



Avaya Solution & Interoperability Test Lab

Application Notes for DiVitas Mobile Unified Communications with Avaya Communication Manager and Avaya SIP Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate the DiVitas Mobile Unified Communications (Mobile UC) solution with Avaya Communication Manager and Avaya SIP Enablement Services. The DiVitas Mobile UC solution provides the seamless convergence of WiFi and cellular networks enabling roaming (back and forth) between the two networks. The DiVitas solution includes the DiVitas Server and the DiVitas Clients. The DiVitas Server connects over the network to mobile handsets running the DiVitas Client, such as the Nokia E- and N-Series, and connects to the PSTN through Avaya Communication Manager and Avaya SIP Enablement Services using a SIP trunk.

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

1. Introduction

These Application Notes describe the configuration steps required to integrate the DiVitas Mobile Unified Communications (Mobile UC) solution with Avaya Communication Manager and Avaya SIP Enablement Services. The DiVitas Mobile UC solution provides the seamless convergence of WiFi and cellular networks enabling roaming (back and forth) between the two networks. The DiVitas solution includes the DiVitas Server and the DiVitas Clients. The DiVitas Server connects over the network to mobile handsets running the DiVitas Client, such as the Nokia E- and N-Series, and connects to the PSTN through Avaya Communication Manager and Avaya SIP Enablement Services using a SIP trunk using a SIP trunk.

Figure 1 illustrates a sample configuration consisting of a pair of Avaya S8710 Servers running Avaya Communication Manager, an Avaya G650 Media Gateway, Avaya SIP Enablement Services (SES), and dual-mode wireless telephones registered with DiVitas Mobile Unified Communications. The solution described herein is also applicable to other Avaya Servers and Media Gateways. Avaya 4600 Series H.323 IP Telephones, Avaya 9600 Series SIP Telephones, and Avaya analog and digital telephones were included in the configuration to verify calls with the SIP-based DiVitas Mobile UC Server and DiVitas Clients. Calls were also routed from the DiVitas Clients to the PSTN through Avaya SES. A SIP trunk was established between the DiVitas Mobile UC Server and Avaya SES. The DiVitas Server is configured as a trusted host in Avaya SES. The DiVitas Server supports the G.711 codec using RFC2833 for DTMF. The Avaya G650 Media Gateway connected to the PSTN via an ISDN-PRI trunk.

