



Application Notes for Configuring the Hitachi Cable WirelessIP 5000 with Avaya Communication Manager and Avaya SIP Enablement Services using RADIUS Authentication over Meru Networks Wireless Infrastructure - Issue 1.0

Abstract

These Application Notes describe the steps for configuring the Hitachi Cable WirelessIP 5000 to communicate with Avaya Communication Manager and Avaya SIP Enablement Services (SES). The Hitachi Cable WirelessIP 5000 is a wireless SIP telephone that registers with Avaya SIP Enablement Services (SES). Emphasis of the testing was placed on verifying good voice quality from the Hitachi Cable WirelessIP 5000 and its ability to interoperate with Avaya SIP Enablement Services. Information in these Application Notes has been obtained through *DeveloperConnection* compliance testing and additional technical discussions. Testing was conducted via the *DeveloperConnection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

Avaya Communication Manager and Avaya SIP Enablement Services (SES) have the capability to extend advanced telephony features to SIP stations. This feature set can be extended to non-Avaya SIP phones such as the Hitachi Cable WirelessIP 5000.

These Application Notes describe a solution for configuring the Hitachi Cable WirelessIP 5000 to interoperate with Avaya Communication Manager and Avaya SIP Enablement Services (SES). The Hitachi Cable WirelessIP 5000 is a wireless SIP telephone capable of registering with the Avaya SIP Enablement Services (SES). Quality of Service was achieved through the use of Hitachi Cable WirelessIP 5000 telephone Layer-3 (DiffServ) setup and Meru Networks native support for SIP. Authentication is provided by the use of 802.1x authentication against Steel Belted Radius Server.

1.1. Configuration

Figure 1 illustrates the configuration used in these Application Notes. The extension numbers used by the Hitachi Cable WirelessIP 5000 phones are registered to Avaya SIP Enablement Services (SES) and are administered as Outboard Proxy SIP (OPS) stations in Avaya Communication Manager. As a result, each Hitachi Cable WirelessIP 5000 has access to OPS¹ features available from Avaya Communication Manager. The names of the Meru Networks Access Points (APs) “AP-6”, “AP-7”, and “AP-9” were automatically assigned by the Meru Networks MC500 Controller as each AP was connected onto the network.

¹ Depending on the Avaya server product, the acronym OPS stands for two different feature names that are functionally equivalent. For SIP Enablement Services, the extended features capability is referred to as Outboard Proxy SIP. This capability is provided by Avaya Communication Manager as part of a more general feature extension package known as Off-PBX Stations, which can be applied to other remote devices such as cell phones. For that reason, the administration screens in this document will refer to the latter name or “off-pbx-telephone.” For the purposes of the Avaya SIP offer and these Application Notes, the terms can be used interchangeably.

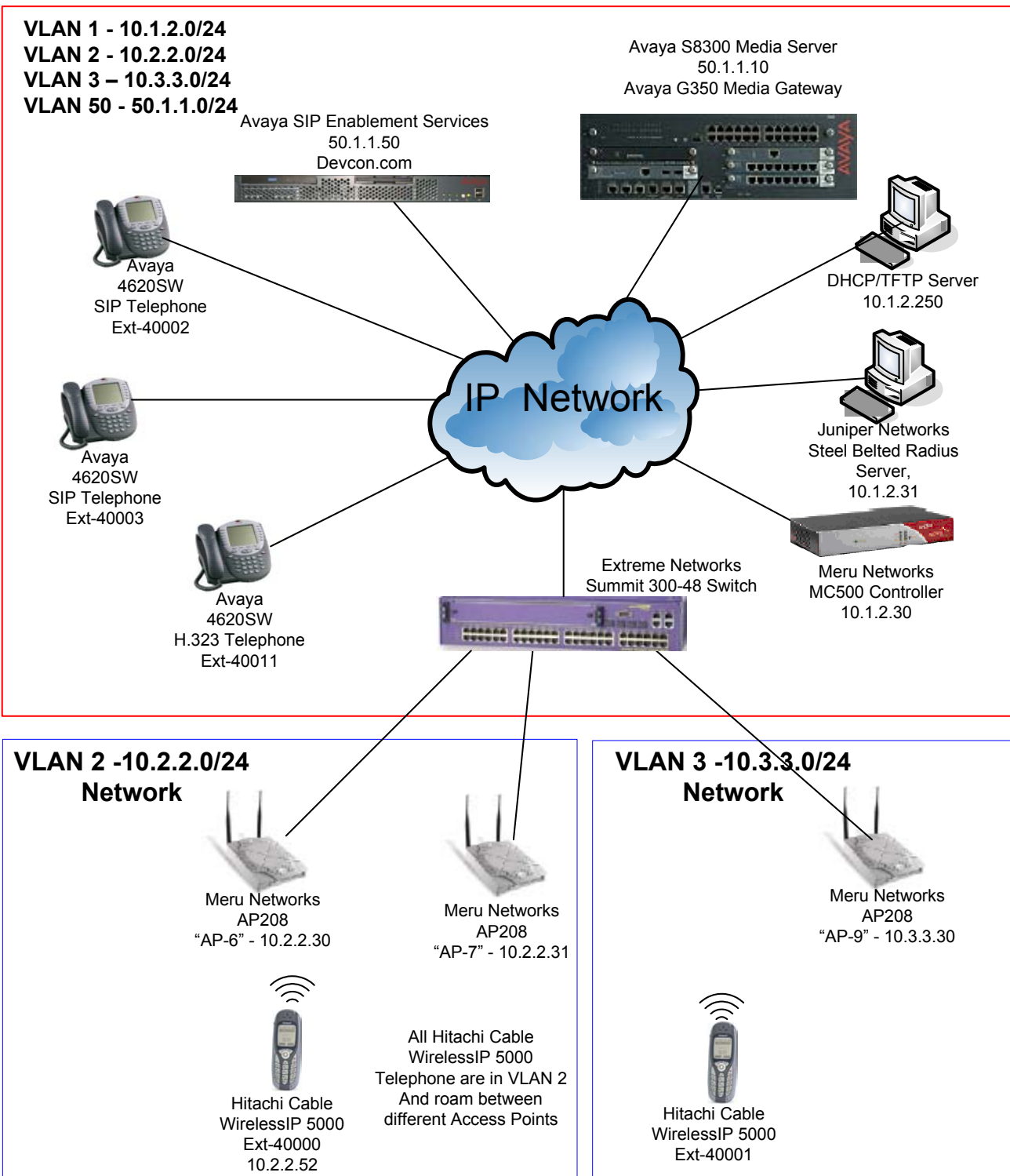


Figure 1: Sample Network Configuration

2. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300 Media Server with Avaya G350 Media Gateway	Communication Manager 3.1 (R03.1-01.0.628.6)
Avaya SIP Enablement Services (SES)	3.1 (build 18)
Avaya 4610SW/4620SW SIP Telephones	2.2.21a
Avaya 4620SW H.323 IP Telephone	2.2.3
Extreme Networks Summit 300-48 Switch	ExtremeWare 7.4e.1.5
Meru Networks MC500 Controller	3.1.3-7
Meru Networks AP208	N/A
Juniper Networks Steel Belted Radius Server	5.03.1532
Hitachi Cable WirelessIP 5000 telephone	Software release 2.2.1 Boot Rom 1.0.4

3. Configure Avaya Communication Manager

This section highlights the important commands for defining SIP telephones on Avaya Communication Manager. For complete documentation, see references [1], [2], [4], [5], and [6]. Use the System Access Terminal (SAT) interface to perform these steps. Log in with the appropriate credentials.

3.1. Verify OPS Capacity

Use the display **system-parameters customer-options** command to verify that **Maximum Off-PBX Telephones – OPS** has been set to a value that will accommodate the number of phones to be supported. Contact Avaya or Avaya Business Partner to increase or change the maximum Off-PBX-Telephones allowed.

```
change system-parameters customer-options                               Page 1 of 10
                                OPTIONAL FEATURES
G3 Version: V13
Location: 1
Platform: 13
Location: 1
Platform: 13
                                RFA System ID (SID): 1
                                RFA Module ID (MID): 1
                                USED
                                Platform Maximum Ports: 900 48
                                Maximum Stations: 40 20
                                Maximum XMOBILE Stations: 0 0
                                Maximum Off-PBX Telephones - EC500: 50 0
                                Maximum Off-PBX Telephones - OPS: 50 10
                                Maximum Off-PBX Telephones - SCCAN: 0 0
(NOTE: You must logoff & login to effect the permission changes.)
```

3.2. Add New Stations to Avaya Communication Manager

Using the **add station** command, add a station for each SIP phone to be supported. The sample configuration uses **6408D+** for the station type. The **Port** must be set to **X**, since this will be used as SIP Station. Use the appropriate COS value. Make sure that the station has three (3) **call-appr** buttons for **Button Assignment**. The number of call-appr buttons must match the call limit set in the **off-pbx-telephone station-mapping** command for this extension, which will be configured in a later step. Repeat the following steps to add additional SIP telephone extensions.

add station 40000		Page 1 of 4
STATION		
Extension: 40000	Lock Messages? n	BCC: 0
Type: 6408D+	Security Code:	TN: 1
Port: X	Coverage Path 1	COR: 1
Name: SIP40000	Coverage Path 2:	COS: 1
STATION OPTIONS		
Loss Group: 2		
Data Module? n		
Speakerphone: 2-way		
Display Language: english		
Loss Group: 2	Personalized Ringing Pattern: 1	
Data Module? n	Message Lamp Ext: 40000	
Speakerphone: 2-way	Mute Button Enabled? y	
	Media Complex Ext:	
	IP SoftPhone? N	

add station 40000		Page 3 of 4
STATION		
SITE DATA		
Room:	Headset? n	
Jack:	Speaker? n	
Cable:	Mounting: d	
Floor:	Cord Length: 0	
Building:	Set Color:	
ABBREVIATED DIALING		
List1:	List2:	List3:
BUTTON ASSIGNMENTS		
1: call-appr	5:	
2: call-appr	6:	
3: call-appr	7:	

Use the **change off-pbx-telephone station-mapping** command to map Avaya Communication Manager extensions to the Avaya SIP Enablement Services (SES) extensions. The **Station Extension** is the extension number configured with the **add station** command. The **Phone Number** is the number that will be used in SES for the media server extension. Make sure the **Call Limit** is equal to the number of call-appr buttons set using the **add station** command. In the **Trunk Selection** field, enter the trunk-group number for the trunk-group configured between Avaya Communication Manager and the Avaya SIP Enablement Services server. Select the **Configuration Set** number applicable for this configuration. The sample configuration uses **Configuration Set 1**. For additional information related to Avaya Communication Manager and Off-PBX-Station support, refer to references [2], [4], and [5].

change off-pbx-telephone station-mapping 40000					Page 1 of 2
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION					
Station Extension	Application	Dial Prefix	Phone Number	Trunk Selection	Configuration Set
40000	OPS	-	40000	1	1
40001	OPS	-	40001	1	1
change off-pbx-telephone station-mapping 40000					Page 2 of 2
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION					
Station Extension	Call Limit	Mapping Mode	Calls Allowed	Bridged Calls	
40000	3	both	all	both	
40001	3	both	all	both	

The screenshot below shows the settings for **trunk-group 1**.

display trunk-group 1		Page 1 of 20	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: To CCS	COR: 1	TN: 1	TAC: 101
Direction: two-way	Outgoing Display? n		
Dial Access? n	Busy Threshold: 255	Night Service:	
Queue Length: 0			
Service Type: tie	Auth Code? n		
		Signaling Group: 1	
		Number of Members: 24	
TRUNK PARAMETERS			
Unicode Name? y			
		Redirect On OPTIM Failure: 5000	
SCCAN? n	Digital Loss Group: 18		

The screenshot below shows the settings for **configuration-set 1**.

change off-pbx-telephone configuration-set 1	Page 1 of 1
CONFIGURATION SET: 1	
Configuration Set Description: Remote Extension	
Calling Number Style: network	
CDR for Origination: phone-number	
CDR for Calls to EC500 Destination? y	
Fast Connect on Origination? n	
Post Connect Dialing Options: dtmf	
Cellular Voice Mail Detection: none	
Barge-in Tone? n	
Identity When Bridging: principal	

3.3. IP Network Region

Use the **display ip-network-region** command to verify the **UDP Port Min** and **UDP Port Max** settings. These should match the **RTP Port Min** and **RTP Port Max** settings in the Hitachi WirelessIP 5000 in Section 7.5 Step 4. Note the **Call Control PHB Value** and **Audio PHB Value**. The **Signal DSCP** and **Voice DSCP** values set in Section 7.2 Step 5 should be set to the same value.

```
change ip-network-region 1                                     Page 1 of 19
                                                                IP NETWORK REGION

Region: 1
Location: 1           Authoritative Domain: devcon.com
MEDIA PARAMETERS
  Codec Set: 1           Intra-region IP-IP Direct Audio: yes
                        Inter-region IP-IP Direct Audio: yes
                        IP Audio Hairpinning? y
  UDP Port Min: 2048
  UDP Port Max: 3028
DIFFSERV/TOS PARAMETERS
  Call Control PHB Value: 46   RTCP Reporting Enabled? y
  Audio PHB Value: 46         RTCP MONITOR SERVER PARAMETERS
  Video PHB Value: 26         Use Default Server Parameters? y
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
  H.323 Link Bounce Recovery? y   RSVP Enabled? n
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
  Keep-Alive Count: 5
```

