Application Notes for Colubris Intelligent Mobility Solution with Avaya Communication Manager 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, consisting of the Colubris MultiService Controller 5000 Series managing multiple Colubris MultiService Access Points 300 Series (MAPs). Avaya 3600 Series Wireless IP Telephones gained network access through the Colubris MAPs and registered with Avaya Communication Manager. 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.

1. Introduction

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

1.1. Avaya 3631 Wireless IP Telephone

The Avaya 3631 Wireless IP Telephone is a low-cost, 802.11b/g wireless telephone that works with industry-standard, enterprise-grade wireless LANs. It has a color display and an advanced, context-sensitive Avaya one-X mobile user interface

1.2. Avaya 3641 Wireless IP Telephone

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

1.3. Avaya 3645 Wireless IP Telephone

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

1.4. Colubris MultiService Controller 5000 Series

Colubris MultiService Controllers centrally manage the configuration and operation of a network of MultiService Access Points, 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 MSC pushes QoS and security policies to MultiService Access Points at the network edge, where traffic is forwarded directly from source to destination. This highly efficient architecture reduces the amount of wireless traffic on the LAN backbone, when compared with other wireless LAN solutions, and enables cost-effective scalability and migration to high-capacity 802.11n networks.

1.5. Colubris MultiService Access Points 300 Series

Colubris MultiService Access Points (MAPs) bring intelligence to the network edge, providing scalable, seamless wireless access anywhere, anytime. Colubris' enterprise-grade feature set is abundantly rich, dispensing multiple network services, enforcing security and delivering high performance client access, unlike “thin” or “lite” access points. An integral component of the Colubris Intelligent Mobility Solution, MAPs support a plug-and-play automatic configuration and ongoing central control by Colubris MSCs to simplify WLAN deployment and minimize network operating costs.

1.6. Network Diagram

The network diagram shown in **Figure 1** illustrates the environment used for compliance testing. The network consists of an Avaya Communication Manager running on an Avaya S8300 Server with an Avaya G700 Media Gateway, two Avaya 3631 Wireless IP Telephones, two Avaya 3645 Wireless IP Telephones, one Avaya 3641 Wireless IP Telephone, 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 Voice Priority Processor, one Colubris Networks MSC-5100 controller and three Colubris MAP-330 access points. One computer is present in the network providing network services such as DHCP, TFTP, HTTP and RADIUS.

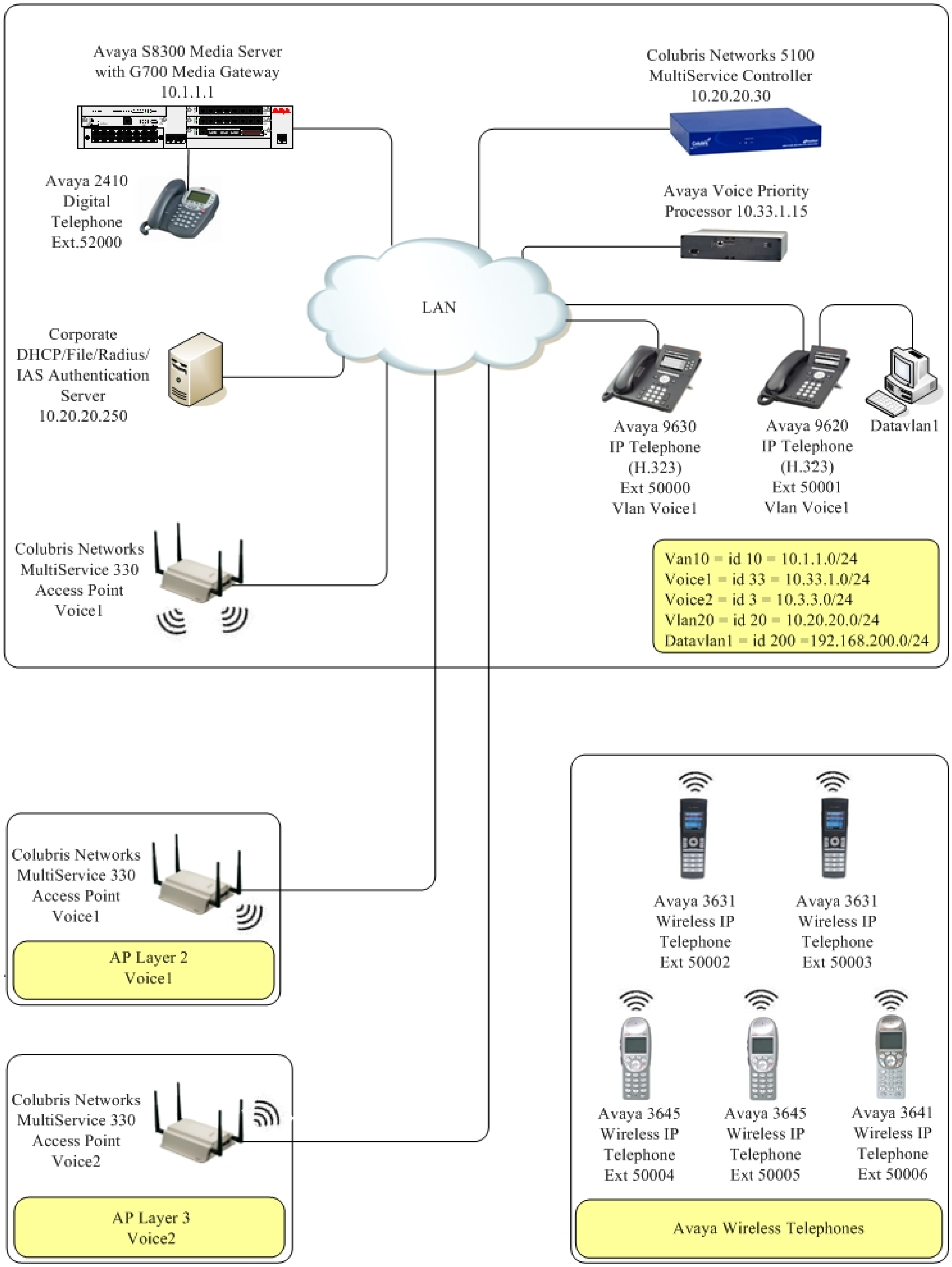


Figure 1: Avaya and Colubris Networks Wireless LAN Configuration

2. Equipment and Software Validated

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

Hardware Component	Software/Firmware
Avaya S8300 Server	Avaya Communication Manager 4.0 (R14x.00.1.731.2)
Avaya G700 Media Gateway MGP MM712 DCP Media Module	 26.31.0 FW 008
Avaya 3631 Wireless Telephone	1.3.0
Avaya 3645 Wireless Telephone	117.016
Avaya 3641 Wireless Telephone	117.016
Avaya Voice Priority Processor	17x.028
Avaya 9620 IP Telephone	Avaya one-X Deskphone Edition 1.5 (H.323)
Avaya 9630 IP Telephone	Avaya one-X Deskphone Edition 1.5 (H.323)
Avaya 2410 Digital Telephone	NA
Colubris Networks MSC-5100	5.2.1
Colubris Networks MAP-330	5.2.1
Microsoft Windows 2003 Server	Internet Authentication Service (IAS)/Radius/File/DHCP

3. Configure Avaya Communication Manager

This section shows the necessary steps in configuring Avaya Communication Manager. Start a SAT terminal session to Avaya Communication Manager and access the system using valid login credentials. These Application Notes assume the proper licensing and customer options for Avaya Communication Manager have been installed. For detailed information on the installation, maintenance, and configuration of Avaya Communication Manager, please refer to **Section 13 [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 Wireless IP Telephones should use **Type 4620** as their station **Type** as in the example below. For complete references on how to administer these types of stations please refer to **Section 13 [1]** and **[2].**

```
change station 40002                                            Page   1 of   5
                                     STATION

Extension: 40002                         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: 40002
            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

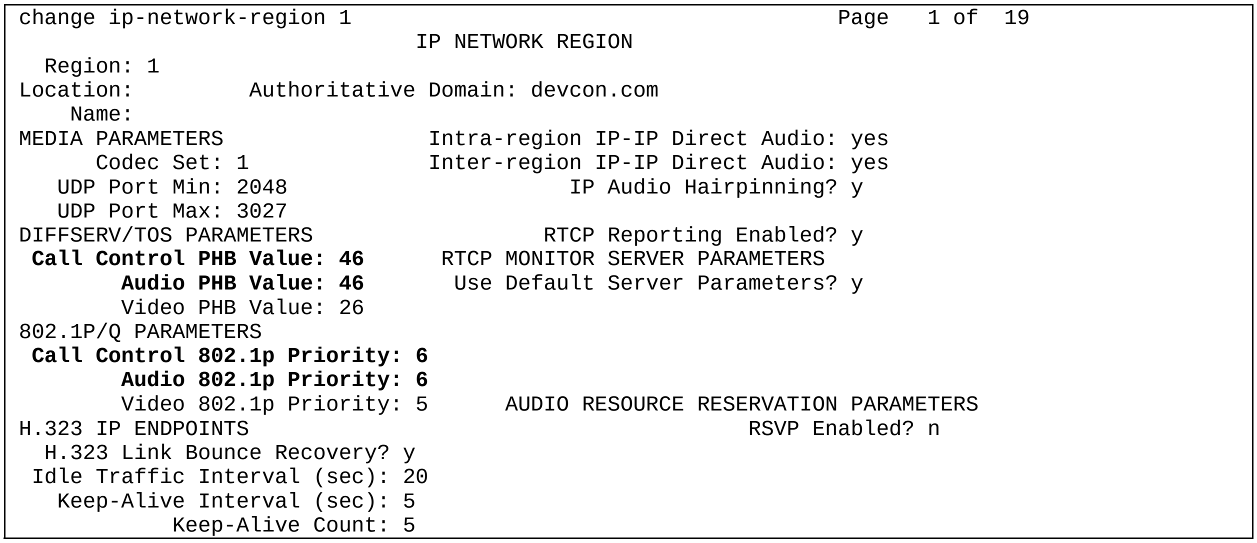
IP networks were originally designed to carry data on a best-effort delivery basis, which meant that all traffic had equal priority and an equal chance of being delivered in a timely manner. As a result, all traffic had an equal chance of being dropped when congestion occurred. To carry voice, Quality of Service (QoS) has to be implemented throughout the entire 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 2 802.1.p/Q priority and Layer 3 Differentiated Services (DiffServ). The Colubris MAPs can be configured to prioritize VoIP traffic based on these values.

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.

For this example configuration, the DIFFSERV/TOS PARAMETERS and 802.1P/Q PARAMETERS were set to 46 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 **46**
- **Audio PHB Value** set to **46**
- **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: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       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 Avaya Voice Priority Processor

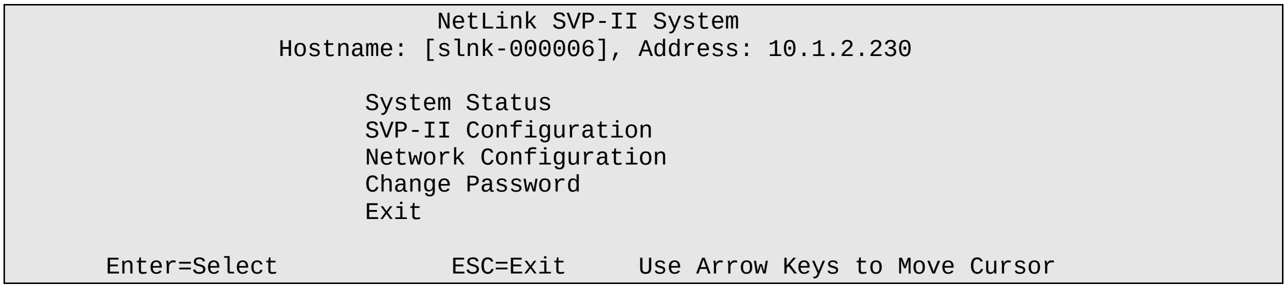
The Avaya Voice Priority Processor (AVPP) utilizes SpectraLink Voice Priority (SVP) as the Quality of Service (QoS) mechanism supported by the Avaya 3641/3645 Wireless IP Telephones and the Colubris MAPs to reduce jitter and delay for voice traffic over the wireless network.

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 MAPs 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.



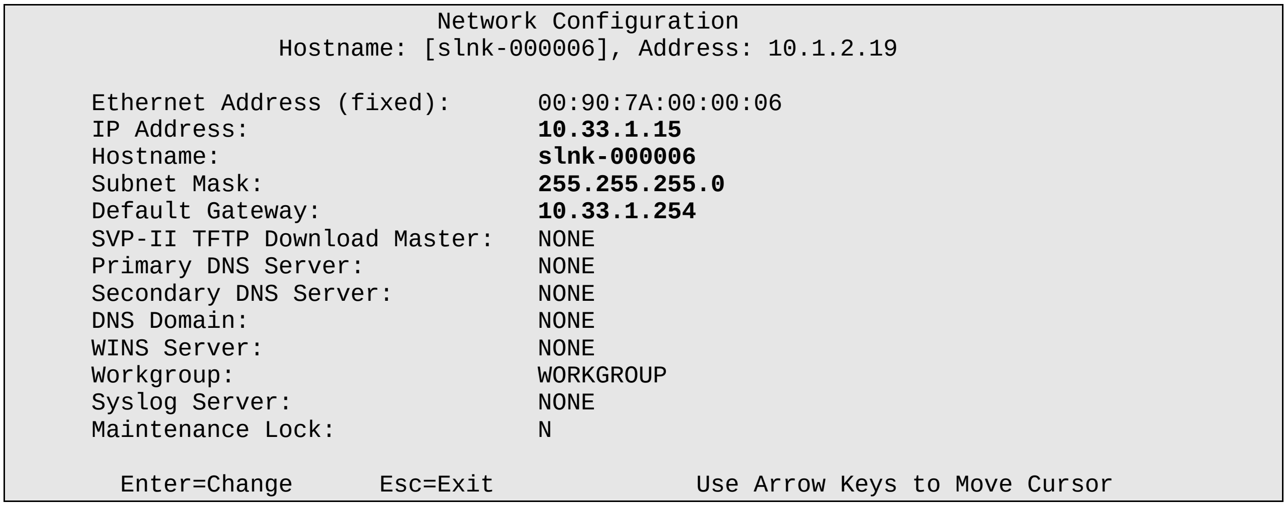
```
                              NetLink SVP-II System
                   Hostname: [slnk-000006], Address: 10.1.2.230

