



**Application Notes for a HP Networking Mobility Solution  
using the E-MSM760 Mobility Controller with an Avaya  
Aura™ Telephony Infrastructure and Avaya Wireless 3631  
IP Telephones in a Converged Wireless VoIP and Data  
Network - Issue 1.0**

**Abstract**

These Application Notes describe the configuration of a wireless Voice over IP (VoIP) solution consisting of the HP Networking E-MSM760 Mobility Controller managing multiple HP Networking E-MSM Access Points with an Avaya Aura™ Telephony Infrastructure and Avaya Wireless 3631 IP Telephones in a converged wireless VoIP and data network. Emphasis of the testing was placed on verifying prioritization of wireless VoIP traffic on calls associated with the Avaya 3631 wireless IP telephones.

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

# 1. Introduction

These Application Notes describe the configuration of a wireless Voice over IP (VoIP) solution consisting of the HP Networking E-MSM760 Mobility Controller managing multiple HP Networking E-MSM Access Points with an Avaya Aura™ Telephony Infrastructure consisting of Avaya Aura™ Communication Manager, Avaya Aura™ Session Manager, Avaya Modular Messaging, Avaya Aura™ Communication Manager Messaging and Avaya 3631 Wireless IP Telephones in a converged wired/wireless Voice over IP and Data Network. The Avaya 3631 Wireless IP Telephones gained network access through the HP Networking E-MSM Access Points and registered with Communication Manager.

## 1.1. Interoperability Compliance Testing

Interoperability compliance testing covered feature functionality, serviceability, and Quality of Service (QoS).

Compliance testing emphasis was placed on verifying Layer 2 roaming, Multiple Encryption & Authentication types, Wi-Fi Multimedia (WMM) QoS and the prioritization of wireless VoIP traffic and voice quality in a converged VoIP and Data network.

### Feature functionality tested:

- QoS - Wi-Fi Multimedia (WMM)
- Multiple ESSIDs
- Multiple Encryption & Authentication types - Clear, WPA2-CCMP and WPA2 CCMP with 802.1x authentication
- VLANs
- Layer 2 roaming

### The following telephony features were verified:

- Attended/Unattended Transfer
- Conference call add/drop/participation
- Multiple call appearances
- Caller ID operation
- Call Forwarding
- Call Park/Call Pickup
- Bridged Call Appearances
- Voicemail using Communication Manager Messaging
- Message Waiting Indicator (MWI)
- Hold/Return from hold
- Direct IP Media (Shuffling)
- G.711 and G.729 codecs

### **Serviceability testing:**

- Serviceability testing was conducted to verify the ability of the Avaya/HP solution to recover from adverse conditions, such as power cycling network devices and disconnecting cables between the LAN interfaces. In all cases, the ability to recover after the network normalized was verified.

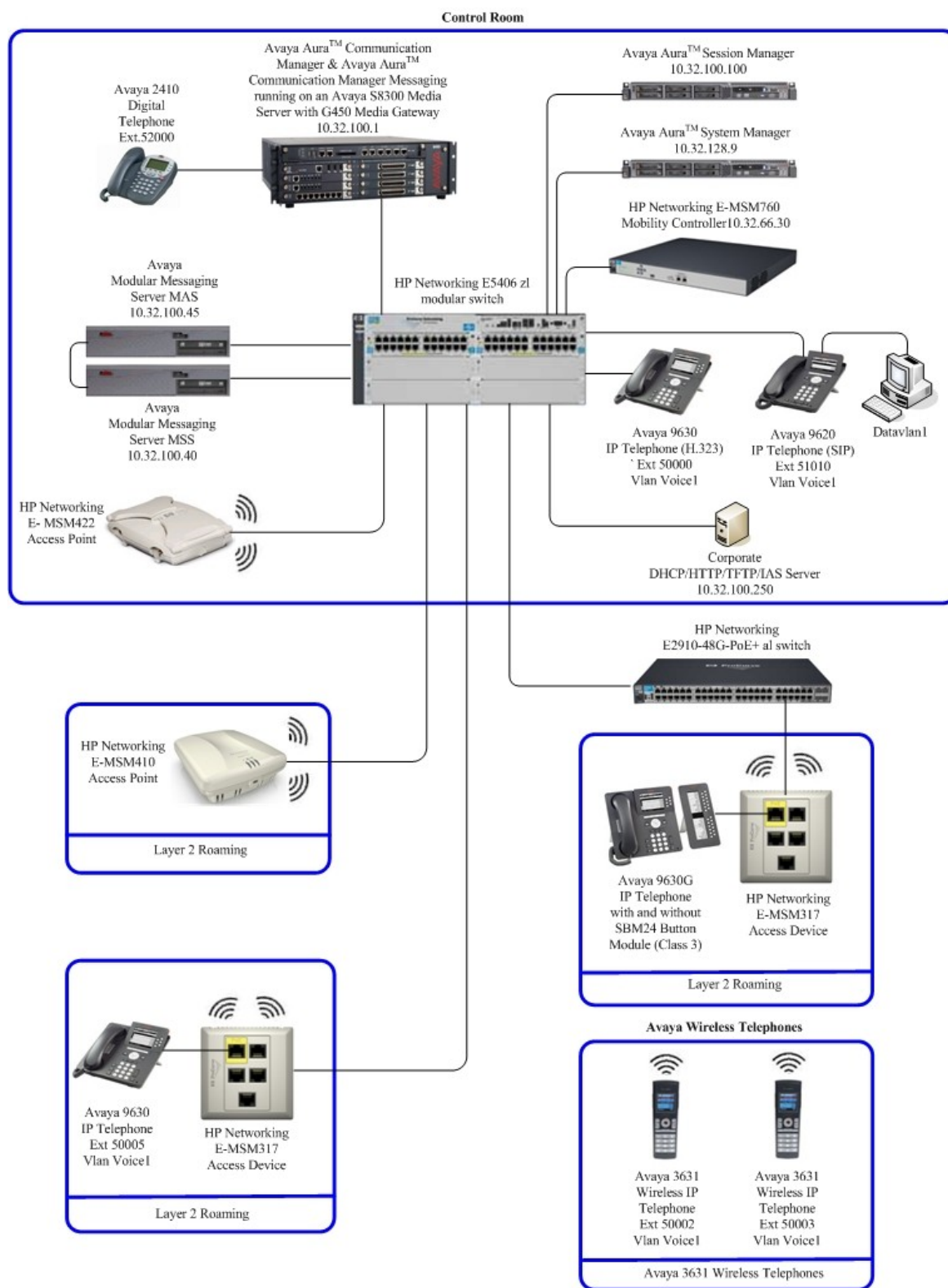
## **1.2. Support**

For technical support on HP Networking products, consult the support pages at:

[www.hp.com/networking/customercare](http://www.hp.com/networking/customercare)

## **2. Reference Configuration**

The network diagram shown in **Figure 1** illustrates the network environment used for the compliance test. The network consists of an Avaya Aura™ Telephony Infrastructure including Avaya Aura™ Communication Manager running on an Avaya S8300 Server with an Avaya G450 Media Gateway, an Avaya S8800 server running Avaya Aura™ Session Manager, Avaya Modular Messaging, multiple Avaya 9600 Series H.323 and SIP Telephones, and an Avaya 2420 Digital Telephone. These Avaya components were interconnected via a HP Networking E5406zl Switch and a HP Networking E2910-48G-PoE+ al Switch, which also provides connectivity to the HP Networking Mobility Solution. The HP Networking Mobility Solution consists of a HP Networking E-MSM760 Mobility Controller, HP Networking E-MSM412 and E-MSM422 Access Points, and HP Networking E-MSM317 Access Devices. One computer is present in the network providing network services such as Radius, DHCP, HTTP, and TFTP.