3.4. Configure Audio Codec

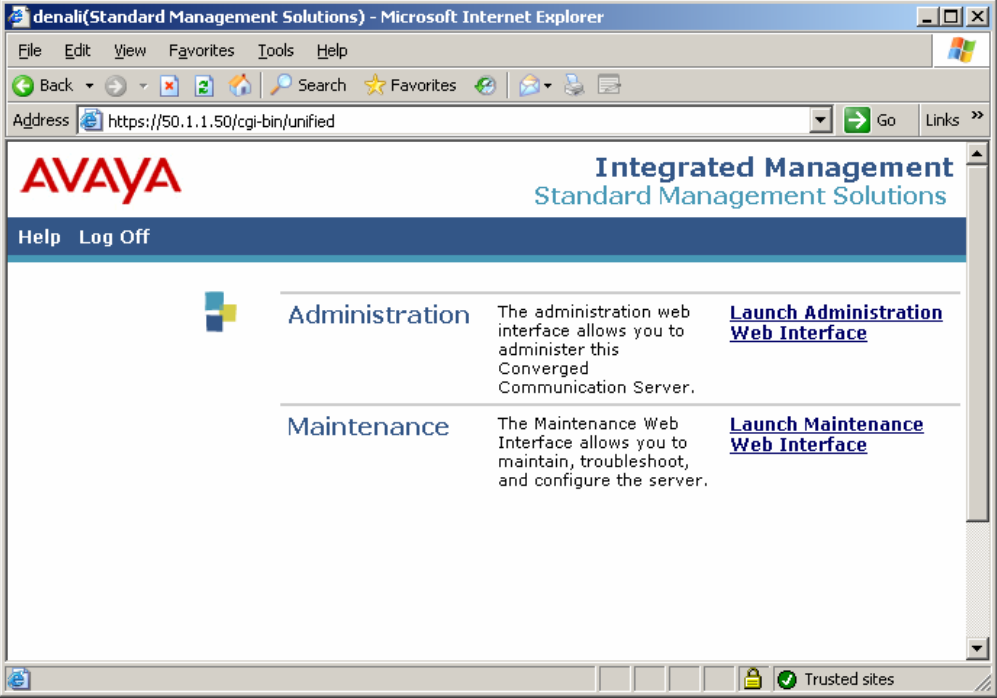
Use the **change ip-codec-set** command to configure the codec set Avaya Communication Manager and Avaya telephones will use to communicate with the WirelessIP 5000 handset. Both G.711MU and G.729AB codecs are supported by WirelessIP 5000 handset.

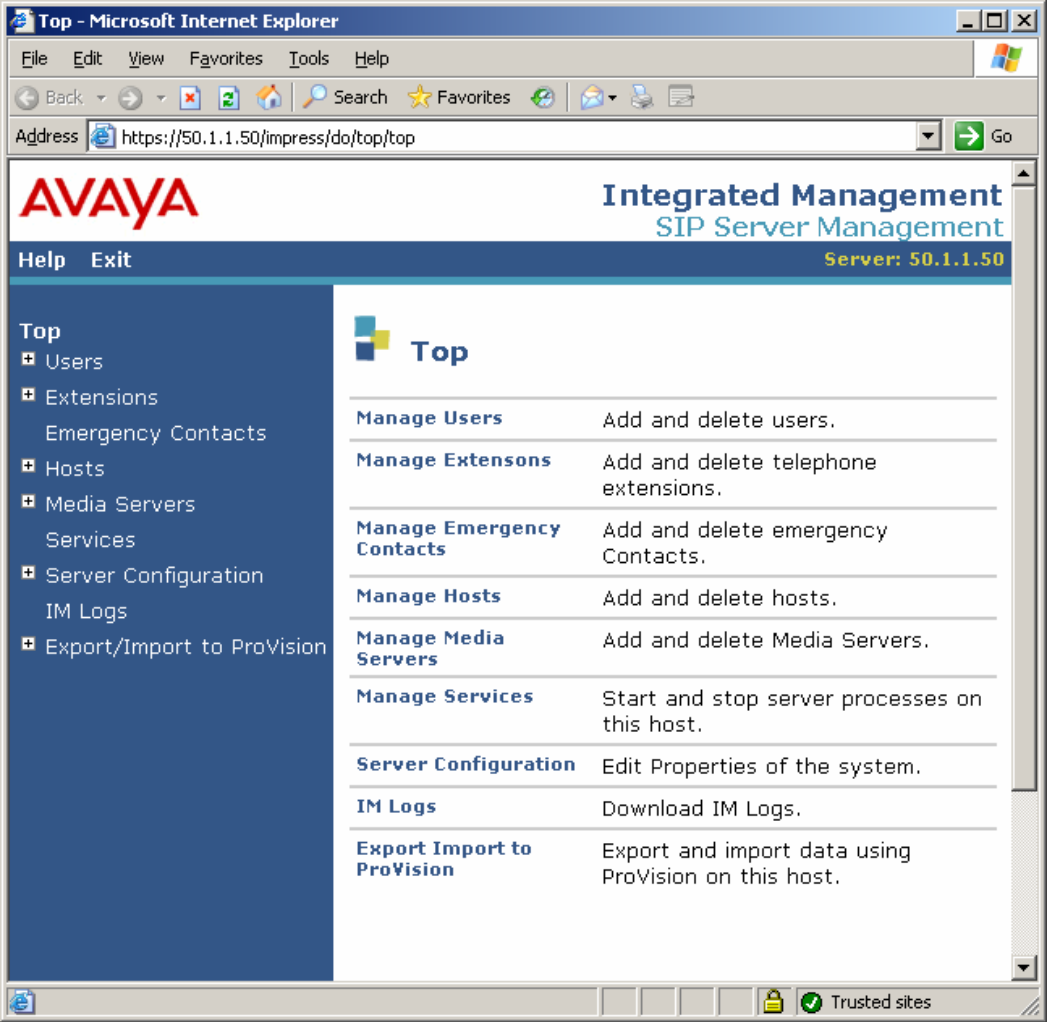
```
change ip-codec-set 1                                         Page 1 of 2
                                                                IP Codec Set

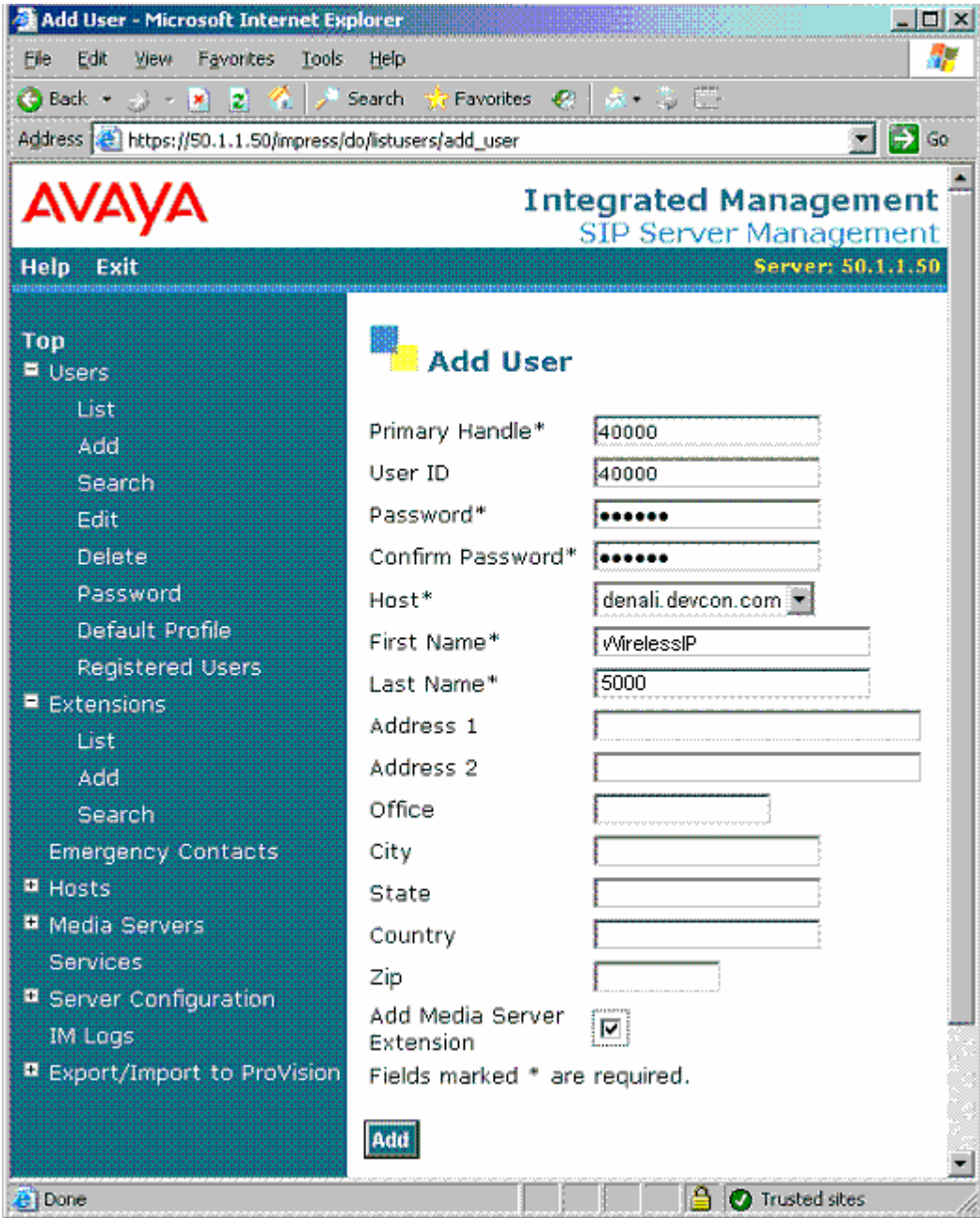
Codec Set: 1
Audio      Silence      Frames      Packet
Codec      Suppression   Per Pkt    Size(ms)
1: G.711MU      n           2          20
2: G.729AB      n           2          20
```


4. Configure Avaya SIP Enablement Services

The following steps describe the configuration of the Avaya SIP Enablement Services (SES) to support WirelessIP 5000 handset.

Step	Description
1.	<p>Avaya SES is configured using a web browser. Set the URL to the IP address of the SES, and log in using appropriate user name and password. The URL in the sample configuration is https://50.1.1.50/admin. Select Launch Administration Web Interface to continue.</p> 

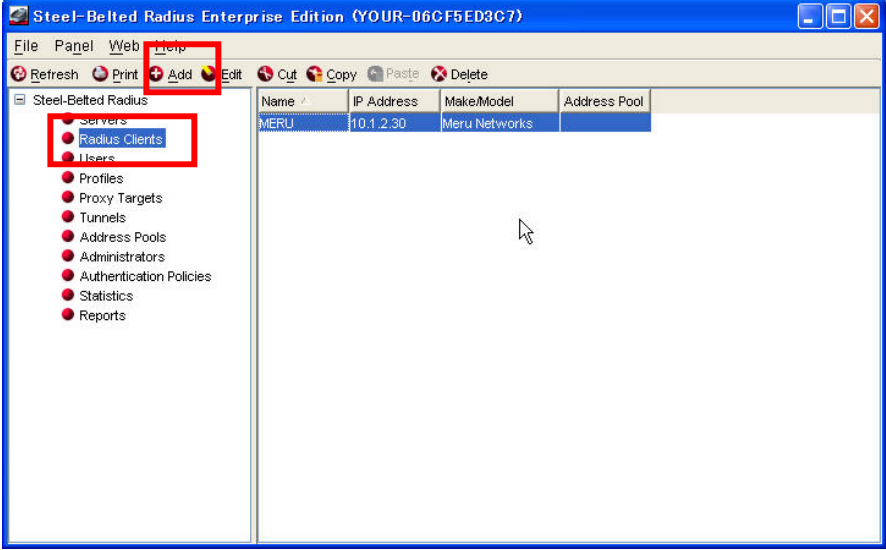
Step	Description																				
2.	<p>Click on the “+” sign next to Users on the left side to expand the selection. Select Add from the list under Users to add a new user.</p>  <table border="1" data-bbox="673 661 1323 1165"> <thead> <tr> <th colspan="2">Top</th> </tr> </thead> <tbody> <tr> <td>Manage Users</td> <td>Add and delete users.</td> </tr> <tr> <td>Manage Extensions</td> <td>Add and delete telephone extensions.</td> </tr> <tr> <td>Manage Emergency Contacts</td> <td>Add and delete emergency Contacts.</td> </tr> <tr> <td>Manage Hosts</td> <td>Add and delete hosts.</td> </tr> <tr> <td>Manage Media Servers</td> <td>Add and delete Media Servers.</td> </tr> <tr> <td>Manage Services</td> <td>Start and stop server processes on this host.</td> </tr> <tr> <td>Server Configuration</td> <td>Edit Properties of the system.</td> </tr> <tr> <td>IM Logs</td> <td>Download IM Logs.</td> </tr> <tr> <td>Export Import to ProVision</td> <td>Export and import data using ProVision on this host.</td> </tr> </tbody> </table>	Top		Manage Users	Add and delete users.	Manage Extensions	Add and delete telephone extensions.	Manage Emergency Contacts	Add and delete emergency Contacts.	Manage Hosts	Add and delete hosts.	Manage Media Servers	Add and delete Media Servers.	Manage Services	Start and stop server processes on this host.	Server Configuration	Edit Properties of the system.	IM Logs	Download IM Logs.	Export Import to ProVision	Export and import data using ProVision on this host.
Top																					
Manage Users	Add and delete users.																				
Manage Extensions	Add and delete telephone extensions.																				
Manage Emergency Contacts	Add and delete emergency Contacts.																				
Manage Hosts	Add and delete hosts.																				
Manage Media Servers	Add and delete Media Servers.																				
Manage Services	Start and stop server processes on this host.																				
Server Configuration	Edit Properties of the system.																				
IM Logs	Download IM Logs.																				
Export Import to ProVision	Export and import data using ProVision on this host.																				

