

Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Hitachi Cable WirelessIP-5000-A SIP Telephone with Avaya Communication Manager and Avaya SIP Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration process for interoperability between the Hitachi Cable WirelessIP-5000-A SIP Telephone with Avaya Communication Manager and Avaya SIP Enablement Services. Information in these Application Notes has been obtained through Developer*Connection* compliance testing. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

Avaya Communication Manager and Avaya SIP Enablement Services have the capability to extend advanced telephony features to SIP stations. These features can be extended to non-Avaya SIP telephones such as the Hitachi Cable WirelessIP-5000-A SIP Telephone.

These Application Notes describe a sample solution for configuring the Hitachi Cable WirelessIP-5000-A SIP Telephone to interoperate with Avaya Communication Manager and Avaya SIP Enablement Services through an Aruba Networks wireless network. The Hitachi Cable WirelessIP-5000-A SIP Telephone is an 802.11b/g wireless SIP telephone capable of registering with Avaya SIP Enablement Services. The Hitachi Cable WirelessIP-5000-A SIP Telephone can be identified from other Hitachi Cable model telephones by the asterisk shaped speaker found on the back of the phone, see **Section 5.1 Step 1**. The Hitachi Cable WirelessIP-5000-A SIP Telephone has many additional features and supports a wide array of industry standards, please refer to **Section 10 [3]** or the complete list of features and standards support.

1.1. Network Diagram

The network diagram shown in **Figure 1** illustrates the testing environment used for compliance testing. The network consists of an Avaya Communication Manager, Avaya SIP Enablement Services, wired IP telephones, wireless IP telephones, software based IP telephones, a digital telephone, and the wireless network infrastructure described below. Also included is Avaya IA 770 INTUITY AUDIX (IA770), which is bundled with Avaya Communication Manager and provides voicemail services. Two computers are also present in the network providing network services such as DHCP, TFTP, HTTP and RADIUS. The RADIUS service was provided by Microsoft Internet Authentication Server (IAS).

The wired IP telephones include the Avaya 9630, the Avaya 4610SW and the Avaya 4625SW IP Telephones. The wireless IP telephones are the Hitachi Cable WirelessIP-5000-A SIP Telephones. Present in the network is an Avaya 2420 Digital Telephone, which is directly connected to Avaya Communication Manager. Two wireless laptops, one running Avaya one-X Desktop Edition and the other running Avaya IP Softphone, are connected to the network.

The wireless network is provided by Aruba Networks and consists of an Aruba 2400 Mobility Controller and Aruba Access Points. Access point models include the Aruba AP-60, AP-65 and AP-70. Only one of the access points is on the same IP subnet as the Aruba 2400 Mobility Controller. The other two access points are on separate IP subnets.

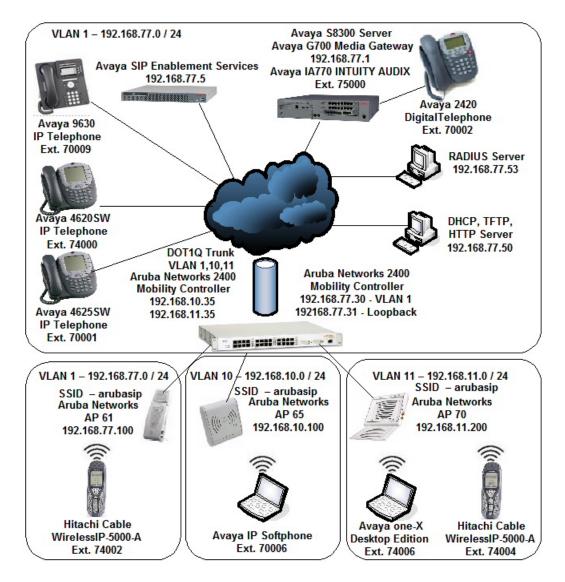


Figure 1: Sample Network Diagram for Hitachi Cable WirelessIP-5000-A SIP Telephone with Avaya Communication Manager and Avaya SIP Enablement Services

2. Equipment and Software Validated

The following equipment and software were used for the test environment:

Equipment	Software				
Avaya S8300 Server	Avaya Communication				
	Manager				
	4.0 (R014x.00.0.730.5)				
	Avaya IA 770 INTUITY				
	AUDIX				
	4.0-11.0				
Avaya G700 Media Gateway	26.31.0				
MM711 Analog Media Module	HW04 / FW87				
MM712 DCP Media Module	HW05 / FW08				
Avaya SIP Enablement Services	3.1.2 (SES-3.1.2.0-309.0)				
Avaya 4610SW IP Telephone (SIP)	2.2.2				
Avaya 4625SW IP Telephone (H.323)	2.8				
Avaya 9630 IP Telephone (H.323)	1.5				
Avaya 2420 Digital Telephone	N/A				
Avaya one-X Desktop Edition	2.1 SP1				
Avaya IP Softphone	6.0.0.25				
Aruba 2400 Mobility Controller	3.1.0.7				
Aruba AP-60, AP-65, AP-70	3.1.0.7				
Hitachi Cable WirelessIP-5000-A SIP Telephone	Software : 2.5.1				
	Boot Rom : 1.1.4				
Microsoft 2003 Server Internet Authentication Server	5.2.3790.0				

3. Avaya Communication Manager and Avaya SIP Enablement Services Configuration

All of the telephones configured in the sample network in **Figure 1** were administered as H.323 or SIP stations in Avaya Communication Manager and Avaya SIP Enablement Services. SIP stations were administered as Off-PBX stations in Avaya Communication Manager. For complete references on how to administer these types of stations please refer to **Section 10** [1] and [2]. No additional or special configurations are needed in order for the Hitachi Cable WirelessIP-5000-A SIP Telephone to interoperate with Avaya Communication Manager or Avaya SIP Enablement Services. However, there are some configuration parameters regarding the IP network region in which Avaya Communication Manager resides, that the Hitachi Cable WirelessIP-5000-A SIP Telephone needs to match.