**Figure 1: Network Configuration**

### 3. Equipment and Software Validated

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

Equipment	Software/Firmware
<b><i>Avaya PBX Products</i></b>	
Avaya S8300 Server running Avaya Aura™ Communication Manager	Avaya Aura™ Communication Manager 6.0
Avaya G450 Media Gateway (Corporate Site) MGP MM712 DCP Media Module	30.13.2 HW9
<b><i>Avaya Aura™ Session Manager</i></b>	
Avaya Aura™ Session Manager	6.0
Avaya Aura™ System Manager	6.0
<b><i>Avaya Messaging (Voice Mail) Products</i></b>	
Avaya Modular Messaging - Messaging Application Server (MAS)	5.2
Avaya Modular Messaging - Message Storage Server (MSS)	5.2
Avaya Aura™ Communication Manager Messaging (CMM)	6.0
<b><i>Avaya Telephony Sets</i></b>	
Avaya 9600 Series IP Telephones	(H.323 3.1.1) and (SIP 2.6)
Avaya 3631 Wireless Telephone	V1.509
Avaya 2410 Digital Telephone	5.0
<b><i>HP Products</i></b>	
HP Networking E-MSM760 Mobility Controller	5.3.6.0-01-8252
HP Networking E-MSM422 Access Point	5.3.6.0-01-8252
HP Networking E-MSM412 Access Point	5.3.6.0-01-8252
HP Networking E-MSM317 Access Device	5.3.6.0-01-8252
HP Networking E2910-48G-PoE+ al Switch	W14.38
HP Networking E5406zl Switch	K.14.60
<b><i>MS Products</i></b>	
Microsoft Windows 2003 Server	Microsoft Windows 2003 Server

## 4. Configure QoS on Communication Manager

This section describes the steps required for Communication Manager to support the configuration shown in **Figure 1**. The following pages provide instructions on how to administer the required configuration parameters. The assumption is that the appropriate license has been installed on the servers and that login credentials are available. It is assumed that the reader has a basic understanding of the administration of Communication Manager and has access to the System Administration Terminal (SAT). For detailed information on the installation, maintenance, and configuration of Communication Manager, please consult references in **Section 9, [1] through [3]**.

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. QoS is now utilized to prioritize VoIP traffic and should be implemented throughout the entire network.

In order to achieve prioritization of VoIP traffic, the VoIP traffic must be classified. The Avaya Aura™ telephony infrastructure supports both IEEE 802.1p and DiffServ.

There were two IP network region's used for this sample configuration, one for Avaya wired IP telephones and one for Avaya wireless IP telephones. The DiffServ and 802.1p/Q values configured here will be downloaded to the Avaya H.323 IP wired and wireless telephones via Communication Manager. Avaya SIP Telephones will get QoS settings by downloading the 46xxsettings file from the HTTP server (not shown in this document). For more information on QoS settings please refer to **Section 9, [1] through [3]**.

## 4.1. Configure the IP Network Region for Wired IP Telephones

The Differentiated Services Code Point (DSCP) value of 46 will be used for both PHB values. DSCP 46 represents the traffic class of premium and the traffic type voice. Set the **Call Control PHB Value** to **46** and the **Audio PHB Value** to **46**. **Call Control 802.1p Priority** and **Audio 802.1p Priority** are set to **6**.

1.	<p>From the SAT, use the <b>change ip-network-region 1</b> command to change the DIFFSERV/TOS PARAMETERS and 802.1P/Q PARAMETERS settings. Change the following:</p> <ul style="list-style-type: none"><li>• <b>Call Control PHB Value</b> set to <b>46</b></li><li>• <b>Audio PHB Value</b> set to <b>46</b></li><li>• <b>Call Control 802.1p</b> set to <b>6</b></li><li>• <b>Audio 802.1p priority</b> set to <b>6</b></li></ul>
2.	<p>On <b>Page 3</b>, add the following options for <b>dst rgn 3</b>:</p> <ul style="list-style-type: none"><li>• <b>codec set</b> should be set to <b>1</b></li></ul> <p>Note: <b>direct WAN</b>, <b>Units</b> and <b>IGAR</b> will populate automatically.</p>

```
change ip-network-region 1                                     Page 1 of 19

                                IP NETWORK REGION
Region: 1
Location:                      Authoritative Domain: dev4.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
```

```
change ip-network-region 1                                     Page 3 of 19

Source Region: 1          Inter Network Region Connection Management      I      M
                                G      A      e
dst codec direct  WAN-BW-limits  Video      Intervening      Dyn  A  G  a
rgn set  WAN  Units      Total Norm  Prio Shr  Regions      CAC  R  L  s
1      1
2
3      1      y      NoLimit                                n
```

## 5. Configure the HP Networking E-MSM760 Mobility Controller and HP Networking E-MSM Access Points

The following steps detail the initial configuration for the HP Networking Mobility Solution used for compliance testing. The configuration on the HP Networking E-MSM760 Mobility 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. Refer to “HP Networking E-MSM760 Mobility Controller Administrator’s Guide” for additional information regarding the configuration displayed in this section.

### 5.1. Configure HP Networking E-MSM760 Mobility Controller

Step	
1.	<p>Configure HP Networking E-MSM760 Mobility Controller as depicted in <b>Figure 1</b>. Using the built-in web-based <b>Management Tool</b>, the supported web browsers are Microsoft Internet Explorer 6.0 or higher and Mozilla Firefox 1.5 or higher.</p> <ol style="list-style-type: none"><li>1. Connect the LAN port of the computer being used to the LAN port on the E-MSM760.</li><li>2. Configure the computer with the static IP address <b>192.168.1.2/24</b>.</li><li>3. Start the <b>Management Tool</b> as follows: Start a web browser and enter <b>https://192.168.1.1</b>. Press <b>Enter</b>.</li><li>4. Log in to the HP Networking E-MSM760 using default credentials which can be obtained from the HP Networking E-MSM760 Mobility Controller documentation.</li></ol>



**Step**

2.

Set the HP Networking E-MSM760 Mobility Controller IP address.

Select **Network** → **Ports** → **LAN port** (not shown). Set the **IP address** to **10.32.66.30** and the mask to **255.255.255.0**. Press **Save** to continue.

