



Avaya Solution & Interoperability Test Lab

Application Notes for Spectralink Wireless Server 6500/400 with Avaya Aura® Communication Manager and Avaya Aura® Session Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the Spectralink Wireless Server 6500/400 to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. Functionality was validated and compliance testing was conducted in order to verify proper operation.

Readers should pay attention to Section 2, in particular the scope of testing as outlined in Section 2.1 as well as any observations noted in Section 2.2, to ensure that their own use cases are adequately covered by this scope and results.

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

1. Introduction

The Spectralink Wireless Server is a wireless Digital Enhanced Cordless Telecommunications (DECT) solution capable of communicating via Session Initiation Protocol (SIP) with Avaya Aura® Session Manager. The Spectralink Wireless Server combines wireless DECT with SIP IP telephony. Each Spectralink Wireless Server can register up to 4,096 wireless DECT phones and handle up to 1,024 simultaneous calls.

2. General Test Approach and Test Results

The compliance testing focused on the ability of the Spectralink Wireless Server and Spectralink DECT handsets to interoperate with Communication Manager and Session Manager and various Avaya telephones, including SIP, H.323, digital and analog. The interoperability compliance test included feature and serviceability testing. The Spectralink Butterfly and 76 Series handsets functioned correctly with good audio quality in both directions. All test cases were executed manually.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The interoperability compliance test included functionality, failover and serviceability testing. The main objective was to verify Spectralink Wireless Server interoperability with Communication Manager and Session Manager.

Functionality was tested across a range of basic telephony operations including:

- Basic calls to/from Avaya and Spectralink DECT handsets
- Call Hold
- Call Transfer (Blind and Attended)
- Call Forwarding
- Conference Call Participation
- Message Waiting Indicator
- Caller ID
- Call Park
- Multiple Call Appearances
- G.711MU, G.711A, and G.729 Codecs
- Media Shuffling
- Extension to Cellular (EC500)
- Base Station Roaming
- Base Station Failure

Failover testing was performed by disconnecting one of the active base stations. Serviceability tests were performed by resetting and reconnecting the Spectralink DECT handsets, and restarting the Spectralink Wireless Server.

2.2. Test Results

Spectralink successfully achieved the above objectives. All test cases passed.

Testing was completed with the Spectralink Wireless Server 6500. The Spectralink Wireless Server 400 was not used in compliance testing; however, Spectralink has provided the following statement:

"We, Spectralink Corporation, hereby confirm that the following IP-DECT servers

- Spectralink IP DECT Server 400
- Spectralink IP DECT Server 6500

are based on the same platform and therefore:

- Use identical SIP stack
- Use identical XML-RPC API for messaging
- Use the same firmware for support of both platforms"

2.3. Support

For technical support on Spectralink products, contact Spectralink at technicalsupport@spectralink.com, or refer to <http://support.spectralink.com>.

3. Reference Configuration

Figure 1 illustrates the setup used for compliance testing. The configuration enabled Communication Manager and Session Manager, to interoperate with the Spectralink Wireless Server using SIP. Spectralink DECT handsets register with the Spectralink Wireless Server via the Spectralink Base Stations and the Spectralink Wireless Server functions as a SIP Proxy for the Spectralink DECT handsets.

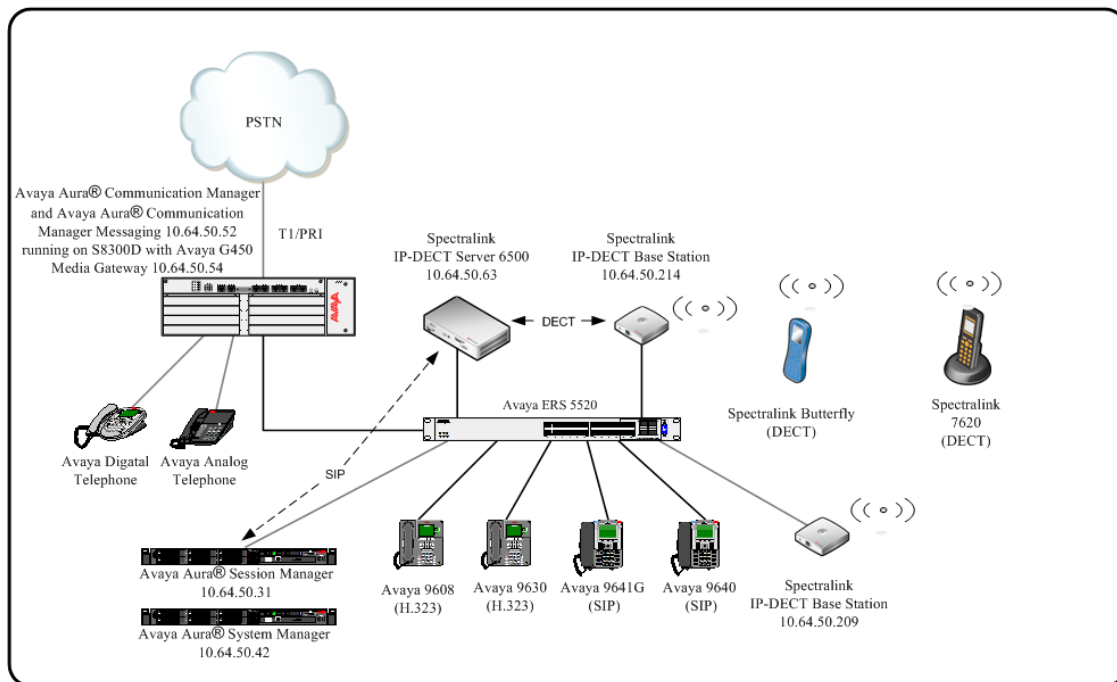


Figure 1: Spectralink Wireless Server Solution

4. Equipment and Software Validated

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

Equipment	Software/Firmware
<i>Avaya PBX Products</i>	
Avaya Aura® Communication Manager	6.3 SP6
Avaya Aura® Session Manager	6.3.8
<i>Avaya Messaging (Voice Mail) Products</i>	
Avaya Aura® Communication Manager Messaging	6.3 SP6
<i>Avaya Endpoints</i>	
Avaya 96xx Series IP Deskphone	(H.323 3.2) (SIP 2.6)
Avaya 96x1 Series IP Deskphone	(H.323 6.4) (SIP 6.4)
Avaya Digital Telephone	R39
Avaya Analog Telephone	NA
<i>Spectralink Products</i>	
Spectralink Wireless Server 6500	PCS14B_
Spectralink IP DECT Base Station	PCS14B_
Spectralink 76-Series Handsets	PCS14HB
Spectralink Butterfly Series Handsets	PCS14HB