Description
The output of the " display ip-network-region " command is shown below. The fields highlighted in bold will need to be configured to match on the Hitachi Cable WirelessIP-5000-A SIP Telephone.
display ip-network-region 1 Page 1 of 19 IP NETWORK REGION Region: 1 Authoritative Domain: devcon7.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? n UDP Port Max: 3327 IP Audio Hairpinning? n DIFFSERV/TOS PARAMETERS RTCP Reporting Enabled? y Call Control PHB Value: 46 RTCP MONITOR SERVER PARAMETERS Audio PHB Value: 26 Use Default Server Parameters? y Video PHB Value: 26 Solor.1p Priority: 6 Audio 802.1p Priority: 6 Audio 802.1p Priority: 5 AUDIO RESOURCE RESERVATION PARAMETERS RSVP Enabled? n H.323 IP ENDPOINTS RSVP Enabled? n H.323 Link Bounce Recovery? y RSVP Enabled? n H.323 Link Bounce Recovery? y RSVP Enabled? n H.323 Link Bounce Recovery? y ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh

4. Aruba 2400 Mobility Controller Configuration

The following steps detail the initial configuration for the Aruba Networks wireless network used for the compliance testing. The initial configuration is performed on a factory default system using the serial or console interface to provision the IP addressing and configure the local switch ports on the Aruba 2400 Mobility Controller. Once the system is initially provisioned, the remaining configurations are shown from the web interface.

Step	Description
1.	To perform the initial configuration on the Aruba 2400 Mobility Controller, setup a serial connection from a PC or laptop. Setup a terminal session with the following parameters:
	• 9600 baud
	 8 bits no parity
	• 1 stop bit
	No flow control
	Log into the Aruba 2400 Mobility Controller using default credentials which can be obtained from the Aruba Networks documentation, see Section 10 [5]. Provision the System name , VLAN 1 interface IP address , VLAN 1 interface subnet mask , IP Default gateway , Switch Role and confirm US country code on the Aruba 2400 Mobility Controller. Once all the information has been configured, the system confirms the acceptance of these changes and requires a reboot.
	Enter System name [Aruba2400]: Aruba2400 Enter VLAN 1 interface IP address [172.16.0.254]: 192.168.77.30 Enter VLAN 1 interface subnet mask [255.255.255.0]: 255.255.255.0 Enter IP Default gateway [none]: 192.168.77.254 Enter Switch Role, (master local) [master]: master This controller is restricted to Country code US for United States, please confirm (yes no)?: yes
	If you accept the changes the switch will restart! Type <ctrl-p> to go back and change answer for any question</ctrl-p>
	Do you wish to accept the changes (yes no) yes System will now restart!

Step	Description						
2.	Once the system has rebooted, login to the Command Line Interface (CLI) to provision the						
	loopback interface on the Aruba 2400 Mobility Controller. The configuration of the loopback						
	interface is required when using multiple VLANs. This requires a reboot of the system for the						
	changes made to the loopback interface.						
	(Aruba2400) #configure t						
	(Aruba2400) (config) #interface loopback						
	(Aruba2400) (config-loop)# ip address 192.168.77.31						
	Switch IP Address is Modified. Switch should be rebooted now						
	(Aruba2400) (config-loop)#end						
	(Aruba2400) #write mem						
	Saving Configuration						
	Configuration Saved.						
	(Aruba2400) #reload						
	Do you really want to reset the system (y/n) : y System will now restart!						

Step	Description
3.	Once the system has rebooted, login to the CLI to provision the local switch ports and save the configuration. The remainder of the configuration will be carried out using the web interface which can be accessed by using any web browser to access either the VLAN 1 or loopback IP address of the Aruba 2400 Mobility Controller.
	(Aruba2400) #configure t
	! Create the two additional VLANs, VLAN 10 and VLAN 11 ! (Aruba2400) (config) # vlan 10 (Aruba2400) (config) # vlan 11
	! Provision the IP address on the two additional VLANs ! (Aruba2400) (config) #interface vlan 10 (Aruba2400) (config-subif)# ip address 192.168.10.35 255.255.255.0
	(Aruba2400) (config-subif)# interface vlan 11 (Aruba2400) (config-subif)# ip address 192.168.11.35 255.255.255.0
	<pre>! Provision the local switch ports ! (Aruba2400) (config) #interface fastethernet 1/0 (Aruba2400) (config-if)#switchport mode access (Aruba2400) (config-if)#switchport access vlan 1</pre>
	<pre>(Aruba2400) (config-if)#interface fastethernet 1/2 (Aruba2400) (config-if)#switchport mode access (Aruba2400) (config-if)#switchport access vlan 10</pre>
	<pre>(Aruba2400) (config-if)#interface fastethernet 1/4 (Aruba2400) (config-if)#switchport mode access (Aruba2400) (config-if)#switchport access vlan 11</pre>
	<pre>(Aruba2400) (config-if)#interface gigabitethernet 1/25 (Aruba2400) (config-if)#switchport mode trunk (Aruba2400) (config-if)#switchport trunk allowed vlan 1,10,11 (Aruba2400) (config-if)#end</pre>
	! Save the Configuration ! (Aruba2400) # write memory