HP ProCurve Networking MSM760 System name: SG9503P017

Home Logout

Network Security VPN Controlled APs Authentication Public access Users Management Status Tools

Ports Address allocation Bandwidth control CDP DNS IP routes NAT RIP IP QoS IGMP proxy

Summary

Controlled APs

Synchronized 0

Detected 0

Configured 0

Network Tree

Service Controller

LAN port configuration

Addressing

IP address: 10.32.66.30

Mask: 255.255.255.0

Link settings

Speed: AUTO

Duplex: AUTO

(Currently: 1000 Mbps Full Duplex)

Management address

IP address:

Mask:

Cancel Save

**Step**

3.

Set the default gateway for the HP Networking E-MSM760 Mobility Controller.

Under **Network Tree**, select **Service Controller** → **Network** → **IP routes**. Set the **Gateway** to **10.32.66.254** and the **Metric** to **1**. Press **Add** to continue.

HP ProCurve Networking MSM760 System name: SG9503P017

Home Logout

Network Security VPN Controlled APs Authentication Public access Users Management Status Tools

Ports Address allocation Bandwidth control CDP DNS IP routes NAT RIP IP QoS IGMP proxy

Summary

Controlled APs

Synchronized 4

Detected 4

Configured 4

Network Tree

Service Controller

Active routes

Interface	Destination	Mask	Gateway	Metric	Delete
LAN port	10.32.66.0	255.255.255.0	*	0	
					Add

Default routes

Interface	Gateway	Metric	Delete
	10.32.66.254	1	
			Add

Persistent routes

Interface	Destination	Mask	Gateway	Delete
PPTP Client				
				Add

## 5.2. Configure Radius Server

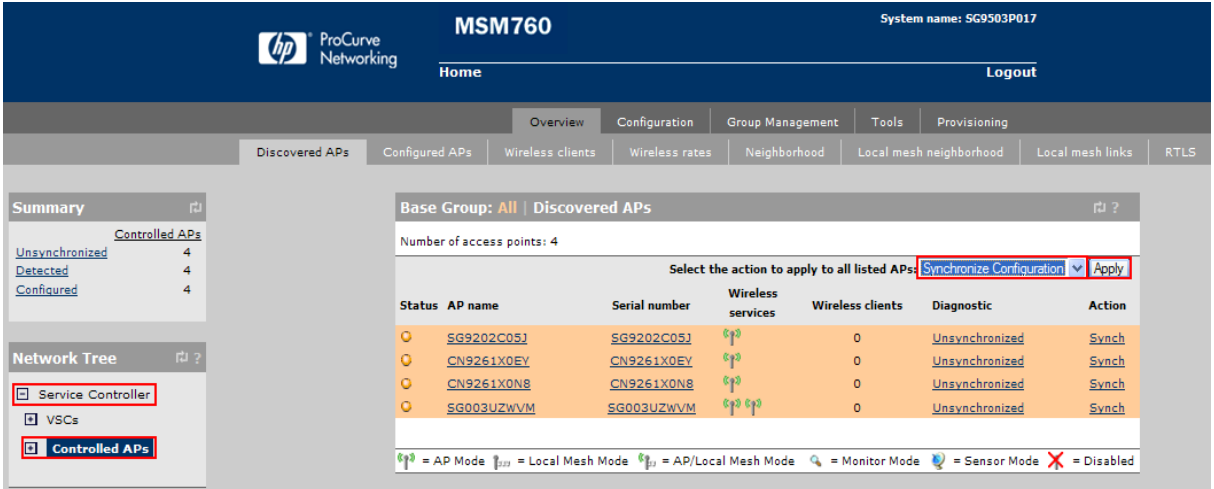
### Configure Radius Server Profile

Under **Network Tree**, select **Service Controller** → **Authentication** → **RADIUS profiles** → **Add New Profile**. Set the **Profile name** to **RAD**, **Server address** to **10.32.100.250**, and the **Secret/Confirm secret** to whatever is set on the RADIUS server. Contact the administrator of the Radius server to obtain the secret password. Press **Save** to continue.

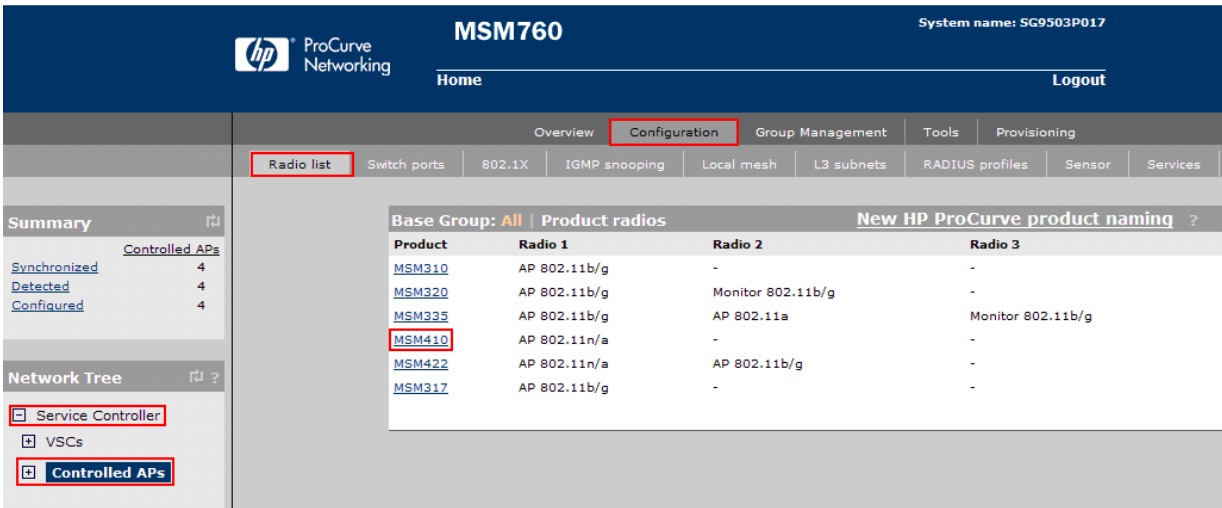
The screenshot displays the HP ProCurve MSM760 configuration web interface. The top navigation bar includes the HP logo, 'ProCurve Networking', the device name 'MSM760', and the system name 'SG9503P017'. A 'Logout' link is also present. Below the navigation bar, a series of tabs are visible: Network, Security, VPN, Controlled APs, Authentication (highlighted with a red box), Public access, Users, Management, Status, Tools, and Maintenance. Under the 'Authentication' tab, a sub-tab 'RADIUS profiles' is also highlighted with a red box. On the left sidebar, the 'Network Tree' section shows a tree structure with 'Service Controller' highlighted by a red box. The main content area is titled 'Add/Edit RADIUS profile'. It contains several sections: 'Profile name' with a text field containing 'RAD' (highlighted with a red box); 'Primary RADIUS server' with fields for 'Server address' (10.32.100.250), 'Secret' (masked with dots), and 'Confirm secret' (masked with dots), all highlighted with a red box; 'Settings' with fields for 'Authentication port' (1645), 'Accounting port' (1813), 'Retry interval' (10 seconds), 'Retry timeout' (60 seconds), 'Authentication method' (MSCHAPv2), and 'NAS ID' (SG9503P017); 'Secondary RADIUS server (optional)' with fields for 'Server address', 'Secret', and 'Confirm secret'; and 'Authentication realms' with a section for 'Associated realms' and a 'New realm' section with 'Remove' and 'Add' buttons. At the bottom of the form, there are 'Cancel', 'Delete', and 'Save' buttons, with the 'Save' button highlighted by a red box.

