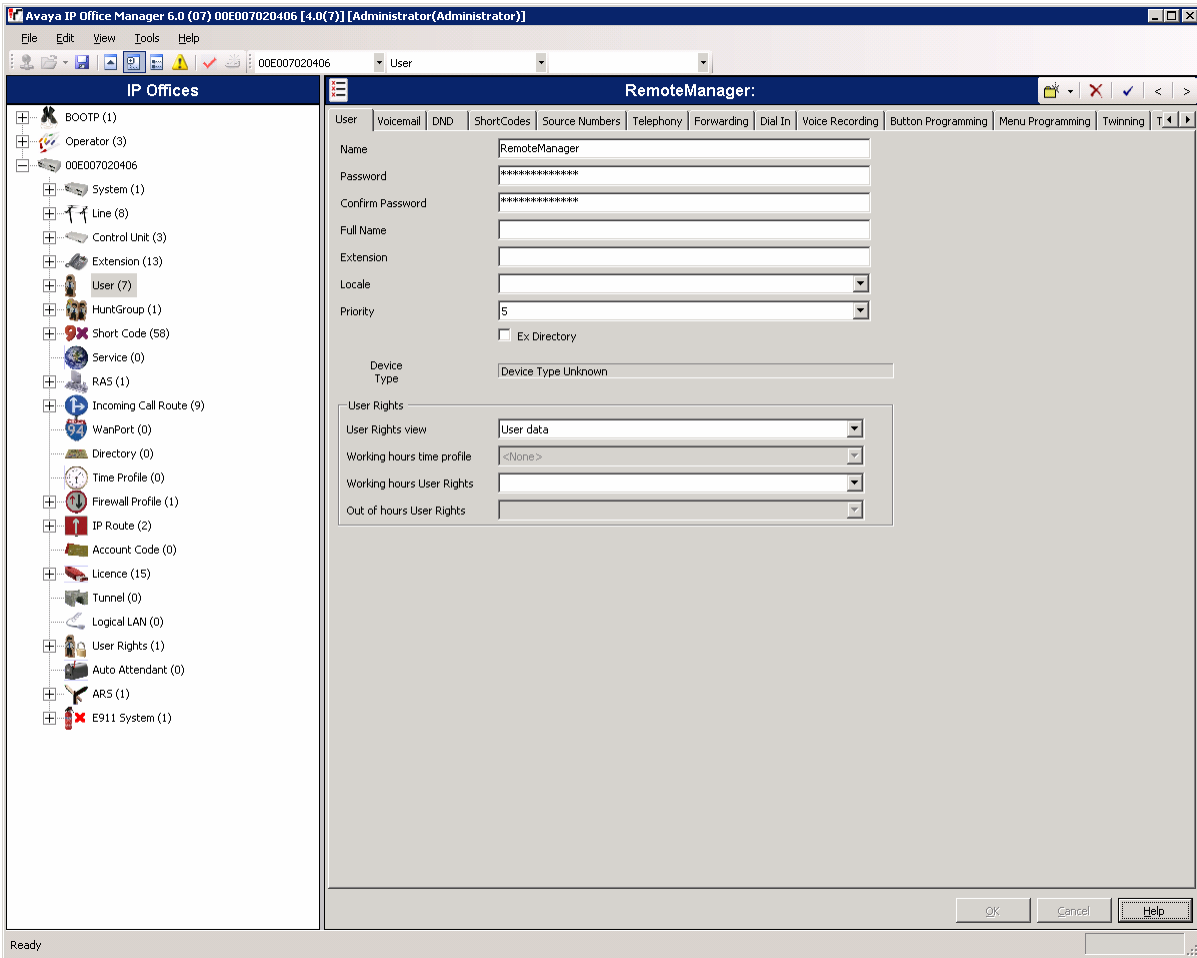The following equipment and software were used for the sample configuration provided:

Hardware Component	Version
Avaya IP Office (IP406v2)	4.1 (9)
Avaya 3616 Wireless Telephone	96.049
Avaya 3645 Wireless Telephone	117.016
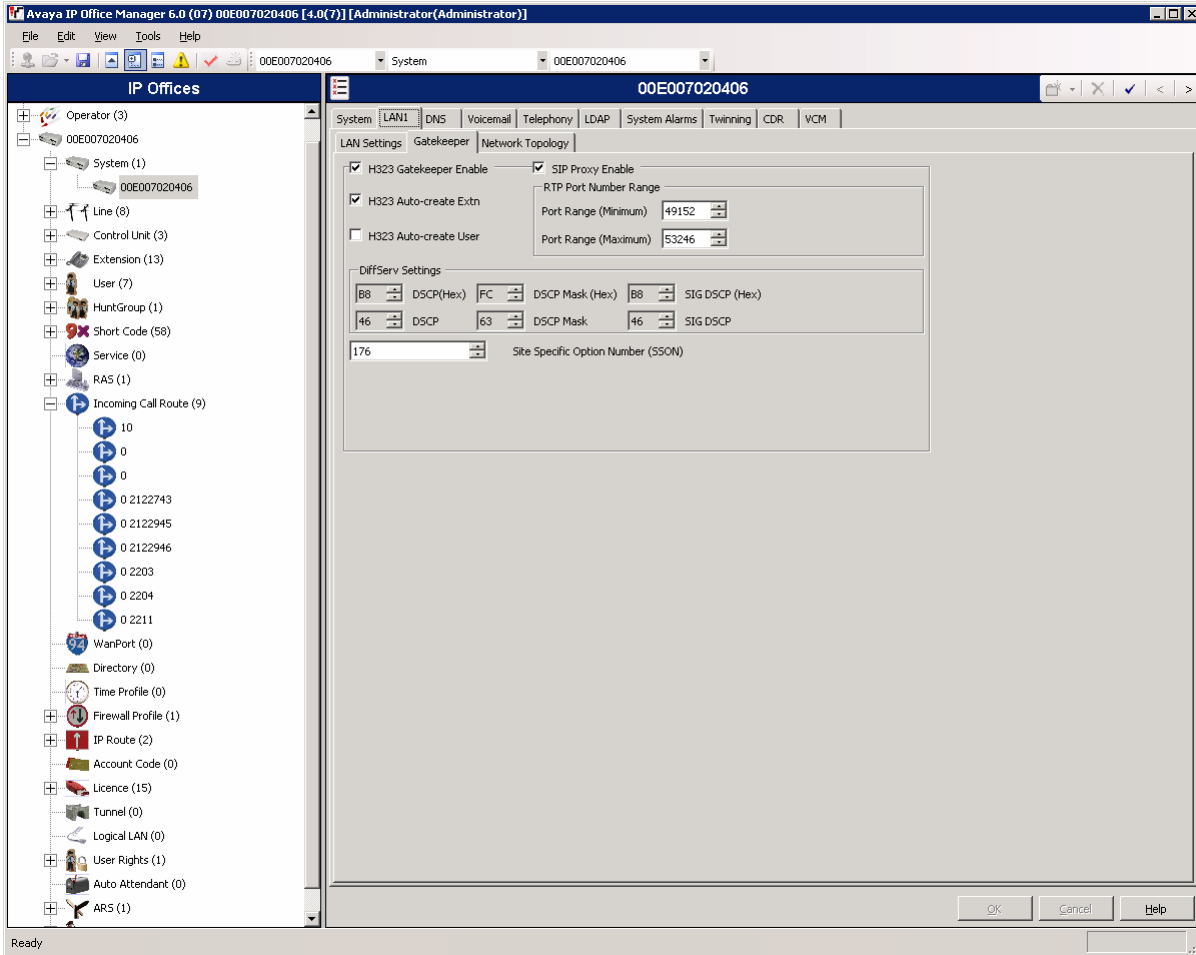
Avaya 3641 Wireless Telephone	117.016
Avaya Voice Priority Processor	17x.028
Avaya 5620SW IP Telephone	2.3
Avaya 5610SW IP Telephone	2.3
Avaya 2410 Digital Telephone	5.0
Colubris Networks MSC-5100	5.2.1
Colubris Networks MAP-330	5.2.1
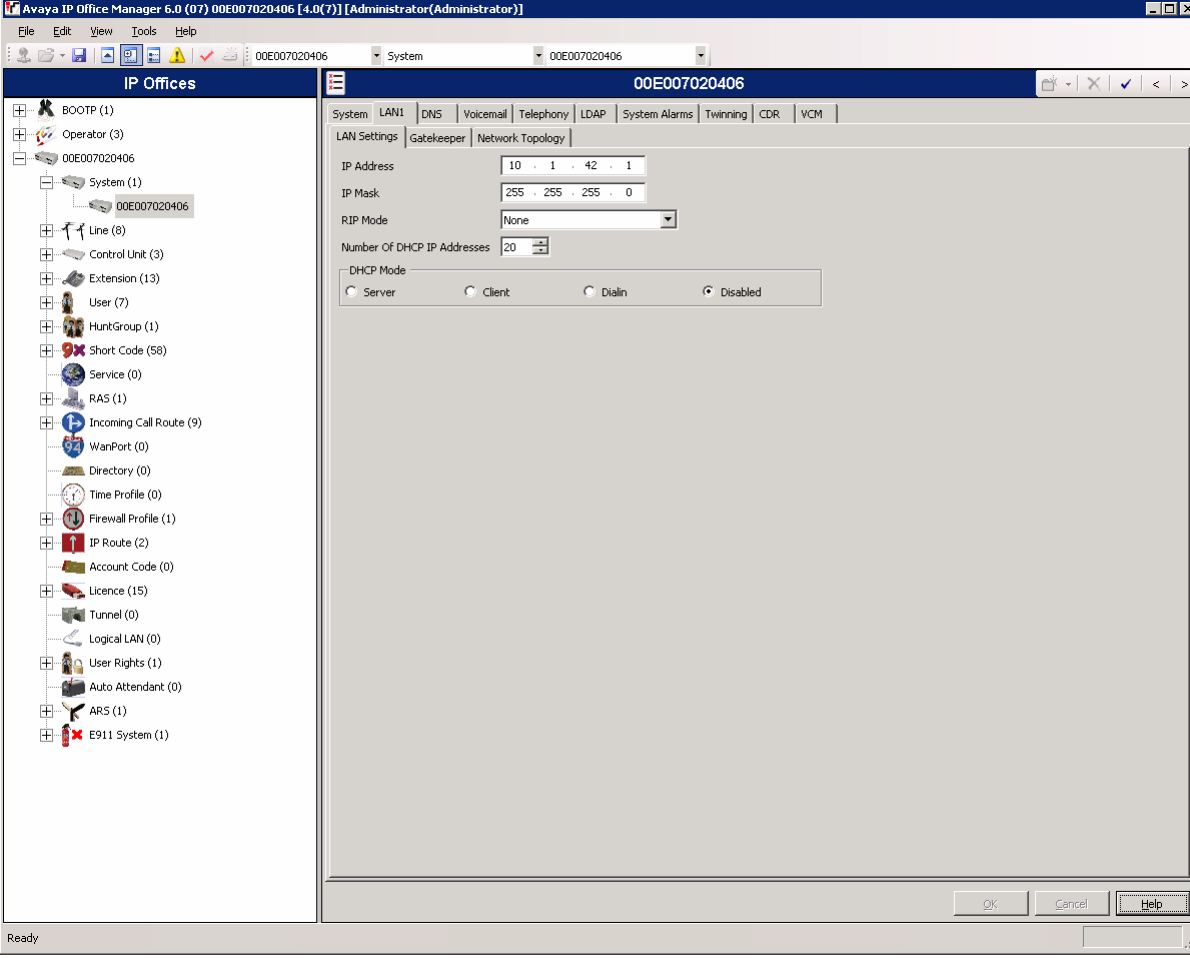
3. Avaya IP Office Settings