5. Configure Avaya Aura® Communication Manager

This section describes the steps required for Communication Manager to support the configuration in **Figure 1**. The following pages provide step-by-step instructions on how to administer parameters specific to the Spectralink solution only. The assumption is that the appropriate license and authentication files have been installed on the servers and that login and password credentials are available and that the reader has a basic understanding of the administration of Communication Manager and Session Manager. It is assumed that all other connections, e.g., to PSTN, to LAN, are configured and will not be covered in this document. The reader will need access to the System Administration Terminal screen (SAT). For detailed information on the installation, maintenance, and configuration of Communication Manager, please refer to **Section 10**.

5.1. Configure Node-Names IP

In the **IP NODE NAMES** form, assign the name and IP address of Session Manager. This is used to terminate the SIP Entity Link with Session Manager. The names will be used in the signaling group configuration.

Enter the **change node-names ip** command. Specify node names and security module IP address for Session Manager.

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
abacus2	10.64.50.64	
cms	10.64.10.85	
default	0.0.0.0	
iq1	10.64.50.15	
msgserver	10.64.50.52	
procr	10.64.50.52	
procr6	::	
sm5031	10.64.50.31	
util5022	10.64.50.22	
		(9 of 9 administered node-names were displayed)
		Use 'list node-names' command to see all the administered node-names

5.2. IP Codec Set and IP Network Region

Enter the **change ip-codec-set g** command, where “g” is a number between 1 and 7, inclusive, and enter “**G.711MU**” for **Audio Codec**. This IP codec set will be selected later in the IP Network Region form to define which codecs may be used within an IP network region.

Note: During compliance testing G.711MU, G.711A, and G.729 were used.

change ip-codec-set 1

Page 1 of 2

IP CODEC SET

Codec Set: 1

Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)
1: G.711MU	n	2	20
2: G.711A	n	2	20
3: G.729	n	2	20
4:			
5:			
6:			
7:			

Media Encryption

1: none

2:

3:

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is *d4f27.com*. By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G450 Media gateway. The **IP Network Region** form also specifies the **IP Codec Set** to be used for Desk Phone calls. This IP codec set is used when its corresponding network region (i.e., IP Network Region '1') is specified in the SIP signaling groups.

Enter the **change ip-network-region h** command, where "h" is a number between 1 and 250, inclusive. On page 1 of the **ip-network-region** form, set **Codec Set** to the number of the IP codec set configured in previous step. Accept the default values for the other fields.

change ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1		
Location: 1	Authoritative Domain: d4f27.com	
Name:	Stub Network Region: n	
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes
Codec Set: 1	Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	IP Audio Hairpinning? y	
UDP Port Max: 65535		
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46		
Audio PHB Value: 46		
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5	AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 IP ENDPOINTS	RSVP Enabled? n	
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		

5.3. Configure Signaling and Trunk Groups

Add a signaling group for calls that need to be routed to SIP Endpoints registered with Session Manager. Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the Signaling Group form as shown below:

- Set the **Group Type** field to *sip*.
- Specify the Communication Manager (procr) and the Session Manager as the two endpoints of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These field values were configured in the **IP Node Names** form shown in **Section 5.1**.
- Compliance testing used TLS and port value of *5061* in the **Near-end Listen Port** and the **Far-end Listen Port** fields. If the **Far-end Network Region** field is configured, the codec for the call will be selected from the IP codec set assigned to that network region.
- Enter the domain name in the **Far-end Domain** field. In this configuration, the domain name is *d4f27.com*.
- The **DTMF over IP** field is set to the default value of *rtp-payload*. Communication Manager supports DTMF transmission using RFC 2833.
- The default values for the other fields may be used.

add signaling-group 2		Page 1 of 2
SIGNALING GROUP		
Group Number: 2	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y	Peer Server: Others	
Near-end Node Name: procr	Far-end Node Name: sm5031	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain: d4f27.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	
ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh		

Configure the **Trunk Group** form shown below for outgoing calls to be routed to Session Manager.

- Set the **Group Type** field to “sip”.
- Enter a meaningful name/description for **Group Name**.
- Enter a **Trunk Access Code (TAC)** that is valid under the provisioned dial plan
- Set the **Service Type** field to “tie”.
- Specify the **Signaling Group** associated with this trunk group.
- Specify the **Number of Members** supported by this SIP trunk group
- The default values for the other fields may be used.

add trunk-group 2		Page 1 of 21	
TRUNK GROUP			
Group Number: 20	Group Type: sip	CDR Reports: y	
Group Name: To Session Manager	COR: 1	TN: 1	TAC: *002
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type:	Auth Code? n	Member Assignment Method: auto	
		Signaling Group: 2	
		Number of Members: 10	

5.4. Dial Plan and Access Codes

The dial plan defines what digit strings are defined as extensions and access codes. Feature access codes (fac) can be used to invoke specific PBX features.