### 5.3. Connect and Configure the HP Networking E-MSM Access Points

All HP Networking E-MSM Access Points in **Figure 1** are located in the same layer 2 subnet as the E-MSM760 Mobility Controller and will be discovered by the E-MSM760 Mobility Controller via the automated discovery mechanism built into the E-MSM Controller. The HP Networking E-MSM Access Points can be manually configured to connect to the E-MSM Controller, but it is outside the scope of testing and will not be covered in this document.

Step																																				
1.	<p>After connecting the E-MSM Access Point to the same layer 2 subnet as the E-MSM760 Mobility Controller, verify that they have been discovered. Under <b>Network Tree</b>, click <b>Service Controller</b> → <b>Controlled APs</b> → <b>Overview</b> → <b>Discovered APs</b>. The discovered APs may need to be Accepted or Synchronized. In the example below, The AP's need to be Synchronized. Select <b>Synchronize Configuration</b> from the <b>Select the action to apply to all listed APs</b> drop-down list and click <b>Apply</b>.</p>  <table border="1"><caption>Discovered APs Table</caption><thead><tr><th>Status</th><th>AP name</th><th>Serial number</th><th>Wireless services</th><th>Wireless clients</th><th>Diagnostic</th><th>Action</th></tr></thead><tbody><tr><td>Unsync</td><td>SG9202C05J</td><td>SG9202C05J</td><td>AP</td><td>0</td><td>Unsync</td><td>Synch</td></tr><tr><td>Unsync</td><td>CN9261X0EY</td><td>CN9261X0EY</td><td>AP</td><td>0</td><td>Unsync</td><td>Synch</td></tr><tr><td>Unsync</td><td>CN9261X0N8</td><td>CN9261X0N8</td><td>AP</td><td>0</td><td>Unsync</td><td>Synch</td></tr><tr><td>Unsync</td><td>SG003UZWVM</td><td>SG003UZWVM</td><td>AP</td><td>0</td><td>Unsync</td><td>Synch</td></tr></tbody></table>	Status	AP name	Serial number	Wireless services	Wireless clients	Diagnostic	Action	Unsync	SG9202C05J	SG9202C05J	AP	0	Unsync	Synch	Unsync	CN9261X0EY	CN9261X0EY	AP	0	Unsync	Synch	Unsync	CN9261X0N8	CN9261X0N8	AP	0	Unsync	Synch	Unsync	SG003UZWVM	SG003UZWVM	AP	0	Unsync	Synch
Status	AP name	Serial number	Wireless services	Wireless clients	Diagnostic	Action																														
Unsync	SG9202C05J	SG9202C05J	AP	0	Unsync	Synch																														
Unsync	CN9261X0EY	CN9261X0EY	AP	0	Unsync	Synch																														
Unsync	CN9261X0N8	CN9261X0N8	AP	0	Unsync	Synch																														
Unsync	SG003UZWVM	SG003UZWVM	AP	0	Unsync	Synch																														

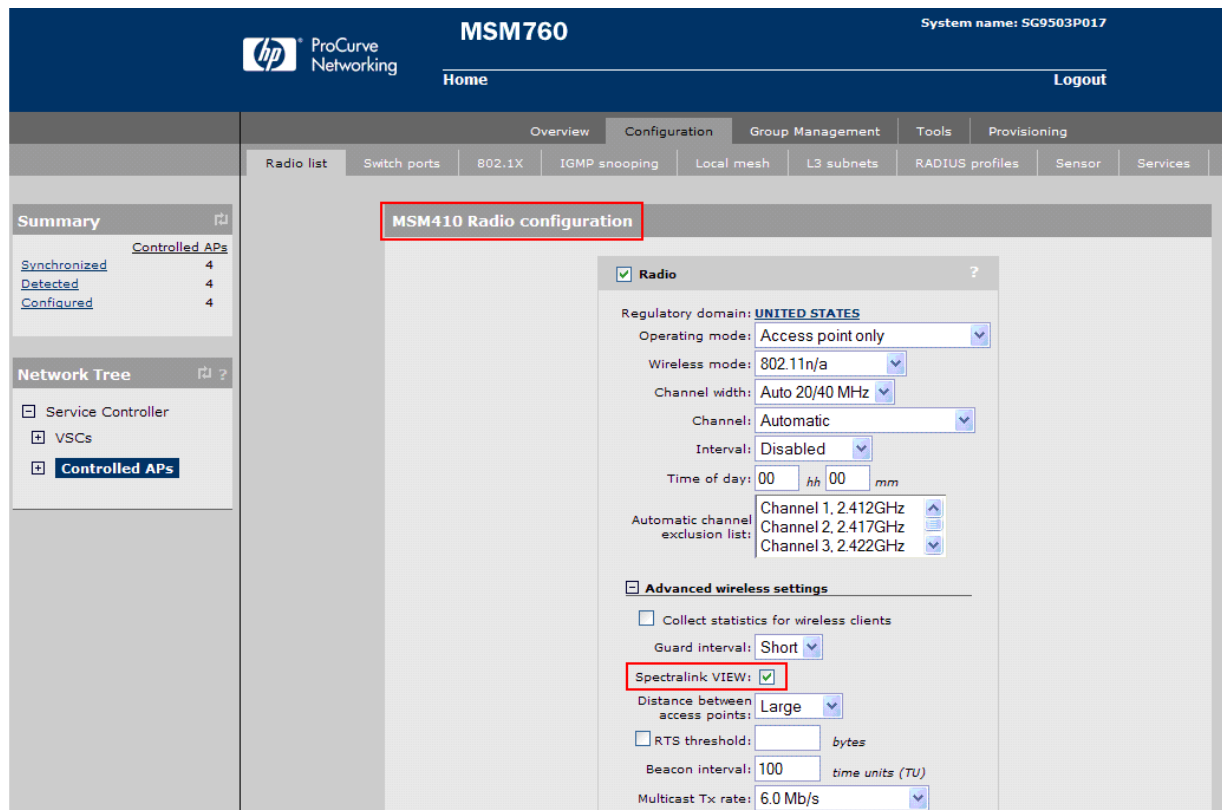
**Step 2.** Under **Network Tree**, select **Service Controller** → **Controlled APs** → **Configuration** → **Radio list**. Double click on a **Product ID**. E-MSM410 was used for this example.



The screenshot shows the HP ProCurve MSM760 configuration page. The 'Radio list' tab is active, displaying a table of product radios. The 'MSM410' product is highlighted. The 'Network Tree' on the left shows 'Service Controller' and 'Controlled APs'.