This section was included to verify that Avaya IP Office was configured correctly. Except where stated, the parameters in all steps are the default settings and are supplied for reference. For all other provisioning information such as provisioning of the trunks, call coverage, and extensions, please refer to the Avaya IP Office product documentation in Section 13.

Step	Description
1.	Avaya IP Office is configured via the Avaya IP Office Manager program. Log into the Avaya IP Office Manager PC and select **Start → Programs → IP Office → Manager** to launch the Avaya IP Office Manager application. Log into the Avaya IP Office Manager application using the appropriate credentials.

Step	Description
2.	Avaya IP Office Manager Window. The main Avaya IP Office Manager window appears. The following steps refer to the Configuration Tree, which is in the left pane of the window.

Step	Description
3.	Verify H323 Gatekeeper information.
	The Avaya IP Telephones will get Differentiated Services information from the Avaya IP Office. In the Manager window, go to the Configuration Tree and click **System** , select the **LAN1** tab, then select the **Gatekeeper** tab. Verify that the **DiffServ Settings** for **DSCP** and **SIG DSCP** are set to **46** and **46,** respectively.

Step	Description
4.	Disable DHCP server on Avaya IP Office. From the Configuration Tree, double-click **System**. Select the **LAN1** tab, then select the **LAN Settings** tab. Set the **DHCP Mode** to **Disabled**. Click **OK** to continue.

TMA; Reviewed:
SPOC 2/13/2008

Solution & Interoperability Test Lab Application Notes
©2008 Avaya Inc. All Rights Reserved.

8 of 29
Colubris-IPO

5.	Configure the Avaya Voice Priority Processor information on Avaya IP Office. From the Configuration Tree, click **System**. Enter the IP address into the **AVPP IP Address** field. Click **OK** to continue.

Step	Description
6.	Verify Direct Media Path. From the Configuration Tree, select **Extension**. Click on the IP telephone extension to verify. Select the **VoIP** tab. Verify that **Allow Direct Media Path** is checked. Click **OK** to continue.

4. Configure the Avaya Voice Priority Processor

The Avaya Voice Priority Processor (AVPP) utilizes SpectraLink Voice Priority (SVP) as the Quality of Service (QoS) mechanism supported by the Avaya 3641/3645 Wireless IP Telephones and the Colubris MAP-330s to reduce jitter and delay for voice traffic over the wireless network.

The AVPP performs three major functions. First, it is a required component to utilize the maximum transmission speed available in the Avaya Wireless Telephones that support 802.11B and 80211G. Secondly, SVP allows the Colubris MAP-330s and the Avaya Wireless IP Telephones to transmit their voice packets immediately, while other devices must wait a random back off period as required by the 802.11 standard. This reduces delay for the voice packets. Lastly, the AVPP is required to serve as a "gateway" between the Avaya Wireless IP Telephones and the Avaya IP Telephony infrastructure. Since the wireless telephones support SVP, their packets are directed to the AVPP so that the SVP header information can be removed before the packets are forwarded to Avaya Communication Manager.

To configure the AVPP, connect a PC or laptop to the serial port of the AVPP using a straight through serial cable. Run a terminal emulation program with the following configuration:

- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow Control: None

Once connected, the AVPP login screen is presented. Log in as *admin*. The **AVPP System Menu** is displayed as shown in **Figure 1**. After configuring an IP address to the AVPP, a Telnet session may be used to modify the AVPP configuration.

```
                         NetLink SVP-II System
               Hostname: [slnk-000006], Address: 10.1.2.230

                     System Status
                     SVP-II Configuration
                     Network Configuration
                     Change Password
                     Exit


     Enter=Select           ESC=Exit      Use Arrow Keys to Move Cursor
```
Figure 1: AVPP System Menu

From the **AVPP System Menu**, select **Network Configuration** to configure the IP address, subnet mask, and default gateway of the AVPP.

```
                        Network Configuration
                Hostname: [slnk-000006], Address: 10.1.2.19

     Ethernet Address (fixed):      00:90:7A:00:00:06
     IP Address:                    10.33.1.15
     Hostname:                      slnk-000006
     Subnet Mask:                   255.255.255.0
     Default Gateway:               10.33.1.254
     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
     Maintenance Lock:              N


        Enter=Change      Esc=Exit            Use Arrow Keys to Move Cursor
```
Figure 2: Network Configuration