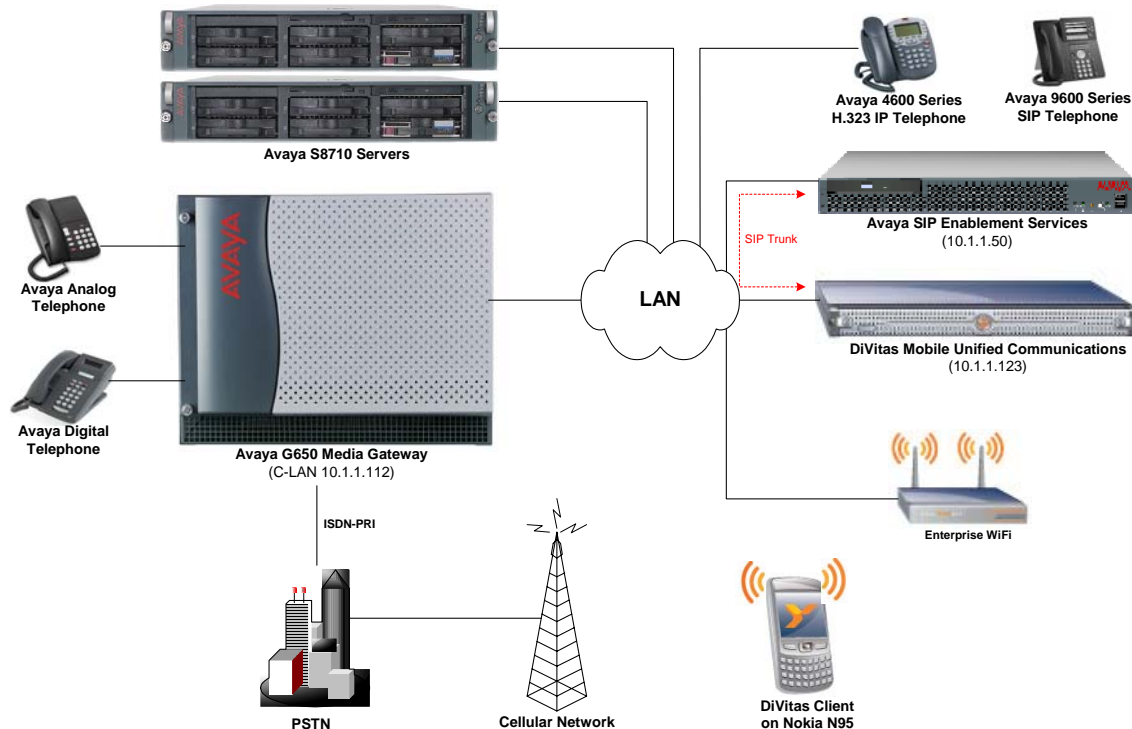


Figure 1: DiVitas Mobile Unified Communications with Avaya SIP-based Network

2. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8710 Server with G650 Media Gateway	Avaya Communication Manager 5.0 (R015x.00.0.825.4)
Avaya SIP Enablement Services	5.0 (SES-5.0.0.0-825.31)
Avaya 4600 Series IP Telephones	2.8 (H.323)
Avaya 9600 Series IP Telephones	2.0.4 (SIP)
Avaya 6400 Series Digital Telephones	--
Avaya Analog Telephones	--
DiVitas Mobile Unified Communications	2.1
DiVitas Client on Nokia N95	2.1

Table 1: Equipment and Software Validated

3. Configure Avaya Communication Manager

This section describes the procedure for configuring a SIP trunk between Avaya Communication Manager and Avaya SES, simultaneous ringing between a desktop phone and a DiVitas Client, and call routing. Avaya Communication Manager configuration was performed using the System Access Terminal (SAT). Refer to [1] and [3] for additional details.

3.1. Configure SIP Trunk

This section covers the configuration of the SIP trunk between Avaya Communication Manager and Avaya SES. Configuration of the IP network region and IP codec set is also included.

Enter the **display system-parameters customer-options** command to verify that the number of SIP trunks supported by the system is sufficient per the customer's requirements. If not, contact an authorized Avaya account representative to obtain additional licenses.

```
display system-parameters customer-options                               Page 2 of 10
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                                    USED
      Maximum Administered H.323 Trunks: 100 40
      Maximum Concurrently Registered IP Stations: 12000 2
      Maximum Administered Remote Office Trunks: 0 0
Maximum Concurrently Registered Remote Office Stations: 0 0
      Maximum Concurrently Registered IP eCons: 0 0
      Max Concur Registered Unauthenticated H.323 Stations: 5 0
      Maximum Video Capable H.323 Stations: 10 0
      Maximum Video Capable IP Softphones: 10 0
      Maximum Administered SIP Trunks: 200 130
Maximum Administered Ad-hoc Video Conferencing Ports: 0 0
      Maximum Number of DS1 Boards with Echo Cancellation: 1 0
      Maximum TN2501 VAL Boards: 10 1
      Maximum Media Gateway VAL Sources: 50 0
      Maximum TN2602 Boards with 80 VoIP Channels: 128 1
      Maximum TN2602 Boards with 320 VoIP Channels: 128 0
      Maximum Number of Expanded Meet-me Conference Ports: 0 0

(NOTE: You must logoff & login to effect the permission changes.)
```

Figure 2: System-Parameters Customer-Options Form

In the **IP Node Names** form, associate a name with the IP addresses of Avaya SES and the C-LAN board in the Avaya G650 Media Gateway.

```
change node-names ip                                                    Page 1 of 2
                                IP NODE NAMES
      Name                      IP Address
clan                        10.1.1.112
medpro                        10.1.1.116
ses-he                      10.1.1.50
```