Use the **display dialplan analysis** command to display the dial plan. This information will be used in subsequent steps and sections. Extensions beginning with 6 were used for the Avaya and Spectralink Endpoints.

display dialplan analysis						Page 1 of 12		
DIAL PLAN ANALYSIS TABLE								
Location: all						Percent Full: 2		
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
2	8	ext						
3	5	aar						
4	5	ext						
5	5	udp						
6	5	ext						
7	5	ext						
8	1	fac						
9	1	fac						
*	4	dac						

Use the “**change feature-access-codes**” command to assign feature access codes for **AAR** and **ARS** (if not already assigned) that is consistent with the existing dial plan.

change feature-access-codes		Page	1 of 10
FEATURE ACCESS CODE (FAC)			
Abbreviated Dialing List1 Access Code:			
Abbreviated Dialing List2 Access Code:			
Abbreviated Dialing List3 Access Code:			
Abbreviated Dial - Prgm Group List Access Code:			
Announcement Access Code:			
Answer Back Access Code:			
Attendant Access Code:			
Auto Alternate Routing (AAR) Access Code: 8			
Auto Route Selection (ARS) - Access Code 1: 9		Access Code 2:	
Automatic Callback Activation:		Deactivation:	
Call Forwarding Activation Busy/DA:		All:	Deactivation:
Call Forwarding Enhanced Status:		Act:	Deactivation:
Call Park Access Code:			
Call Pickup Access Code:			
CAS Remote Hold/Answer Hold-Unhold Access Code:			
CDR Account Code Access Code:			
Change COR Access Code:			
Change Coverage Access Code:			
Conditional Call Extend Activation:		Deactivation:	
Contact Closure Open Code:		Close Code:	

- For the **Dialed String**, enter the extensions reachable via Session Manager.
- Set the **Total Min** and **Total Max** fields to the number length.
- Set the **Route Pattern** to the route pattern defined in **Section 5.5** that directs calls to the trunk connected to the Avaya Aura® Session Manager.
- Set the **Call Type** to *aar*.

change aar analysis 6							
AAR DIGIT ANALYSIS TABLE							
Location: all							
Percent Full: 2							
	Dialed String	Total Min Max		Route Pattern	Call Type	Node Num	ANI Reqd
61		5	5	3	aar		n
69997		5	5	99	aar		n
8		7	7	254	aar		n
9		12	12	1	aar		n

5.7. Configure EC500

5.7.1. Configure Stations and Off-PBX Station Mapping For Mobile Devices

Each mobile device will be associated with a station extension configured on Communication Manager. The station extension may represent a physical desk phone or an extension with no phone logged in to it. In the case of the compliance test extensions 60002 and 61006 were configured on Communication Manager.

To associate a mobile device to each of these station extensions requires an off-pbx station mapping as shown below.

In general, a mobile device will be associated with an existing desk phone for which the Communication Manager Station extension will already be configured. However, in the case of mobile devices that are not associated with a physical phone then a station must be added.

Use the **change station 61020** command to modify the station for this user. Enter a value of enabled for the **EC500 State:** field.

change station 61020		Page 2 of 6
STATION		
FEATURE OPTIONS		
LWC Reception: spe	Coverage Msg Retrieval? y	
LWC Activation? y	Auto Answer: none	
CDR Privacy? n	Data Restriction? n	
Per Button Ring Control? n	Idle Appearance Preference? n	
Bridged Call Alerting? n	Bridged Idle Line Preference? n	
Active Station Ringing: single	Restrict Last Appearance? y	
H.320 Conversion? n	Per Station CPN - Send Calling Number?	
	EC500 State: enabled	
MWI Served User Type:	Coverage After Forwarding? s	
AUDIX Name:		
Remote Softphone Emergency Calls: as-on-local	Direct IP-IP Audio Connections? y	
Emergency Location Ext: 61020	Always Use? n IP Audio Hairpinning? n	

To create the mapping between a desktop extension and a mobile device, use the **change off-pbx-telephone station-mapping x** command, where **x** is the desktop extension to be mapped. Multiple station extensions can be added at the same time. Enter the parameters as described below.

- Enter the desktop extension for the **Station Extension**.
- Enter *EC500* for the **Application**.
- Enter the mobile extension for the **Phone Number**.
- Enter *ars* for **Trunk Selection**. This instructs Communication Manager to use the ARS tables to determine how to route this call.
- Enter an off-pbx-telephone configuration set to use with this call. The default values for configuration set 1 were used for compliance testing.

change off-pbx-telephone station-mapping 61020							Page	1	of	3
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION										
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set	Dual Mode			
61020	OPS	-		61020	aar	1				
61020	EC500	-		17205551212	ars	1				

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Locations that can be occupied by SIP Entities
- SIP Entities corresponding to Session Manager, and Communication Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed

Configuration is accomplished by accessing the browser-based GUI of System Manager using the URL “https://<ip-address>/SMGR”, where <ip-address> is the IP address of System Manager. Log in with the appropriate credentials.

6.1. Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Do this by selecting **Domains** on the left and clicking the **New** button (not shown) on the right. The following screen will then be shown. Provide the following:

- Name: The authoritative domain name (e.g., d4f27.com).
- Type: Select SIP
- Notes: Descriptive text (optional).

Click **Commit**.

The screenshot shows the Avaya Aura System Manager 6.3 web interface. The top navigation bar includes the Avaya logo, the text 'Aura System Manager 6.3', and a 'Last Logged on at July 25, 2014 12:50 PM' status. Below the navigation bar, there are tabs for 'Home' and 'Routing'. The 'Routing' tab is active, and a sidebar on the left lists various routing-related options: 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The 'Domains' option is selected. The main content area is titled 'Domain Management' and shows a table with one item. The table has columns for 'Name', 'Type', and 'Notes'. The 'Name' column contains 'd4f27.com', the 'Type' column contains 'sip', and the 'Notes' column is empty. There are 'Commit' and 'Cancel' buttons at the bottom right of the table. A 'Filter: Enable' link is also visible in the top right corner of the table area.

Name	Type	Notes
d4f27.com	sip	

6.2. Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management. To add a location, select **Locations** on the left and click on the **New** button (not shown) on the right. The following screen will then be shown. Provide the following:

Under *General*:

- Name: A descriptive name.
- Notes: Descriptive text (optional).

Under Location Pattern:

- IP Address Pattern: A pattern used to logically identify the location.
- Notes: Descriptive text (optional).

The location configured below is where Communication Manager and Session Manager reside. Click **Commit** to save the Location definition.

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Locations

Help ?