From the **AVPP System Menu**, select **SVP-II Configuration** to configure the **Phones per Access Point** and the **802.11 Rate** fields. In this configuration, the **802.11 Rate** of the AVPP was configured to *Automatic*, as shown in **Figure 3**, to allow the wireless telephones to determine their rate (up to 54Mbps), as opposed to the AVPP limiting the transmission rate of the wireless telephones to 1/2 Mbps.

```
                         SVP-II Configuration
                Hostname: [slnk-000006], Address: 10.33.1.15

     Phones per Access Point:       10
     802.11 Rate:                   Automatic
     SVP-II Master:                 10.33.1.15
     SVP-II Mode:                   Netlink IP
     Ethernet link:                 100mbps/full duplex
     System Locked:                 N
     Maintenance Lock:              N
     Reset System


        Enter=Change      Esc=Exit            Use Arrow Keys to Move Cursor
```
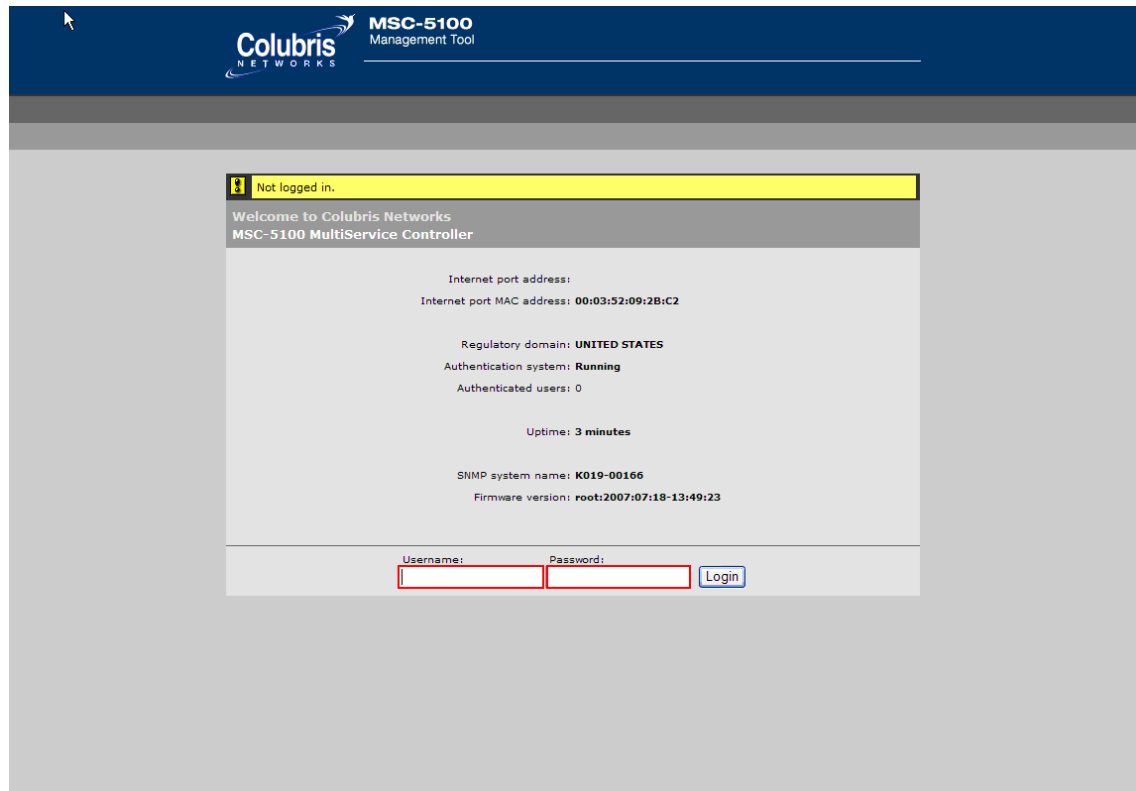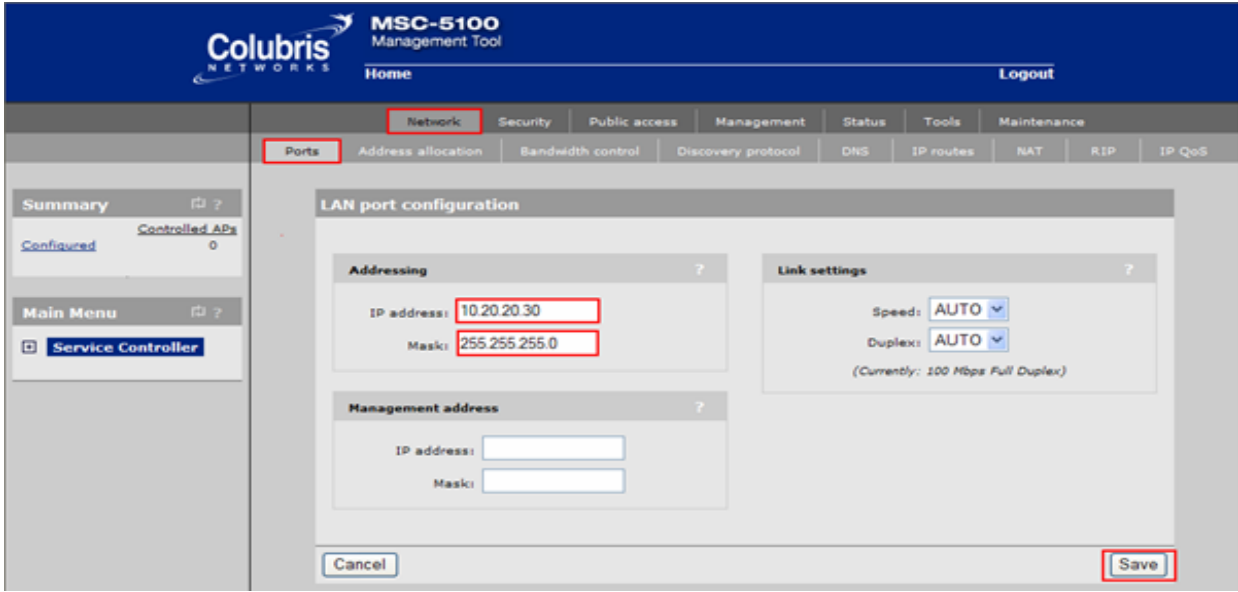**Figure 3: SVP-II Configuration**

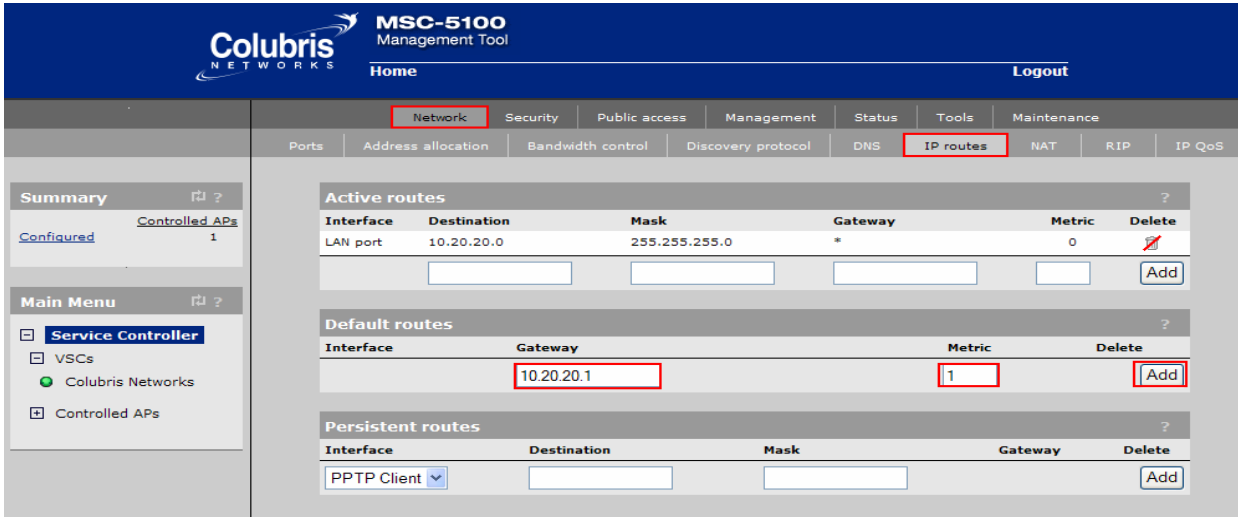# 5. Configure the Colubris Networks MSC-5100 Controller and MAP-330s

The following steps detail the initial configuration for the Colubris Intelligent Mobility Solution used for the compliance testing. The configuration on the Colubris MSC-5100 was administered via the Web configuration tool. Except where stated the parameters in all steps are the default settings and are supplied for reference. Refer to Section **13 [8]** for additional information regarding the configuration displayed in this section.