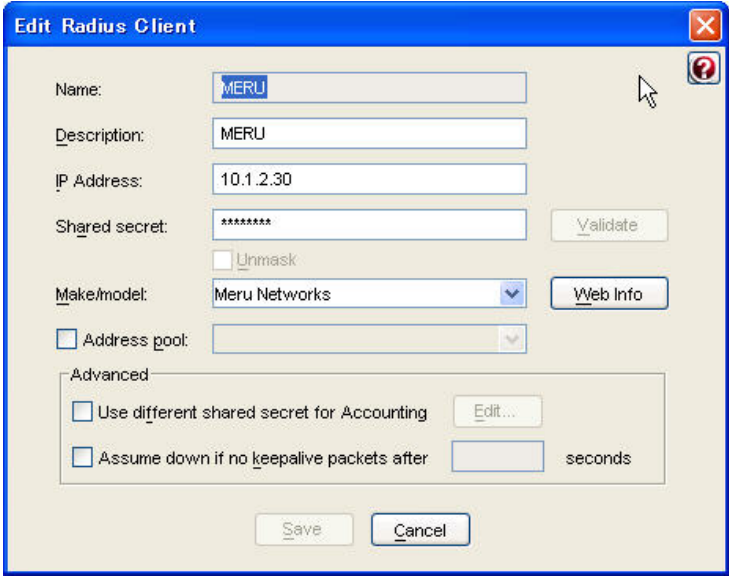
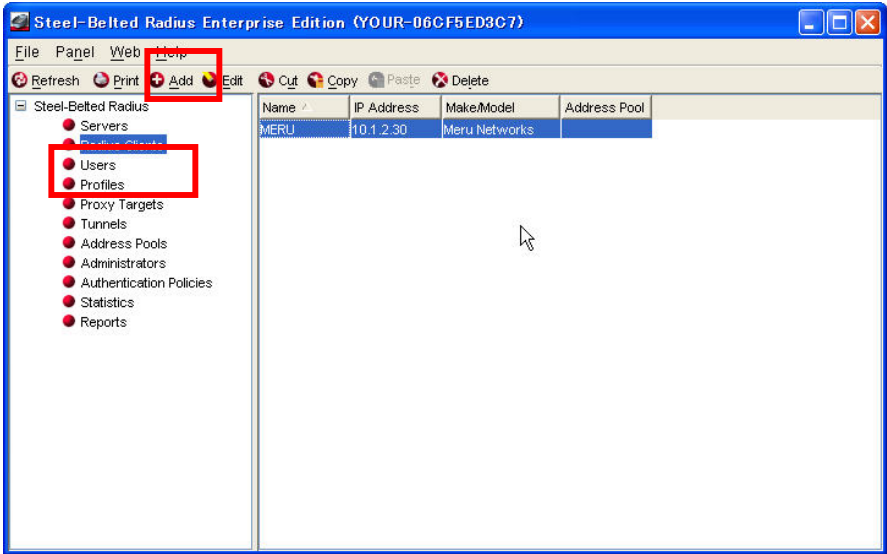
Step	Description
3.	<p>Enter the phone number in both the Primary Handle and User ID. Enter the password for this extension. Select the appropriate SES server for the Host field. The First Name and Last Name are for informational purpose only, but are required fields. Check the Add Media Server Extension field at the bottom. Click Add to continue.</p>
	 <p>The screenshot shows the 'Add User' form in the Avaya Integrated Management SIP Server Management interface. The form is displayed in a Microsoft Internet Explorer window with the address bar showing 'https://50.1.1.50/impress/do/listusers/add_user'. The Avaya logo and 'Integrated Management SIP Server Management' text are at the top. A sidebar on the left contains a navigation menu with options like Users, Extensions, Hosts, Media Servers, etc. The main form area contains the following fields and controls:</p> <ul style="list-style-type: none"> Primary Handle*: Text input field containing '40000'. User ID: Text input field containing '40000'. Password*: Password input field with masked characters '.....'. Confirm Password*: Password input field with masked characters '.....'. Host*: Dropdown menu showing 'denali.devcon.com'. First Name*: Text input field containing 'vWirelessIP'. Last Name*: Text input field containing '5000'. Address 1: Text input field. Address 2: Text input field. Office: Text input field. City: Text input field. State: Text input field. Country: Text input field. Zip: Text input field. Add Media Server Extension: A checkbox that is checked. Fields marked * are required.: A note at the bottom of the form. Add: A button at the bottom left of the form.

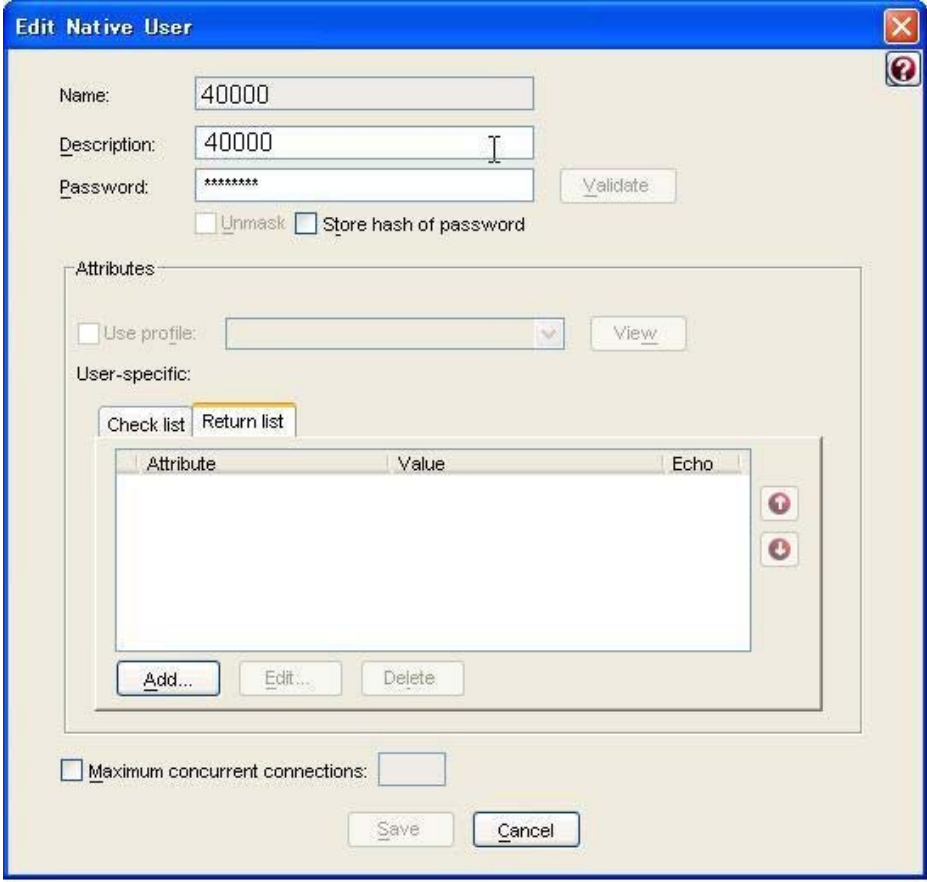
Step	Description
4.	<p>Type in the phone number in the Extension field. The Extension field must match the extension configured in Section 3.2. Click Add to complete.</p> 
5.	Click update on the bottom of the left blue panel to implement all the changes.

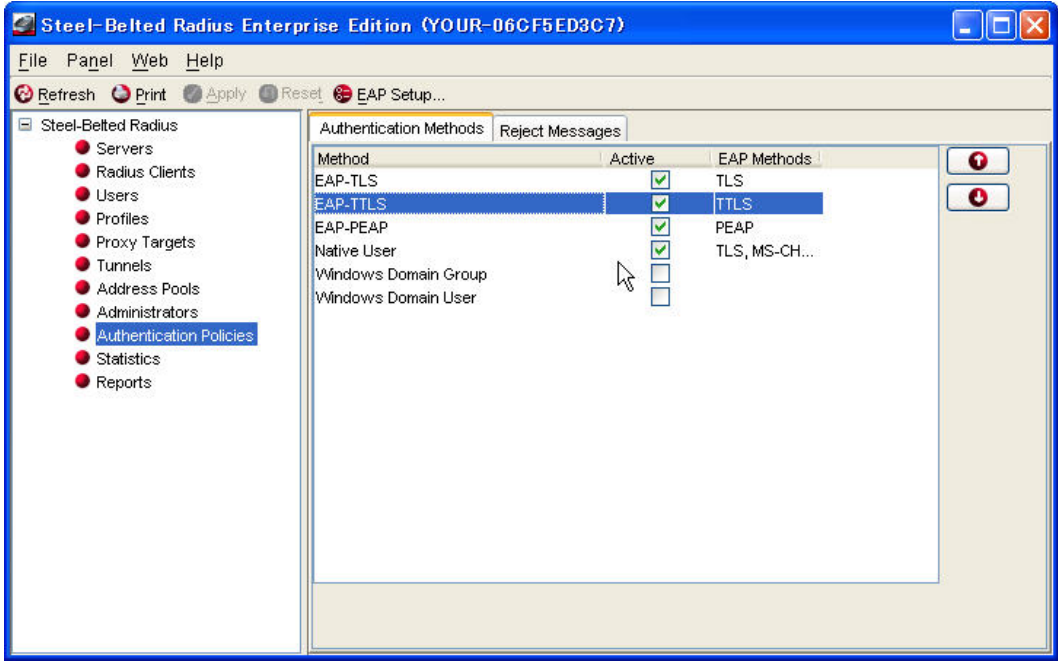
5. Configure the Juniper Networks Steel Belted Radius (SBR) Server

The following steps describe the configuration for the Steel Belted Radius Server in the sample configuration.

Step	Description
1.	<p>From the Steel Belted Radius Server GUI, select the Radius Clients field on the left. Click Add from the menu bar to display the Add Radius Client pop-up window.</p> 

Step	Description
2.	<p>The following Edit Radius Client pop-up window shows the information that needs to be entered to add a Radius Client. The IP address is the address of the Meru Controller. Enter a Shared secret string. This same string will be needed in configuring the Meru Controller in Section 5 Step 5. Click Save to complete.</p> 
3.	<p>From the Steel Belted Radius Server GUI, select the Users field on the left. Click Add from the menu bar to display the Add Native Users pop-up window.</p> 

Step	Description
4.	<p>The following Edit Native User pop-up window shows the information that needs to be entered to add a Native User. Enter a Name, Description and Password for the new user. The name is the station number. Click Save to complete. This Name and Password will need to be entered into the WirelessIP 5000 handset. Repeat Step 3 and 4 for each WirelessIP 5000 handset.</p> 

Step	Description
5.	<p>From the Steel Belted Radius Server GUI, select the Authentication Policies field on the left. Click the check box for EAP-TTLS to make it Active.</p> 

6. Configure the Meru Networks MC500 Controller

The following steps describe the configuration for the Meru Networks wireless setup in the sample configuration.