Location Details

Commit

Cancel

General

* Name:

d4f27_l1

Notes:

Dial Plan Transparency in Survivable Mode

Enabled:

☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units:

Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location):

1000

Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location):

1000

Kbit/Sec

* Minimum Multimedia Bandwidth:

64

Kbit/Sec

* Default Audio Bandwidth:

80

Kbit/sec

Alarm Threshold

Overall Alarm Threshold:

80

%

Multimedia Alarm Threshold:

80

%

* Latency before Overall Alarm Trigger:

5

Minutes

* Latency before Multimedia Alarm Trigger:

5

Minutes

Location Pattern

Add

Remove

1 Item

Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.64.50.*	

Select : All, None

Commit

Cancel

6.3. Add SIP Entities

In the sample configuration, a SIP Entity is added for Session Manager, and Communication Manager.

6.3.1. Avaya Aura® Session Manager

A SIP Entity must be added for Session Manager. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Provide the following:

Under *General*:

- Name: A descriptive name.
- FQDN or IP Address: IP address of the signaling interface on Session Manager.
- Type: Select Session Manager.
- Location: Select one of the locations defined previously.
- Time Zone: Time zone for this location.

Defaults may be used for the remaining fields. Click **Commit** to save each SIP Entity definition.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top navigation bar includes the Avaya logo, the text 'Aura® System Manager 6.3', and a 'Last Logged on at July 25, 2014 12:50 PM' status. A 'Go to...' search bar and a 'Log off admin' link are also present. The left sidebar contains a menu with 'Routing' selected, and sub-items: Domains, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area shows the breadcrumb 'Home / Elements / Routing / SIP Entities' and a 'Help ?' link. The 'SIP Entity Details' form is titled 'General' and includes a 'Commit' button and a 'Cancel' button. The form fields are: 'Name' (text input with value 'sm5031'), 'FQDN or IP Address' (text input with value '10.64.50.31'), 'Type' (dropdown menu with 'Session Manager' selected), 'Notes' (text input), 'Location' (dropdown menu with 'd4f27_11' selected), 'Outbound Proxy' (dropdown menu), 'Time Zone' (dropdown menu with 'America/Denver' selected), 'Credential name' (text input), and 'SIP Link Monitoring' (dropdown menu with 'Use Session Manager Configuration' selected). A 'SIP Link Monitoring' link is also visible in the bottom left of the form area.

6.3.2. Avaya Aura® Communication Manager

A SIP Entity must be added for Communication Manager. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Provide the following:

Under *General*:

- Name: A descriptive name.
- FQDN or IP Address: FQDN or IP address of the signaling interface (e.g.,Procr) in the G450 telephony system.
- Type: Select CM.
- Location: Select one of the locations defined previously.
- Time Zone: Time zone for this location.

Defaults may be used for the remaining fields. Click **Commit** to save each SIP Entity definition.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and includes a breadcrumb trail 'Home / Elements / Routing / SIP Entities'. At the top right of the main area are 'Commit' and 'Cancel' buttons, and a 'Help ?' link. The form is divided into three sections: 'General', 'Loop Detection', and 'SIP Link Monitoring'. The 'General' section contains fields for: Name (cm5052), FQDN or IP Address (cm5052.d4f27.com), Type (CM), Notes, Adaptation, Location (d4f27_11), Time Zone (America/Denver), SIP Timer B/F (in seconds) (4), Credential name, Call Detail Recording (none), Loop Detection Mode (Off), and SIP Link Monitoring (Link Monitoring Enabled).

6.4. Add Entity Links

The SIP trunk from Session Manager to Communication Manager are described by Entity Links. To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

- Name: A descriptive name.
- SIP Entity 1: Select the Session Manager.
- Protocol: Select TLS as the transport protocol.
- Port: Port number to which the other system sends SIP Requests (e.g., 5061 for TLS).
- SIP Entity 2: Select the Communication Manager.
- Port: Port number to which the other system sends SIP Requests (e.g., 5061 for TLS).
- Connection Policy: Select Trusted.

The following screens display the configuration of the entity link is for the connection between Session Manager and Communication Manager.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with options: Home, Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links (selected), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Entity Links' and shows a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, Port, Connection Policy, Deny New Service, and Notes. The item in the table is 'sm5031_cm5052_5061' with the following values: SIP Entity 1: sm5031, Protocol: TLS, Port: 5061, SIP Entity 2: cm5052, DNS Override: (unchecked), Port: 5061, Connection Policy: trusted, Deny New Service: (unchecked), and Notes: (empty). The table is filtered by 'Filter: Enable'. The interface also includes a 'Commit' button and a 'Cancel' button at the bottom right of the table area.

6.5. Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.3**. One routing policy was added for Communication Manager. To add a routing policy, select **Routing Policies** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under *General*:

Enter a descriptive name in **Name**.

Under *SIP Entity as Destination*:

Click **Select**, and then select the appropriate SIP entity to which this routing policy applies.

Defaults can be used for the remaining fields. Click **Commit** to save each Routing Policy definition. The following screen shows the Routing Policy for Communication Manager.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies (selected), Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Routing Policy Details' and includes 'Commit' and 'Cancel' buttons. Under the 'General' tab, the 'Name' field is set to 'cm5052', 'Disabled' is unchecked, 'Retries' is set to 0, and the 'Notes' field is empty. Under the 'SIP Entity as Destination' tab, a 'Select' button is visible. Below this, a table lists the selected SIP entity:

Name	FQDN or IP Address	Type	Notes
cm5052	cm5052.d4f27.com	CM	

6.6. Add Dial Patterns

Dial patterns must be defined that will direct calls to the appropriate SIP Entity. In the sample configuration, 12-digit numbers beginning with “91” will be routed to Communication Manager. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Provide the following:

Under *General*:

- Pattern: Dialed number or prefix.
- Min Minimum length of dialed number.
- Max Maximum length of dialed number.
- SIP Domain SIP domain of dial pattern.
- Notes Comment on purpose of dial pattern.