5.1. Configure Colubris MSC-5100 Controller

Step	Description:
1.	Configure Colubris Controller in the WLAN as depicted in **Figure 1**. Configure the Colubris MSC-5100 using the built-in web-based **Management Tool.** Access this tool by establishing a web browser connection to the Colubris MSC-5100. Supported web browsers are Microsoft Internet Explorer 6.0 or higher and Mozilla Firefox 1.5 or higher. 1. Connect the LAN port of the computer being used to the LAN port on the Colubris MSC-5100. 2. Configure the computer with the static IP address **192.168.1.2/24.** 3. Start the **Management Tool** as follows: Start your web browser and enter **https://192.168.1.1.** Click **Enter**. 4. Log into the Colubris MSC-5100 controller using default credentials which can be obtained from the Colubris MSC-5100 controller documentation in Section 13.

Step	Description:
2	Set Colubris MSC-5100 network address Select **Network → Ports**. Set the **IP address** to **10.20.20.30** and the mask to **255.255.255.0**. Click **Save** to continue.

Step	Description:
3	Set Colubris MSC-5100 Default Gateway Select **Network → IP routes**. Set the **Gateway** to **10.20.20.1** and the **Metric** to **1**. Click **Add** to continue.

5.2. Configure Colubris MAP-330 Access Points
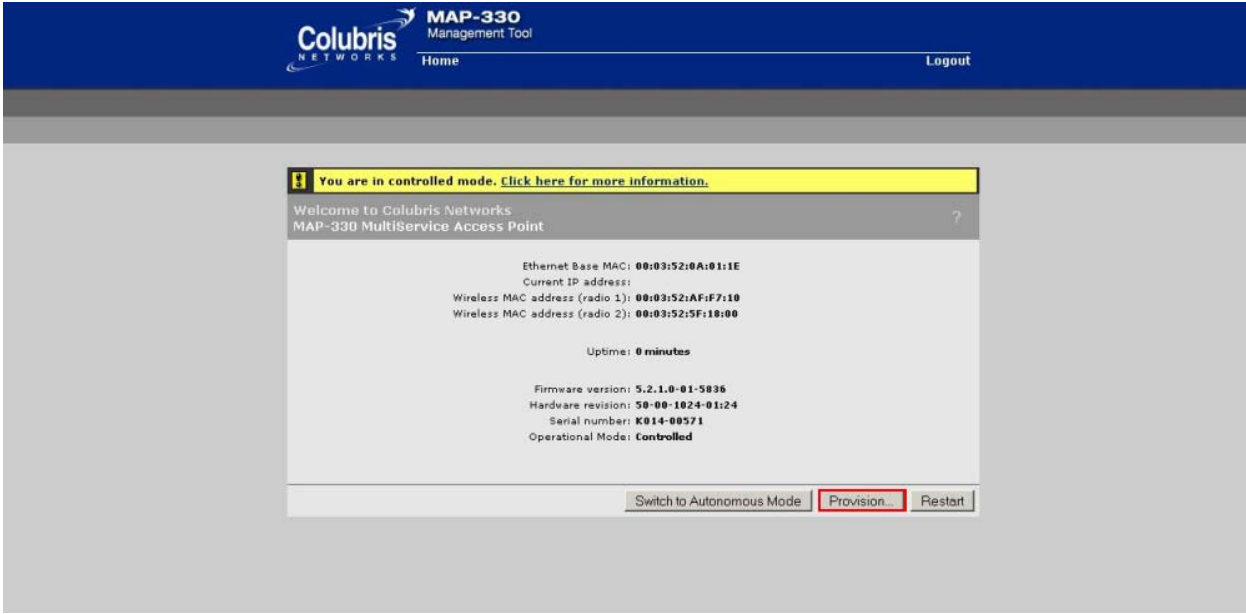
Colubris MAP-330s 1 and 2 are located on the same Layer2 subnet as the Colubris MSC-5100 and will discover the Colubris MSC-5100 using Colubris' automated discovery mechanism. Colubris MAP-330s can be manually configured to connect to the Colubris MSC-5100. For compliance testing Colubris MAP-330 3 was placed on VLAN20 for Layer3 roaming and was manually configured.
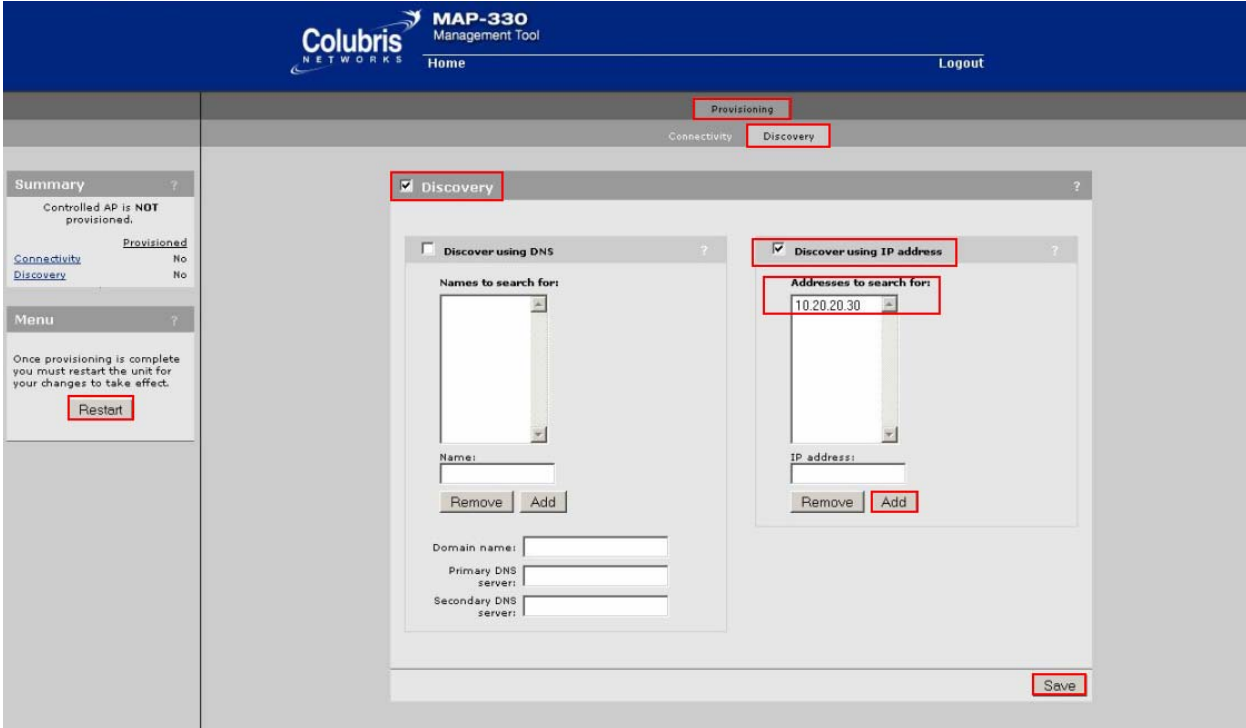
One of three methods can be used to enable the Colubris MAP-330 to discover and connect to the Colubris MSC-5100:
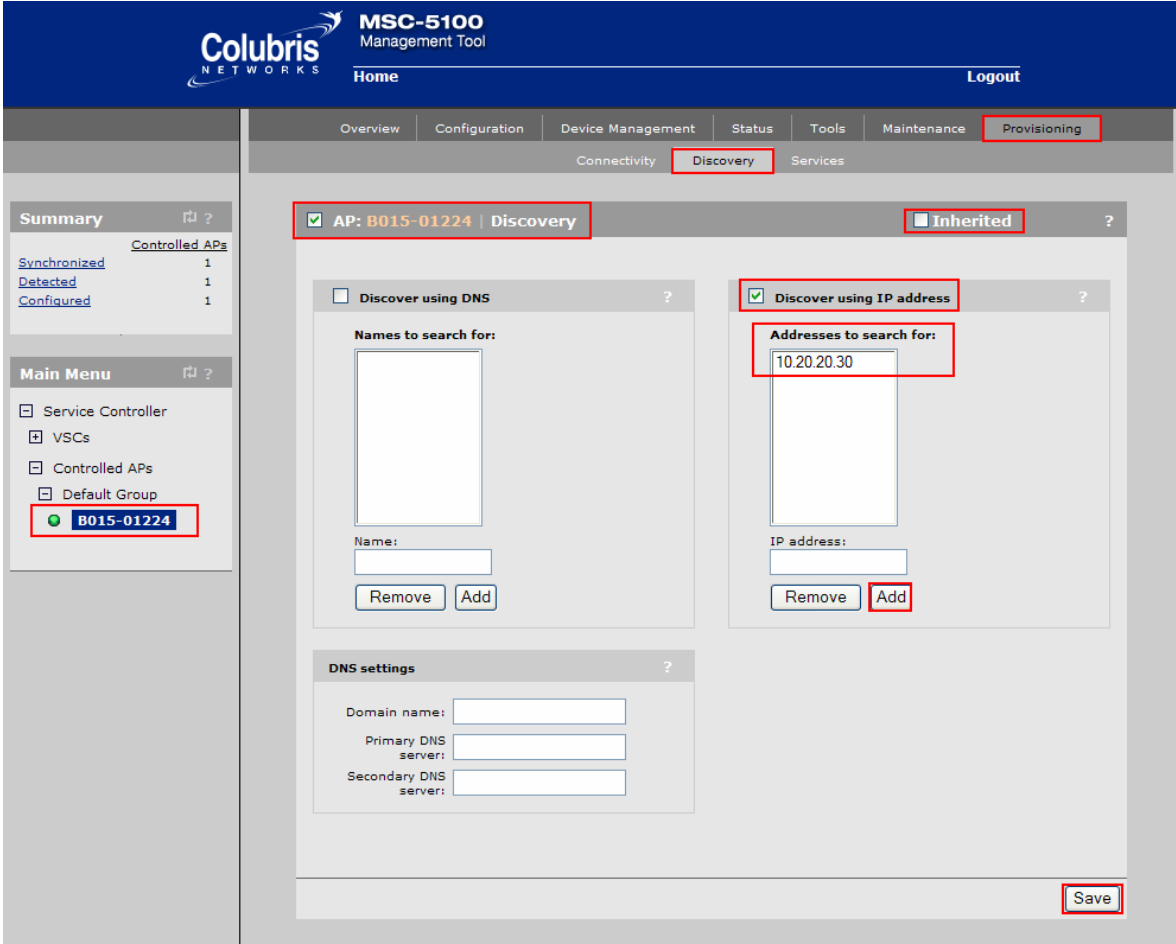
1) Local provisioning
2) DHCP discovery
3) DNS discovery