                         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.



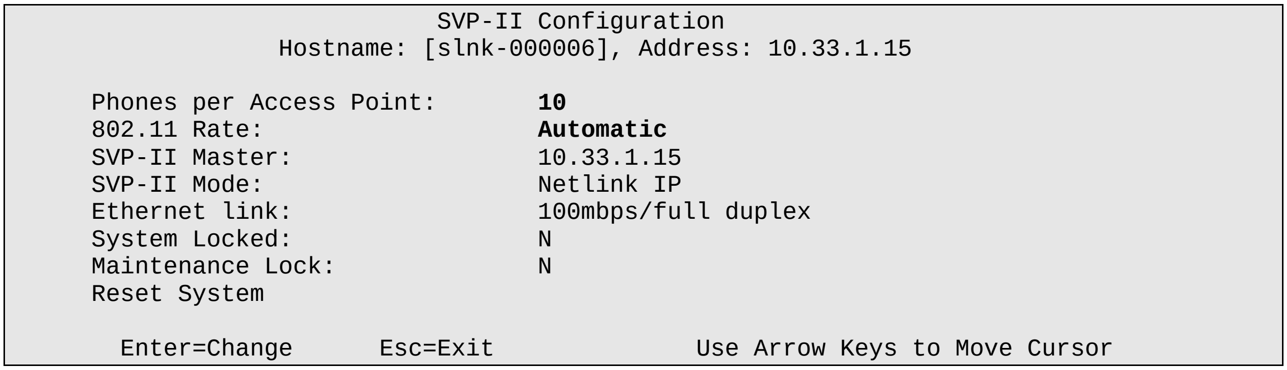
```
                              Network Configuration
                   Hostname: [slnk-000006], Address: 10.1.2.19

      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 **SVPP-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 its 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 MAPs

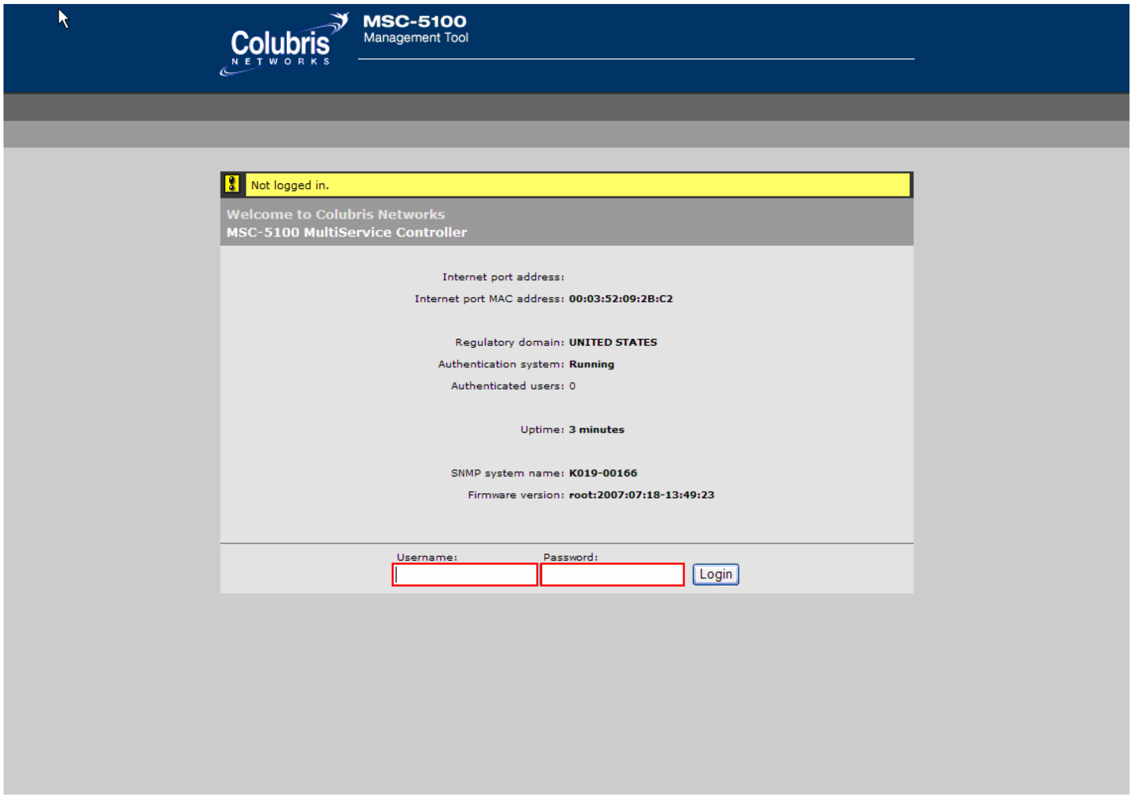
The following steps detail the initial configuration for the Colubris Intelligent Mobility Solution used for the compliance testing. The configuration on the Colubris Networks MSC-5100 was administered via the Web configuration tool. Except where stated the parameters in all steps are the default settings and are supplied for reference. Refer to “MSC-5000 Series Administrator’s Guide” for additional information regarding the configuration displayed in this section.

5.1. Configure Colubris Networks MSC-5100 Controller

<table>
<tr><th>Step</th><th><b>Description:</b> Configure Colubris Networks Controller in the WLAN as depicted in <b>Figure 1</b>.</th></tr>
<tr><td>1.</td><td>

Configure the MSC using the built-in web-based **Management Tool.** Access this tool by establishing a web browser connection to the MSC. 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 MSC.
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.** Press Enter.
4. Log in to the Colubris Networks MSC-5100 controller using default credentials which can be obtained from the Colubris Networks MSC-5100 controller documentation.



Not logged in.

Welcome to Colubris Networks
MSC-5100 MultiService Controller

Internet port address:
Internet port MAC address: 00:03:52:09:2B:C2

Regulatory domain: UNITED STATES
Authentication system: Running
Authenticated users: 0

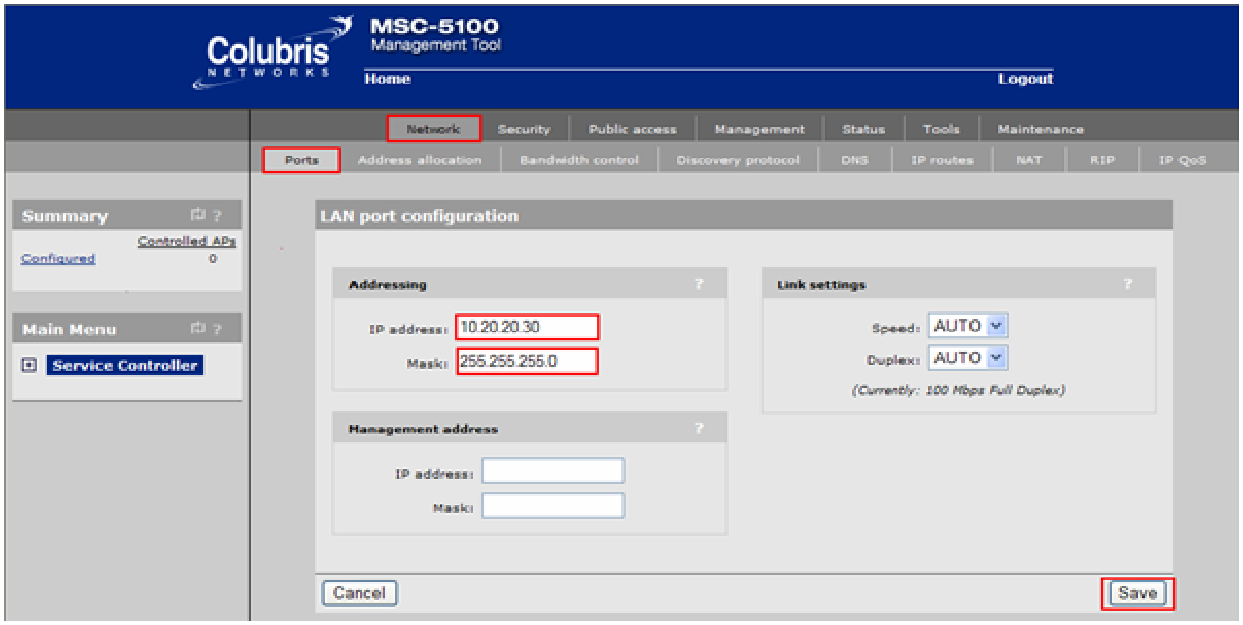
Uptime: 3 minutes

SNMP system name: K019-00166
Firmware version: root:2007:07:18-13:49:23

Username: Password:

</td></tr>
</table>

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



Summary: Controlled APs — Configured 0

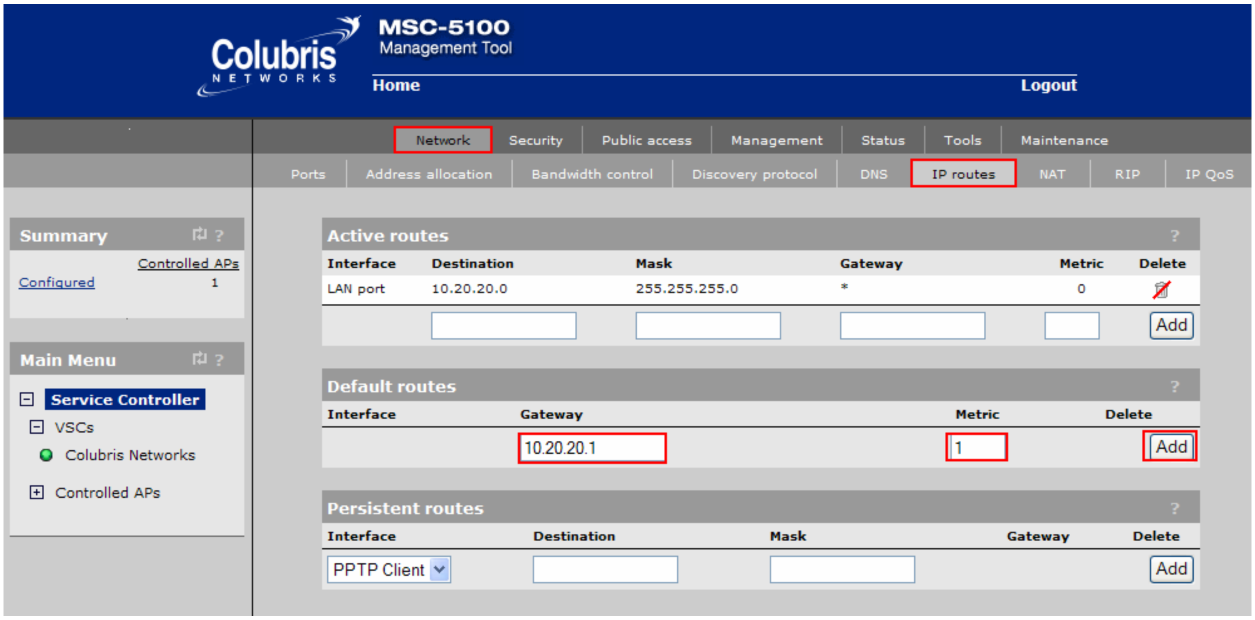
LAN port configuration

Addressing
IP address: 10.20.20.30
Mask: 255.255.255.0

Link settings
Speed: AUTO
Duplex: AUTO
(Currently: 100 Mbps Full Duplex)

Management address
IP address:
Mask:

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



Summary: Controlled APs — Configured 1

Active routes

Interface	Destination	Mask	Gateway	Metric	Delete
LAN port	10.20.20.0	255.255.255.0	*	0	

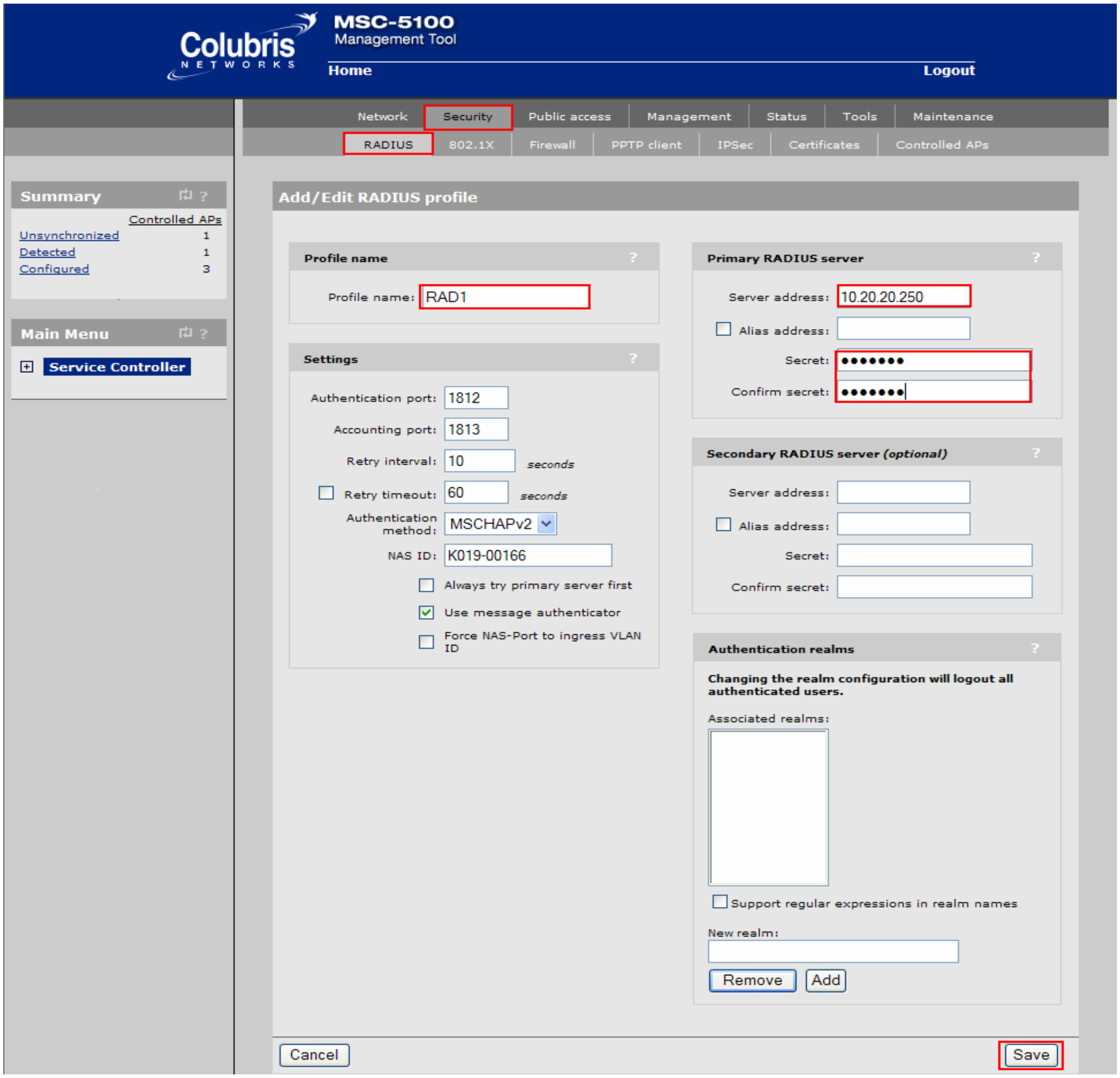
Default routes

Interface	Gateway	Metric	Delete
	10.20.20.1	1	Add

Persistent routes

Interface	Destination	Mask	Gateway	Delete
PPTP Client				Add

5.2. Configure Radius Server

Step	**Description:** Configure Radius Server Profile
1.	Select **Security → RADIUS → Add New Profile**. Set the **Profile name**: to **RAD1, Server address** to **10.20.20.250** and set the **Secret/Confirm secret** to what is set on the RADIUS server. Contact the administrator of the Radius server to obtain the secret password. Press **Save** to continue. 

Summary

	Controlled APs
Unsynchronized	1
Detected	1
Configured	3

Add/Edit RADIUS profile

Profile name

Profile name: RAD1

Settings

Authentication port: 1812

Accounting port: 1813

Retry interval: 10 seconds

□ Retry timeout: 60 seconds