Under *Originating Locations and Routing Policies*:

Click **Add**, and then select the appropriate location and routing policy from the list.

Default values can be used for the remaining fields. Click **Commit** to save this dial pattern.

AVAYA
Aura® System Manager 6.3

Last Logged on at July 25, 2014 12:50 PM
Go to... Log off admin

Home / Elements / Routing / Dial Patterns

Routing

Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults

Dial Pattern Details

Commit Cancel

General

* Pattern: 91

* Min: 12

* Max: 12

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: d4f27.com

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
-ALL-		cmS052	0	<input type="checkbox"/>	cmS052	

Select : All, None

Denied Originating Locations

Add Remove

0 Items

Originating Location	Notes
----------------------	-------

Commit Cancel

7. Configure Spectralink Wireless Server

This section focuses only on the configuration of the Spectralink Wireless Server solution. The values configured in this section were used during the compliance tests. The procedures include the following areas:

- Administer Spectralink Wireless Server IP address
- Administer DECT handset subscription
- Enable Call Forward feature code
- Administer SIP configuration
- Administer DECT users
- Administer Spectralink Base Station IP address
- Administer Wireless Sever host

7.1. Administer Spectralink Wireless Server IP address

The default IP address of a Spectralink Wireless Server is 192.168.0.1. Connect a PC directly to the Spectralink Wireless Server with an Ethernet crossover cable. Open up an Internet browser and type in the following URL, <http://192.168.0.1>. From the menu, click on **Configuration** → **General** and enter the following:

- Method Select “Use Static IP address”
- IP addr Enter IP address
- Netmask Enter subnet mask address
- Gateway Enter default gateway address
- DNS primary Server Enter DNS IP address (Optional)
- NTP Server Enter NTP Server IP Address (Optional)
- Time Zone Select Time Zone (Optional)

Click **Save** to save changes.

The screenshot shows the 'General Configuration' page for the 'IP-DECT Server 6500'. The page has a blue header with the Spectralink logo and navigation tabs: Status, Configuration (selected), Users, Administration, Firmware, and Statistics. Under 'Configuration', there are sub-tabs: General (selected), Wireless Server, Media Resource, Security, Certificates, SIP, Provisioning, Import/Export, and Statistics. The main content area is divided into sections for IPv4, IPv6, Ethernet, DNS, NTP, UPnP, Remote syslog, and SNMP. The IPv4 section is expanded, showing fields for Method (set to 'Use static IP address'), IP addr (10.64.50.63), Netmask (255.255.255.0), Gateway (10.64.50.1), and MTU. The IPv6 section shows Method set to 'Disabled'. The Ethernet section shows VLAN set to 10. The DNS section shows Hostname, Domain, Primary Server, and Secondary Server fields. The NTP section shows Server (10.64.101.45), Time zone (Mountain Time), and Posix timezone string (MST7MDT,M3.2.0/02:00:00,M11.1.0/0). The UPnP section shows Enabled checked, Broadcast announcements unchecked, and Remote syslog unchecked. The Remote syslog section shows Host, Port (514), Facility (16 Local 0), and Level (info) fields. The SNMP section shows Enabled unchecked, Community (public), Trap host, Trap community, System location, and System contact fields. At the bottom, there are 'Save', 'Cancel', and 'Reboot now' buttons. A small note at the bottom states: '*) Required field **) Require restart © Spectralink Europe ApS All rights reserved.'

7.2. Administer DECT handset subscription

From the menu, click on **Configuration** → **Wireless Server**. Under the **DECT** section, check the box next to **Subscription Allowed**.

Click **Save** to save changes.

The screenshot displays the 'IP-DECT Server 6500' configuration interface. The top navigation bar includes 'Status', 'Configuration', 'Users', 'Administration', 'Firmware', and 'Statistics'. The 'Configuration' tab is active, and the 'Wireless Server' sub-tab is selected. The main content area is titled 'Wireless Server Configuration' and contains several sections:

- DECT**: Includes 'Subscription allowed' (checked), 'Authenticate calls' (unchecked), 'Encrypt voice/data' (set to 'Disabled'), 'System access code' (empty), and 'Send date and time' (checked).
- Media resources**: Includes 'Allow new' (checked).
- Base stations**: Includes 'Allow new' (checked), 'Multicast signaling **' (unchecked), 'Multicast address **' (239.255.1.11), and 'Multicast TTL **' (1).
- Application interface**: Includes 'Username *' (GW-DECT/admin), 'New password' (empty), 'New password again' (empty), 'Enable MSF' (checked), 'Enable XML-RPC' (unchecked), and 'Internal messaging' (checked).
- Feature codes**: Includes 'Enable' (unchecked), 'Call forward unconditional - enable' (*21*\$#), and 'Call forward unconditional - disable' (#21#).
- Language**: Includes 'Phone Language **' (English).

At the bottom, there are 'Save' and 'Cancel' buttons, and a note: '* Required field ** Require restart'. The footer indicates '© Spectralink Europe ApS All rights reserved.'

7.3. Enable Call Forward Feature Code

From the menu, click on **Configuration → Wireless Server**. Under the **Feature Codes** section, check the box next to **Enable**.

Click **Save** to save changes.

The screenshot displays the 'Wireless Server Configuration' page for the 'IP-DECT Server 6500'. The page is organized into several sections with expandable/collapsible headers:

- DECT**
 - Subscription allowed: ☒
 - Authenticate calls: ☐
 - Encrypt voice/data: Disabled (dropdown menu)
 - System access code:
 - Send date and time: ☒
- Media resources**
 - Allow new: ☒
- Base stations**
 - Allow new: ☒
 - Multicast signaling **: ☐
 - Multicast address **: 239.255.1.11
 - Multicast TTL **: 1
- Application interface**
 - Username *: GW-DECT/admin
 - New password:
 - New password again:
 - Enable MSF: ☒
 - Enable XML-RPC: ☐
 - Internal messaging: ☒
- Feature codes**
 - Enable: ☒
 - Call forward unconditional - enable: *21*\$#
 - Call forward unconditional - disable: #21#
- Language**
 - Phone Language **: English (dropdown menu)

At the bottom of the configuration area, there are 'Save' and 'Cancel' buttons. Below these buttons, a small note states: '* Required field ** Require restart'. The footer of the page reads: '© Spectralink Europe ApS All rights reserved.'