The DHCP and DNS methods require Colubris vendor specific attributes to be added to the DHCP server, or previously defined DNS names to be added to the corporate DNS server. For more information on these options, consult the MSC-5000 Series Administrator's Guide in Section **13 [8]** provided with the equipment.

Local provisioning is done directly on the Colubris MAP-330specifying either the IP address(es) of the Colubris MSC-5100s or the DNS name of the Colubris MSC-5100s as defined on the corporate DNS servers. A local IP address can also be configured on the Colubris MAP-330 if no DHCP server is available, however in this example, the Colubris MAP-330 will receive an IP address from the DHCP server on its local network. Obtain the IP address given to the Colubris MAP-330 from the DHCP server, perform the following steps:
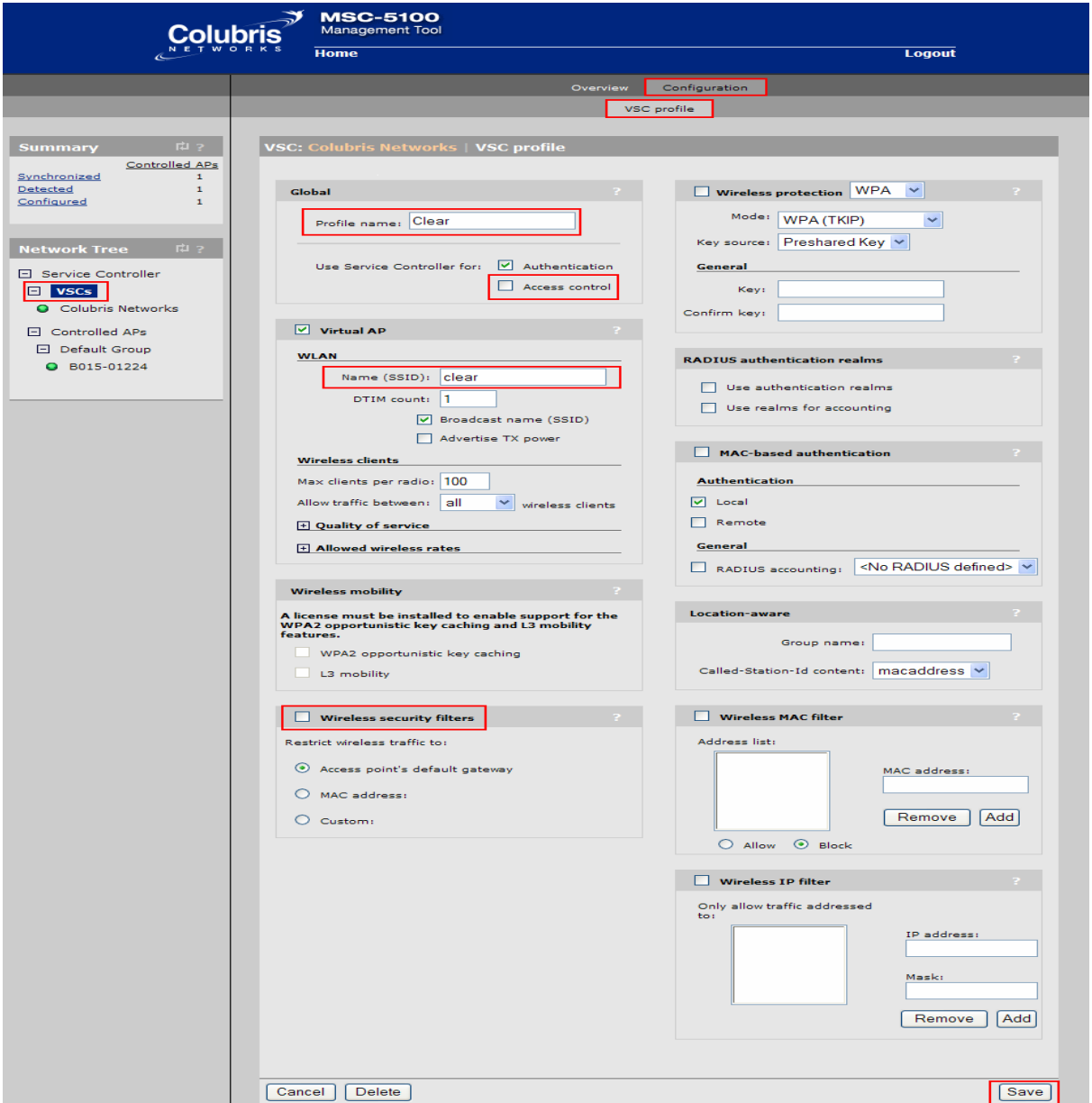
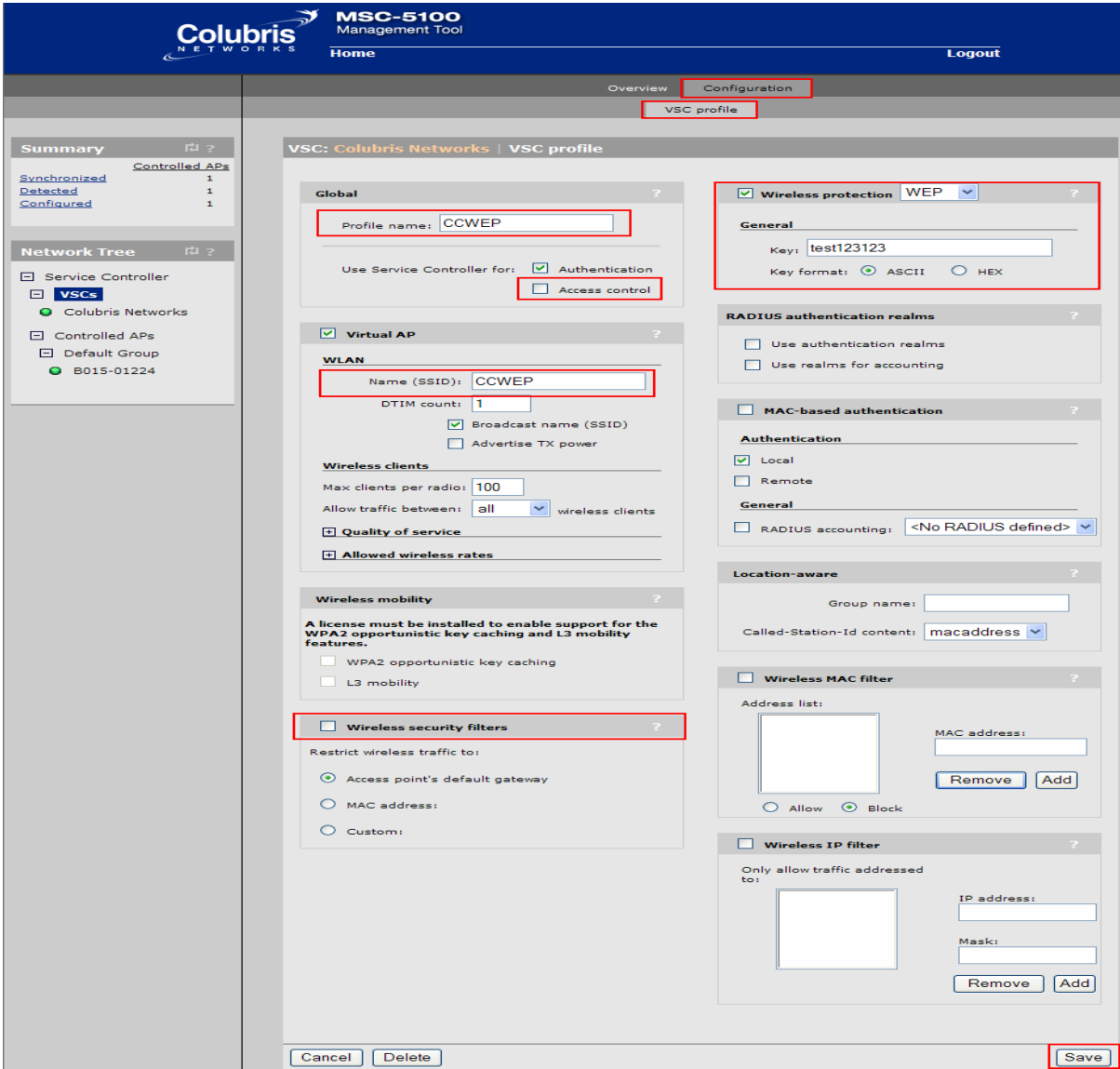| Step	Description:
1.	Login into Colubris MAP-330 3 Connect to the web interface of the Colubris MAP-330, log in using the appropriate administrator crendentials and click the '**Provision**' button.