Authentication method: MSCHAPv2

NAS ID: K019-00166

□ Always try primary server first

☑ Use message authenticator

□ Force NAS-Port to ingress VLAN ID

Primary RADIUS server

Server address: 10.20.20.250

□ Alias address:

Secret: •••••••

Confirm secret: •••••••

Secondary RADIUS server *(optional)*

Server address:

□ Alias address:

Secret:

Confirm secret:

Authentication realms

Changing the realm configuration will logout all authenticated users.

Associated realms:

□ Support regular expressions in realm names

New realm:

5.3. Configure Colubris Networks MAP-330 Access Points

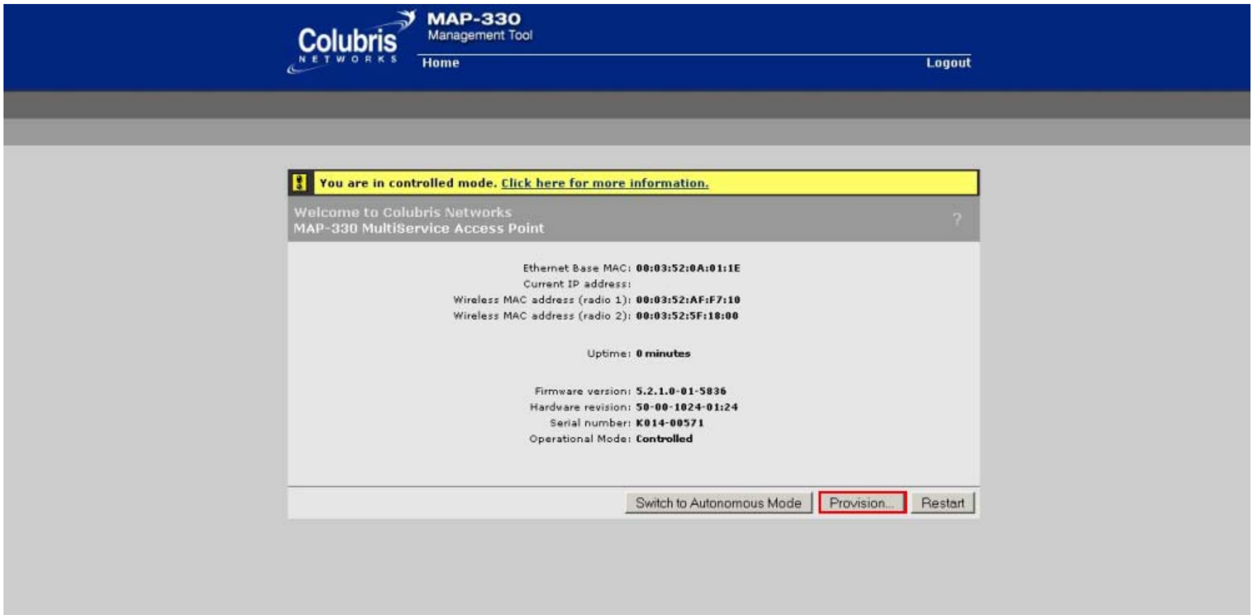
MAPs 1 and 2 are located on the same layer 2 subnet as the MSC and will discover the MSC using Colubris' automated discovery mechanism. MAPs can be manually configured to connect to the MSC. For compliance testing MAP 3 was placed on VLAN20 for Layer 3 roaming and was manually configured.

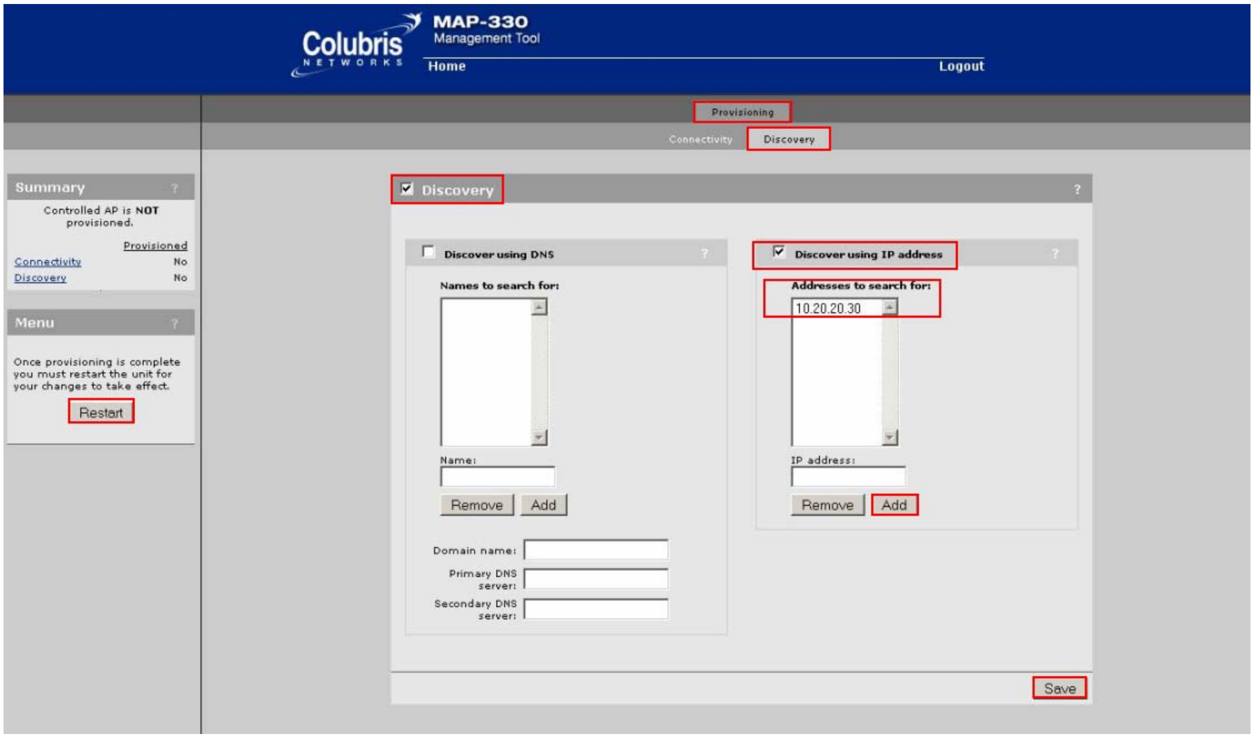
One of the three methods can be used to enable the MAP to discover and connect to the MSC:

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" provided with the equipment.

Local provisioning is done directly on the MAP specifying either the IP address(es) of the MSCs or the DNS name of the MSCs as defined on the corporate DNS servers. A local IP address can also be configured on the MAP if no DHCP server is available, however in this example, the MAP will receive an IP address from the DHCP server on its local network. Obtain the IP address given to the MAP from the DHCP server, perform the following steps:

Step	**Description**: Login into AP-3
1.	Connect to the web interface of the MAP and log in using a user/password of admin/admin and click the '**Provision**' button  Colubris NETWORKS MAP-330 Management Tool Home Logout ? Switch to Autonomous Mode Provision... Restart You are in controlled mode. Click here for more information. Welcome to Colubris Networks MAP-330 MultiService Access Point Ethernet Base MAC: 00:03:52:0A:01:1E Current IP address: Wireless MAC address (radio 1): 00:03:52:AF:F7:10 Wireless MAC address (radio 2): 00:03:52:5F:18:00 Uptime: 0 minutes Firmware version: 5.2.1.0-01-5836 Hardware revision: 50-00-1024-01:24 Serial number: K014-00571 Operational Mode: Controlled

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

☑ Discovery

☐ Discover using DNS

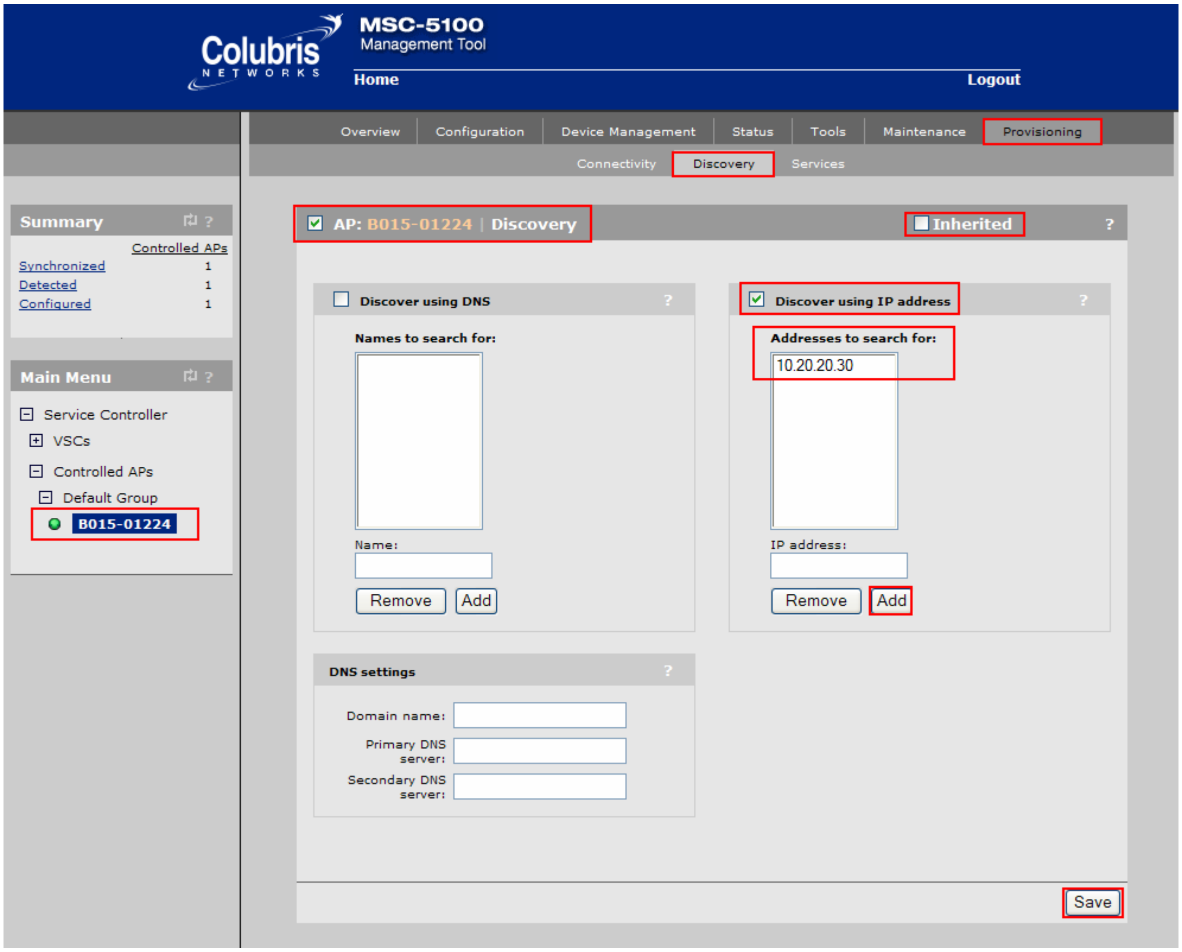
☑ Discover using IP address

Addresses to search for: 10.20.20.30

Controlled AP is **NOT** provisioned.

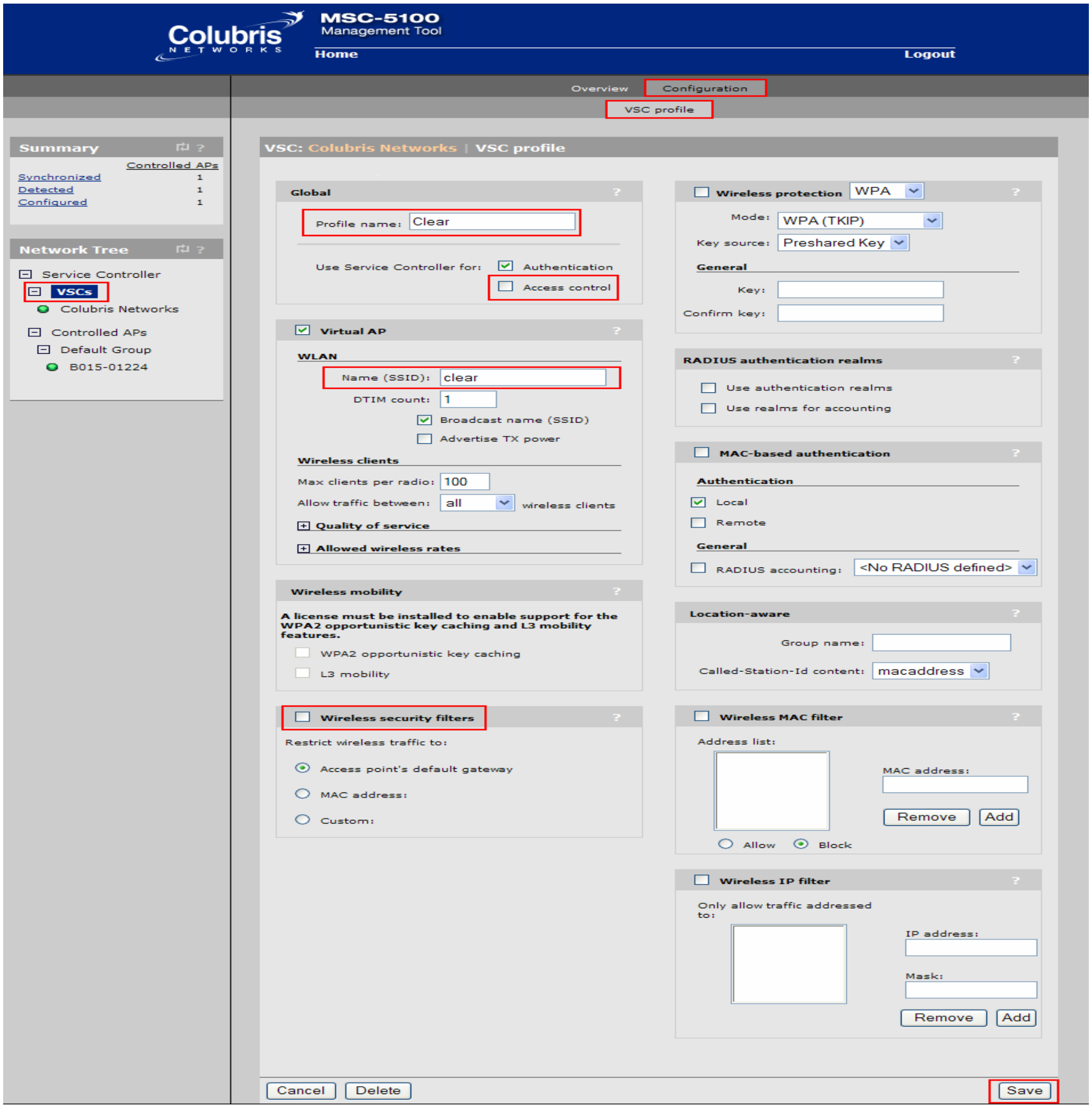
	Provisioned
Connectivity	No
Discovery	No

Once provisioning is complete you must restart the unit for your changes to take effect.

Step	**Description:** Enter the provisioning information on the MSC
3.	Enter the provisioning information on the MSC. a) Click the name of the newly connected MAP in the left pane. b) Click on the **Provisioning** tab in the upper window c) Click on the **Discovery** tab d) Uncheck the **Inherited** box e) Check the box in the upper-left corner for MAP **AP:B015-01224 | Discovery,** each MAP will have a unique number. f) Check the '**Discover using IP address'** and reenter the IP address of the MSC  ☑ AP: B015-01224 | Discovery □ Inherited □ Discover using DNS ☑ Discover using IP address Addresses to search for: 10.20.20.30 Colubris NETWORKS MSC-5100 Management Tool Home Logout Overview Configuration Device Management Status Tools Maintenance Provisioning Connectivity Discovery Services Summary Controlled APs Synchronized 1 Detected 1 Configured 1 Main Menu Service Controller VSCs Controlled APs Default Group B015-01224 Names to search for: Name: Remove Add IP address: Remove Add DNS settings Domain name: Primary DNS server: Secondary DNS server: Save