7.4. Administer SIP Configuration

This section details settings needed to create the SIP connection from the Spectralink Wireless Server to Communication Manager and Session Manager. Preferred audio codecs and message waiting indications are also set. From the menu, go to **Configuration → SIP** and enter the following:

- General Section:
 - Local Port: **5060**
 - Transport: **UDP**
 - Default Domain: Enter domain name (e.g. **d4f27.com**)
- Proxies Section:
 - Proxy 1: **Enter sip:<IP Address of Session Manager> for the sip URI.**
- Message waiting indication Section:
 - Enable indication: Check the checkbox
 - Enable subscription: Check the checkbox
- Under Media Section, Select preferred codecs and priority

spectralink **IP-DECT Server 6500**

[Status](#)
[Configuration](#)
[Users](#)
[Administration](#)
[Firmware](#)
[Statistics](#)

[General](#)
[Wireless Server](#)
[Media Resource](#)
[Security](#)
[Certificates](#)
[SIP](#)
[Provisioning](#)
[Import/Export](#)

SIP Configuration

General

Local port * **

Transport * **

DNS method * **

Default domain * **

Register each endpoint on separate port ** ☐

Send all messages to current registrar ** ☐

Registration expire(sec) *

Max forwards *

Client transaction timeout(msec) *

SIP type of service (TOS/Diffserv) * **

SIP 802.1p Class-of-Service *

GRUU ☒

Use SIPs URI ☒

TLS allow insecure ** ☐

TCP ephemeral port in contact address ** ☐

Proxies

	Priority	Weight	URI
Proxy 1 **	<input type="text" value="1"/>	<input type="text" value="100"/>	<input type="text" value="sip:10.64.50.31"/>
Proxy 2 **	<input type="text" value="2"/>	<input type="text" value="100"/>	<input type="text"/>
Proxy 3 **	<input type="text" value="3"/>	<input type="text" value="100"/>	<input type="text"/>
Proxy 4 **	<input type="text" value="4"/>	<input type="text" value="100"/>	<input type="text"/>

Authentication

Default user

Default password

Realm

DTMF signalling

Send as RTP (rfc2833) ☒

Offered rfc2833 payload type

Send as SIP INFO ☐

Tone duration(msec) *

Message waiting indication

Enable indication ☒

Enable subscription ** ☒

Subscription expire(sec) *

Media

Packet duration(msec) *

Media type of service (TOS/Diffserv) *

Media 802.1p Class-of-Service *

Port range start * **

Codec priority *

-
-
-
-
-
-

SDP answer with preferred codec ☐

SDP answer with a single codec ☐

Ignore SDP version ☐

Call status

Play on-hold tone ☒

Display status messages ☒

☒ key ends overlap dialing ☐

Call waiting ☒

*) Required field **) Require restart
 © Spectralink Europe ApS All rights reserved

- Click on **Save** to save changes.

7.5. Administer DECT users

From the menu, go to **Users** → **List Users** and click on the **New** button to add a new user.

The screenshot displays the 'IP-DECT Server 6500' web interface. The top navigation bar includes 'Status', 'Configuration', 'Users', 'Administration', 'Firmware', and 'Statistics'. The 'Users' tab is active, and the 'List Users' sub-tab is selected. Below the navigation bar, there is a 'User List' section with an 'Overview' tab. The overview shows the System ARI as '10046545364 [10 26 b2 bd 00]' and a summary of users: 2 total, 2 subscribed, and 2 registered. A 'New' button is located below the summary. Below the overview, there is a search bar and a table of users. The table has columns for 'Enabled', 'User', 'Displayname', 'IPEI', 'Handset', 'Firmware', 'Subscription', and 'Registration'. Two users are listed: one with User ID 61020 and another with User ID 61021. Both users are enabled and have a green checkmark in the 'Registration' column. The table is followed by a pagination bar showing 'Showing 1 to 2 of 2 entries' and buttons for 'First', 'Previous', '1', 'Next', and 'Last'. At the bottom of the page, there is a small copyright notice: '© Spectralink Europe ApS All rights reserved.'

Enabled	User	Displayname	IPEI	Handset	Firmware	Subscription	Registration
✓	61020	61020	05003 0105863	Spectralink Butterfly	14H	✓	✓
✓	61021	61021	05003 0284374	Spectralink 7620	14H	✓	✓

Enter the following in the new **User** window:

- **IPEI:** Enter the handset IPEI
- **Access Code** Enter a desired access code (Optional)
- **Standby Text** Enter desired standby text (Optional)
- **Username / Extension** Enter the extension number used to register with Session Manager
- **Domain** Enter the SIP domain name used in **Section 6.1**
- **Displayname** Enter a desired display name (Optional)
- **Authentication User** Enter the user defined for Session Manager
- **Authentication Password** Enter password for user.

The screenshot shows the 'IP-DECT Server 6500' web interface. The top navigation bar includes 'Status', 'Configuration', 'Users', 'Administration', 'Firmware', and 'Statistics'. Below this, there are sub-tabs for 'List Users' and 'Import/Export'. The main content area is titled 'User' and contains the following fields:

- DECT device** (header)
- Model
- Software part number
- Firmware
- IPEI
- Access code
- User** (header)
- Standby text
- Disabled ☐
- SIP** (header)
- Username / Extension *
- Domain
- Displayname
- Authentication user
- Authentication password
- Features** (header)
- Call forward unconditional

At the bottom of the form are three buttons: 'Save', 'Delete', and 'Cancel'. Below the buttons is a small note: '* Required field'. The footer of the page reads '© Spectralink Europe ApS All rights reserved'.

Click on **Save** to save changes.