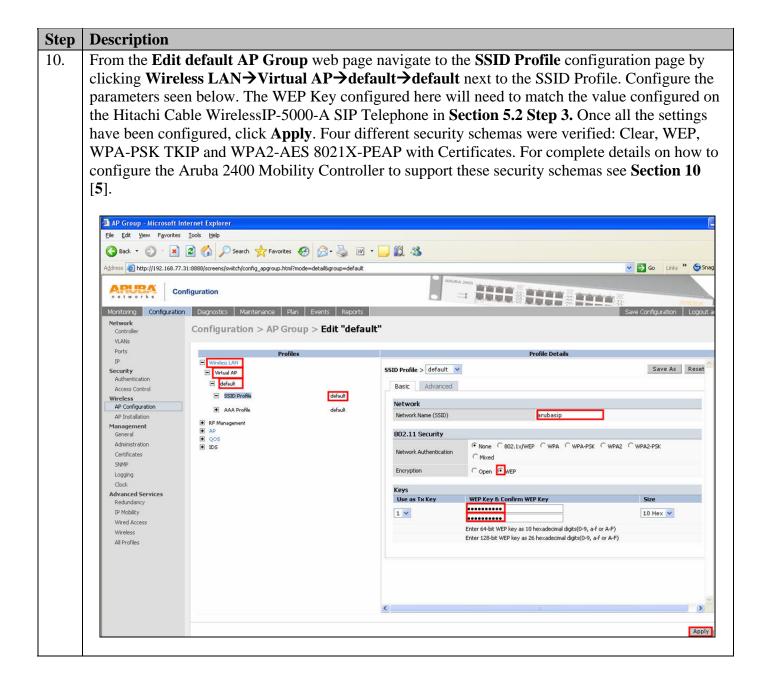
Step	Description
4.	In order for the Aruba access points to automatically register to the Aruba 2400 Mobility Controller the DHCP server needs to be configured in order to provide two options (Option 43 and 60). There are other methods, such as using DNS, in order for the Aruba access points to automatically register to Aruba Mobility Controllers. In the sample network, DHCP options 43 and 60 were used to provide the IP address to the Aruba 2400 Mobility Controller. Modify the DHCP server to provide Options 43 and 60. The ASCII value configured for DHCP Option 43 is the IP address of the loopback interface on the Aruba 2400 Mobility Controller. Option 60 needs to be configured to provide a String value which contains "Aruba Access Point". The combination of these two DHCP options is what enables the Aruba access points to automatically register to the Aruba Mobility Controller.
	Scope Options ? × General Advanced

Step	Description
<u>Step</u> 5.	Description Using a web browser, open a connection to the Aruba 2400 Mobility Controller by putting the IP address of the Aruba 2400 Mobility Controller's loopback interface into the URL (http://192.168.77.31 was used in the sample network). The user is presented with a login screen and must provide credentials in order to receive access to the system. Refer to Section 10 [5] for information about obtaining login credentials. Image: the system of the system o
	System Name : Aruba2400

Step	Description									
6.	Once logged into the Aruba 2400	0 Mobility Controller, the user is presented with the following								
	status screen which indicates details such as number of controller and access points the system has found. No access points have been plugged into the controller and none are shown at this time.									
	Tourid. No access points have bee	is points have been plugged into the controller and note are shown at this time.								
	Monitoring - Microsof	oft Internet Explorer								
	Eile Edit View Favorite	tes Iools Help								
	G Back - 🐑 - 💌	x 😰 🏠 🔎 Search 👷 Favorites 🤣 😥 - 🌺 👿 - 📙 🎇								
	Address 🛃 http://192.168.7	.77.31:8888/screens/wmsi/monitor.summary.html								
	ARUBA N	Monitoring								
	Monitoring Configurat	ation Diagnostics Maintenance Plan Events Reports								
	Network									
	Network Summary	Network Summary								
	All WLAN Controllers	WLAN Network Status								
	All Access Points	Total Total IPSEC IPSEC								
	All Air Monitors	Up Down Up Down								
	All Wired Access Points Global Events	WLAN Controllers 1 0								
	Controller	Access Points <u>Q</u> <u>Q</u> <u>Q</u>								
	Controller Summary	Air Monitors Q Q Q Q								
	Access Points	Wired Access Points Q Q Q Q								
	Wired Access Points	Unprovisioned Access Points 0								
	Wired Mux Ports	Duplicate AP Name 0								
		RADIUS Servers 0 0								
	Air Monitors Clients	LDAP Servers 0 0								
	Blacklist Clients	WLAN Performance Summary								
	Ports	Last 5 Min Last Hour All								
		Load Balancing Events 0 0 0								
	Inventory	Interference Events 0 0 0								
	Local Events	Bandwidth Exceeded 0 0 0								
	WLAN <no found="" ssids=""></no>	Error Threshold Exceeded Q Q Q								
	Debug									
	Local Clients									
	Process Logs									
	Custom Logs <no custom="" found="" logs=""></no>	1>								

Step	Description										
7.	At this time three access points were p one access point per VLAN (VLAN 1 of the sample network. Refresh the we access points have been found.	, VLAN 10, and V	/LA	AN 1	1).	See Fi	igure	e 1 fo	or an il	llustrat	
	🗿 Monitoring - Microsoft	Internet Explorer									
	Elle Edit View Favorites	Iools Help									
	G Back - 🕥 - 💌	💈 🏠 🔎 Search 🔸	Favo	rites	0	🔊 • 🎍	W				
	Address 🛃 http://192.168.77	.31:8888/screens/wmsi/monitor.su	immary	.html?							
	Monitoring Configuration Network Network	Monitoring Monitoring Configuration Diagnostics Maintenance Plan Events Reports Network									
	All WLAN Controllers	WLAN Network Status									
	All Access Points All Air Monitors	ment network status	Total	Total	IPSEC	IPSEC					
	All Wired Access Points		Up	Down	Up	Down					
	Global Events	WLAN Controllers Access Points	1	0							
	Controller	Air Monitors	2	0	0	Q Q					
	Controller Summary	Wired Access Points	0	0	0	2					
	Access Points	Unprovisioned Access Points	0								
	Wired Access Points	Duplicate AP Name	0								
	Wired Mux Ports	RADIUS Servers	0	0							
	Air Monitors	LDAP Servers	0	0							
	Clients Blacklist Clients	WLAN Performance Sur	nmary	,		1					
	Ports			lin Last	Hour	All					
	Inventory	Load Balancing Events		Q		0					
	Local Events	Interference Events	-	Q		0					
	WLAN	Bandwidth Exceeded		0		0					
	aruba-ap	Error Threshold Exceeded	8	Q		Q					
	Debug										
	Local Clients										
	Process Logs Custom Logs										
	<no custom="" found="" logs=""></no>										