Step	Description
1.	<p>To perform the initial configuration of the Meru Networks MC500 Controller, set up a serial connection from a PC or laptop. On the PC or laptop, set up a terminal session as follows:</p> <ul style="list-style-type: none"> ▪ 115200 baud ▪ 8 bits ▪ no parity ▪ 1 stop bit <p>Log in via the Meru command-line interface (CLI) using appropriate credentials. The CLI prompt displayed depends on the hostname of the MC500 Controller. At the CLI prompt, type configure terminal to enter configuration mode. After assigning an IP address to the MC500 Controller in the step below, a telnet session may be used to access the CLI of the MC500 Controller.</p>


Step	Description
2.	<p>Assign a host name, IP address, and default gateway to the MC500 Controller. In addition, specify the IP address of the DHCP server. This enables DHCP relay on the MC500 Controller to allow dynamic IP addressing for the wireless IP endpoints. The MC500 Controller does not get its IP address from the DHCP server.</p> <pre> MC500# configure terminal MC500 (config)# hostname MC500 MC500 (config)# ip address 10.1.2.30 255.255.255.0 MC500 (config)# ip default-gateway 10.1.2.1 MC500 (config)# ip dhcp-server 10.1.2.250 </pre>
3.	<p>Configure the three Access Points (APs) in the WLAN configuration depicted in Figure 1. AP-6, AP-7 and AP-9 are in different subnets than the MC500 Controller. Therefore these APs are configured for Layer 3 connectivity, which requires the MC500 Controller IP address to be specified.</p> <pre> MC500 (config)# ap 6 MC500 (config)# description AP-6 MC500 (config)# mac-address 00:0c:e6:00:40:58 MC500 (config-ap)# connectivity l3-preferred MC500 (config-ap-connectivity)# ip address 10.2.2.30 255.255.255.0 MC500 (config-ap-connectivity)# ip default-gateway 10.2.2.1 MC500 (config-ap-connectivity)# controller ip 10.1.2.30 MC500 (config-ap-connectivity)# end MC500 (config)# ap 7 MC500 (config)# description AP-7 MC500 (config)# mac-address 00:0c:e6:00:40:6c MC500 (config-ap)# connectivity l3-preferred MC500 (config-ap-connectivity)# ip address 10.2.2.31 255.255.255.0 MC500 (config-ap-connectivity)# ip default-gateway 10.2.2.1 MC500 (config-ap-connectivity)# controller ip 10.1.2.30 MC500 (config-ap-connectivity)# end MC500 (config)# ap 9 MC500 (config)# description AP-9 MC500 (config)# mac-address 00:0c:e6:00:3e:e1 MC500 (config-ap)# connectivity l3-preferred MC500 (config-ap-connectivity)# ip address 10.3.3.30 255.255.255.0 MC500 (config-ap-connectivity)# ip default-gateway 10.3.3.1 MC500 (config-ap-connectivity)# controller ip 10.1.2.30 MC500 (config-ap-connectivity)# end </pre>


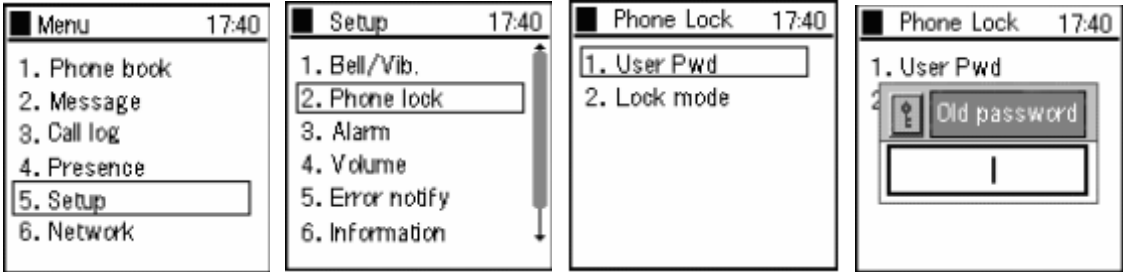

Step	Description
4.	<p>The Hitachi WirelessIP 5000 that register with Avaya SIP Enablement Services are all assigned to VLAN 2. Create a VLAN named vlan2 with a tag of 2. Assign an IP address, default gateway, and DHCP server to the VLAN interface. This enables 802.1Q trunking on the MC500 Controller for VLAN 2 only. In this configuration, VLAN 2 was mapped to ESSID sip, to be configured in Step 6.</p> <pre>MC500 (config)# vlan vlan2 tag 2 MC500 (config-vlan)# ip address 10.2.2.35 255.255.255.0 MC500 (config-vlan)# ip default-gateway 10.2.2.1 MC500 (config-vlan)# ip dhcp-server 10.1.2.250 MC500 (config-vlan)# exit</pre>
5.	<p>To require the wireless IP endpoints to use RADIUS authentication, create a security profile that will be assigned to the ESSID in Step 6. Security profile eap was configured to support 802.1x authentication. The key must match the Shared Secret configured in Section 5 Step 2.</p> <pre>MC500 (config)# radius-profile RADIUS-SRV MC500 (config-radius)# ip-address 10.1.2.31 MC500 (config- radius)# key 1234 MC500 (config- radius)# exit MC500 (config)# security-profile radius MC500 (config-security)# allowed-l2-modes 802.1x MC500 (config-security)# encryption-modes wep128 MC500 (config-security)# radius-server primary RADIUS-SRV MC500 (config-security)# exit</pre>
6.	<p>Create ESSID EAP and assign security profile radius and VLAN2 that was created in Step 4 to this ESSID.</p> <pre>MC500 (config)# essid EAP MC500 (config-essid)# security-profile radius MC500 (config-essid)# vlan name vlan2 MC500 (config-essid)# vlan support radius-and-configured-vlan MC500 (config-essid)# ssid EAP MC500 (config-essid)# ap-discovery join-virtual-ap MC500 (config-essid)# exit</pre>
7.	<p>After making the configuration changes, save the changes using the following command:</p> <pre>MC500# copy running-config startup-config</pre>
8.	<p>Some configuration commands require a MC500 Controller reboot for the changes to take effect. To manually reboot the MC500 Controller and its associated Access Points, use the following command:</p> <pre>MC500# reload all</pre>

7. Configure the Hitachi Cable WirelessIP 5000


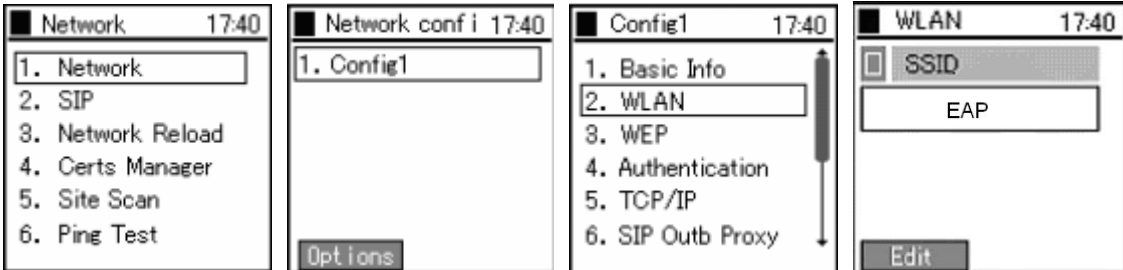
The following steps describe the configuration for the Hitachi Cable WirelessIP 5000 telephone to interoperate with Avaya SIP Enablement Services (SES).

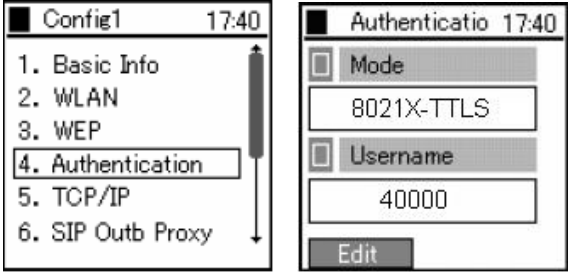
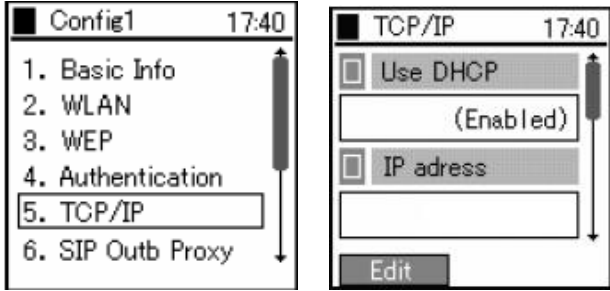
7.1. Log into the Hitachi Cable WirelessIP 5000

Step	Description
1.	<p>The Hitachi Cable WirelessIP 5000 telephone is shown below. Some of the buttons are highlighted to facilitate referencing in this document.</p>  <p>Note: A full explanation of the Hitachi Cable WirelessIP 5000 is beyond the scope of this document. Refer to the Hitachi Cable documentation [8] for additional details.</p>
2.	<p>Press and hold the END Key to turn on the Hitachi Cable WirelessIP 5000.</p>

Step	Description
3.	<p data-bbox="277 163 1382 195">Begin configuration by pressing the LeftSoft key. This will display the Menu screen.</p>  <p data-bbox="277 541 1382 646">From the Menu screen, press the key sequence “5”, “2”, “1” (Setup→Phone lock→User Pwd) to display the login prompt. Enter the appropriate password and press in the Joystick to enter.</p> <div data-bbox="277 688 1393 957">  </div> <p data-bbox="277 999 1040 1031">The Admin menu screen below will appear after logging in.</p> 

7.2. Network Configuration for Hitachi Cable WirelessIP 5000

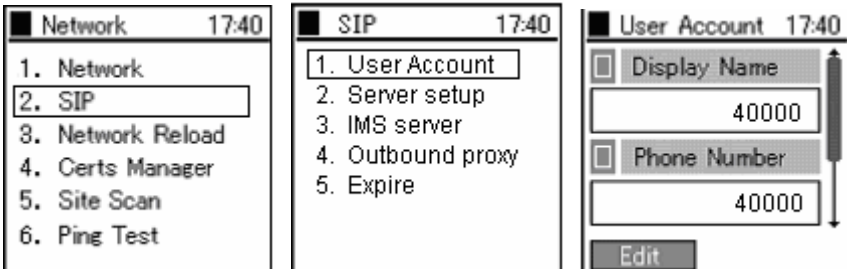
Step	Description
1.	<p>From the Admin menu screen, press “1” to select Network.</p>  <p>From the Network menu screen, press the key sequence “1”, “1”, “2” (Network→Config1→WLAN) to access the WLAN screen. Press the LeftSoft key to select Edit. Use the keypad to enter the SSID, which must match the SSID configured on the wireless network. The sample configuration uses the SSID EAP. Press in the Joystick to save.</p>  <p>Note: Push the LeftSoft key and push the Joystick left/right to change between Upper/Lower case letters, special characters or numbers. Press in the Joystick to select the highlighted selection. Press the CLR key to move back up one menu screen.</p>

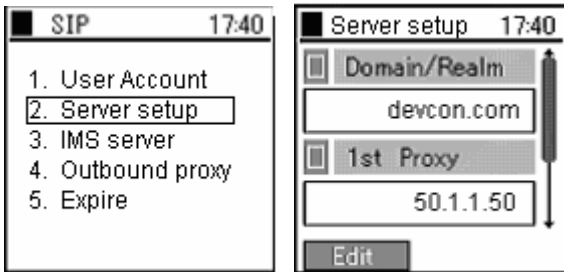
Step	Description
<p>2.</p>	<p>From Config1 menu screen, press “4” (Authentication) to display the Authentication menu screen. Press the LeftSoft key to edit.</p> <div data-bbox="277 268 841 537">  </div> <ol style="list-style-type: none"> 1. Push the joystick to the left or right in the Mode field until the desired authentication mode is displayed. The sample configuration uses 8021X-TTLS for authentication. 2. Push downward on the joystick to highlight the Username field. Enter a user name that is configured on the Steel Belted RADIUS (SBR) Server in Section 5 Step 4. 3. Push downward on the joystick to highlight the Password field (not shown above). Enter the Password that was configured in Section 5 Step 4. 4. Press in on the joystick to save.
<p>3.</p>	<p>From the Config1 menu screen, press “5” (TCP/IP) to display the TCP/IP menu screen. Press the LeftSoft key to edit.</p> <div data-bbox="277 978 883 1266">  </div> <ol style="list-style-type: none"> 1. Push the joystick to the left or right in the Use DHCP field to Enable DHCP on the WirelessIP 5000 handset. This allows the WirelessIP 5000 to automatically obtain an IP address from the DHCP Server. 2. Press in on the joystick to save.

Step	Description									
4.	<p>From the Config1 menu screen, press “6” (SIP Outb Proxy) to display the SIP Outb Proxy menu screen. Press the LeftSoft key to edit. Use the keypad on the Hitachi Cable WirelessIP 5000 telephone to enter the IP address of the Avaya SIP Enablement Services (SES) Server. The Avaya SIP Enablement Services Server in the sample network has IP address 50.1.1.50. Press in the Joystick to save.</p> <div><div><div>■ Config1 17:40</div><div><div>1. Basic Info</div><div>2. WLAN</div><div>3. WEP</div><div>4. Authentication</div><div>5. TCP/IP</div><div>6. SIP Outb Proxy</div></div></div><div><div>■ SIP Outb Prox 17:40</div><div><div>□ Config1</div><div>50.1.1.50</div></div><div>Edit</div></div></div>									
5.	<p>From the Config1 menu screen, press “8”(IP DiffServ) to display the IP DiffServ menu screen. Press the LeftSoft key to edit. Use the keypad on the phone to enter the appropriate DiffServ value in hex. The sample configuration uses the value below. This is also the same value configured in the ip-network-region of Avaya Communication Manager.</p> <table><tr><td></td><td>Hex</td><td>Decimal</td></tr><tr><td>Signal DSCP</td><td>0x2e</td><td>46</td></tr><tr><td>Voice DSCP</td><td>0x2e</td><td>46</td></tr></table> <div><div><div>■ Config1 17:40</div><div><div>3. WEP</div><div>4. Authentication</div><div>5. TCP/IP</div><div>6. SIP Outb Proxy</div><div>7. NAT Traversal</div><div>8. IP DiffServ</div></div></div><div><div>■ IP DiffServ 17:40</div><div><div>□ Signal DSCP</div><div>0x2e</div><div>□ Voice DSCP</div><div>0x2e</div></div><div>Edit</div></div></div>		Hex	Decimal	Signal DSCP	0x2e	46	Voice DSCP	0x2e	46
	Hex	Decimal								
Signal DSCP	0x2e	46								
Voice DSCP	0x2e	46								

7.3. SIP Configuration for the Hitachi Cable WirelessIP 5000

The following steps describe the SIP configuration for the Hitachi Cable WirelessIP 5000 telephone.