Figure 3: IP Nodes Names

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Avaya SES. In this configuration, the domain name is *east.devcon.com*. By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between SIP endpoints without using media resources in the Avaya G650 Media Gateway. The **IP Network Region** form also specifies the **IP Codec Set** to be used for local calls and calls routed over the SIP trunk to Avaya SES. This codec set is used when its corresponding network region (i.e., IP Network Region '1') is specified in the SIP signaling group as shown in **Figure 6**. The IP network region for local and outgoing trunk calls may be different.

```

change ip-network-region 2                                     Page 1 of 19
                                     IP NETWORK REGION
  Region: 2
Location:      Authoritative Domain: east.devcon.com
  Name:
MEDIA PARAMETERS      Intra-region IP-IP Direct Audio: yes
  Codec Set: 2        Inter-region IP-IP Direct Audio: yes
  UDP Port Min: 2048      IP Audio Hairpinning? y
  UDP Port Max: 3029
DIFFSERV/TOS PARAMETERS      RTCP Reporting Enabled? n
  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
  Keep-Alive Count: 5

```

Figure 4: IP Network Region

In the **IP Codec Set** form, select the audio codec type supported for calls routed over the SIP trunk. The form is accessed via the **change ip-codec-set 2** command. Note that IP codec set '2' was specified in IP Network Region '2' shown in **Figure 4**. The default settings of the **ip-codec-set** form are shown below. Currently, the DiVitas Mobile Unified Communications solution supports the G.711 codec.

```

change ip-codec-set 2                                     Page 1 of 2
                                     IP Codec Set
  Codec Set: 2
  Audio      Silence      Frames      Packet
  Codec      Suppression  Per Pkt    Size(ms)
1: G.711MU      n          2          20
2:
3:

```

Figure 5: IP Codec Set

Prior to configuring a SIP trunk group for communication with Avaya SES, a SIP signaling group must be configured. Configure the **Signaling Group** form as shown in **Figure 6**:

- Set the **Group Type** field to *sip*.
- The **Transport Method** field will default to *tls* (Transport Layer Security).
- Specify the C-LAN board in the G650 Media Gateway and Avaya SES as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These field values are taken from the **IP Node Names** form shown in **Figure 3**.
- Ensure that the recommended TLS port value of *5061* is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- Specify the IP network region to be used for outgoing calls that use this signaling group in **Far-end Network Region** field. The codec type for the outgoing call is derived from the IP codec set specified in the IP network region. In this configuration, IP network region '2' and IP codec set '2' is used which allows the G.711mu-law codec for the call.
- Enter the domain name of Avaya SIP Enablement Services in the **Far-end Domain** field. In this configuration, the domain name is *east.devcon.com*. This domain is specified in the Uniform Resource Identifier (URI) of the "SIP To Address" in the INVITE message. Mis-configuring this field may prevent calls from being successfully established to other SIP endpoints or to the PSTN.
- If calls to/from SIP endpoints are to be shuffled, then the **Direct IP-IP Audio Connections** field must be set to 'y'.
- The **DTMF over IP** field should be set to the default value of *rtp-payload*. Avaya Communication Manager supports DTMF transmission using RFC 2833. The default values for the other fields may be used.

```

change signaling-group 2                               Page 1 of 1
                SIGNALING GROUP

Group Number: 2          Group Type: sip
                        Transport Method: tls

Near-end Node Name: clan          Far-end Node Name: ses-he
Near-end Listen Port: 5061       Far-end Listen Port: 5061
                                Far-end Network Region: 2
Far-end Domain: east.devcon.com

                                Bypass If IP Threshold Exceeded? n

DTMF over IP: rtp-payload        Direct IP-IP Audio Connections? y
                                IP Audio Hairpinning? n
Enable Layer 3 Test? n
Session Establishment Timer(min): 120

```

Figure 6: Signaling Group

Configure the **Trunk Group** form as shown in **Figure 7**. Set the **Group Type** field to *sip*, set the **Service Type** field to *tie*, specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. For SIP calls, two trunk members are used for the duration of the call. Configure the other fields in bold and accept the default values for the remaining fields.

```

change trunk-group 2                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 2                                         Group Type: sip           CDR Reports: y
  Group Name: To Avaya SES                            COR: 1                   TN: 1           TAC: 102
  Direction: two-way                                   Outgoing Display? n
Dial Access? n                                         Night Service:
Queue Length: 0
Service Type: tie                                     Auth Code? n
                                                         Signaling Group: 2
                                                         Number of Members: 10
  