Step	Description								
8.	Navigate to the A	Il Access Po	oints web	page by	clicking A	All Access	Points fro	om the me	enu present
	on the left side of the web page. This page can be used to quickly gauge the connectivity between								
	the Aruba 2400 Mobility Controller and the Aruba access points.								
	Monitoring - Microsoft Ele Edit View Favorites	and the second se							
						- <u>664</u>			
	G Back • 🕥 - 💌	The second second second		and the second second	to the second				
	Address 🛃 http://192.168.77.	31:8888/screens/switch	/switch_mon.html?n	node=nwaps8sta	tus=up				
	ARURA notworks Mo	nitoring					ARUBA 24		
	Monitoring Configuration	n Diagnostics	Maintenance	Plan Events	Reports				
	Network Network Summary	Network >	All Access	Points					
	All WLAN Controllers	Global APs							
	All Access Points All Air Monitors	Name	AP Group *	Status *		AP Type *	Switch IP 🕈	and the second second second second	.bg Channel *
	All Wired Access Points	00:0b:86:c0:c8:e4 00:0b:86:c2:0a:20	default default	up	192.168.10.201 192.168.77.100	65	<u>192.168.77.31</u> 192.168.77.31	0	52
	Global Events Controller	00:0b:86:c5:5e:98	default	up	192.168.11.200		192.168.77.31	0	48
	Controller Summary						1 1-3 of 3 1	D 💌	
	Access Points								
9.	Navigate to the E	dit default	AP web pa	age by cl	icking Co	nfigurati	on→AP		
	Configuration→		1	0,0	U	0			
	AP Group - Microsoft Internet	t Explorer							
	Ele Edit View Favorites Tools								
	🚱 Back 🔹 🐑 - 💌 🛃	🏠 🔎 Search 🤺 F	avorites 🚱 🔗	• 🍓 🗷 •	J 🛍 🚳				
	Address 1 http://192.168.77.31:8888	8/screens/switch/config_apgr	oup.html		10.1				So Links
						ARUBA 2400	and a second		
	n o t w o r k s Configur	ation				二 原原			1.22
		iagnostics Maintenario	e Plan Events	Reports					Save Configuration
	Network Controller CO	onfiguration > A	P Group						
	VLANs	AP Group AP Specific							
	Ports IP	· Landarda			Name				Action
	Security	efault			Manic			Edit	and the second se
	Authentication Access Control	New							
	Wireless AP Configuration								
	Concerning and the								
1									



	Description	A J	• • • • • • • • • • • • • • • • • • • •		A .]		- 41		
	Navigate to the arrows, scroll do								
				,) option be	comes visio	le and check		
Wireless Multimedia (WMM) check box. Click Apply.									
	🗿 AP Group - Microsoft In	ternet Explorer							
	Eile Edit View Favorites	Iools Help	s 🚱 🚖 ર 🥁 🕡 •	11. 43.					
		31:8888/screens/switch/config_apgroup.htm					💌 🛃 Go Links 🎽 🌀 Si		
	networks	nfiguration		- =		HUTT	R Aller		
	Monitoring Configuration Network Controller	Diagnostics Maintenance F Configuration > AP G		:"			Save Configuration Logou		
	VLANs Ports IP	Prof	files		Prof	file Details			
	Security Authentication Access Control	Virtual AP default		SSID Profile > default v			Save As Reset		
	Access Control.								
	🗿 AP Group - Microsoft In	ternet Explorer							
	Eile Edit View Favorites	Iools Help							
	🌀 Back 🝷 🕥 - 💌	💈 🏠 🔎 Search 👷 Favorites	s 🚱 🍰 🎍 🗷 •	📙 🛍 🖓					
	Address () http://192.168.77.3	31:8888/screens/switch/config_apgroup.htm	nl?mode=detail&group=default				Go Links » 😏 Si		
	and the second sec			ARUBA 3	and March 199	a Maria			
	ARUBA networks Cor	nfiguration		• =	: :::::	+++			
	Monitoring Configuration	Diagnostics Maintenance P	Plan Events Reports				Save Configuration Logou		
	Network	Configuration > AP G	roun > Edit "default	,n					
	Controller VLANs	configuration > AP of	oup > Luit delaut	5) 					
	Ports	Prof	iles		Prof	île Details			
	IP Security	Wireless LAN Virtual AP		Station Ageout Time	1000 sec	Retry Limit	4		
	Authentication Access Control	🖃 default		RTS Threshold	2333 bytes	Short Preamble			
	Wireless	SSID Profile	default	Max Associations	64	Wireless Multimedia (WMM)			
	AP Configuration AP Installation	💽 AAA Profile	default	902il Compatibility Mode		Hide SSID			
	Management	RF Management Ap		Deny_Broadcast Probes		Local Probe Response	V		
	General Administration	 QOS IDS 							
	Certificates			Battery Boost		WEP Key 1	Retype:		
	SNMP Logging								
	Clock			WEP Key 2	Retype:	WEP Key 3	Retype:		
	Advanced Services Redundancy								
	IP Mobility								
				WEP Key 4	Retype:	WEP Transmit Key Index	1 💌		
	Wired Access Wireless					8			
	Wired Access								
	Wired Access Wireless			WPA Hexkey	Retype:	WPA Passphrase	Retype:		
	Wired Access Wireless			WPA Hexkey	Retype:	WPA Passphrase	Retype:		
	Wired Access Wireless			WPA Hexkey Maximum Transmit Failures	Retype:	WPA Passphrase	Retype:		
	Wired Access Wireless					WPA Passphrase			
	Wired Access Wireless					WPA Passphrase			