Step	Description										
1.	<p>From the Network menu screen, press the key sequence “2”, “1” (SIP→User Account) to display the User Account menu screen.</p> <div></div> <p>Press the LeftSoft key to edit. Push the Joystick upward or downward to scroll and enter the following information. The sample below uses extension 40000. The User Password must match what is configured in the Avaya SIP Enablement Services server for the extension being configured.</p> <table><tr><td>Display Name</td><td>40000</td></tr><tr><td>Phone Number</td><td>40000</td></tr><tr><td>User ID</td><td>40000</td></tr><tr><td>User Password</td><td>123456</td></tr><tr><td>URL scheme</td><td>sip</td></tr></table> <p>Press in the Joystick to save and return to the SIP menu screen.</p> <p>Note: Make sure that each Hitachi Cable WirelessIP 5000 telephone has the appropriate User ID and User Password as this information will be used to register the phone with the Avaya SIP Enablement Services Server.</p>	Display Name	40000	Phone Number	40000	User ID	40000	User Password	123456	URL scheme	sip
Display Name	40000										
Phone Number	40000										
User ID	40000										
User Password	123456										
URL scheme	sip										

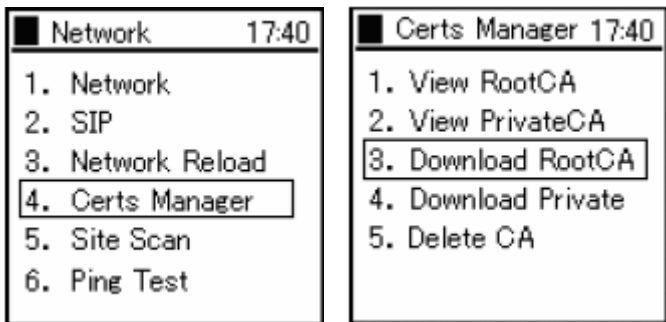

Step	Description						
2.	<p>From the SIP menu screen, press “2” (Server setup) to display the Server setup menu screen.</p> <div></div> <p>Press the LeftSoft key to edit. Push the Joystick upward or downward to scroll and enter the Domain/Realm and 1st Proxy information. Press in the Joystick to save and return to the SIP menu screen.</p> <p>The sample configuration uses the following information:</p> <table><tr><td>Domain/Realm</td><td><i>devcon.com</i></td><td>Domain of the SES server</td></tr><tr><td>1st Proxy</td><td><i>50.1.1.50</i></td><td>IP address of the SES server</td></tr></table>	Domain/Realm	<i>devcon.com</i>	Domain of the SES server	1st Proxy	<i>50.1.1.50</i>	IP address of the SES server
Domain/Realm	<i>devcon.com</i>	Domain of the SES server					
1st Proxy	<i>50.1.1.50</i>	IP address of the SES server					
3.	Press the END key to exit out of the menu.						

7.4. Loading of the Certificate on the Hitachi Cable WirelessIP 5000

The following steps describe the steps necessary to load the Certificate onto the WirelessIP 5000 handset required for 802.1X authentication.

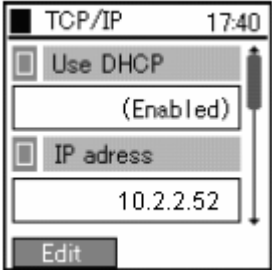
Note: The issuance and administration of the authentication Certificate is beyond the scope of this document.

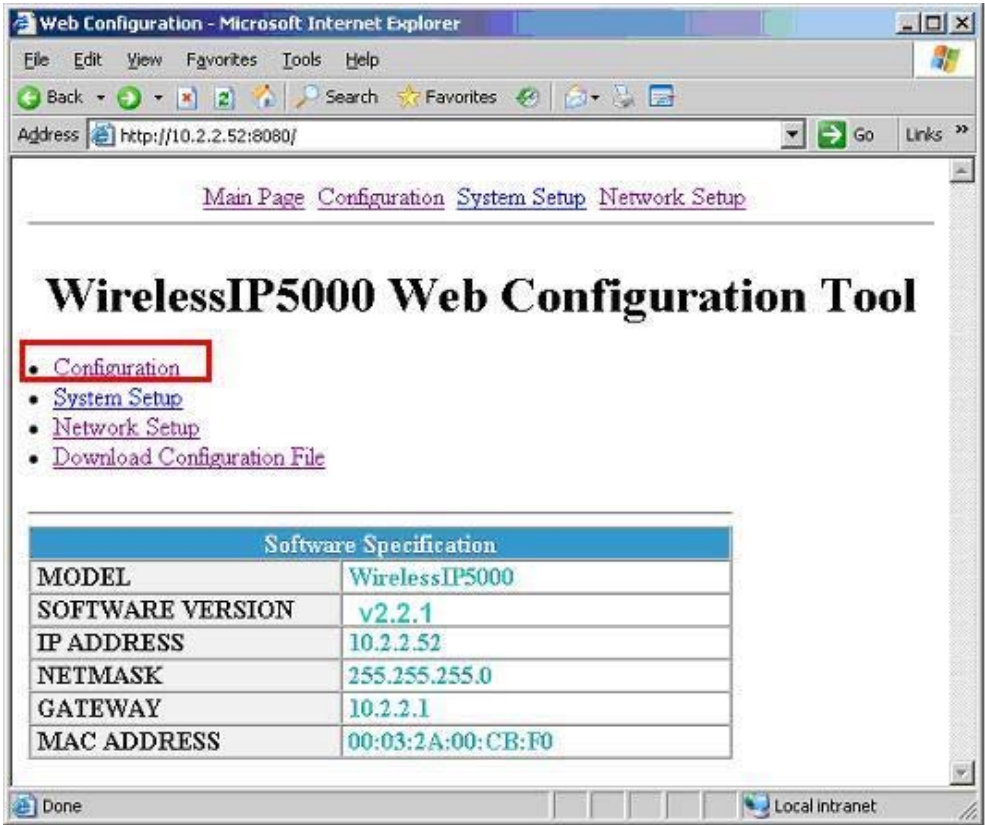
To download the Certificate from the TFTP Server to the WirelessIP 5000 handset, it must be able to connect to the wireless network. Therefore, it may be necessary to associate the handset with another SSID that does not require 802.1X authentication, download the certificate, then reconfigure the handset to use 802.1X authentication. Consult the Hitachi Cable documents [7] and [8] for additional methods for downloading the certificate to the WirelessIP 5000.

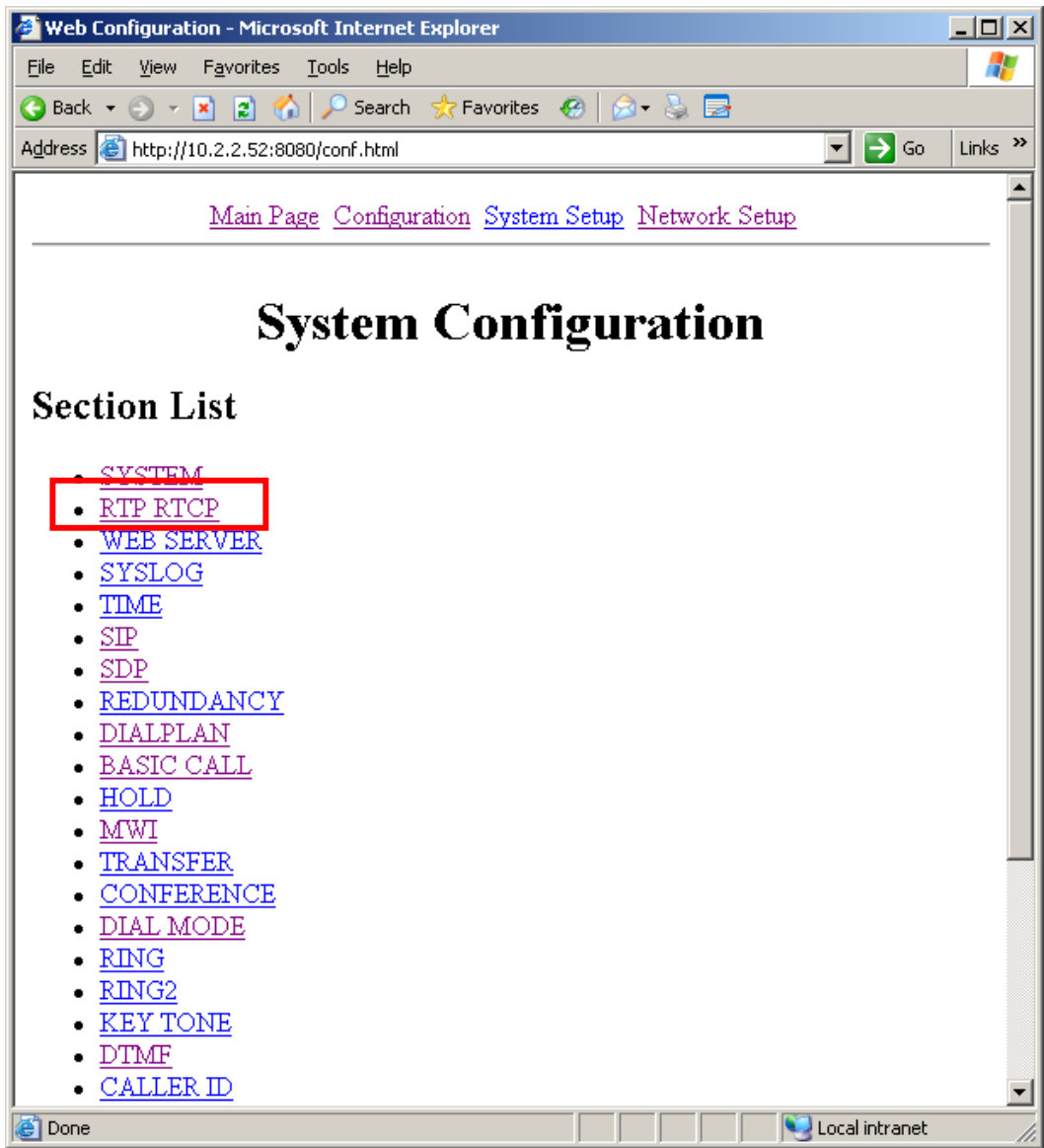
Step	Description
1.	<p data-bbox="277 195 1404 268">From the Network menu screen, press “4” (Certs Manager) to display the Certs manager menu screen. Press “3” (Download RootCA) to begin the download process.</p> <div data-bbox="277 300 938 619">  </div> <p data-bbox="277 657 1404 835">A warning message is displayed. Press down on the Joystick to acknowledge the warning message. Push the joystick to left or right to select Yes for “Upgrade Root Certificate?” and press down on the Joystick. Enter the TFTP server IP address using the handset keypad. Use the “*” to enter the dot. Press in the Joystick to save and begin download of the Certificate.</p> <div data-bbox="277 873 1261 1192">  </div>

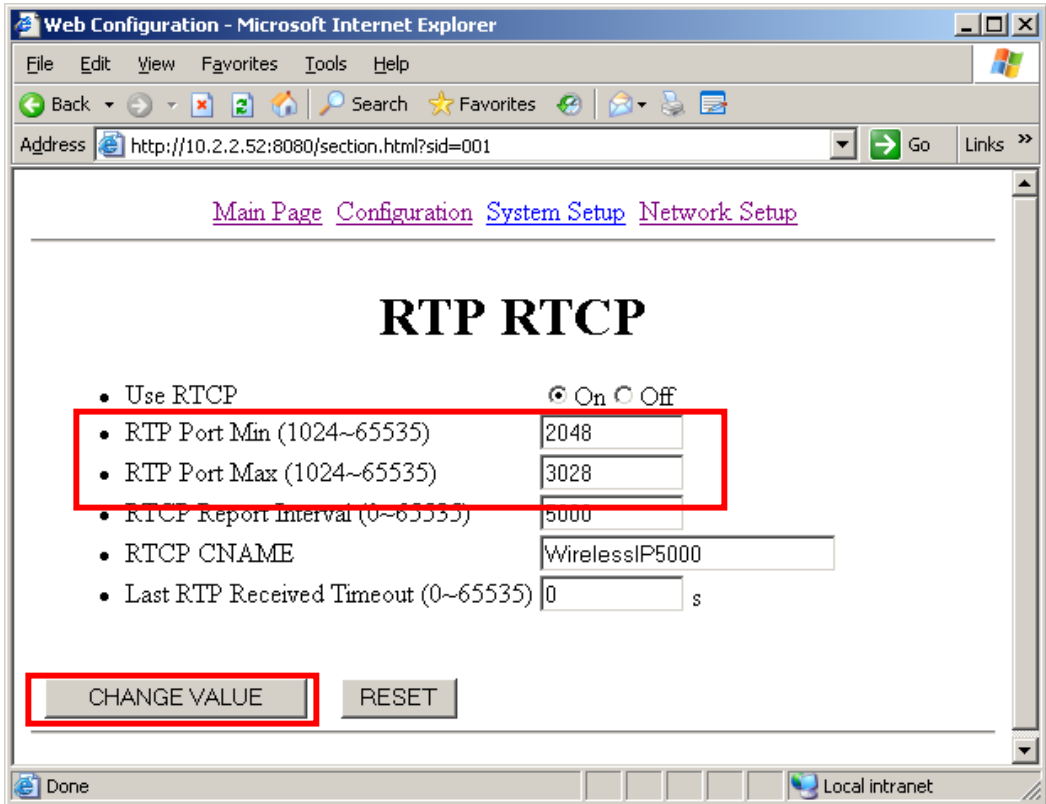
7.5. Other Hitachi Cable WirelessIP 5000 Telephone Configuration