```

Figure 7: Trunk Group – Page 1

On Page 2 of the trunk group form, set the **Numbering Format** field to *public*. This field specifies the format of the calling party number sent to the far-end.

```

change trunk-group 2                                     Page 3 of 21
TRUNK FEATURES
  ACA Assignment? n                                     Measured: none
                                                         Maintenance Tests? y
                                                         Numbering Format: public
                                                         UUI Treatment: service-provider
                                                         Replace Restricted Numbers? n
                                                         Replace Unavailable Numbers? n
Show ANSWERED BY on Display? y
  
```

Figure 8: Trunk Group – Page 2

Configure the **Public/Unknown Numbering Format** form to send the calling party number to the far-end. Add an entry so that local stations with a 5-digit extension beginning with '6' and whose calls are routed over SIP trunk group '2' have the number sent to the far-end for display purposes. In the example shown in **Figure 9**, a CPN prefix is added to 5-digit extensions beginning with '6' and routed over trunk group '2' so that a 10-digit calling party number (e.g., extension 60004 is converted to 7328560004) is sent to the far-end. If the **CPN Prefix** field is left blank and the **CPN Len** field is set to '5', then the 5-digit extension corresponding to the calling party will be sent to the far-end to be displayed on the Nokia N95 (i.e., DiVitas Client) phone display. Additional entries may be included to cover other extensions.

```
change public-unknown-numbering 6                               Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT
Ext Ext      Trk      CPN      Total
Len Code    Grp(s)   Prefix   CPN
5  6         2         73285   5
Total Administered: 32
Maximum Entries: 9999
```

Figure 9: Public Unknown Numbering Format

3.2. Simultaneous Ringing

This section describes how to enable simultaneous ringing between a desktop IP phone on Avaya Communication Manager and a DiVitas Client.

Although not required, a Nokia N95 DiVitas Client may be associated with a desk phone configured on Avaya Communication Manager. This would allow a desk phone and the DiVitas Client to ring simultaneously when a call is received. The call can then be answered by either the desk phone or the DiVitas Client. To configure simultaneous ringing for the DiVitas Client, first configure a station as shown in **Figure 10**. In this example, the station maps to an H.323 IP phone with an extension of 61003 and the DiVitas Client has an extension of 40000. The station may or may not share the same extension as the DiVitas Client.

```
add station 61003                                             Page 1 of 5
STATION
Extension: 61003      Lock Messages? n      BCC: 0
Type: 4610           Security Code: XXXXXX TN: 1
Port: S00042         Coverage Path 1:      COR: 1
Name: H323-61003     Coverage Path 2:      COS: 1
                    Hunt-to Station:
STATION OPTIONS
Loss Group: 19      Time of Day Lock Table:
                    Personalized Ringing Pattern: 1
                    Message Lamp Ext: 61003
Speakerphone: 2-way Mute Button Enabled? y
Display Language: english
Survivable GK Node Name:
Survivable COR: internal
Survivable Trunk Dest? y
Media Complex Ext:
IP SoftPhone? n
Customizable Labels? y
```

Figure 10: Station

To allow a call to the H.323 IP phone to be delivered to the DiVitas Client at the same time, the **Stations with Off-PBX Telephone Integration** form must be configured. On this form, specify the extension of the SIP endpoint and set the **Application** field to *CSP*. The **Phone Number** field is set to the digits to be sent over the SIP trunk. As previously mentioned, the **Station Extension** and **Phone Number** fields may match if the extensions of the desk phone and the DiVitas Client are the same. Finally, the **Trunk Selection** field is set to '2', the SIP trunk group number. This field specifies the trunk group used to route the call. Another option for routing a call over a SIP trunk group is to use Auto Alternate Routing (AAR) or Auto Route Selection (ARS) routing instead. In this case, the **Trunk Selection** field would be set to *aar* or *ars*. Configuration of other AAR or ARS forms would also be required. Refer to [1] for information on routing calls using AAR or ARS. Repeat this step for each DiVitas Client associated with a desk phone.

change off-pbx-telephone station-mapping 61003							Page	1 of	2
STATIONS WITH OFF-PBX TELEPHONE INTEGRATION									
Station Extension	Application	Dial Prefix	CC	Phone Number	Trunk Selection	Config Set			
61003	CSP	-	-	40000	2	1			

Figure 11: Stations with Off-PBX Telephone Integration

3.3. Call Routing

This section describes how to configure call routing from Avaya Communication Manager to a DiVitas Client using AAR.