Step	Description
12.	Navigate to the Server Configuration web page by clicking Configuration \rightarrow Authentication \rightarrow + RADIUS Server (the + becomes a – once it is clicked). Enter a descriptive label for the name of the RADIUS Server being added to the system, then click Add. In the sample network the name "Dev7-Radius" was chosen.
	Switch General Configuration - Microsoft Internet Explorer Ele Edt View Favorites Tools Help
	🚱 Back 🔹 🕥 - 💌 😰 🏠 🔎 Search 🤺 Favorites 🤣 😥 - 🌺 🔟 - 🗾 🎇 🦓
	Address a http://192.168.77.31:8888/screens/switch/config_controller.html?mode=servers
	Configuration
	Monitoring Configuration Diagnostics Maintenance Plan Events Reports Network Controller Security > Authentication > Servers Security
	VLANs Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced Ports
	IP Server Group RADIUS Server
	Access Control Dev7-Radius Add
13.	After the RADIUS Server has been added to the system, it now becomes a clickable item that will open a configuration dialogue for the RADIUS Server. Click on the name of the RADIUS Server configured in the previous step.
	Switch General Configuration - Microsoft Internet Explorer
	Elle Edt Yew Favorites Iools Help Image: Back Image: Second Seco
	Address ahttp://192.168.77.31:8888/screens/switch/config_controller.html?mode=servers
	Configuration
	Monitoring Configuration Diagnostics Maintenance Plan Events Reports
	Controller Security > Authentication > Servers VLANs Servers AAA Profiles L2 Authentication L3 Authentication User Rules
	Ports IP Security RADIUS Server Instance
	Authentication RADIUS Server Dev7-Radius Access Control Dev7-Radius Add
	AP Configuration

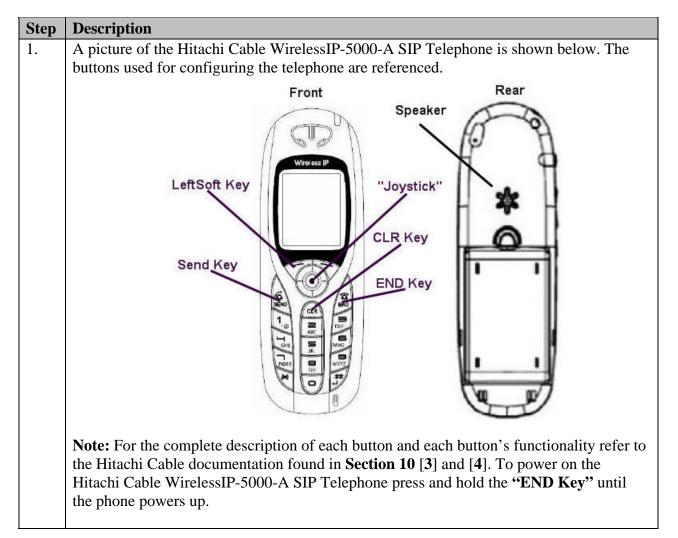
Description					
configuration value configu Click Apply . Mobility Con	screen. Configure th red for the Key field For complete details troller see Section 1	ne Host field to l will need to r s on the RADI	b be the IP addr natch the value	ess of the RAI configured on	DIUS Server. The the RADIUS Server.
Approximation of the second					L.
) 🙈 • 🔜 🗑 • 🥅 🕯	a 38		
		The second se			🗸 🄁 Go 🛛 Links 🎽 🌀 Snagi
			ARUBA 2400	*	
n etworks Co	onfiguration				Alterna
	on Diagnostics Maintenance Plan	Events Reports			Save Configuration Logout ac
Network Controller	Security > Authentication	> Servers			
VLANs Ports	Servers AAA Profiles L2 Aut	entication L3 Authentication	n User Rules Advanced		
IP	🗈 Server Group	DADIIIS Server > Dev7	Padius		Save As Reset
Security Authentication Access Control Wireless AP Configuration	RADIUS Server	Host	192.168.77.53	Кеу	Retype:
AP Installation	LDAP Server	Auth Port	1812	Acct Port	1813
General	Internal DB	Retransmits	3	Timeout	5 sec
Administration Certificates	TACACS Server	NAS ID	E	NAS IP	
SNMP		Use MD5		Mode	
Clock Advanced Services Redundancy IP Mobility Wireless All Profiles		٢			Vilga
	After clicking configuration value configu Click Apply. Mobility Con	After clicking on the name of the configuration screen. Configure th value configured for the Key field Click Apply . For complete details Mobility Controller see Section 1	After clicking on the name of the RADIUS Serve configuration screen. Configure the Host field to value configured for the Key field will need to r Click Apply. For complete details on the RADI Mobility Controller see Section 10 [5].	After clicking on the name of the RADIUS Server the user is pr configuration screen. Configure the Host field to be the IP addr value configured for the Key field will need to match the value Click Apply. For complete details on the RADIUS/802.1X com Mobility Controller see Section 10 [5].	After clicking on the name of the RADIUS Server the user is presented with the configuration screen. Configure the Host field to be the IP address of the RADivalue configured for the Key field will need to match the value configured on Click Apply. For complete details on the RADIUS/802.1X configuration on the Mobility Controller see Section 10 [5].

5. Hitachi Cable WirelessIP-5000-A SIP Telephone Configuration

The following steps describe the configuration process for the Hitachi Cable WirelessIP-5000-A SIP Telephone to connect to a wireless network and register with Avaya SIP Enablement Services.

1.2. Administering the Initial Configuration of the Hitachi Cable WirelessIP-5000-A SIP Telephone

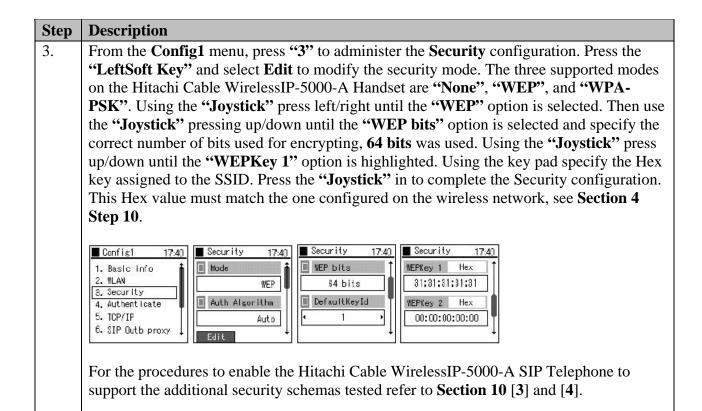
In order to connect the Hitachi Cable WirelessIP-5000-A SIP Telephone to a wireless network the user must first configure the telephone to create the initial WiFi binding. The user can either use the buttons on the face of the telephone or a USB cable connection to a computer with a specific software application. Once the Hitachi Cable WirelessIP-5000-A Telephone has a WiFi binding with an IP address, the user can complete the configuration process using the web server built into the telephone. There are some vendor specific configuration dependencies in the configuration file, consult with Hitachi support for specific inquiries.