Product	Radio 1	Radio 2	Radio 3
MSM310	AP 802.11b/g	-	-
MSM320	AP 802.11b/g	Monitor 802.11b/g	-
MSM335	AP 802.11b/g	AP 802.11a	Monitor 802.11b/g
MSM410	AP 802.11n/a	-	-
MSM422	AP 802.11n/a	AP 802.11b/g	-
MSM317	AP 802.11b/g	-	-

**Step 3.** The E-MSM410 Radio configuration box will appear, Under **Advanced wireless setting**, check the box next to **Spectralink VIEW**. Scroll to the bottom of the page and press the **Save** button to continue. Repeat **Step 2** and **3** for all **Products/Radios**.



The screenshot shows the HP ProCurve MSM760 configuration page with the 'MSM410 Radio configuration' dialog box open. The 'Spectralink VIEW' checkbox is checked under 'Advanced wireless settings'.

**MSM410 Radio configuration**

☒ **Radio**

Regulatory domain: **UNITED STATES**

Operating mode: **Access point only**

Wireless mode: **802.11n/a**

Channel width: **Auto 20/40 MHz**

Channel: **Automatic**

Interval: **Disabled**

Time of day: **00** **00**

Automatic channel exclusion list: **Channel 1, 2.412GHz**, **Channel 2, 2.417GHz**, **Channel 3, 2.422GHz**

☒ **Advanced wireless settings**

☐ Collect statistics for wireless clients

Guard interval: **Short**

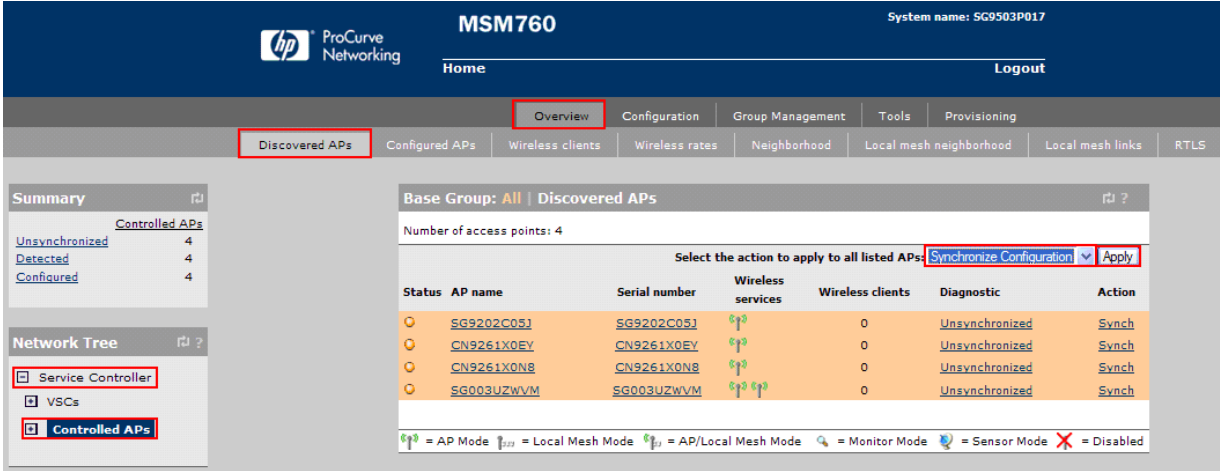
☒ **Spectralink VIEW**

Distance between access points: **Large**

☐ RTS threshold: **bytes**

Beacon interval: **100** **time units (TU)**

Multicast Tx rate: **6.0 Mb/s**

<b>Step</b> 4.	<p>Under <b>Network Tree</b>, select <b>Service Controller</b> → <b>Controlled APs</b> → <b>Overview</b> → <b>Discovered APs</b>, Select <b>Synchronize Configuration</b> from the <b>Select the action to apply to all listed APs</b> drop-down list and click <b>Apply</b>.</p>  <p>The screenshot shows the HP ProCurve MSM760 web interface. The 'Network Tree' on the left has 'Service Controller' and 'Controlled APs' highlighted. The main area displays 'Discovered APs' with a table of access points. A dropdown menu is open, showing 'Synchronize Configuration' selected, and an 'Apply' button is visible.</p> <table border="1"> <thead> <tr> <th>Status</th> <th>AP name</th> <th>Serial number</th> <th>Wireless services</th> <th>Wireless clients</th> <th>Diagnostic</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>○</td> <td>SG9202C05J</td> <td>SG9202C05J</td> <td>1</td> <td>0</td> <td>Unsynchronized</td> <td>Synch</td> </tr> <tr> <td>○</td> <td>CN9261X0EY</td> <td>CN9261X0EY</td> <td>1</td> <td>0</td> <td>Unsynchronized</td> <td>Synch</td> </tr> <tr> <td>○</td> <td>CN9261X0N8</td> <td>CN9261X0N8</td> <td>1</td> <td>0</td> <td>Unsynchronized</td> <td>Synch</td> </tr> <tr> <td>○</td> <td>SG003UZWVM</td> <td>SG003UZWVM</td> <td>1</td> <td>0</td> <td>Unsynchronized</td> <td>Synch</td> </tr> </tbody> </table> <p>Legend:    = AP Mode    = Local Mesh Mode    = AP/Local Mesh Mode    = Monitor Mode    = Sensor Mode    = Disabled       </p>	Status	AP name	Serial number	Wireless services	Wireless clients	Diagnostic	Action	○	SG9202C05J	SG9202C05J	1	0	Unsynchronized	Synch	○	CN9261X0EY	CN9261X0EY	1	0	Unsynchronized	Synch	○	CN9261X0N8	CN9261X0N8	1	0	Unsynchronized	Synch	○	SG003UZWVM	SG003UZWVM	1	0	Unsynchronized	Synch
Status	AP name	Serial number	Wireless services	Wireless clients	Diagnostic	Action																														
○	SG9202C05J	SG9202C05J	1	0	Unsynchronized	Synch																														
○	CN9261X0EY	CN9261X0EY	1	0	Unsynchronized	Synch																														
○	CN9261X0N8	CN9261X0N8	1	0	Unsynchronized	Synch																														
○	SG003UZWVM	SG003UZWVM	1	0	Unsynchronized	Synch																														

## 5.4.Create and Configure the VSC (SSID) for the voice network

Three different security schemas were tested for the voice wireless traffic - Clear, WPA2-PSK AES/CCMP and WPA2 AES/CCMP with 802.1x authentication. Administration of the Clear and WPA2 CCMP SSIDs will not be covered in these Application Notes.

**Note:** The HP Networking E-MSM760 Mobility Controller uses the term Virtual Service Community (VSC) to refer to an SSID.

Under **Network Tree**, select **Service Controller** → **VSCs** → **Add new VSC profile (not shown)**. In the VSC window, change the **Profile name** to **wmm-voice**, uncheck the **Access control** box, change the **SSID** to **wmm-voice**, uncheck the **Wireless security filters** (not shown), check **Wireless protection** box, select **WPA** from the **Wireless protection drop-down 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** under **Authentication**, select **RADIUS** radio button and choose the **RAD1** server that was previously defined in **Step 5.2**. Expand the **Quality of service** section, select **VSC Based Very-high** from the **Priority mechanism** drop-down list. Scroll to the bottom of the page and press the **Save** button to continue.