5.4. Create and Configure Extended Service Set IDs (ESSID)

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

Step	**Description:** Create Clear ESSID and assign security profile
1.	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** box, change the **SSID** to **Clear**, uncheck the **Wireless security filters** box. Press the **Save** button to continue. 

Colubris NETWORKS MSC-5100 Management Tool

Home Logout

Overview Configuration

VSC profile

Summary

	Controlled APs
Synchronized	1
Detected	1
Configured	1

Network Tree

⊟ Service Controller
⊟ VSCs
● Colubris Networks
⊟ Controlled APs
⊟ Default Group
● B015-01224

VSC: Colubris Networks | VSC profile

Global

Profile name: Clear

Use Service Controller for: ☑ Authentication
☐ Access control

☑ Virtual AP

WLAN

Name (SSID): clear

DTIM count: 1

☑ Broadcast name (SSID)

☐ Advertise TX power

Wireless clients

Max clients per radio: 100

Allow traffic between: all wireless clients

⊞ Quality of service

⊞ Allowed wireless rates

Wireless mobility

A license must be installed to enable support for the WPA2 opportunistic key caching and L3 mobility features.

☐ WPA2 opportunistic key caching

☐ L3 mobility

☐ Wireless security filters

Restrict wireless traffic to:

● Access point's default gateway

○ MAC address:

○ Custom:

☐ Wireless protection WPA

Mode: WPA (TKIP)

Key source: Preshared Key

General

Key:

Confirm key:

RADIUS authentication realms

☐ Use authentication realms

☐ Use realms for accounting

☐ MAC-based authentication

Authentication

☑ Local

☐ Remote

General

☐ RADIUS accounting: <No RADIUS defined>

Location-aware

Group name:

Called-Station-Id content: macaddress

☐ Wireless MAC filter

Address list:

MAC address:

Remove Add

○ Allow ● Block

☐ Wireless IP filter

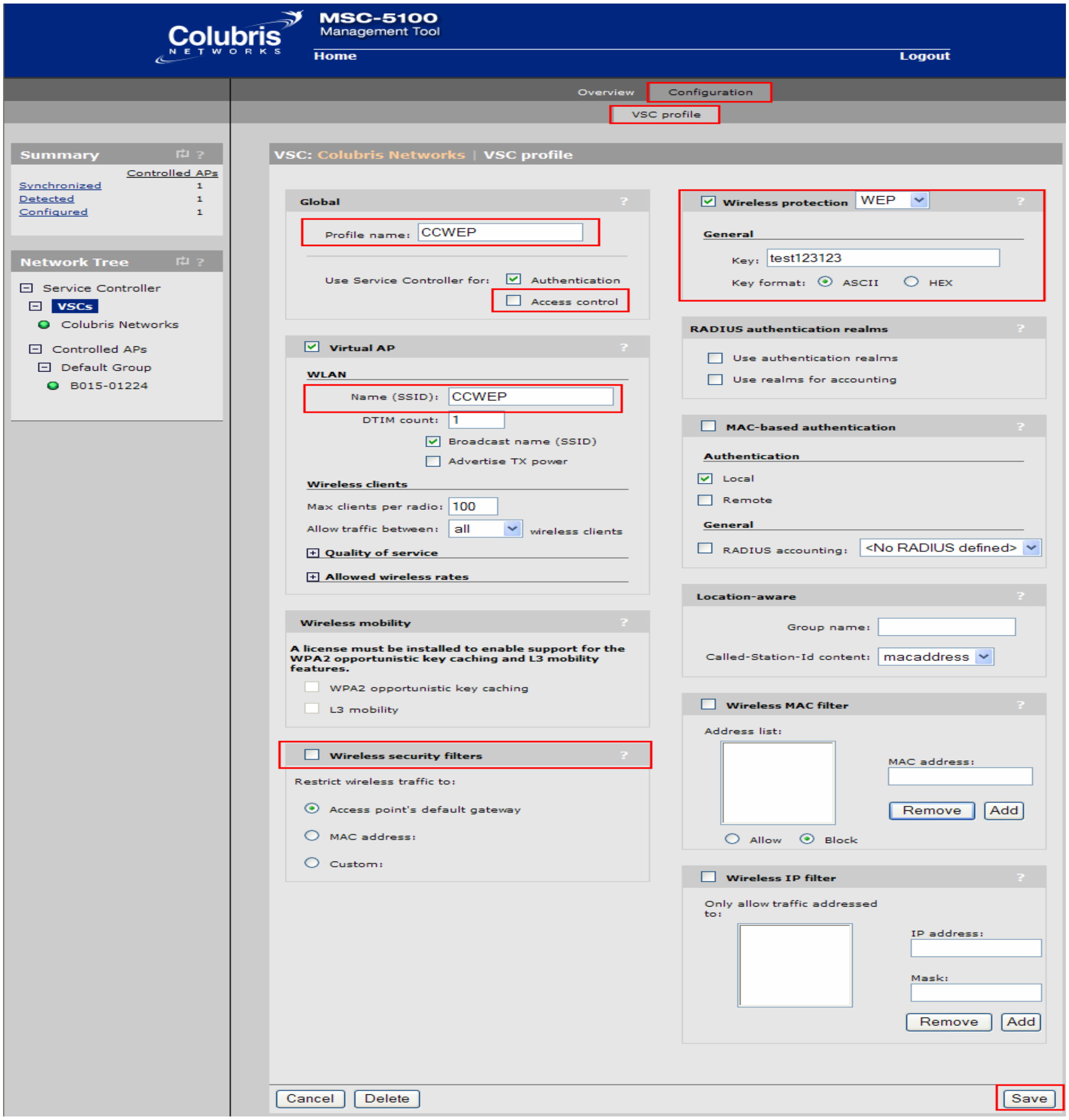
Only allow traffic addressed to:

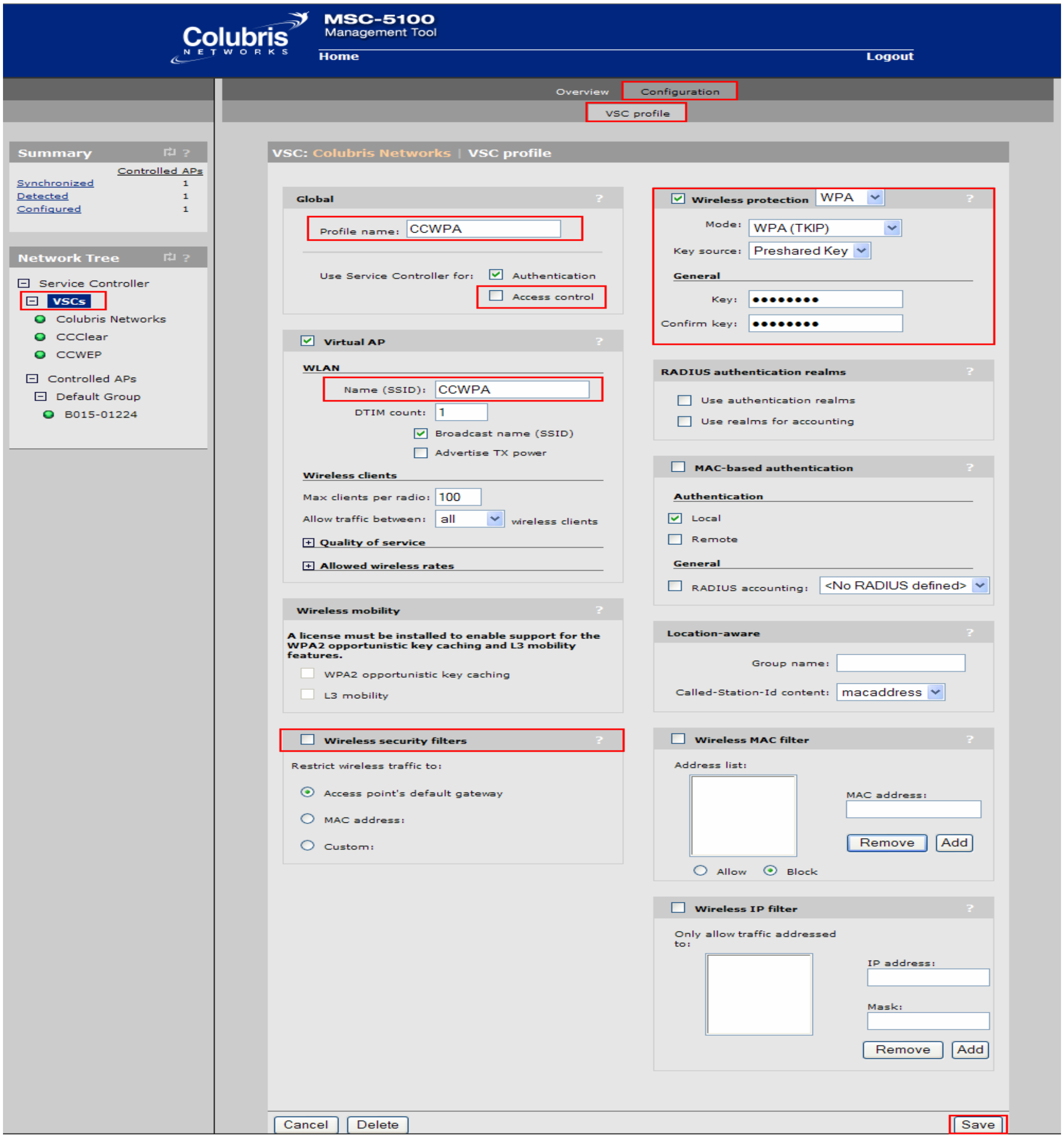
IP address:

Mask:

Remove Add

Cancel Delete Save

Step	**Description:** Configure ESSID WEP
2.	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 **SSID** to **CCWEP**, and uncheck the **Wireless security filters** box. Check **Wireless protection** and select **WEP from the** pull-down list, enter “test123123” in the Key field. Press the **Save** button to continue.  Colubris NETWORKS MSC-5100 Management Tool Home Logout Overview Configuration VSC profile Summary: Controlled APs — Synchronized 1, Detected 1, Configured 1 Network Tree: ⊟ Service Controller, ⊟ VSCs, Colubris Networks, ⊟ Controlled APs, ⊟ Default Group, B015-01224 VSC: Colubris Networks | VSC profile Global Profile name: CCWEP Use Service Controller for: ☑ Authentication ☐ Access control ☑ Virtual AP WLAN Name (SSID): CCWEP DTIM count: 1 ☑ Broadcast name (SSID) ☐ Advertise TX power Wireless clients Max clients per radio: 100 Allow traffic between: all wireless clients ⊞ Quality of service ⊞ Allowed wireless rates Wireless mobility A license must be installed to enable support for the WPA2 