7.6. Administer Spectralink Base Station IP address

The default IP address of a Spectralink Base Station is 192.168.0.1. Connect a PC directly to the Base Station with an Ethernet crossover cable. Open up an Internet browser and type in the following URL, <http://192.168.0.1>. From the menu, click on **Configuration** → **General** and enter the following:

- Use Static IP address Click the button to select
- IP addr Enter IP address
- Netmask Enter subnet mask
- Gateway Enter default gateway IP address
- NTP Server Enter NTP Server IP Address (Optional)

Click **Save** to save changes.

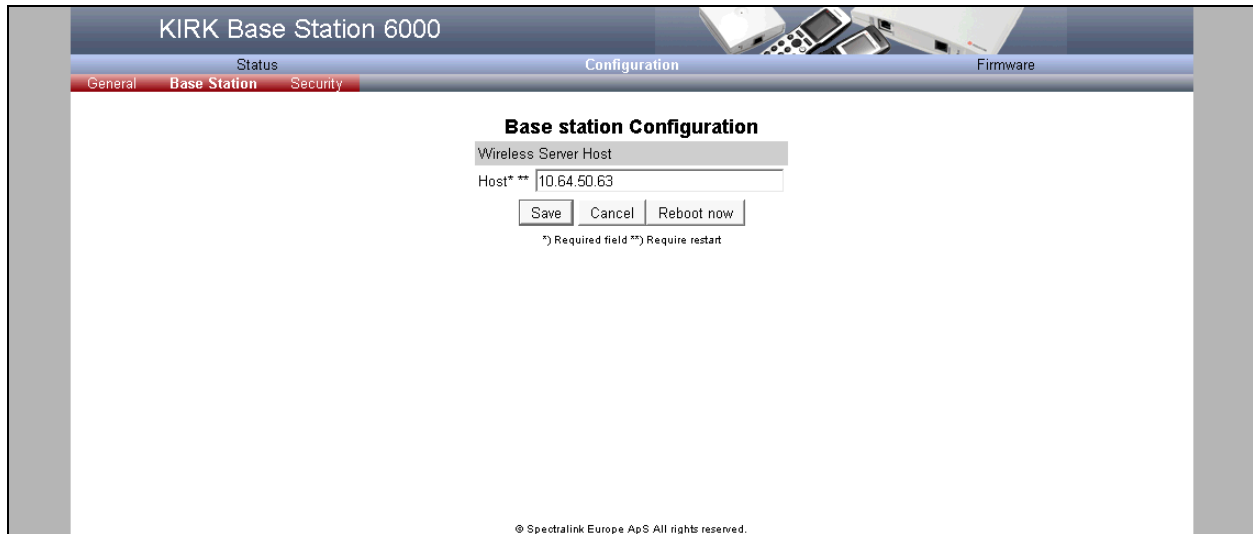
The screenshot shows the 'KIRK Base Station 6000' configuration interface. The top navigation bar includes 'Status', 'Configuration', and 'Firmware'. The 'Configuration' tab is active, and the 'General' sub-tab is selected. The 'General Configuration' section contains the following fields and options:

- IP**
 - DHCP assigned: ☐
 - Use static IP address: ☒
 - IP addr*:
 - Netmask **:
 - Gateway **:
 - MTU **:
 - VLAN **:
- DNS**
 - Domain:
 - Primary Server:
 - Secondary Server:
- NTP**
 - Server:
- UPnP**
 - Enabled **: ☒
 - Broadcast announcements **: ☐
- Remote syslog**
 - Host:
 - Port *:
 - Facility *:
 - Level *:

At the bottom, there are three buttons: 'Save', 'Cancel', and 'Reboot now'. Below the buttons, a small note states: '* Required field ** Require restart'. At the very bottom, the copyright notice reads: '© Spectralink Europe ApS All rights reserved.'

7.7. Administer Wireless Sever host

From the menu, go to **Configuration** → **Base Station** and for **Host** enter the ip address of the Spectralink Wireless Server 6500 configured in **Section 6.1**.
Click **Save** to save changes.



The screenshot displays the web interface for the KIRK Base Station 6000. At the top, the title bar reads "KIRK Base Station 6000". Below it, a navigation menu includes "Status", "Configuration", and "Firmware". The "Configuration" tab is active, and within it, the "Base Station" sub-tab is selected. The main content area is titled "Base station Configuration" and contains a section for "Wireless Server Host". A text field labeled "Host**" contains the IP address "10.64.50.63". Below the text field are three buttons: "Save", "Cancel", and "Reboot now". A small note at the bottom of the configuration area states: "*) Required field **) Require restart". The footer of the page reads "© Spectralink Europe ApS All rights reserved."

8. Verification Steps

The following steps may be used to verify the configuration:

8.1. Verify Registered spectralink Endpoints on Avaya Aura® Session Manager

From the System Manager GUI select **Elements** → **Session Manager** → (Not Shown). From the left pane select **System Status** → **User Registrations**. Find and verify that the spectralink endpoints are registered.

Note: The spectralink endpoints will use the IP address of the spectralink Wireless Server.

Avaya Aura® System Manager 6.3

Last Logged on at August 6, 2014 10:24 AM

Home / Elements / Session Manager / System Status / User Registrations

User Registrations

Select rows to send notifications to devices. Click on Details column for complete registration status.