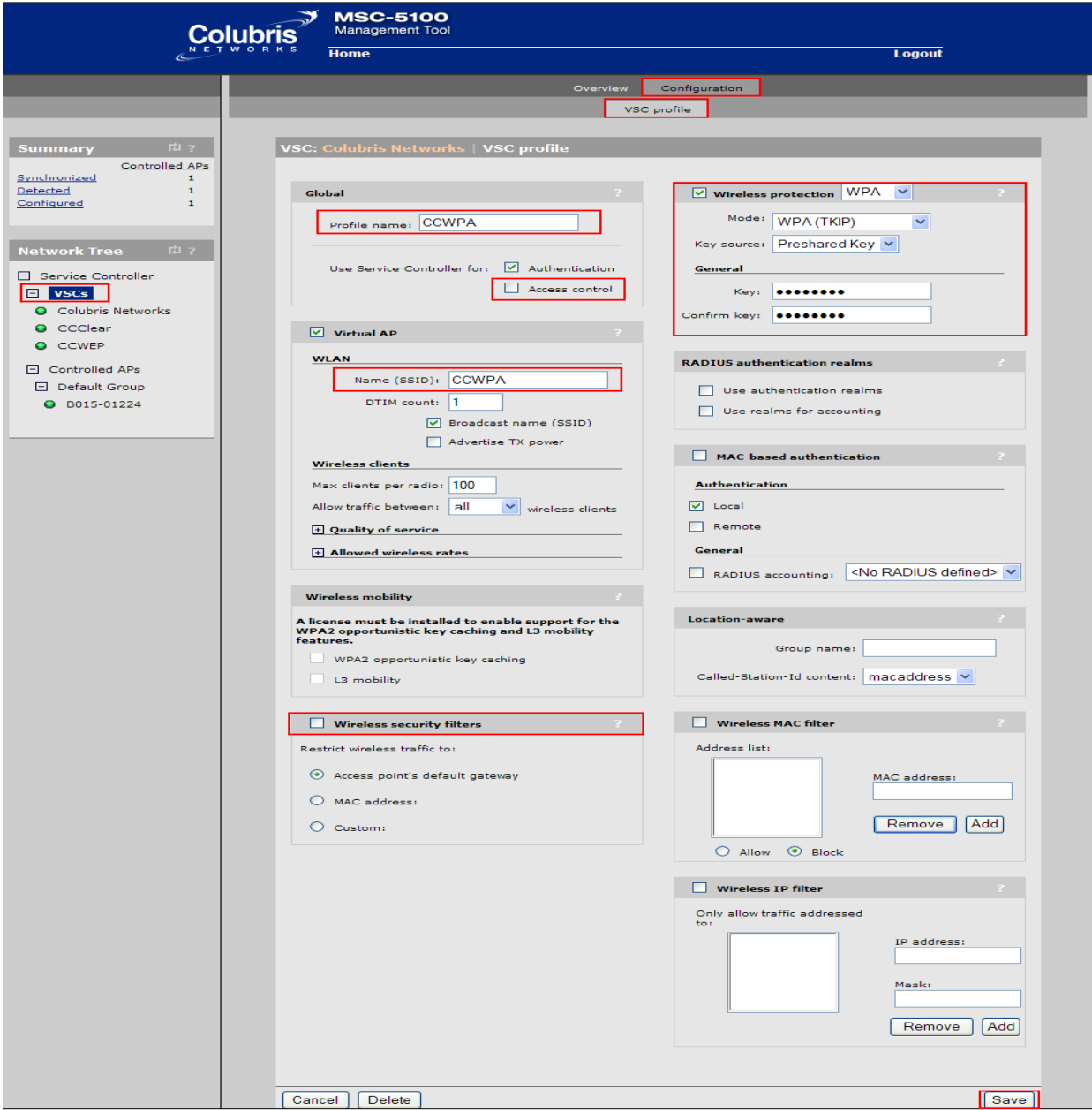| Step	Description:
2.	Colubris MSC-5100 discovery Navigate to the **Discovery** configuration page by clicking **Provisioning → Discovery**. Check the **Discovery** check box in the upper-left corner of the window. Check the '**Discover using IP address**' box, enter the IP address of the Colubris MSC-5100 into the **IP address** field, click **Add** and then **Save.** From the left pane, click **Restart**. The Colubris MAP-330 will reboot and use the new provisioned information to connect to the Colubris MSC-5100. Close this browser window and go back to the Colubris MSC-5100's management window to continue.