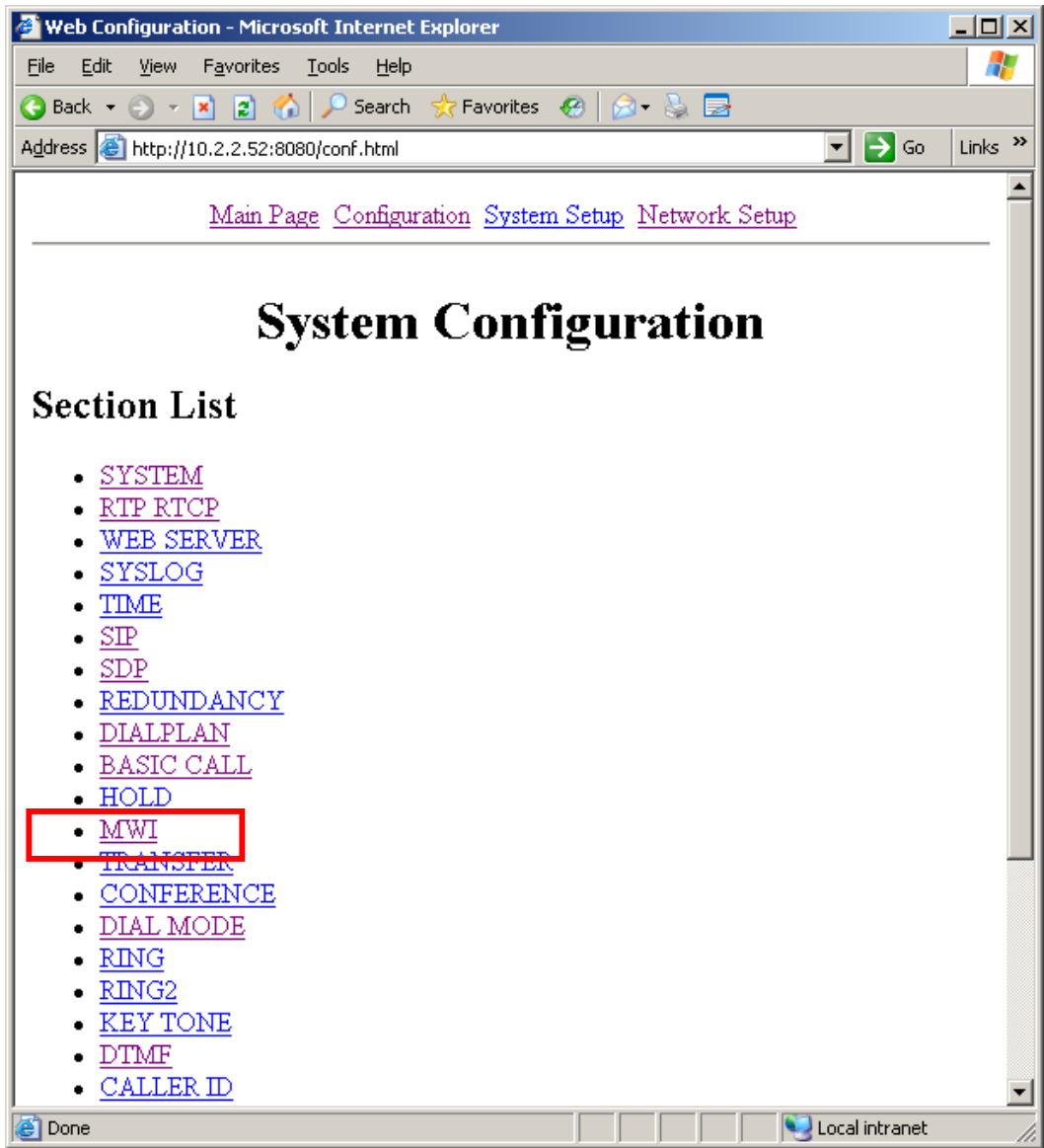
This section describes other settings that are not accessible through the keypad from the Hitachi Cable WirelessIP 5000 telephone. The following settings are accessible using the Hitachi Cable Web Server interface.

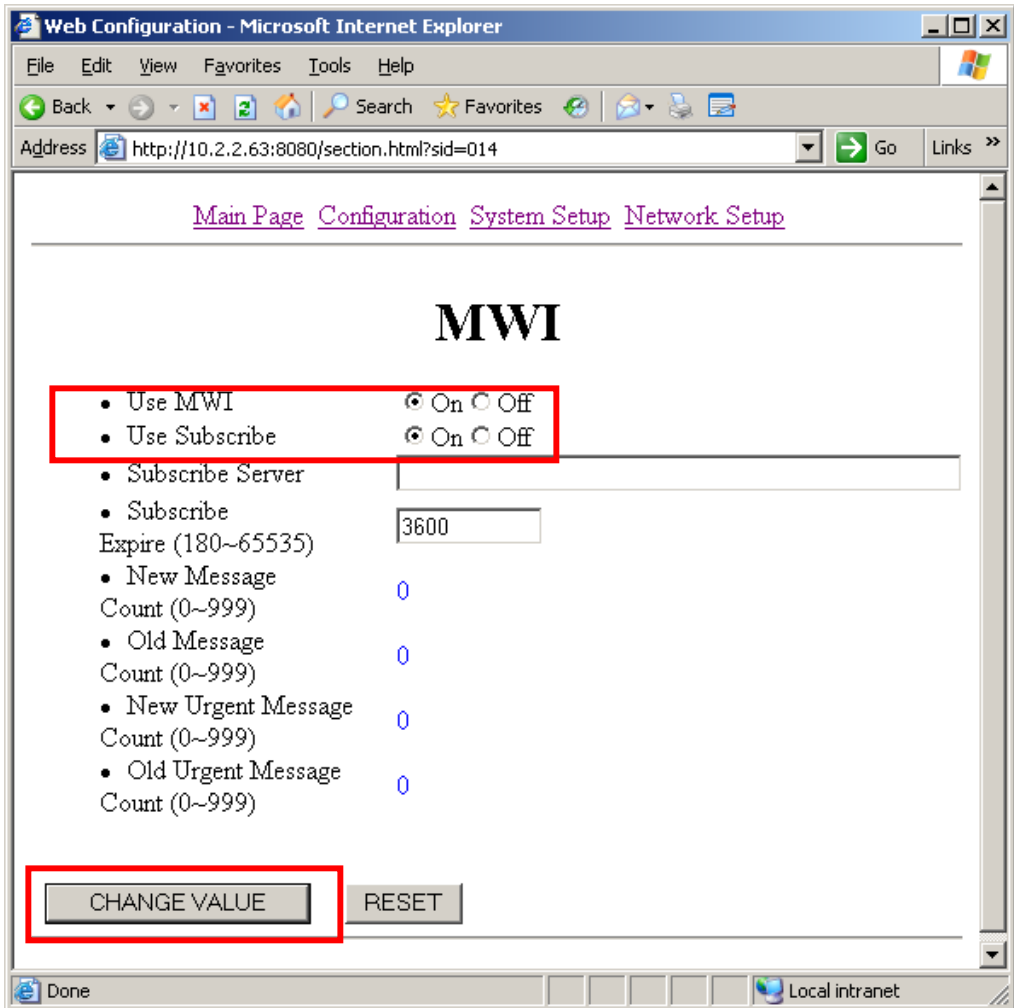
Step	Description
1.	<p>To obtain the IP address information for the Hitachi Cable WirelessIP 5000 telephone, press the LeftSoft key to display the Menu. Press the key sequence “5”, “6”, “1”(Setup→Information→TCP/IP) to display the TCP/IP information for the Hitachi Cable WirelessIP 5000 telephone.</p> 

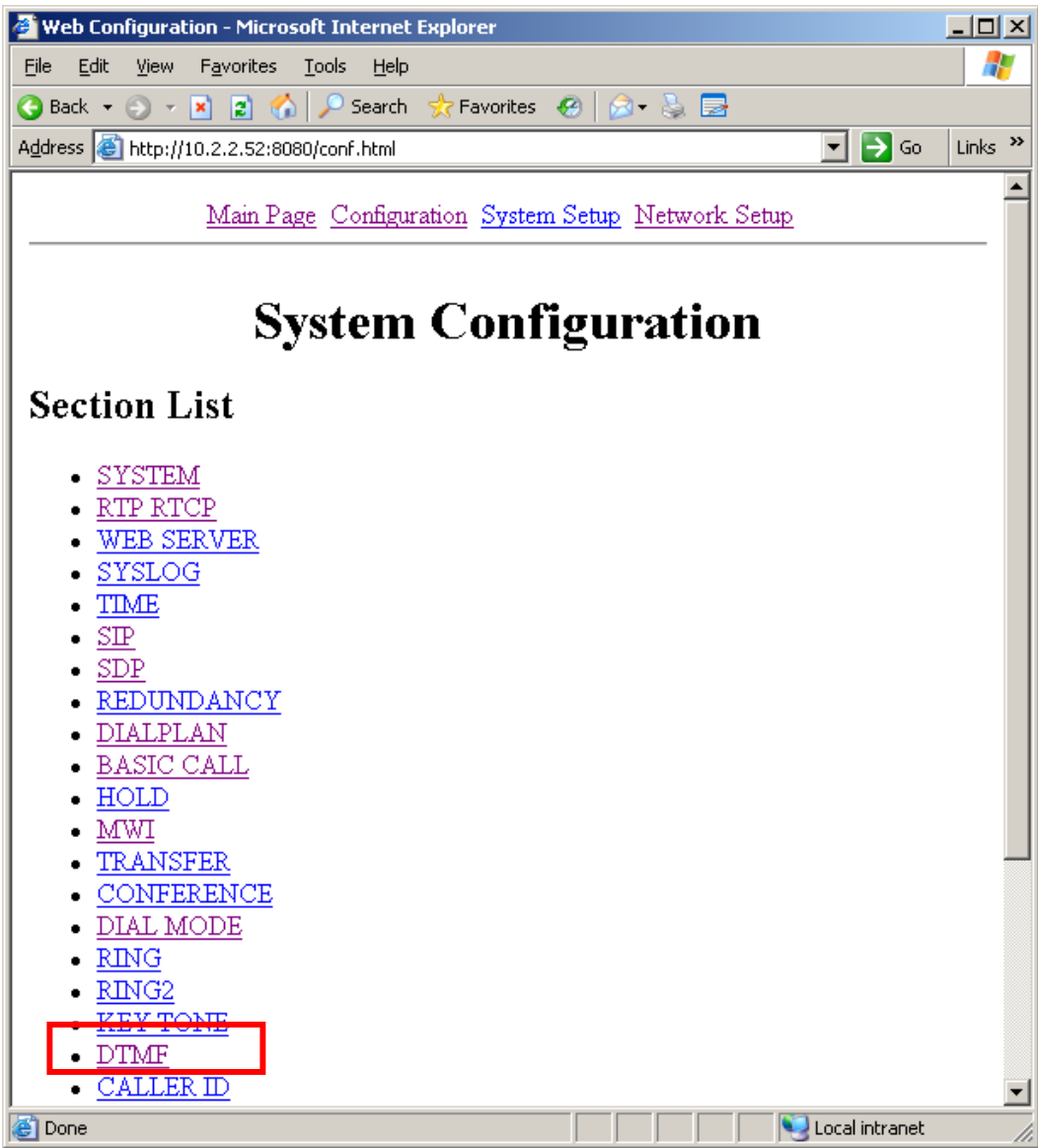
Step	Description														
2.	<p>From a Web browser, enter the IP address of the Hitachi Cable WirelessIP 5000 telephone with port 8080 (e.g. http://10.2.2.52:8080). The Hitachi Cable Wireless IP 5000 in the sample configuration has IP address 10.2.2.52. Enter the appropriate User Name and Password when prompted to log in. The following WirelessIP 5000 Web Configuration Tool will appear. Click on Configuration.</p>  <table border="1"> <thead> <tr> <th colspan="2">Software Specification</th> </tr> </thead> <tbody> <tr> <td>MODEL</td> <td>WirelessIP5000</td> </tr> <tr> <td>SOFTWARE VERSION</td> <td>v2.2.1</td> </tr> <tr> <td>IP ADDRESS</td> <td>10.2.2.52</td> </tr> <tr> <td>NETMASK</td> <td>255.255.255.0</td> </tr> <tr> <td>GATEWAY</td> <td>10.2.2.1</td> </tr> <tr> <td>MAC ADDRESS</td> <td>00:03:2A:00:CB:F0</td> </tr> </tbody> </table>	Software Specification		MODEL	WirelessIP5000	SOFTWARE VERSION	v2.2.1	IP ADDRESS	10.2.2.52	NETMASK	255.255.255.0	GATEWAY	10.2.2.1	MAC ADDRESS	00:03:2A:00:CB:F0
Software Specification															
MODEL	WirelessIP5000														
SOFTWARE VERSION	v2.2.1														
IP ADDRESS	10.2.2.52														
NETMASK	255.255.255.0														
GATEWAY	10.2.2.1														
MAC ADDRESS	00:03:2A:00:CB:F0														