Step	Description
2.	Once the phone has powered up, press the "LeftSoft Key" to enter the menu.
	Tail Image: Constraint of the second secon
	From the Menu screen, use the key sequence "5", "2", "1" (Setup→Phone lock→User
	Pwd) in order to obtain access to the Admin menu. Enter the correct password for
	accessing the Admin menu and press the "Joystick" in. A password is required to access this menu, for additional information refer to Section 10 [4].
	Menu17401. Phone bock2. Message3. Call log4. Presence5. Setup6. Network
	The user is now presented with the Admin menu.
	Admin 17:40 1.Network config 2. Password 3. Upgrede 4. Error log 5. WEB server 6. Phone reset

1.3. Administering the Network Configuration for Hitachi Cable WirelessIP-5000-A SIP Telephone

Step	Description
1.	From the Admin menu, press "1" to select "Network config". Admin 1740 1.Network confis 2. Password 3. Upgrede 4. Error log 5. WEB server 6. Phone reset From the Network config menu use the key sequence "1", "1", "2" (Network config→Config1→WLAN) to access the WLAN menu. Press the "LeftSoft Key" to select Edit. Use the keypad to enter the SSID, which must match the SSID configured on the wireless network.
	Network confi 17:40 Network confi 17:40 1. Network config 1. Config1 2. SIP 1. Config1 3. Network reload 1. Config1 4. Certs manager 5. Site scan 6. Ping test Cptions
2.	From the Config1 menu press " 5 " to configure the TCP/IP parameters for the Hitachi Cable WirelessIP-5000-A SIP Telephone. If DHCP is not enabled press the " LeftSoft Key " and select Edit then using the " JoyStick " toggle left/right to enable DHCP.



1.4. Administering the SIP Configuration on Hitachi Cable WirelessIP-5000-A SIP Telephone

Step	Description
1.	From the Config1 menu, press "6" to specify the SIP Outb proxy . Use the " LeftSoft Key " and select Edit . Enter 192.168.77.5 , which is the IP address of Avaya SIP Enablement Services.
	Config1 17:40 1. Basic info Config1 2. NLAN Image: Config1 3. Security 192.168.77.5 4. Authenticate Image: Config1 5. TCP/IP Edit 6. SIP Outb proxy Edit

2.	From the Network config menu, press "2", "1" (SIP→User Account) to specify the SIP		
	and User Account information. Press the "LeftSoft Key" and select Edit to input the User Account information into the Hitachi Cable WirelessIP-5000-A SIP Telephone. Using the "JoyStick" navigate by pressing up/down and enter the following information. The URL scheme must be selected using the "JoyStick" by toggling left/right until SIP is configured. Press the "JoyStick" inward to input the newly specified parameters. In order to configure the User ID, User Password and URL Scheme the operator must navigate by pressing the "Joystick" down until those options appear.		
	Display Name 74002		
	 Phone Number 74002 User ID 74002 		
	 User ID 74002 User Password 123456 		
	URL Scheme SIP		
	Network confi 17:40 SIP 17:40 1. Network confis 1. User account Display name 2. SIP 2. Server setup 74002		
	3. Network reload 3. IMS server 4. Certs manager 4. Outbound proxy		
	5. Site scan 5. Expire 74002		
	Edit +		
3.	From the SIP menu, press "2" to enter the Server setup configuration menu. Press the " LeftSoft Key " and select Edit to configure the Server setup information. Using the keypad configure the Domain/Realm , 1 st Proxy and 1 st Registrar information. Press the " JoyStick " inward to input the newly specified parameters. To navigate to the 1 st Registrar press the " Joystick " down to scroll the screen. The Domain/Realm is the domain name of Avaya SIP Enablement Services. The 1 st Proxy and 1 st Registrar are the IP address of Avaya SIP Enablement Services, 192.168.77.5 in the sample network.		
	Domain/Realm devcon7.com		
	• 1 st Proxy 192.168.77.5		
	• 1 st Registrar 192.168.77.5		
	SJP 17.40 1. User account Domain/Realm 2. Server setup devcon7.com 3. IMS server 1st Proxy 4. Outbound proxy 1st Proxy 5. Expire Identity		

Step	Description		
4.	From the SIP menu, press "4" to enter the Outbound proxy configuration menu. Press		
	the "LeftSoft Key" and select Edit to input the Outbound proxy information. Press the		
	"JoyStick" inward to input the newly specified parameters. Press the "END Key" to exit		
	the Admin menu of the Hitachi Cable WirelessIP-5000-A SIP Telephone. The		
	Outbound proxy is the IP address of Avaya SIP Enablement Services, 192.168.77.5 in		
	the sample network.		
	SIP 17:40 Outbound prox 17:40		
	1. User account		
	2. Server setup 3. IMS server		
	4. Outbound proxy		
	5. Expire		
	Edit		

1.5. Administering Additional Configuration Information on Hitachi Cable WirelessIP-5000-A SIP Telephone

This section details other configurations necessary for interoperability between the Hitachi Cable WirelessIP-5000-A SIP Telephones with Avaya SIP Enablement Services Server. The following settings are configured by using the web server built-in to the Hitachi Cable WirelessIP-5000-A SIP Telephone and require a web browser (such as Internet Explorer). Only modifications made to default values are shown.