opportunistic key caching and L3 mobility features. ☐ WPA2 opportunistic key caching ☐ L3 mobility ☐ Wireless security filters Restrict wireless traffic to: ● Access point's default gateway ○ MAC address: ○ Custom: ☑ Wireless protection WEP General Key: test123123 Key format: ● ASCII ○ HEX RADIUS authentication realms ☐ Use authentication realms ☐ Use realms for accounting ☐ MAC-based authentication Authentication ☑ Local ☐ Remote General ☐ RADIUS accounting: <No RADIUS defined> Location-aware Group name: Called-Station-Id content: macaddress ☐ Wireless MAC filter Address list: MAC address: Remove Add ○ Allow ● Block ☐ Wireless IP filter Only allow traffic addressed to: IP address: Mask: Remove Add Cancel Delete Save

Step	**Description:** Configure ESSID WPA-PSK
3.	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** box, change the **SSID** to **CCWPA**, uncheck the '**Wireless security filters**', select **WPA** from the **Wireless protection drop-down** list, and select **WPA (TKIP)** from the **Mode** drop-down list. Under **General,** enter the **Key** information. Press the **Save** button to continue. 

Summary

	Controlled APs
Synchronized	1
Detected	1
Configured	1

Network Tree
- Service Controller
  - VSCs
    - Colubris Networks
    - CCClear
    - CCWEP
  - Controlled APs
    - Default Group
      - B015-01224

VSC: Colubris Networks | VSC profile

Global
- Profile name: CCWPA
- Use Service Controller for: ☑ Authentication
- □ Access control

☑ Virtual AP
- WLAN
- Name (SSID): CCWPA
- DTIM count: 1
- ☑ Broadcast name (SSID)
- □ Advertise TX power
- Wireless clients
- Max clients per radio: 100
- Allow traffic between: all wireless clients
- ⊞ Quality of service
- ⊞ Allowed wireless rates

Wireless mobility
- A license must be installed to enable support for the WPA2 opportunistic key caching and L3 mobility features.
- □ WPA2 opportunistic key caching
- □ L3 mobility

□ Wireless security filters
- Restrict wireless traffic to:
- ● Access point's default gateway
- ○ MAC address:
- ○ Custom:

☑ Wireless protection WPA
- Mode: WPA (TKIP)
- Key source: Preshared Key
- General
- Key: ••••••••
- Confirm key: ••••••••

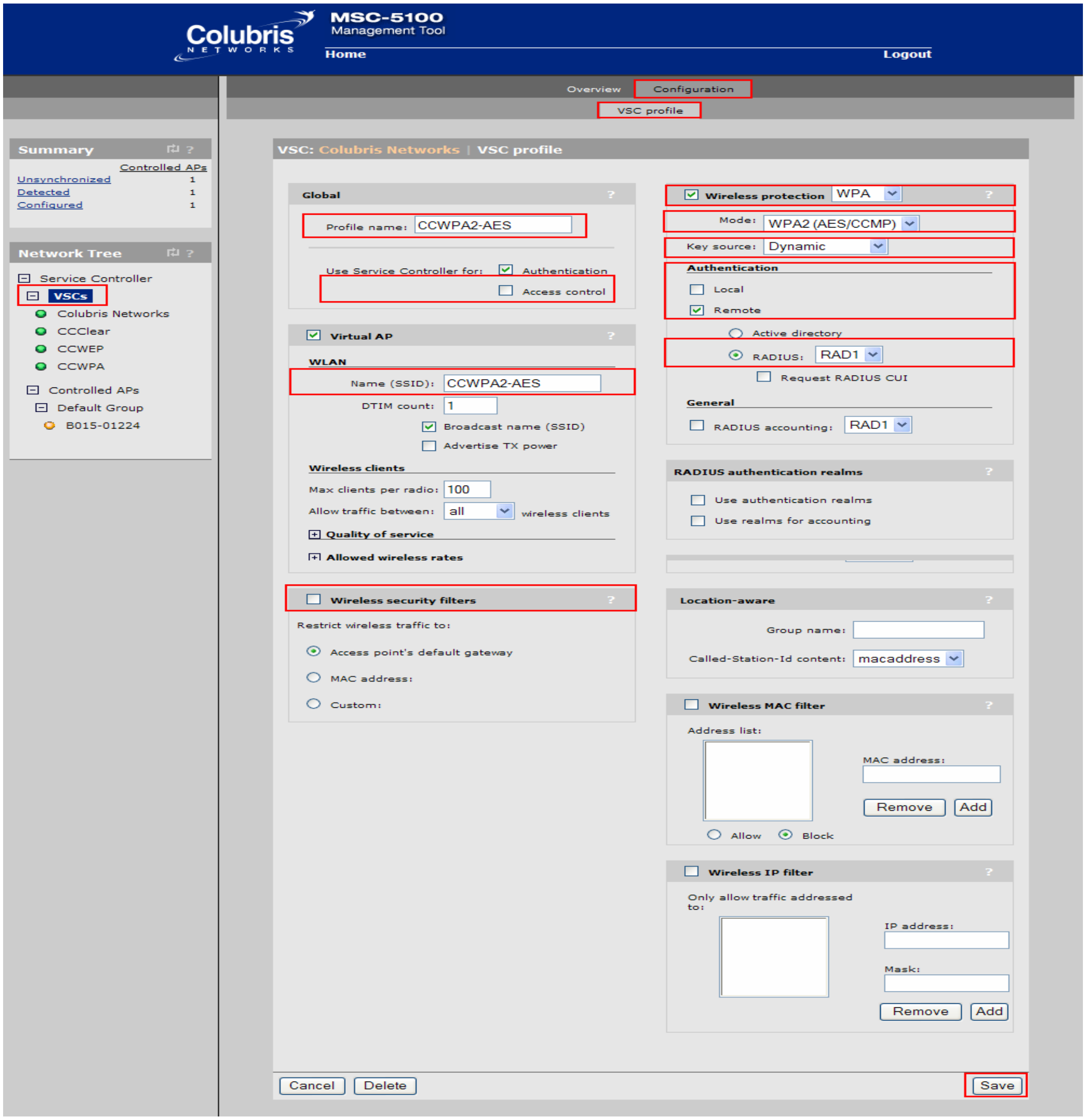
RADIUS authentication realms
- □ Use authentication realms
- □ Use realms for accounting

□ MAC-based authentication
- Authentication
- ☑ Local
- □ Remote
- General
- □ RADIUS accounting: <No RADIUS defined>

Location-aware
- Group name:
- Called-Station-Id content: macaddress

□ Wireless MAC filter
- Address list:
- MAC address:
- ○ Allow ● Block

□ Wireless IP filter
- Only allow traffic addressed to:
- IP address:
- Mask:

Step	**Description:** Configure ESSID WPA2-AES
4.	Click on **VSCs** in the left window. Click '**Add new VSC profile.** In the VSC window, change the Profile name to **CCWPA2-AES**, uncheck the '**Access control'** box, change the **SSID** to **CCWPA2-AES**, uncheck the **Wireless security filters**, select **WPA** from the **Wireless protection** list, select **WPA2 (AES/CCMP)** from the **Mode** drop-down list, select **Dynamic** from the **Key source** drop-down list, uncheck **Local** and check **Remote** from the **Authentication** box, select **RADIUS** and choose the **RAD1** server that was previously defined in **Step 5.2**. Press the **Save** button to continue. 

MSC-5100 Management Tool