TMA; Reviewed:
SPOC 2/13/2008

Solution & Interoperability Test Lab Application Notes
©2008 Avaya Inc. All Rights Reserved.

18 of 29
Colubris-IPO

Step	Description:
3.	Enter the provisioning information on the Colubris MSC-5100.

- Click the name of the newly connected Colubris MAP-330 in the left pane.
- Click on the **Provisioning** tab in the upper window
- Click on the **Discovery** tab
- Uncheck the **Inherited** box
- Check the box in the upper-left corner for Colubris MAP-330 **AP:B015-01224 | Discovery,** each Colubris MAP-330 will have a unique number.
- Check the '**Discover using IP address'** check box and reenter the IP address of the Colubris MSC-5100
- click the **Save** button

 |

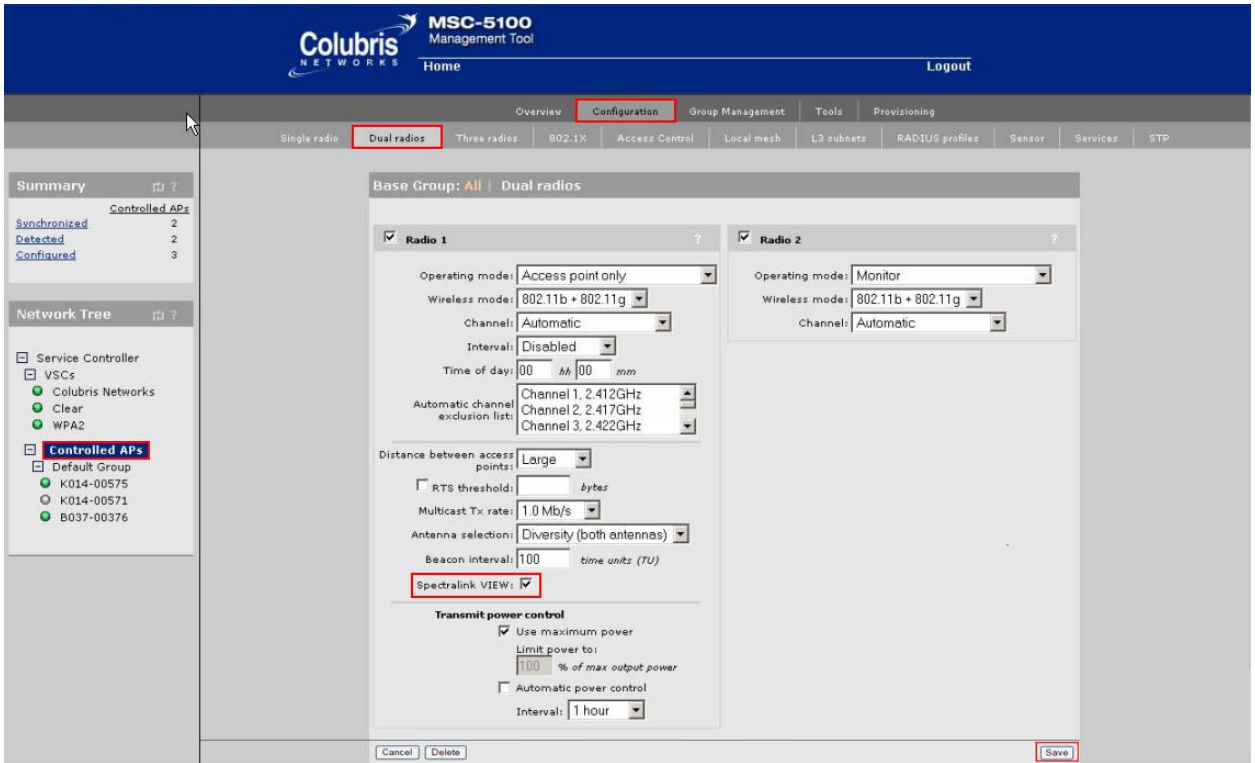## 5.3. Create and Configure Extended Service Set IDs (ESSID)

Colubris uses the term Virtual Service Community (VSC) to refer to an ESSID.

Step	Description:
1.	Create Clear ESSID and assign security profile Click on **VSCs** in the left window. Click **Add new VSC profile.** In the VSC window, change the **Profile name** to **Clear**, uncheck the **Access control** check box, change the **Name SSID** to **clear**, uncheck the **Wireless security filters** box. Click the **Save** button to continue.

TMA; Reviewed:
SPOC 2/13/2008

Solution & Interoperability Test Lab Application Notes
©2008 Avaya Inc. All Rights Reserved.

20 of 29
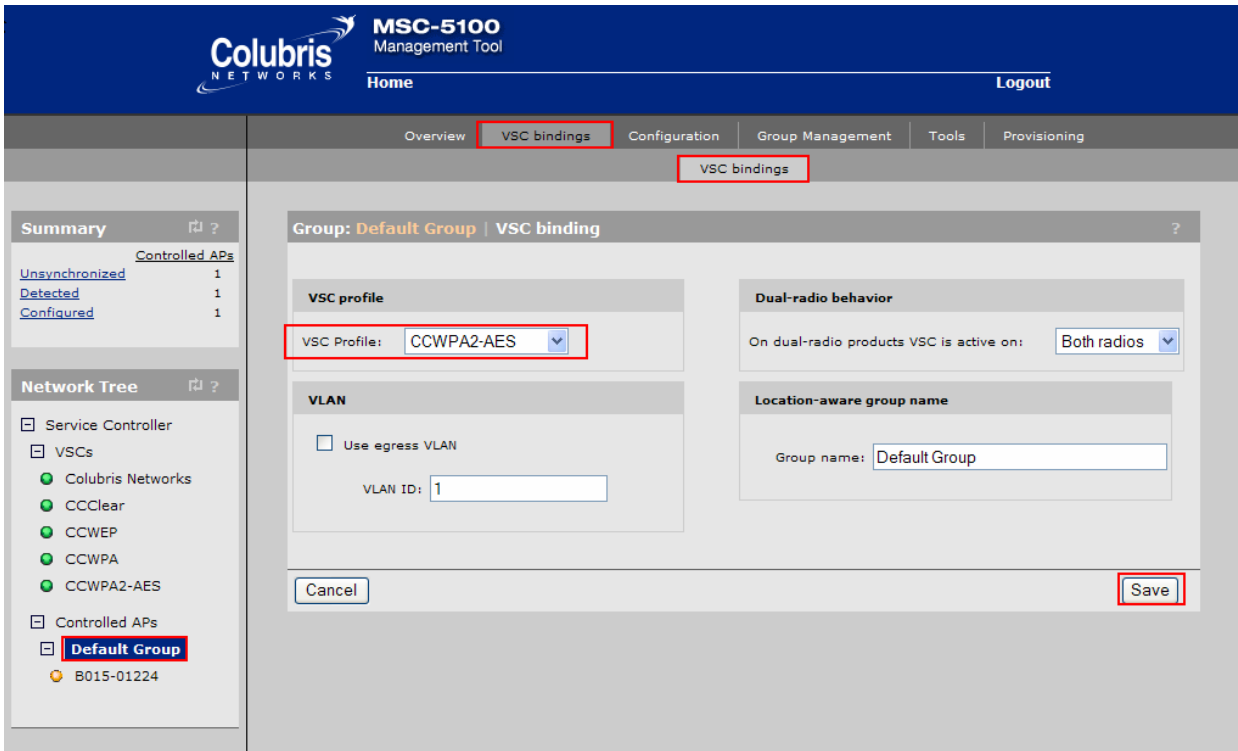Colubris-IPO

Step	Description:
2.	Configure ESSID WEP Click on **VSCs** in the left window. Click **Add new VSC profile.** In the VSC window, change the **Profile name** to **CCWEP**, uncheck the **Access control** box, change the **Nane SSID** to **CCWEP**, and uncheck the **Wireless security filters** box. Check **Wireless protection** and select **WEP from the** pull-down list, enter the key value set in the Avaya 3600 Telephones in the **Key** field, compliance testing used **test123123**. Click the **Save** button to continue.