Step	Description	
1.	In order to verify the web server is running on the Hitachi Cable WirelessIP-5000-A SIP Telephone use the Admin menu. From the Admin menu, press "5" to check the status of the web server. Should the web server be disabled, use the " JoyStick " and toggle left/right and select Enabled . Press the " JoyStick " inward.	
	Admin 17:40 1. Network config 2. Password 3. Ubgrede 4. Error log 5. WEB server 6. Phone reset To obtain the IP address assigned via DHCP to the Hitachi Cable WirelessIP-5000-A SIP	
	Telephone use the key sequence "5", "6", "1" (Setup→Information→TCP/IP) from the Menu menu.	
	Menu17:40Setup17:401. Phone book2. Phone lock1. TDP/IP2. Message3. Alarm3. Call log4. Yolume4. Presence5. Error notify6. Network6. Information	

Step	Description			
2.	WirelessIP-5000-A address of the teleph server inside the Hit The URL string to a 192.168.77.112) is h username and passw	r running on a PC with IP connectivity to the Hitachi Cable SIP Telephone, administer the telephone as follows. Place the IP none into the URL address field specifying the port 8080. The web achi Cable WirelessIP-5000-A SIP Telephone operates at port 8080. ccess the web server of a telephone (which has an IP address of attp://192.168.77.112:8080. The user will be required to supply a yord to access the web interface, consult the Hitachi Cable ne appropriate credentials, see Section 10 [4]. Click Configuration .		
	Web Configuration - Microso	ft Internet Explorer		
	File Edit View Favorites Tools	Help		
	🚱 Back 🔹 🕥 - 💌 🛃	🏠 🔎 Search 🧙 Favorites 🧑 🔗 - 🌺 🗹 - 🦲 🇱 🧏		
	Address 🛃 http://192.168.77.112:80	80/index.html		
		Main Page Configuration System Setup Network Setup		
	Configuration System Setup Network Setup Download Configuration File	WirelessIP5000A Web Configuration Tool		
	Software Specification			
	MODEL	WirelessIP5000A		
	SOFTWARE VERSION	x2.5.1		
	IP ADDRESS	192.168.77.112		
	NETMASK	255.255.255.0		
	GATEWAY	192.168.77.254		
	MAC ADDRESS	00:03:2A:02:05:02		

Step	Description
3.	From the System Configuration web page, three options need to be configured. Click
	"RTP RTCP", "MWI", and "DTMF" and configure the following parameters.
	Web Configuration - Microsoft Internet Explorer
	File Edit View Favorites Tools Help
	S Back + S - K S C - Search 2 Favorites 2 D + 2 W + 2 K + 2
	Address at http://192.168.77.112:8080/conf.html
	Main Page Configuration System Setup Network Setup
	System Configuration
	Section List
	 SYSTEM RTP RTCP WEB SERVER SYSLOG TIME SIP SDP REDUNDANCY DIALPLAN BASIC CALL HOLD DND MWI TRANSFER CONFERENCE FORWARD DIAL MODE RING RING RING RING RING RING CALLER ID

From the RTP RTCP web page configure the " RTP Port Min (1024~65535)" and		
figured on Avaya		
NGE VALUE".		
24 VO 202000 200-2000		
tem Setup <u>Network Setup</u>		
RTCP		
cribe". Click "CHANGE		
n System Setup Network Setup		
MWI		

Step	Description
6.	From the DTMF web page, use the pull down menu for the Mode field and select
	"RFC2833". Click "CHANGE VALUE".
	Web Configuration - Microsoft Internet Explorer File Edit View Favorites Tools Help
	Search + Search + Favorites C + + + + + + + + + + + + + + + + + +
	Address 🕘 http://192.168.77.112:8080/section.html?sid=037
	Main Page Configuration System Setup Network Setup
	DTMF
	Mode RFC2833
	• Duration (0~1000) 100 ms
	• RFC2833 Volume 10 -
	RFC2833 Payload Type (96~127) 101 Enable Auto DTMF Mode ○ On ⊙ Off
	CHANGE VALUE RESET
7.	From the Main Page, see Step 2, click "Network Setup". From the Network Setup web
/.	page many additional configurations options are presented to the user. Using the
	navigation bars, scroll down to the second half of the web page and using the pull down
	menu configure "DiffServ Signal" and "DiffServ Media" for a value of 46. Use the
	radio button and enable "WMM". Click "CHANGE VALUE".
	• Static NAT Start
	Port (0~9000) • STUN Server
	• STUN 3478
	Port (0~65535) • WPA PSK
	PassPhrase • WPA PSK Key
	• Hee WPA PSK Key
	Hex Mode $\bigcirc On \odot Off$ $\lor \zeta$ • Proactive Key Caching $\bigcirc On \odot Off$
	• PMK (43200
	DMK May
	$\frac{32}{1000}$
	DiffServ Signal 46 v DiffServ Media 46 v
	• WMM Off
	Jitter Buffer Size 60 v ms Payload Type 0.8.18 (CSV Format)
	Multiframe 2.2.2 x10 ms (CSV Format)
	successere cancel Antalia Statement 2
	CHANGE VALUE DELETE RESET

Step	Description		
8.	urn to the Network Setup web page and click "REBOOT". Click "Reboot Now ?".		
	In order for the new configuration to take effect the phone needs to be rebooted.		
	 Web Configuration - Microsoft Internet Explorer File Edit View Favorites Tools Help 		
	🕒 Back + 💿 - 🖹 🖻 🕎 🔎 Search 📌 Favorites 🤣 🎯 + 🍑 🕅 + 🛄 🏭 🖏		
	Address 🕘 http://192.168.77.112:8080/network.html		
	Main Page Configuration System Setup Network Setup		
	Network Setup		
	REBOOT		
	SIP Registration		
	USER ACCOUNT SERVER SETTINGS		
	Network Config		
	[Config1] [Config2] ADD [New Network Profile]		
	Etc.		
	• <u>WIFI</u> • <u>WIFI SCAN</u> • <u>ROAMING</u> • <u>DYNAMIC NETWORK</u>		
	·		
	🚷 Web Configuration - Microsoft Internet Explorer		
	File Edit View Favorites Tools Help		
	🔇 Back 🔹 🕥 - 🖹 🗟 🟠 🔎 Search 📌 Favorites 🤣 🙆 - 🥁 🎬 - 🛄 🎉 🖄		
	Address 🗃 http://192.168.77.112:8080/save.html		
	Main Page Configuration System Setup Network Setup		
	Reboot Now ?		

6. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying the capability of the Hitachi Cable WirelessIP-5000-A SIP Telephone to register with Avaya Communication Manager and Avaya SIP Enablement Services Server. Testing also verified the interoperability between Hitachi Cable WirelessIP-5000-A SIP Telephone, Avaya SIP phones, Avaya H.323 phones, Avaya softphones (SIP and H.323) and Avaya digital phones.

Avaya's formal testing and Declaration of Conformity is provided only on the headsets/handsets that carry the Avaya brand or logo. Avaya may conduct testing of non-Avaya headset/handset to determine interoperability with Avaya phones. However, Avaya does not conduct the testing of non-Avaya headsets/handsets for: Acoustic Pressure, Safety, Hearing Aid Compliance, EMC regulations, or any other tests to ensure conformity with safety, audio quality, long-term reliability or any regulation requirements. As a result, Avaya makes no representations whether a particular non-Avaya headset will work with Avaya's telephones or with a different generation of the same Avaya telephone.

Since there is no industry standard for handset interfaces, different manufacturers utilize different handset/headset interfaces with their telephones. Therefore, any claim made by a headset vendor that its product is compatible with Avaya telephones does not equate to a guarantee that the headset will provide adequate safety protection or audio quality.

1.6. General Test Approach

The general test approach was to register the Hitachi Cable WirelessIP-5000-A SIP Telephone with Avaya Communication Manager and Avaya SIP Enablement Services through the Aruba Networks wireless network. Calls were made between both wired and wireless telephones and specific calling features were exercised. To validate Quality of Service, low priority background traffic was injected into the network and the Aruba Networks wireless network was verified to maintain voice calls while dropping the low priority traffic. Network level tests included verifying roaming from one access point to another.

1.7. Test Results

The Hitachi Cable WirelessIP-5000-A SIP Telephone passed all test cases. The Hitachi Cable WirelessIP-5000-A SIP Telephone was verified to successfully register with Avaya Communication Manager and Avaya SIP Enablement Services. The compliance testing also focused on verifying Quality of Service for voice traffic while low priority background traffic was competing for bandwidth. The Hitachi Cable WirelessIP-5000-A SIP Telephone was verified to roam successfully between access points on the same network (Layer 2 roaming) and between access points on a different network (Layer 3 roaming) while maintaining voice calls. Four different security schemas were tested: Clear, WEP, WPA-PSK TKIP and WPA2-AES 802.1X-PEAP with Certificates. Two codecs were used for testing: G.711MU and G.729AB. Telephone calls were verified to operate correctly with the media path direct between the telephones (shuffling enabled) and with the media path centralized through Avaya Communication Manager (shuffling disabled). Calls were maintained for durations over one minute without degradation to voice quality. The telephony features verified to operate correctly

GSK; Reviewed:
SPOC 7/24/2007

included attended/unattended transfer, conference call participation, conference call add/drop, multiple call appearances, caller ID operation, call forwarding unconditional, call forwarding on busy, call forwarding clear, voicemail using Avaya IA 770 INTUITY AUDIX, MWI, hold and return from hold.

7. Verification Steps

The following steps may be used to verify that the configuration is working properly.

1.8. Avaya Communication Manager and Avaya SIP Enablement Services Server Verification Steps

- Place calls with the Hitachi Cable WirelessIP-5000-A SIP Telephone. Exercise calling features such as conference, transfer and hold and verify proper operation of those features.
- Log into Avaya Communication Manager and verify that the stations are configured as Off-PBX OPS stations see **Section 10** [1].
- Log into Avaya SIP Enablement Services and verify that the SIP stations haven properly administered see Section 10 documents [1] and [2].
- Ensure that Avaya SIP Enablement Services has been updated after any new stations have been configured.

1.9. Hitachi Cable WirelessIP-5000-A SIP Telephone Verification Steps

- Verify that the Hitachi Cable WirelessIP-5000-A SIP Telephone has the correct SSID configured. Use the steps outlined in **Section 5.2 Step 1** to confirm all of the settings are correct.
- Verify that the Hitachi Cable WirelessIP-5000-A SIP Telephone has an IP address assigned and is configured for DHCP, see **Section 5.4 Step 1**.
- Verify that the Hitachi Cable WirelessIP-5000-A SIP Telephone has the correct SIP server configuration. Use the steps outlined in **Section 5.3 Step 3** to confirm all the settings and IP address information are correct.
- Verify that the Hitachi Cable WirelessIP-5000-A SIP Telephone has the correct RTP port information configured. First check the settings configured on the Avaya Communication Manager (see Section 3 Step 1) and verify the Hitachi Cable WirelessIP-5000-A SIP Telephone is configured to use those same settings (see Section 5.4 Step 4).
- Verify the Hitachi Cable WirelessIP-5000-A SIP Telephone can place and receive calls both to and from stations within the network and that two-way audio is heard.

8. Support

For technical support on the Hitachi Cable WirelessIP-5000-A SIP Telephone use the information below.

- **Phone:** 1-914-993-0990
- Email: Hitachi Cable America, White Plains, NY info@hitachi-cable.com
- Web : <u>http://www.wirelessip5000.com/eng/index.html</u>

9. Conclusion

These Applications Notes described the configuration steps to make the Hitachi Cable WirelessIP-5000-A SIP Telephone interoperate with Avaya Communication Manager and Avaya SIP Enablement Services Server through an Aruba Network's 2400 Mobility Controller with Aruba Network's access points.

10. Additional References

- [1] Administrator Guide for Avaya Communication Manager, May 2006, Issue 2.1 Document Number 03-300509
- [2] *Installing and Administering SIP Enablement Services R3.1.1*, August 2006, Issue 2.0, Document Number 03-600768
- [3] WirelessIP5000E-A Administrator Manual, Document Number TD61-2896E
- [4] WirelessIP5000E-A User's Manual, Document Number TD61-2894E
- [5] ArubaOS User Guide Aruba Version 3.1, February 2007, Document Number 0510286-01

©2007 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and TM 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 <u>devconnect@avaya.com</u>.