Summary: Controlled APs — Unsynchronized 1, Detected 1, Configured 1

Network Tree: Service Controller — VSCs: Colubris Networks, CCClear, CCWEP, CCWPA; Controlled APs — Default Group: B015-01224

VSC: Colubris Networks | VSC profile

Global
- Profile name: CCWPA2-AES
- Use Service Controller for: ☑ Authentication
- ☐ Access control

☑ Virtual AP

WLAN
- Name (SSID): CCWPA2-AES
- DTIM count: 1
- ☑ Broadcast name (SSID)
- ☐ Advertise TX power

Wireless clients
- Max clients per radio: 100
- Allow traffic between: all wireless clients
- ⊞ Quality of service
- ⊞ Allowed wireless rates

☐ Wireless security filters
- Restrict wireless traffic to:
- ● Access point's default gateway
- ○ MAC address:
- ○ Custom:

☑ Wireless protection: WPA
- Mode: WPA2 (AES/CCMP)
- Key source: Dynamic

Authentication
- ☐ Local
- ☑ Remote
- ○ Active directory
- ● RADIUS: RAD1
- ☐ Request RADIUS CUI

General
- ☐ RADIUS accounting: RAD1

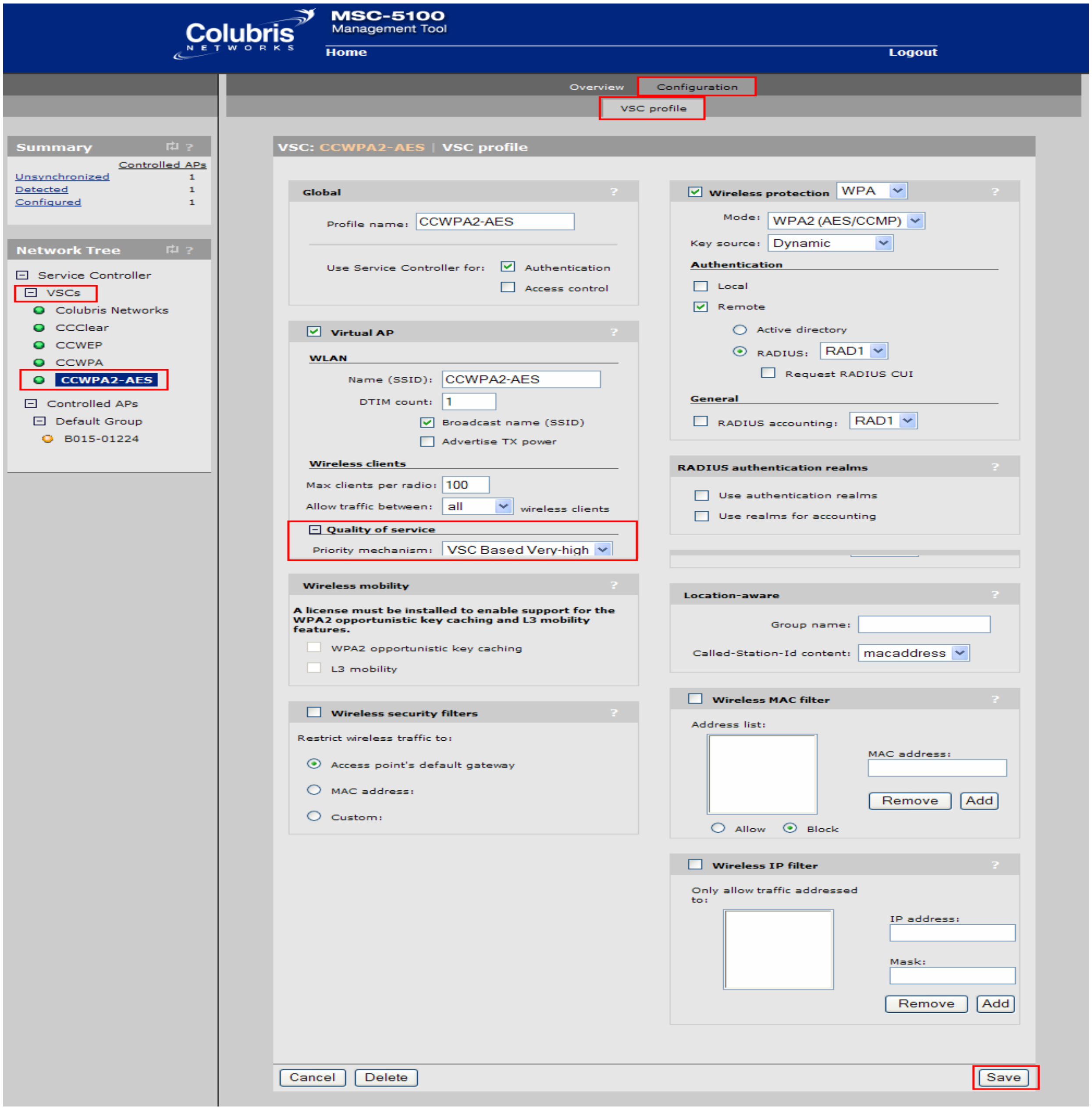
RADIUS authentication realms
- ☐ Use authentication realms
- ☐ Use realms for accounting

Location-aware
- Group name:
- Called-Station-Id content: macaddress

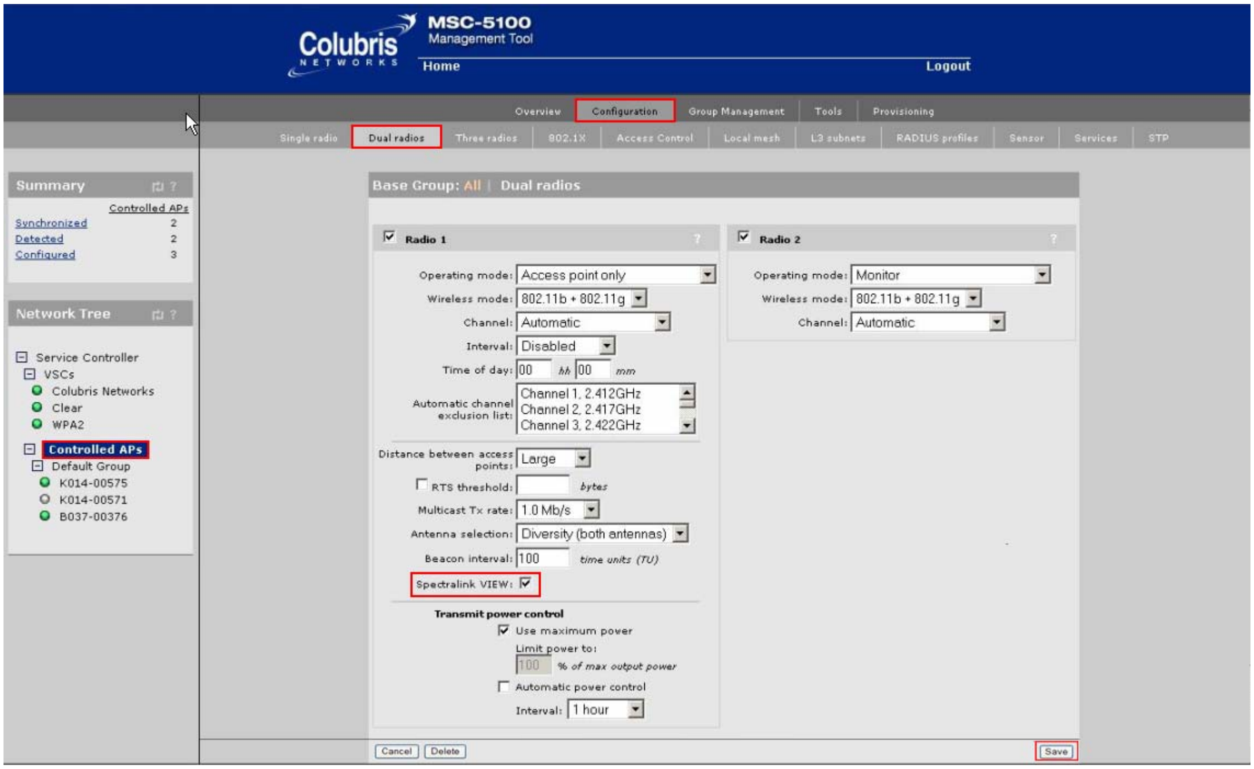
☐ Wireless MAC filter
- Address list:
- MAC address:
- ○ Allow ● Block

☐ Wireless IP filter
- Only allow traffic addressed to:
- IP address:
- Mask:

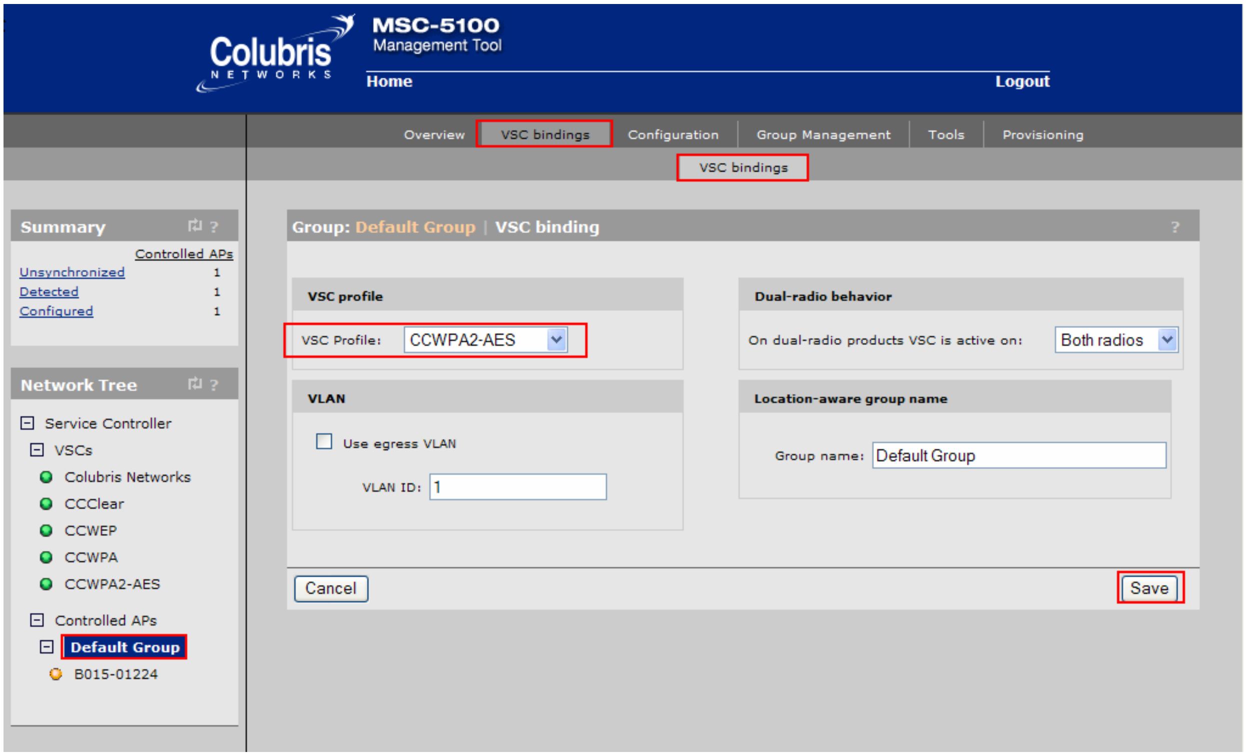
5.5. Configure QoS Polices For Avaya 3631 IP Telephones

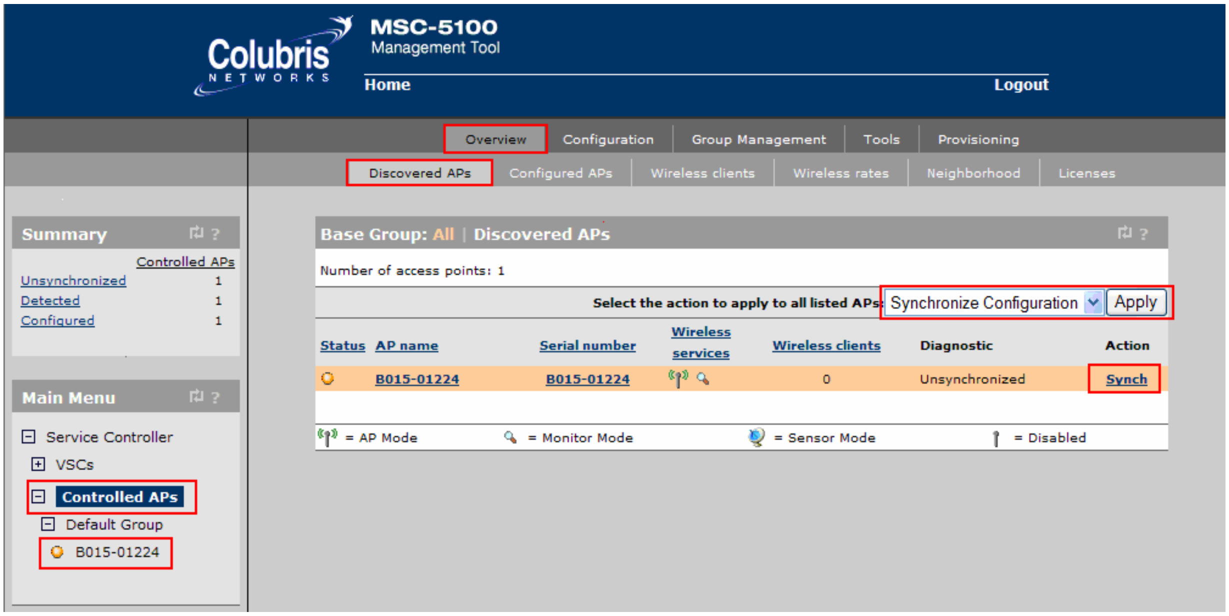
Step	**Description:** Add QoS Rule for Voice ESSID
1.	For this example, ESSID CCWPA2-AES is used to show how to configure QoS for the Avaya 3631 wireless IP Telephones. The same setting can be used with ESSID's Clear, CCWEP and CCWPA. Click on **VSCs** in the left window. select **CCWPA2-AES**, Under the **Quality of service** section, select **VSC Based Very-high** as the **Priority mechanism**. Press the **Save** button to continue.  MSC-5100 Management Tool Home Logout Overview Configuration VSC profile Summary Controlled APs Unsynchronized 1 Detected 1 Configured 1 Network Tree Service Controller VSCs Colubris Networks CCClear CCWEP CCWPA CCWPA2-AES Controlled APs Default Group B015-01224 VSC: CCWPA2-AES | VSC profile Global Profile name: CCWPA2-AES Use Service Controller for: ☑ Authentication ☐ Access control ☑ Virtual AP WLAN Name (SSID): CCWPA2-AES DTIM count: 1 ☑ Broadcast name (SSID) ☐ Advertise TX power Wireless clients Max clients per radio: 100 Allow traffic between: all wireless clients Quality of service Priority mechanism: VSC Based Very-high Wireless mobility A license must be installed to enable support for the WPA2 opportunistic key caching and L3 mobility features. ☐ WPA2 opportunistic key caching ☐ L3 mobility ☐ Wireless security filters Restrict wireless traffic to: ● Access point's default gateway ○ MAC address: ○ Custom: ☑ Wireless protection WPA Mode: WPA2 (AES/CCMP) Key source: Dynamic Authentication ☐ Local ☑ Remote ○ Active directory ● RADIUS: RAD1 ☐ Request RADIUS CUI General ☐ RADIUS accounting: RAD1 RADIUS authentication realms ☐ Use authentication realms ☐ Use realms for accounting Location-aware Group name: Called-Station-Id content: macaddress ☐ Wireless MAC filter Address list: MAC address: Remove Add ○ Allow ● Block ☐ Wireless IP filter Only allow traffic addressed to: IP address: Mask: Remove Add Cancel Delete Save

5.6. Configure QoS Polices for Avaya 3641/3645 IP Telephones