Step	Description:
3.	**ESSID WPA-PSK** Click on **VSCs** in the left window. Click **Add new VSC profile.** In the VSC window, change the **Profile name** to **CCWPA**, uncheck the **Access control** check box, change the **Name SSID** to **CCWPA**, uncheck the **Wireless security filters**, check **the Wireless protection** check box, then select **WPA** from the **Wireless protection** pull down list, and select **WPA (TKIP)** from the **Mode** pull down list. Under **General,** enter the **Key** information. Click the **Save** button to continue.

Solution & Interoperability Test Lab Application Notes
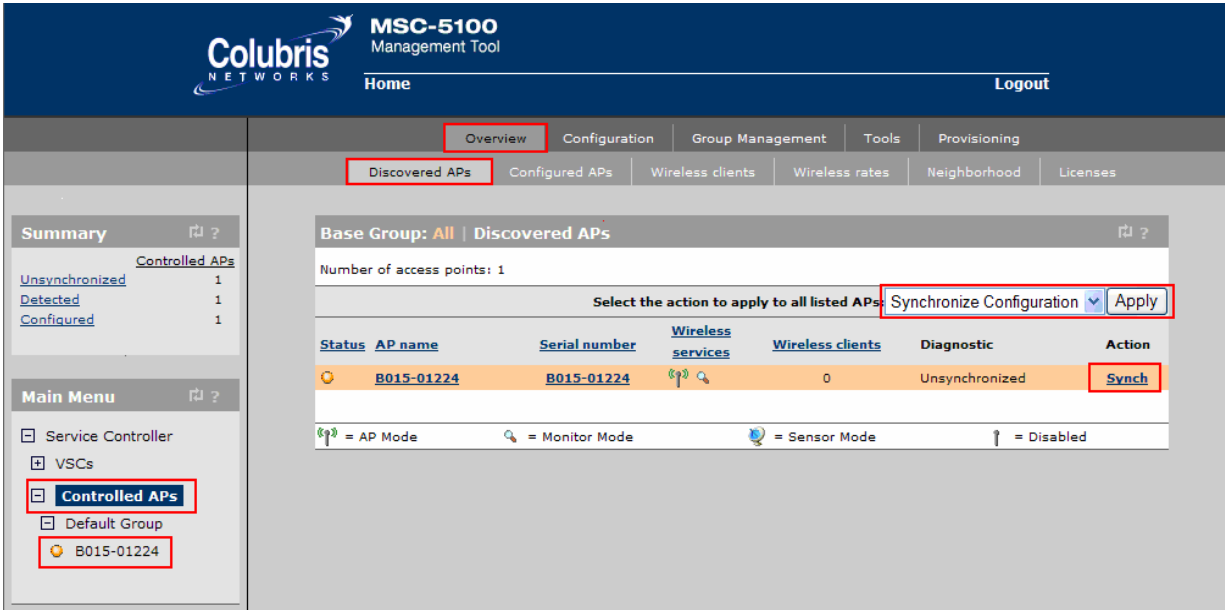
5.4. Configure QoS Polices for Avaya IP Telephones

Step	Description:
1.	Add QoS Rule for Voice ESSID For this example, ESSID CCWPA is used to show how to configure QoS for the Avaya 3641/45 wireless IP Telephones. The same setting can be used with ESSID's Clear and CCWEP. Click on **Controlled APs** in the left window. Check the **Spectralink VIEW** check box. Click the **Save** button to continue.

5.5. Bind the VSCs to the Colubris MAP-330s

Before a VSC can be used, it must be bound to a group of Colubris MAP-330s

Step	Description:
1	Bind VSC's to Colubris MAP-330s Before a VSC can be used, it must be bound to a group of Colubris MAP-330s Click on **Default Group→VSC bindings**. Select the **VSC profile**. Click the **Save** button to continue. Repeat this process for all VSCs that will be used.

Solution & Interoperability Test Lab Application Notes
©2008 Avaya Inc. All Rights Reserved.

Step	Description:
2	Synchronize Colubris MAP/MSC Navigate to the **Discovered APs** configuration page by clicking **Overview → Discovered APs**. Select "**Synchronize Configuration**" in the pull down tab and click **Apply** to synchronize the configuration.

Solution & Interoperability Test Lab Application Notes
©2008 Avaya Inc. All Rights Reserved.

6. Interoperability Compliance Testing

Interoperability compliance testing covered feature functionality, serviceability, and performance testing. Feature functionality testing verified the ability of the Colubris Intelligent Mobility Solution System to provide network access to the Avaya Wireless IP Telephones. The emphasis of testing was on the QoS implementation, multiple encryption methods, and roaming at Layer2 and Layer3.

6.1. General Test Approach

The general test approach was to register the Avaya Wireless IP Telephones with Avaya Communication Manager through the Colubris Intelligent Mobility Solution Calls were made between both wired and wireless telephones and specific calling features were exercised. To validate Quality of Service, low priority background traffic was injected into the wireless network and the Colubris Intelligent Mobility Solution was verified to maintain voice calls while dropping the low priority traffic. Network level tests included verifying Layer2 and Layer3 roaming from one Colubris MAP-330 to another and validating Quality of Service for voice traffic.

6.2. Test Results

The Avaya Wireless IP Telephones with Avaya IP Office utilizing Colubris Intelligent Mobility Solution passed all test cases. The Avaya Wireless IP Telephones were verified to successfully register with Avaya IP Office through the Colubris Intelligent Mobility Solution. The compliance testing also focused on verifying Quality of Service for voice traffic while low priority background traffic was competing for bandwidth. The Avaya Wireless IP Telephones were verified to roam successfully between Colubris MAP-330s on the same network (Layer2 roaming) and between Colubris MAP-330s on a different network (Layer3 roaming) while maintaining voice calls.

Three different security schemas were tested: Clear, WEP-128 and WPA2-PSK TKIP. Two codecs were used for testing 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 IP Office (shuffling disabled). 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, call forwarding unconditional, call forwarding on busy, call forwarding clear and voicemail.

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.

- Ensure that the **ESSID** field value configured in **Section 5.3** on the Colubris MSC-5100 matches the **ESSID** field value on the Avaya Wireless IP Telephones.

- Check that the Avaya Wireless IP Telephones have successfully registered with Avaya IP Office.

- Verify that the Colubris MAP-330s are recognized by the Colubris Controller.

- Place a call between two Avaya Wireless IP Telephones and verify good voice quality in both directions.

8. Support

Technical support for the Colubris can be obtained through the following:

- **Phone:** Phone: 1-866-241-8324
- **Email:** support@colubris.com
- **Web:** http://www.colubris.com/

9. Conclusion

These Application Notes illustrate the procedures necessary for configuring Colubris Intelligent Mobility Solution to support the Avaya 3616 IP Wireless Telephone, Avaya 3641 IP Wireless Telephone, Avaya 3645 IP Wireless Telephone and Avaya IP Office. The Colubris 5000 Series MultiService Controller, as well as the Colubris 300 Series MultiService Access Points were successfully compliance-tested in a converged voice and data network configuration. The Colubris 5000 Series MultiService Controller, as well as the Colubris 300 Series MultiService Access Points were able to support 802.11 b/g/a radio, Layer2 and Layer3, roaming, VLAN Tagging, QoS, and 802.1x authentication with digital CA certificates as well as WPA2 AES and TKIP 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, Issue 3, February 2007
[3] *Administration for Network Connectivity for Avaya Communication Manager,* Doc # 555-233-504, Issue 12, February 2007
[4] *Avaya IP Telephony Implementation Guide*, May 1, 2006
[5] *Avaya 3616 Wireless Telephone and Desktop Charger User Guide* (555-301-709)
[6] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide*
[7] *Avaya 3641/3645 Wireless Telephone and Accessories User Guide,* August 2007

The following Colubris Networks product documentation is provided by Colubris Networks. For additional product and company information, visit http://www.Colubris.com. (access to Colubris Networks documentation may require a support account).

[8] *Documentation CD: Command Reference Release*, *Document Number: 39-01-0016-02*