View: Default Force Unregister AST Device Notifications: Reboot Reload Failback As of 1:31 PM

20 Items Show 15 Filter: Enable

Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered
										Prim Sec Surv
Show	---	Arsenio	Hall	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>
Show	---	Conan	O'Brian	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>
Show	---	Paul	McCartney	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>
Show	61020@d4f27.com	Chuck	Cheese	---	10.64.50.63	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	(AC) <input type="checkbox"/>
Show	---	George	Harrison	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>
Show	---	Bruce	Wayne	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>
Show	---	Tom	Thumb	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>
Show	---	Jay	Leno	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>
Show	61021@d4f27.com	Ringo	Starr	---	10.64.50.63	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	(AC) <input type="checkbox"/>
Show	---	Tinker	Bell	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>
Show	---	Jimmy	Kimmel	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>
Show	61003@d4f27.com	Bo	Jackson	---	10.64.52.209	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	(AC) <input type="checkbox"/>
Show	61001@d4f27.com	Papa	Smurf	---	10.64.52.208	<input type="checkbox"/>	<input type="checkbox"/>	1/1	<input checked="" type="checkbox"/>	(AC) <input type="checkbox"/>
Show	---	Cliff	Bar	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>
Show	---	Mary	Mary	---	---	<input type="checkbox"/>	<input type="checkbox"/>	0/1	<input type="checkbox"/>	<input type="checkbox"/>

Select: All, None Page 1 of 2

8.2. Verify Active Call on Avaya Aura® Communication Manager

From the SAT interface use the status trunk command to determine which port(s) are carrying an active call.

status trunk 2				
TRUNK GROUP STATUS				
Member	Port	Service State	Mtce Connected Ports Busy	
0002/001	T00036	in-service/active	no	T00044
0002/002	T00037	in-service/idle	no	
0002/003	T00038	in-service/idle	no	
0002/004	T00039	in-service/idle	no	
0002/005	T00040	in-service/idle	no	
0002/006	T00041	in-service/idle	no	
0002/007	T00042	in-service/idle	no	
0002/008	T00043	in-service/idle	no	
0002/009	T00044	in-service/active	no	T00036
0002/010	T00045	in-service/idle	no	

The screen shot below displays a g711mu call between an Avaya Deskphone with IP address 10.64.52.209 and the spectralink Wireless Server at IP address 10.64.50.63.

Note: *The spectralink Wireless Server proxies for the DECT phone.*

status trunk 2/001		Page 3 of 3
SRC PORT TO DEST PORT TALKPATH		
src port: T00036		
T00036:TX:10.64.52.209:5004/g711u/20ms		
T00044:RX:10.64.50.63:58364/g711u/20ms		
dst port: T00044		

8.3. Verify Spectralink Wireless Server Status

8.3.1. Quick Status

From the menu, go to **Status** → **General** and verify **Quick Status** green checks indicate proper functionality. Mouse over indicator for a status explanation.

The screenshot displays the Spectralink IP-DECT Server 6500 web interface. The top navigation bar includes tabs for Status, Configuration, Users, Administration, Firmware, and Statistics. The Status tab is active, and the General sub-tab is selected. The main content area shows the General Status page, which includes sections for General, Hardware, Firmware, and Quick status. The Quick status section shows green checkmarks for SIP, Base stations, Media resources, and NTP, and a yellow warning icon for Provisioning.

General Status	
General	
IP address	10.64.50.63
NTP Server	10.64.101.45
Time	2014-08-06 08:02:21
Serial	8447509
MAC address	00:13:d1:80:e6:15
Product ID	000A 9E5A 4BBA 50B7
Production Date	2013-03-21
Hardware	
PartNo	14212520
PCS	02_
Firmware	
PartNo	14218500
PCS	PCS14B_
Build	47171
Quick status	
SIP	✓
Base stations	✓
Media resources	✓
Provisioning	⚠
NTP	✓

© Spectralink Europe ApS All rights reserved.

8.3.2. List Users

From the menu, go to **Users** → **List Users** and verify that each user has subscribed and registered successfully.

The screenshot displays the 'IP-DECT Server 6500' web interface. The top navigation bar includes 'Status', 'Configuration', 'Users', 'Administration', 'Firmware', and 'Statistics'. The 'Users' menu is expanded, showing 'List Users' and 'Import/Export'. The 'User List' page features an 'Overview' section with 'System ARI' 10046545364 [10 26 b2 bd 00] and a summary table:

	Users	Subscribed	Registered
Total	2	2	2

Below the summary is a 'New' button and a search bar. The main table lists users with columns: Enabled, User, Displayname, IPEI, Handset, Firmware, Subscription, and Registration. Two users are listed, both with green checkmarks in the Subscription and Registration columns.

Enabled	User	Displayname	IPEI	Handset	Firmware	Subscription	Registration
✓	61020	61020	05003 0105863	Spectralink Butterfly	14H	✓	✓
✓	61021	61021	05003 0284374	Spectralink 7620	14H	✓	✓

At the bottom, it says 'Showing 1 to 2 of 2 entries' and includes pagination controls: First, Previous, 1 (selected), Next, Last. The footer contains the copyright notice: '© Spectralink Europe ApS All rights reserved.'

8.3.3. Active Call

From the menu, go to **Statistics** → **Active Calls** to display active call details.

The screenshot displays the Spectralink IP-DECT Server 6500 web interface. The top navigation bar includes tabs for Status, Configuration, Users, Administration, Firmware, and Statistics. The 'Statistics' tab is active, and the 'Active Calls' sub-tab is selected. Below the navigation bar, the 'Active Calls' section shows a table with one entry. The table columns are: Established, Duration, Direction, State, Codec, Secure, Local user, and Remote user. The entry shows a call established on 2014-08-06 at 08:10:57, with a duration of 0:11, direction of Outgoing, state of Active(5), codec of PCMU/8000, secure flag of N, local user of 61021, and remote user of 61003. The interface also includes a search bar, a 'Show All entries' dropdown, and pagination controls (First, Previous, 1, Next, Last). The footer of the interface contains the copyright notice: © Spectralink Europe ApS All rights reserved.

Established	Duration	Direction	State	Codec	Secure	Local user	Remote user
2014-08-06 08:10:57	0:11	Outgoing	Active(5)	PCMU/8000	N	61021	61003

9. Conclusion

These Application Notes describe the configuration steps required for the Spectralink Wireless Server 6500/400 solution to successfully interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. All feature functionality and serviceability test cases were completed successfully.

10. Additional References

The documents referenced below were used for additional support and configuration information.

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

[1] *Administering Avaya Aura® Session Manager*, Release 6.3 Issue 5 June 2014

[2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 6.3 Issue 12 June 2014

Product documentation for Spectralink Wireless Solution may be found at:
<http://www.spectralink.com/product-information/dect>

©2014 Avaya Inc. All Rights Reserved.

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

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