Step	**Description:** Add QoS Rule for Voice ESSID
1.	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, CCWEP and CCWPA. Click on **Controlled APs** in the left window. Check the **Spectralink** VIEW box. Press the **Save** button to continue.  Colubris NETWORKS MSC-5100 Management Tool Home Logout Overview Configuration Group Management Tools Provisioning Single radio Dual radios Three radios 802.1X Access Control Local mesh L3 subnets RADIUS profiles Sensor Services STP Cancel Delete Save Summary Controlled APs Synchronized 2 Detected 2 Configured 3 Network Tree Service Controller VSCs Colubris Networks Clear WPA2 Controlled APs Default Group K014-00575 K014-00571 B037-00376 Base Group: All | Dual radios ☑ Radio 1 Operating mode: Access point only Wireless mode: 802.11b + 802.11g Channel: Automatic Interval: Disabled Time of day: 00 hh 00 mm Automatic channel exclusion list: Channel 1, 2.412GHz Channel 2, 2.417GHz Channel 3, 2.422GHz Distance between access points: Large □ RTS threshold: bytes Multicast Tx rate: 1.0 Mb/s Antenna selection: Diversity (both antennas) Beacon interval: 100 time units (TU) Spectralink VIEW: ☑ Transmit power control ☑ Use maximum power Limit power to: 100 % of max output power □ Automatic power control Interval: 1 hour ☑ Radio 2 Operating mode: Monitor Wireless mode: 802.11b + 802.11g Channel: Automatic

5.7. Bind the VSCs to the MAPs

Step	**Description:** Bind VSC's to MAPs
1	Before a VSC can be used, it must be bound to a group of MAPs Click on **Default Group→VSC bindings → Add New Binding**. Select the **VSC profile** to use. Press the **Save** button to continue. Repeat this process for all VSCs that will be used.  Colubris NETWORKS MSC-5100 Management Tool Home Logout Overview VSC bindings Configuration Group Management Tools Provisioning VSC bindings Summary Controlled APs Unsynchronized 1 Detected 1 Configured 1 Network Tree Service Controller VSCs Colubris Networks CCClear CCWEP CCWPA CCWPA2-AES Controlled APs Default Group B015-01224 VSC profile Dual-radio behavior VLAN Location-aware group name Cancel Save Group: Default Group | VSC binding VSC Profile: CCWPA2-AES On dual-radio products VSC is active on: Both radios □ Use egress VLAN VLAN ID: 1 Group name: Default Group

Step	**Description:** Synchronize MAP/MSC
2	Navigate to the **Discovered APs** configuration page by clicking **Overview → Discovered APs**. Chose “**Synchronize Configuration**” in the pull down tab and press **Apply** to synchronize the configuration**.** 

	Controlled APs
Unsynchronized	1
Detected	1
Configured	1

Base Group: All | Discovered APs

Number of access points: 1

Select the action to apply to all listed APs: Synchronize Configuration Apply

Status	AP name	Serial number	Wireless services	Wireless clients	Diagnostic	Action
○	B015-01224	B015-01224		0	Unsynchronized	Synch

= AP Mode = Monitor Mode = Sensor Mode = Disabled

6. Configure Avaya 3631 Wireless IP Telephone

For complete details on all the supported features on the Avaya 3631 Wireless IP Telephone refer **Section 13 [5].**

7. Configure Avaya 3641 Wireless IP Telephone

For complete details on all the supported features on the Avaya 3641 Wireless IP Telephone refer **Section 13 [7].**

8. Configure Avaya 3645 Wireless IP Telephone

For complete details on all the supported features on the Avaya 3645 Wireless IP Telephone refer **Section 13 [7].**