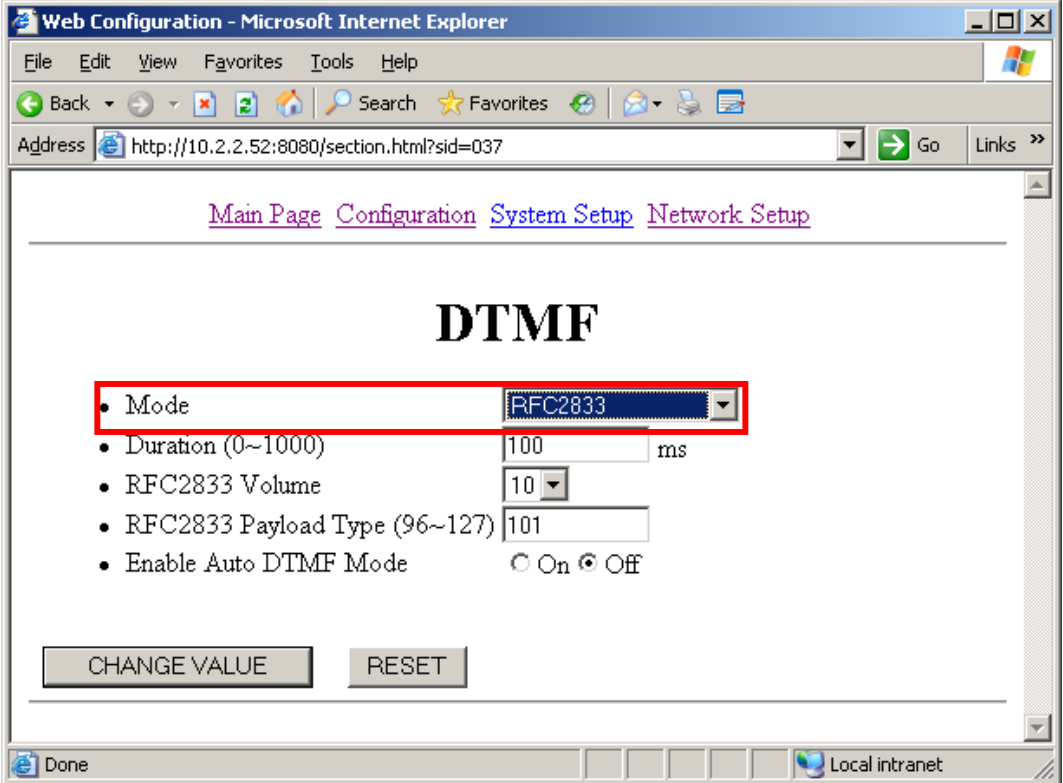
Step	Description
3.	<p>From the System Configuration menu screen, click on RTP RTCP to change RTP port settings.</p>  <p>The screenshot shows a Microsoft Internet Explorer window titled 'Web Configuration - Microsoft Internet Explorer'. The address bar displays 'http://10.2.2.52:8080/conf.html'. The page content includes a navigation bar with links: 'Main Page', 'Configuration', 'System Setup', and 'Network Setup'. Below this is a large heading 'System Configuration' and a section titled 'Section List'. Under 'Section List', there is a list of configuration options: 'SYSTEM', 'RTP RTCP', 'WEB SERVER', 'SYSLOG', 'TIME', 'SIP', 'SDP', 'REDUNDANCY', 'DIALPLAN', 'BASIC CALL', 'HOLD', 'MWI', 'TRANSFER', 'CONFERENCE', 'DIAL MODE', 'RING', 'RING2', 'KEY TONE', 'DTMF', and 'CALLER ID'. The 'RTP RTCP' link is highlighted with a red rectangular box. The status bar at the bottom shows 'Done' and 'Local intranet'.</p>

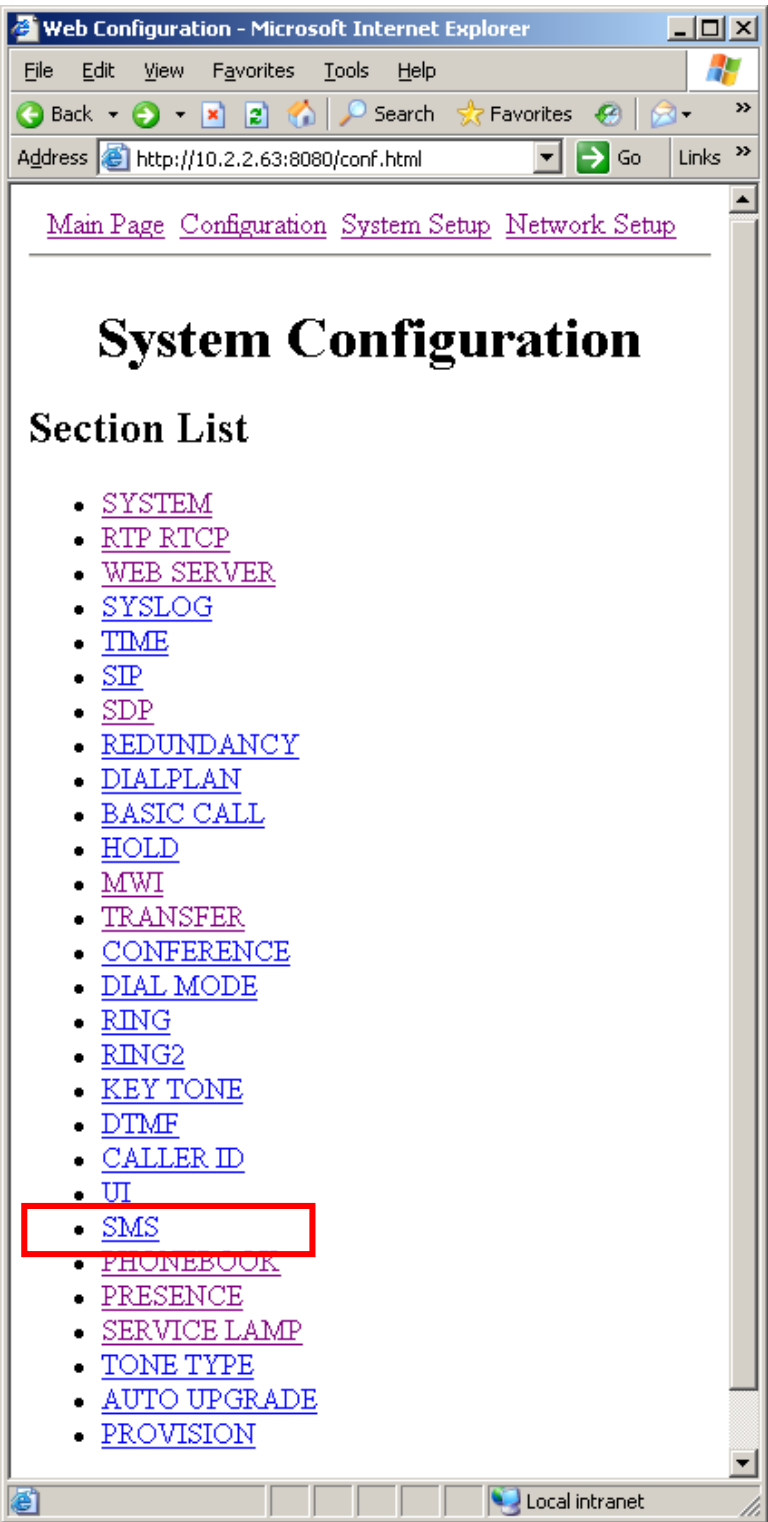
Step	Description				
4.	<p>From the RTP RTCP configuration screen, change the following to match the ip-network-region setting in Avaya Communication Manager in Section 3.3.</p> <table data-bbox="358 268 938 342"> <tr> <td>RTP Port Min (1024~65535)</td><td>2048</td></tr> <tr> <td>RTP Port Max (1024~65535)</td><td>3028</td></tr> </table> <p>Click on CHANGE VALUE to complete.</p> 	RTP Port Min (1024~65535)	2048	RTP Port Max (1024~65535)	3028
RTP Port Min (1024~65535)	2048				
RTP Port Max (1024~65535)	3028				

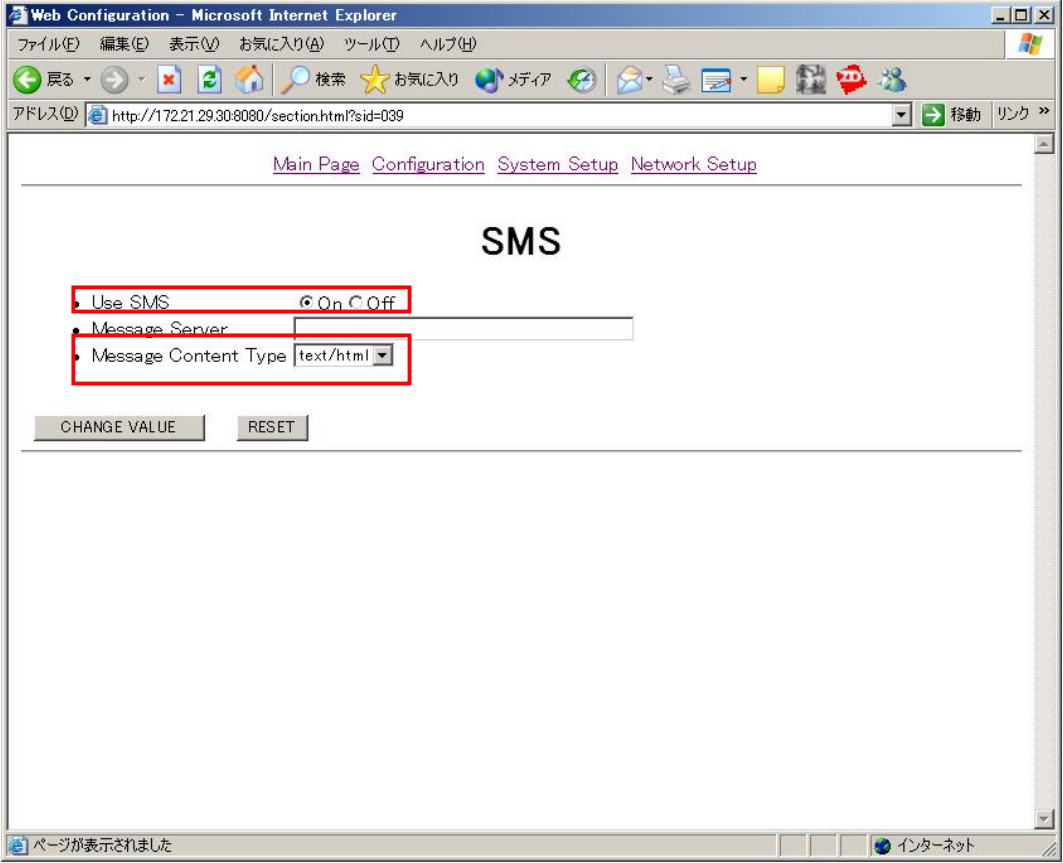
Step	Description
5.	<p>From the System Configuration menu screen, click on MWI.</p>  <p>The screenshot shows a web browser window titled 'Web Configuration - Microsoft Internet Explorer'. The address bar shows 'http://10.2.2.52:8080/conf.html'. The page content includes navigation links at the top: 'Main Page', 'Configuration', 'System Setup', and 'Network Setup'. Below these is the main heading 'System Configuration' and a section titled 'Section List'. This list contains the following items: SYSTEM, RTP RTCP, WEB SERVER, SYSLOG, TIME, SIP, SDP, REDUNDANCY, DIALPLAN, BASIC CALL, HOLD, MWI (highlighted with a red rectangle), TRANSFER, CONFERENCE, DIAL MODE, RING, RING2, KEY TONE, DTMF, and CALLER ID. The status bar at the bottom indicates 'Done' and 'Local intranet'.</p>