The screenshot displays the HP ProCurve MSM760 configuration interface. The top navigation bar includes the HP logo, 'ProCurve Networking', the device name 'MSM760', and the system name 'SG9503P017'. Below this, there are tabs for 'Home' and 'Logout'. The main interface is divided into a left sidebar and a central configuration area.

**Left Sidebar:**

- Summary:** Includes a link to 'Controlled APs'.
- Network Tree:** A tree view showing the hierarchy: 'Service Controller' (selected), 'VSCs', and 'Controlled APs'.

**Central Configuration Area:**

The main configuration area is titled 'VSC: wmm-voice | VSC profile'. It contains several sections:

- Global:**
  - Profile name:** 'wmm-voice' (highlighted with a red box).
  - Use Service Controller for:** 'Authentication' (checked), 'Access control' (unchecked).
- VSC ingress mapping:**
  - SSID:** Selected.
  - Ethernet Switch:** Unselected.
- Virtual AP:**
  - WLAN:**
    - Name (SSID):** 'wmm-voice' (highlighted with a red box).
    - DTIM count:** '1'.
    - Broadcast name (SSID):** Checked.
    - Advertise TX power:** Unchecked.
  - Wireless clients:**
    - Max clients per radio:** '100'.
    - Allow traffic between:** 'all'.
  - Client data tunnel:** Unchecked.
  - Quality of service:**
    - Priority mechanism:** 'VSC Based Very-high' (highlighted with a red box).
    - IP QoS profiles:** '<No IP QoS profiles defined>'.
- Wireless protection:**
  - Wireless protection:** Checked.
  - Mode:** 'WPA2 (AES/CCMP)' (highlighted with a red box).
  - Key source:** 'Dynamic' (highlighted with a red box).
- 802.1X authentication:**
  - Authentication:**
    - Local:** Unchecked.
    - Remote:** Checked (highlighted with a red box).
    - Active directory:** Unchecked.
    - RADIUS:** 'RAD1' (highlighted with a red box).
    - Request RADIUS CUI:** Unchecked.
  - General:**
    - RADIUS accounting:** 'RAD1'.
    - Called-Station-Id content:** 'BSSID'.
- RADIUS authentication realms:**
  - Use authentication realms:** Unchecked.
  - Use realms for accounting:** Unchecked.
- MAC-based authentication:**
  - Authentication:**
    - Local:** Checked.
    - Remote:** Unchecked.

## 5.5. Create and Configure the VSC (SSID) for the data network

**Note:** The HP Networking E-MSM760 Mobility Controller uses the term Virtual Service Community (VSC) to refer to an SSID.

Under **Network Tree**, select **Service Controller** → **VSCs** → **Add new VSC profile (not shown)**. In the VSC window, change the Profile name to **h-data**, uncheck the **Access control** box, change the **SSID** to **h-data**, uncheck the **Wireless security filters** (not shown), check **Wireless protection** box, select **WPA** from the **Wireless protection** list, select **WPA2 (AES/CCMP)** from the **Mode** drop-down list, select **Preshared Key** from the **Key source** drop-down list. Scroll to the bottom of the page and press the **Save** button to continue.

The screenshot displays the HP ProCurve MSM760 configuration interface. The top navigation bar includes the HP logo, 'ProCurve Networking', 'MSM760', 'System name: SG9503P017', 'Home', and 'Logout'. Below this is a tabbed interface with 'Overview' and 'Configuration' tabs, and a sub-tab 'VSC profile'.

On the left, the 'Network Tree' shows a hierarchy: 'Service Controller' (selected), 'VSCs' (selected), and 'Controlled APs'. The 'Summary' section on the left shows 'Controlled APs' with counts for 'Synchronized' (4), 'Detected' (4), and 'Configured' (4).

The main configuration area is titled 'VSC: h-data | VSC profile'. It contains several sections:

- Global**: 'Profile name' is set to 'h-data'. 'Use Service Controller for:' has 'Authentication' checked and 'Access control' unchecked.
- VSC ingress mapping**: 'SSID' is selected.
- Virtual AP**: 'Virtual AP' is checked.
- WLAN**: 'Name (SSID)' is set to 'h-data', 'DTIM count' is '1', 'Broadcast name (SSID)' is checked, and 'Advertise TX power' is unchecked.
- Wireless protection**: 'Wireless protection' is checked, 'WPA' is selected from the dropdown, 'Mode' is 'WPA2 (AES/CCMP)', 'Key source' is 'Preshared Key', and 'Key' and 'Confirm key' fields are filled with dots.
- RADIUS authentication realms**: 'Use authentication realms' and 'Use realms for accounting' are unchecked.
- MAC-based authentication**: 'MAC-based authentication' is unchecked.
- Authentication**: 'Local' is checked, and 'Remote' is unchecked.

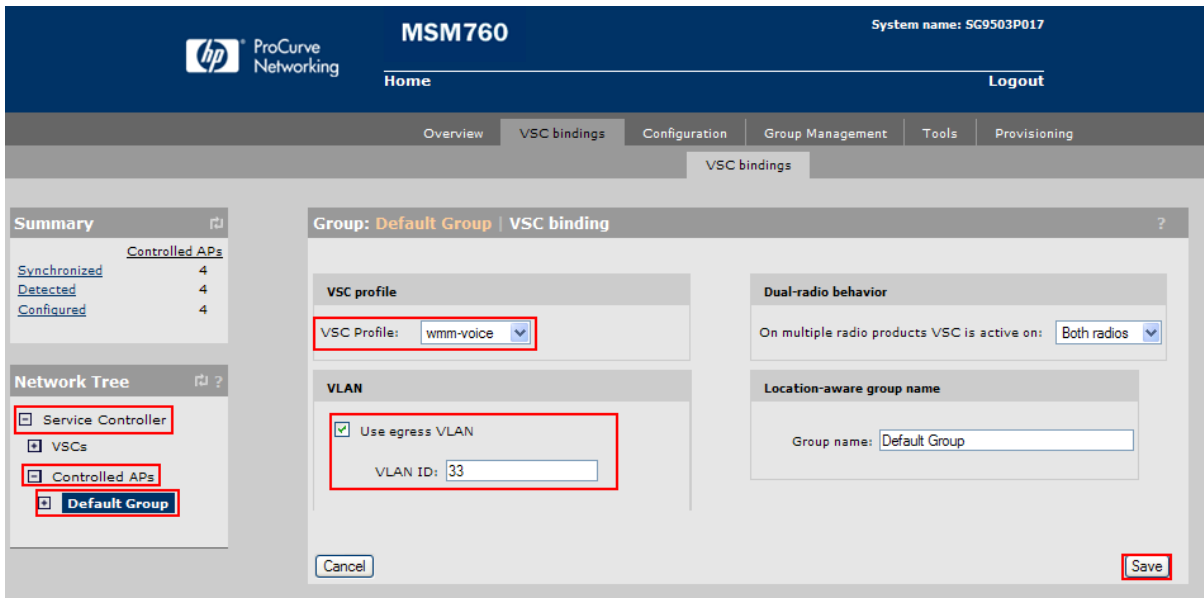
A note at the bottom right states: '\*On radios in pure 802.11n mode WPA2 is always used instead of WPA'.