9. Interoperability Compliance Testing

Interoperability compliance testing covered feature functionality, serviceability, and performance testing. Feature functionality testing verified the ability of the Colubris Networks Wireless LAN System to provide network access to the Avaya Wireless IP Telephones. The emphasis of testing was on the QoS implementation, RADIUS authentication, WPA2 Enterprise and 802.1x encryption methods, and roaming at layer2 and layer3.

9.1. 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 network and the Colubris Intelligent Mobility Solution was verified to maintain voice calls while dropping the low priority traffic. Network level tests included verifying Layer 2 and 3 roaming from one access point to another and validating Quality of Service for voice traffic.

9.2. Test Results

The Avaya Wireless IP Telephones registered with Avaya Communication Manager utilizing Colubris Intelligent Mobility Solution passed all test cases. The Avaya Wireless IP Telephones were verified to successfully register with Avaya Communication Manager through the Colubris Networks Wireless LAN System. 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 was verified to roam successfully between access points on the same network (Layer 2 roaming) and between access points on a different network (Layer 3 roaming) while maintaining voice calls.

Four different security schemas were tested: Clear, WEP-128 and WPA2-PSK TKIP on the Avaya 3641 Wireless IP Telephones and Avaya 3645 Wireless IP Telephones, and Clear, WEP-128, WPA2-PSK TKIP and WPA2-CCMP-802.1X on the Avaya 3641 Wireless IP Telephones. 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 Communication Manager (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, call pick-up, bridged call appearances, voicemail using IA770, Message Waiting Indicator (MWI), hold and return from hold.

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

- Ensure that the **ESSID** field value configured in **Section 5.4**, **Step 1** on the Colubris Networks 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 Communication Manager by typing the **list registered-ip-station** command on the SAT in Avaya Communication Manager.

- Verify that the Colubris Networks MAPs are recognized by the Colubris Networks MSC-5100 Controller.

11. Support

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

- **Phone:** Phone: 1-866-241-8324
- **Email:** support@colubris.com

12. Conclusion

These Application Notes illustrate the procedures necessary for configuring Colubris Networks Wireless LAN equipment to support the Avaya 3631 IP Wireless Telephones, Avaya 3641 IP Wireless Telephones, Avaya 3645 IP Wireless Telephones and Avaya Communication Manager. 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, Layer 2 and Layer 3, roaming, VLAN Tagging, QoS, and 802.1x authentication with digital CA certificates as well as WPA2 AES and TKIP Encryption.

13. 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 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*

[7] *Avaya 3641/3645 Wireless Telephone and Accessories User Guide*, August 2007

The following 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).

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

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.