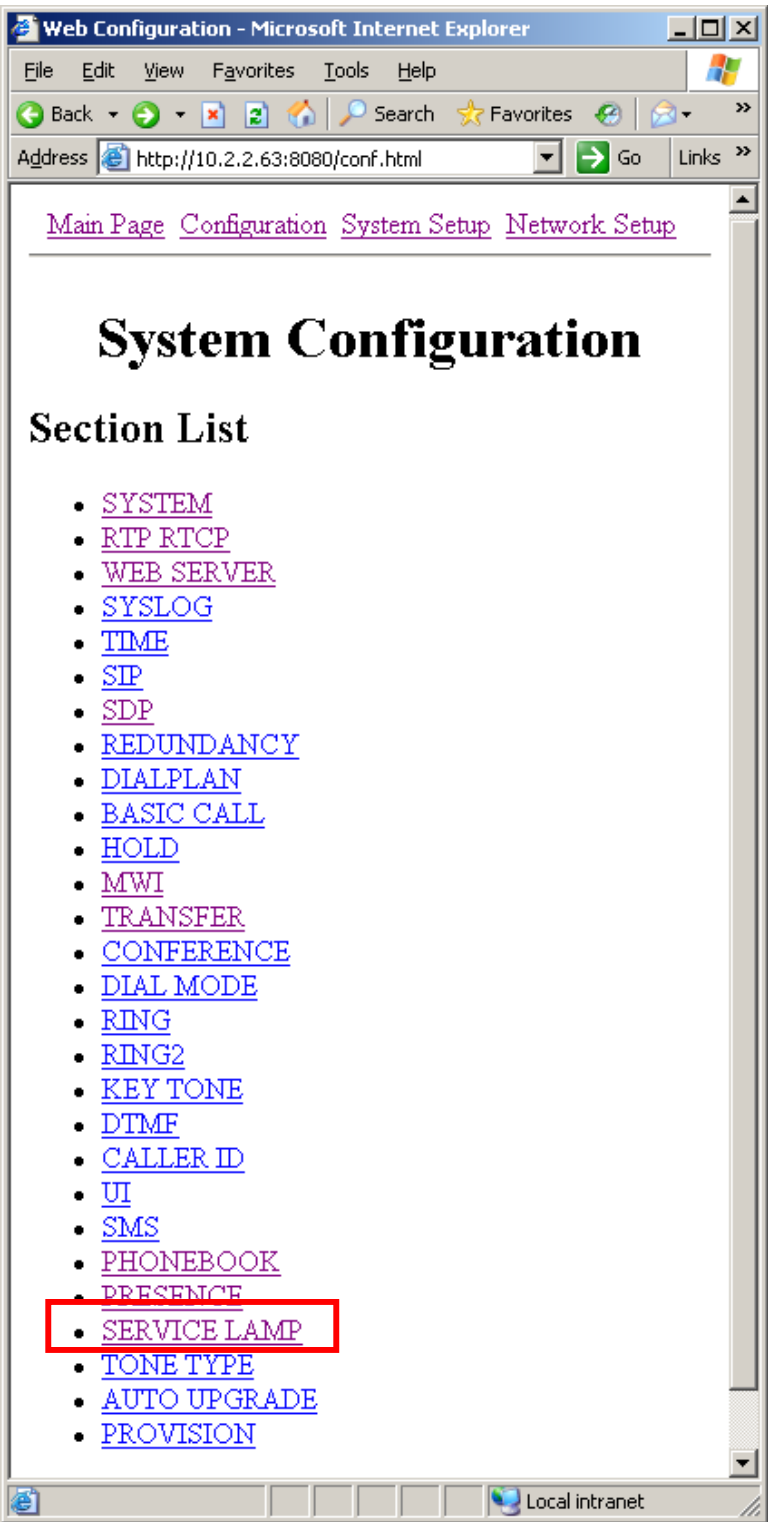
Step	Description
6.	<p>From the MWI menu screen, check the On radio button for Use MWI and Use Subscribe.</p> <p>Click CHANGE VALUE to complete.</p> 

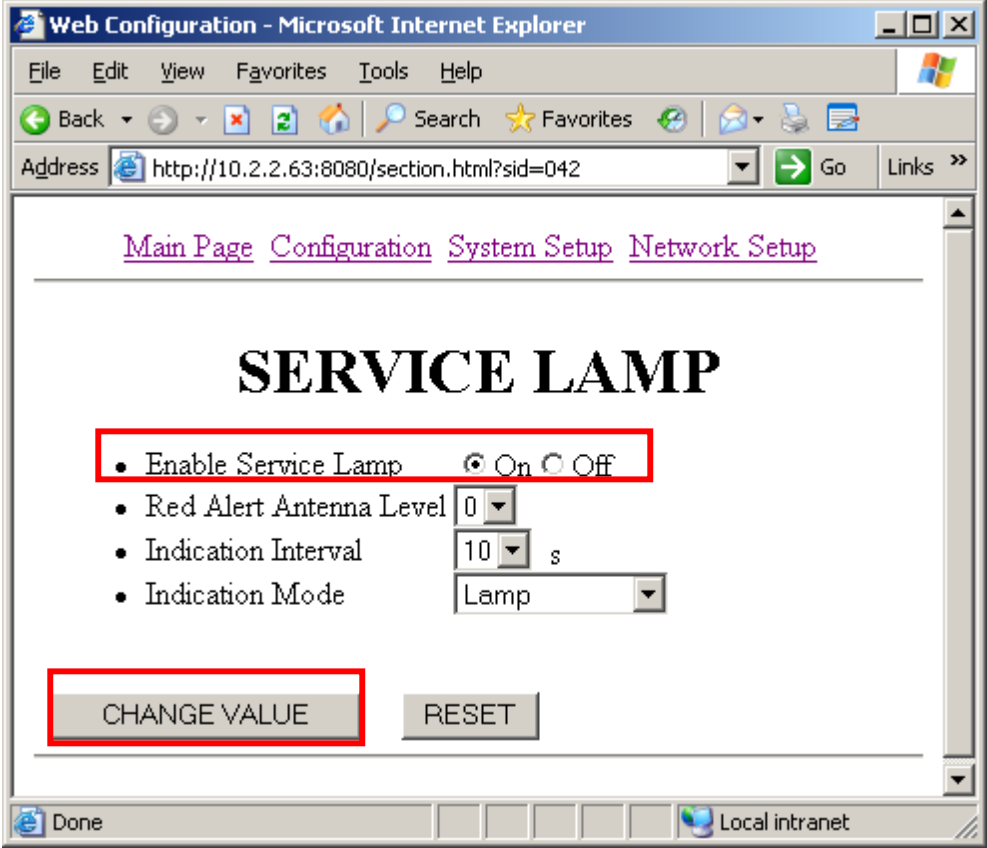
Step	Description
7.	<p>From the System Configuration menu screen, click on DTMF.</p> 

Step	Description
8.	<p>From the DTMF menu screen, change the Mode to RFC2833 from the drop down box.</p> <p>The default Mode “in-Audio” will prevent calls from Shuffling due to capability mismatch. Mode must be set to “RFC2833” for calls to be Shuffled.</p> <p>Click CHANGE VALUE to complete.</p>  <p>The screenshot shows a web browser window titled 'Web Configuration - Microsoft Internet Explorer'. The address bar shows 'http://10.2.2.52:8080/section.html?sid=037'. The page has navigation links: 'Main Page', 'Configuration', 'System Setup', and 'Network Setup'. The main heading is 'DTMF'. Below it, there are several configuration items: <ul style="list-style-type: none"> 'Mode' is a dropdown menu currently showing 'RFC2833', which is highlighted with a red rectangular box. 'Duration (0~1000)' is a text input field with '100' and a unit 'ms'. 'RFC2833 Volume' is a dropdown menu showing '10'. 'RFC2833 Payload Type (96~127)' is a text input field with '101'. 'Enable Auto DTMF Mode' has two radio buttons: 'On' and 'Off', with 'Off' being selected. At the bottom of the configuration area, there are two buttons: 'CHANGE VALUE' and 'RESET'. The browser's status bar at the bottom shows 'Done' and 'Local intranet'.</p>

Step	Description
9.	<p>From the System Configuration menu screen, click on SMS.</p>  <p>The screenshot shows a web browser window titled 'Web Configuration - Microsoft Internet Explorer'. The address bar displays 'http://10.2.2.63:8080/conf.html'. The page content includes a navigation bar with links: 'Main Page', 'Configuration', 'System Setup', and 'Network Setup'. Below this is a large heading 'System Configuration' followed by a 'Section List' of configuration options. The options listed are: SYSTEM, RTP RTCP, WEB SERVER, SYSLOG, TIME, SIP, SDP, REDUNDANCY, DIALPLAN, BASIC CALL, HOLD, MWI, TRANSFER, CONFERENCE, DIAL MODE, RING, RING2, KEY TONE, DTMF, CALLER ID, UI, SMS, PHONEBOOK, PRESENCE, SERVICE LAMP, TONE TYPE, AUTO UPGRADE, and PROVISION. The 'SMS' option is highlighted with a red rectangular box.</p>

Step	Description
10.	<p>From the SMS menu screen, check the On radio button for Use SMS. From the Message Content Type drop down menu, select <i>Text/html</i>.</p> <p>Click CHANGE VALUE to complete.</p> 

Step	Description
11.	<p>From the System Configuration menu screen, click on SERVICE LAMP.</p>  <p>The screenshot shows a web browser window titled "Web Configuration - Microsoft Internet Explorer". The address bar displays "http://10.2.2.63:8080/conf.html". The page content includes a navigation menu at the top with links: Main Page, Configuration, System Setup, and Network Setup. Below this is a large heading "System Configuration". Underneath the heading is a section titled "Section List" which contains a bulleted list of configuration sections. The sections listed are: SYSTEM, RTP RTCP, WEB SERVER, SYSLOG, TIME, SIP, SDP, REDUNDANCY, DIALPLAN, BASIC CALL, HOLD, MWI, TRANSFER, CONFERENCE, DIAL MODE, RING, RING2, KEY TONE, DTMF, CALLER ID, UI, SMS, PHONEBOOK, PRESENCE, SERVICE LAMP, TONE TYPE, AUTO UPGRADE, and PROVISION. The "SERVICE LAMP" link is highlighted with a red rectangular box.</p>

Step	Description
<p>12.</p>	<p>From the SERVICE LAMP menu screen, check the On radio button for Enable Service Lamp.</p> <p>Click CHANGE VALUE to complete.</p> 
<p>13.</p>	<p>Close the Web browser to exit.</p>

8. Interoperability Compliance Testing

The interoperability compliance testing focused on assessing the ability of the Hitachi Cable WirelessIP 5000 telephone to register with Avaya SIP Enablement Services and interoperate with Avaya 4600 series SIP telephones, Avaya SIP Softphone and Avaya 4600 series IP telephone.

8.1. General Test Approach

The general test approach was to place and receive calls through the Hitachi Cable WirelessIP 5000 telephones to and from Avaya 4600 series SIP telephone, Avaya SIP Softphone and Avaya 4600 series IP telephone as configured in **Figure 1**.

The main objectives were to verify:

- The WirelessIP 5000 can place and receive call to and from Avaya 4600 series SIP telephones, Avaya SIP Softphone, and Avaya 4600 series IP telephones.
- The WirelessIP 5000 supports both Shuffled² and Non-Shuffled calls³.
- The WirelessIP 5000 can perform basic native features such as hold, and transfer.
- The WirelessIP 5000 supports QoS using DiffServ.
- The WirelessIP 5000 supports G.711, and G.729 codecs.
- The WirelessIP 5000 supports DTMF.
- The WirelessIP 5000 supports Avaya Off-PBX-Telephone Feature-Name-Extensions such as Forward all calls, Redial, Whisper Page.
- The WirelessIP 5000 supports of 802.1x Authentication using EAP/TTLS
- The WirelessIP 5000 can interoperate with Avaya SIP Softphone via Instant Messaging.

8.2. Test Results

The Hitachi Cable WirelessIP 5000 successfully completed the test objective outline above. Layer-3 (DiffServ) configuration was successfully verified for packets sent from Hitachi Cable WirelessIP 5000 telephones through packet capture. DTMF transmission accuracy was verified using Intuity Audix Voice Mail system as well as Meet-me conference. The Hitachi Cable WirelessIP 5000 telephones provided good voice quality through subjective measurement.

9. Verification Steps

The following steps may be used to verify the configuration:

- Place calls with the Hitachi Cable WirelessIP 5000 telephone.
- Log in to the Avaya SIP Enablement Service (SES) server via the Web browser. The registered users field under Users will also show all registered SIP users.

² In a Shuffled call, Media is send directly between the two telephones.

³ In a Non-Shuffled call, Media between the two telephones are send to the Avaya Media Gateway for mixing.

10. Support

For technical support on the Hitachi Cable WirelessIP 5000 product, contact Hitachi Cable America at 1-914-993-0990, and also refer to www.wirelessip5000.com/eng/index.html.

11. Conclusion

These Application Notes describe the administration steps required to configure the Hitachi Cable WirelessIP 5000 telephone on Avaya SIP Enablement Services (SES) and Avaya Communication Manager in a Meru Networks wireless network.

12. Additional References

- [1] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 2, February 2006
- [2] *Avaya Communication Manager Advanced Administration Quick Reference*, Doc # 03-300364, Issue 2, June 2005 Release 3.0
- [3] *Avaya IA 770 INTUITY AUDIX Messaging Application*, Doc # 11-300532, May 2005
- [4] *Converged Communications Server Installation and Administration*, Doc # 555-245-705, February, 2004
- [5] *Avaya Extension to Cellular and Off-PBX Station (OPS) Installation and Administration Guide Release 3.0*, Doc # 210-100-500, Issue 9, June 2005
- [6] *Configuring SIP IP Telephony Using Avaya SIP Enablement Services, Avaya Communication Manager, and CounterPath eyebeam SIP Softphone*, Issue 1.0, Jan 10, 2006
- [7] *WirelessIP 5000 User's Manual*, TD-2893
- [8] *WirelessIP 5000 Administrator Manual*, TD61-2895

Product documentation for Avaya products may be found at <http://support.avaya.com>

Product documentation for Hitachi Cable WirelessIP 5000 products may be found at <http://www.wirelessip5000.com/eng/index.html> and detailed documentation such as user manuals, administrators manuals, etc, can be obtained directly by contacting Hitachi Cable America, at 1-914-993-0990 or any authorized distributors and resellers.

©2006 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 Developer*Connection* Program at devconnect@avaya.com.