## 5.6. Bind the VSCs to the Access Points

Before a VSC can be used, it must be bound to a group of access points

**Note:** It is assumed that VLAN trunking is enabled on the port of the Ethernet switch that is connected to the HP Networking E-MSM760 Mobility Controller, and that the VLANs for the voice and data networks are assigned.

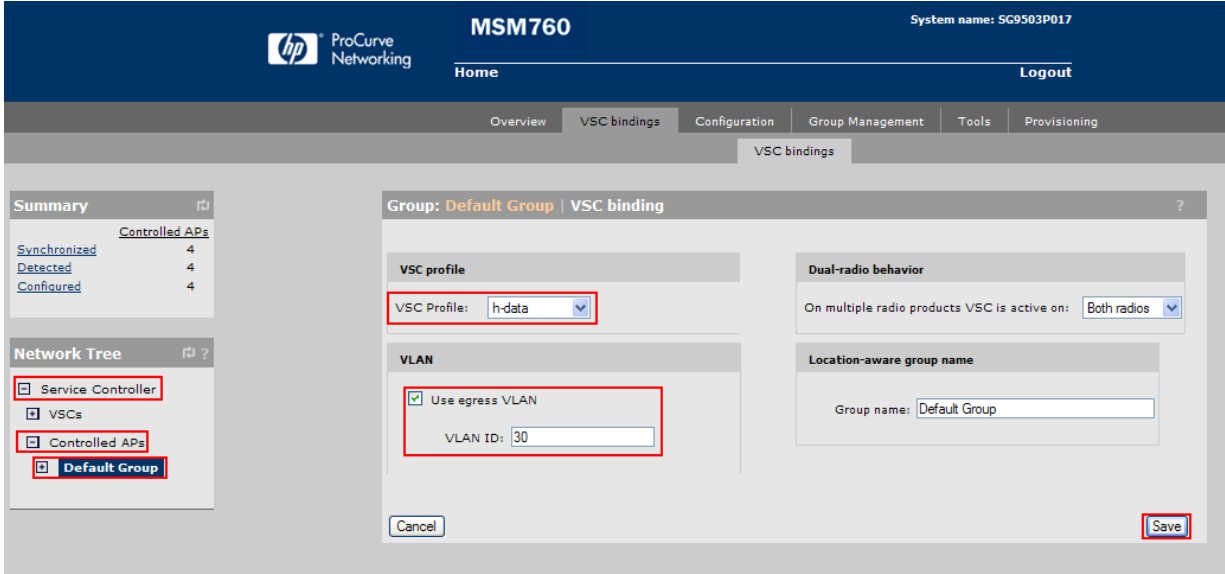
### Bind the Voice VSC

Step	
1.	<p>Under <b>Network Tree</b>, select <b>Service Controller</b> → <b>Controlled APs</b> → <b>Default Group</b> → <b>VSC bindings</b> → <b>Add New Binding (not shown)</b>. Select the <b>VSC profile</b> to use. Under <b>VLAN</b>, check the box for <b>Use egress VLAN</b>, add the vlan ID for the voice network, <b>33</b> was used for compliance testing. Press the <b>Save</b> button to continue. Repeat this process for all VSCs that will be used.</p> 



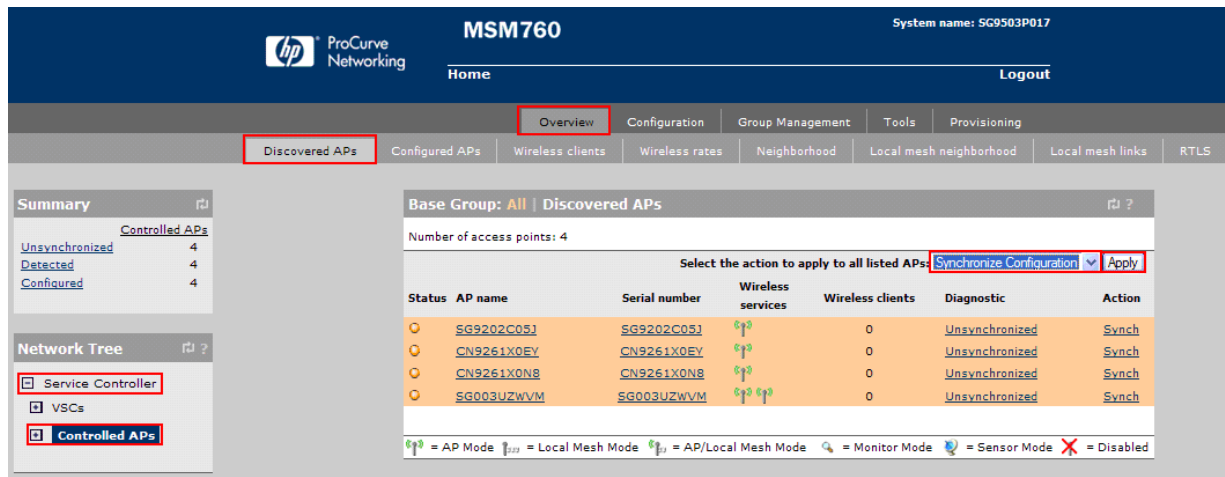
## Bind the Data VSC

<b>Step</b>	Under <b>Network Tree</b> , select <b>Service Controller</b> → <b>Controlled APs</b> → <b>Default Group</b> →
2.	<b>VSC bindings</b> → <b>Add New Binding (not shown)</b> . Select the <b>VSC profile</b> to use. Under <b>VLAN</b> , check the box for <b>Use egress VLAN</b> , add the vlan ID for the data network, <b>30</b> was used for compliance testing. Press the <b>Save</b> button to continue. Repeat this process for all VSCs that will be used.



## Synchronize Configuration

<b>Step</b>	Under <b>Network Tree</b> , select <b>Service Controller</b> → <b>Controlled APs</b> → <b>Overview</b> →
3.	<b>Discovered APs</b> . Select <b>Synchronize Configuration</b> from the <b>Select the action to apply to all listed APs</b> drop-down list and click <b>Apply</b> .



Status	AP name	Serial number	Wireless services	Wireless clients	Diagnostic	Action
○	SG9202C05J	SG9202C05J	📶	0	Unsync	Synch
○	CN9261X0EY	CN9261X0EY	📶	0	Unsync	Synch
○	CN9261X0N8	CN9261X0N8	📶	0	Unsync	Synch
○	SG003UZWVM	SG003UZWVM	📶	0	Unsync	Synch

📶 = AP Mode   📶📶 = Local Mesh Mode   📶📶 = AP/Local Mesh Mode   📶 = Monitor Mode   📶 = Sensor Mode   ✖ = Disabled

## 6. 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 to [4] in Section 9.



## 6.1. 46xxsettings File Options

The 46xxsettings.txt file is used to specify certain phone parameters. It is used by all Avaya 1600, 4600 and 9600 H.323 & SIP Telephones. The 46xxsettings.txt file can be delivered to the Avaya 3631 Wireless IP Telephone through either of the following two methods:

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

For this compliance test, the 46xxsetting file was delivered manually via a USB cable connected between the Avaya 3631 Wireless IP Telephone and a PC. For more information on configuring 46xxsetting options refer to **Section 9 [4]**.

For this example, the ESSID is **wmm-voice**, **Encryption type is WPA2-CCMP** and the Authentication type **802.1x**, as create in **Section 5.2 Step 8**. Add the following information to the 46xxsetting setting file.

```
SET WTPROF1      " wmm-voice"
SET WTSSIDP1     " wmm-voice "
SET DNSSRVRP1    "10.32.100.1"
SET WTWMP1       "1"
SET DOMAIN       "dev4.com"
SET WTSECP1      "5"
SET ENCRYPTP1     "4"
SET EAPTYPEP1    "4"
SET TRUSTCERTS   "cacert1.pem"
```

After the phone reboots, the user is prompted to enter **802.1X ID**, **username**, and **password**. (For PEAP-MSCHAPV2, only specify **ID** and **password**; leave **username** blank.) This is a one-time-only data entry. Data is stored in flash and presented automatically on subsequent authentications. Alternately, the user can enter 802.1x/EAP information as part of Access Profile configuration through phone's display interface.

## 6.2. Downloading 46xxsettings File via USB Cable

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 drivefolder 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.

### 6.3. Downloading Digital Certificates via USB Cable

The Certificate for the Avaya 3631 Wireless IP Telephone is in the PEM format. Certificate filenames are FIXED. The fixed filenames are keyed to the phone Access Profile with which the certificate is associated. So, **cacert1.pem** is filename for certificate used with first Access Profile. To use the certificate with Access Profile 2 or 3, the user must change the filename accordingly.

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 digital certificates 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 **certificate file(s)** onto the USB drive folder associated with the phone.
7. Once the file(s) have 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.

## 6.4. 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 OptionNumbers (SSON) 242 and 176. The default is 242. Note that this parameter can be changed only through the phone's menu interface.

This section describes how to configure the Vendor Class Identifier Code (option 242) on a Microsoft Windows-based DHCP server. Since option 242 is not a predefined option on a Windows DHCP server, add it to the option list for the server. To configure option 242 on the Windows DHCP server:

Step	Description: Configuring DHCP Option 242
1.	<ol style="list-style-type: none"><li>1. On the DHCP server, open the <b>DHCP server administration</b> tool by clicking <b>Start → Administration Tools → DHCP</b>.</li><li>2. Find the DHCP server and right-click on the server name. Select <b>Set Predefined Options</b>.</li><li>3. In the Predefined Options and Values dialog box, click the <b>Add</b> button.</li><li>4. In the Option Type dialog box, enter the following information:<ul style="list-style-type: none"><li>• <b>Name = 242</b></li><li>• <b>Data type = String</b></li><li>• <b>Code = 242</b></li></ul></li><li>5. Click the <b>OK</b> button to save this information.</li><li>6. Add the following <b>String</b> under <b>Value</b>:  <b>MCIPADD=10.32.100.1,MCPORT=1719,HTTPSRVR=10.32.100.250</b></li></ol>

## 7. General Test Approach and Test Results

All feature functionality test cases were performed manually. The general test approach entailed verifying the following:

- Registration, re-registration of Avaya 3631 Wireless IP Telephone with Avaya Aura™ Communication Manager through the HP Networking Mobility Solution.
- Verify Message Waiting Indicator and message retrieval from Avaya Modular Messaging Server and Avaya Aura™ Communication Manager Messaging.
- VoIP calls between the Avaya 3631 Wireless IP Telephones and the wired Avaya Digital/SIP/H.323 Telephones.
- Validated G.711MU and G.729A codecs, shuffling, conferencing, Transfer, Hold/Return from hold, Forwarding, Call Park, Call Pickup, Bridged extension, voicemail, DTMF while traversing the HP Networking Mobility Solution.
- Wireless Roaming, Wireless Security, Wireless Authentication and Wireless Quality of Service.
- Verified that QoS directed the voice signaling and voice media to the higher priority queue based on WMM QoS.
- Validate QoS queues by making and receiving wireless calls while sending a heavy load of low priority data traffic and verifying that good voice quality was achieved.

All feature functionality, serviceability, and QoS performance test cases passed. The Avaya 3631 Wireless IP Telephones successfully registered with Avaya Aura™ Communication Manager utilizing the HP Networking Mobility Solution. The Avaya Wireless 3631 IP Telephones were verified to roam successfully between access points and yielded good voice quality and no calls were lost. Compliance testing also focused on verifying Quality of Service for voice traffic while low priority background traffic was competing for bandwidth. The stability of the Avaya/HP solution was successfully verified through QoS performance and serviceability testing.

## 8. 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.

- Check that the Avaya 3631 Wireless IP Telephones have successfully registered with Communication Manager by typing the **list registered-ip-station** command on the SAT in Communication Manager.
- Ensure that the **SSID** value of the wireless network matches the **SSID** field value configured in **Section 6.1**, on the Avaya 3631 Wireless IP Telephones.
- Place calls from the Avaya 3631 Wireless IP Telephones and verify two-way audio.
- Place a call to the Avaya 3631 Wireless IP Telephones, allow the call to be directed to voicemail, leave a voicemail message and verify the MWI light is turned on.
- Using the Avaya 3631 Wireless IP Telephone that received the voicemail, connect to the voicemail system to retrieve the voicemail and verify the MWI light is turned off.
- Place calls to the Avaya 3631 Wireless IP Telephones and exercise calling features such as transfer, conference and hold.

## 9. Conclusion

These Application Notes illustrate the procedures necessary for configuring the HP Networking E-MSM760 Mobility Controller managing multiple HP Networking E-MSM Access Points with an Avaya Aura™ telephony infrastructure. The HP Networking E-MSM760 Mobility Controller managing multiple HP Networking E-MSM Access Points was successfully compliance-tested in a wireless converged voice and data network configuration. All feature functionality test cases described in **Section 1.1** passed.



## 10. Additional References

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

- [1] *Installing and Configuring Avaya Aura™ Session Manager, Doc ID 03-603473 Release 6.*
- [2] *Administering Avaya Aura™ Session Manager, Doc ID 03-603324, Release 6.0, June 2010*
- [3] *Installing and Configuring Avaya Aura™ Communication Manager, Doc ID 03-603558, Release 6.0 June, 2010*
- [4] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 3.1, Document Number 16-300698.*

The HP product documentation can be found at: [www.hp.com/networking/customercare](http://www.hp.com/networking/customercare)

---

**©2010 Avaya Inc. All Rights Reserved.**

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

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