In the **Dial Plan Analysis Table**, dialed strings beginning with '4' and '6' were configured as extensions. The dialed string beginning with '4' is configured for the extensions assigned to the DiVitas Clients. The dialed string beginning with '6' is configured for local extensions assigned to SIP, H.323, digital, and analog telephones.

change 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				
1	3	dac										
4	5	ext										
5	5	ext										
6	5	ext										
7	1	aar										
8	1	fac										
9	1	fac										
*5	3	fac										
*6	3	fac										
#	3	fac										

Figure 12: Dial Plan Analysis

In this configuration, the DiVitas Clients were assigned 5-digit extensions beginning with '4'. To route calls to the DiVitas Clients, an entry in the **Uniform Dial Plan Table** was added to route calls using AAR.

```

change uniform-dialplan 4                                     Page 1 of 2
                                UNIFORM DIAL PLAN TABLE
                                Percent Full: 0

Matching      Insert      Node
Pattern      Len Del      Digits      Net Conv Num
4            5 0            aar n

```

Figure 13: Uniform Dial Plan

In the **AAR Digit Analysis Table**, dial strings beginning with '4' are routed over route pattern '44'.

```

change aar analysis 4                                       Page 1 of 2
                                AAR DIGIT ANALYSIS TABLE
                                Location: all                 Percent Full: 2

Dialed      Total      Route      Call      Node      ANI
String      Min Max      Pattern    Type      Num      Reqd
4          5 5          44        aar      n

```

Figure 14: AAR Analysis

In **Route Pattern '44'**, calls are routed over SIP trunk group '2' with no digit manipulation being performed. The exact dial string is sent to Avaya SES and routed based on that number.

```

change route-pattern 44                                     Page 1 of 3
                                Pattern Number: 44  Pattern Name: DiVitas MUC
                                SCCAN? n      Secure SIP? n
  Grp FRL NPA Pfx Hop Toll No.  Inserted      DCS/  IXC
  No   Mrk Lmt List Del  Digits      QSIG
                                Dgts      Intw
1: 2   0
2:
3:
4:
5:
6:
                                n  user
                                n  user
                                n  user
                                n  user
                                n  user

  BCC VALUE  TSC CA-TSC      ITC BCIE Service/Feature PARM  No. Numbering LAR
  0 1 2 M 4 W      Request      rest
                                Subaddress
1: y y y y y n  n      rest      none
2: y y y y y n  n      rest      none
3: y y y y y n  n      rest      none
4: y y y y y n  n      rest      none
5: y y y y y n  n      rest      none
6: y y y y y n  n      rest      none

```

Figure 15: Route Pattern

4. Configure Avaya SIP Enablement Services

This section describes the steps for configuring Avaya SES to communicate with Avaya Communication Manager and the DiVitas Mobile Unified Communications Server. The DiVitas UC Server will be configured as a trusted host on Avaya SES. A host map will be created in Avaya SES for all the calls destined for the DiVitas UC Server and Media Server Maps will be created for routing calls to the PSTN and other stations on Avaya Communication Manager. Refer to [3] for additional information on configuring Avaya SES.

Avaya SIP Enablement Services is configured via an Internet browser using the Administration web interface. To access the Administration web interface, enter *http://<ip-addr>/admin* as the URL in the Internet browser, where *<ip-addr>* is the IP address of Avaya SES. Log in with the appropriate credentials and select the Launch Administration Web Interface link.

To verify the system properties, including the SIP domain and the IP address of Avaya SES, select **Server Configuration**→**System Properties** link on the left pane of the of the Administration web interface. The **System Properties** are shown in **Figure 16**.

The screenshot shows the Avaya Integrated Management SIP Server Management web interface. The header includes the Avaya logo and the text 'Integrated Management SIP Server Management'. Below the header, there is a navigation menu on the left with options like 'Users', 'Adjunct Systems', 'Certificate Management', 'Conferences', 'Export/Import to ProVision', 'Hosts', 'Media Servers', 'Media Server Extensions', 'Server Configuration', 'SIP Phone Settings', 'Survivable Call Processors', 'System Status', 'Trace Logger', and 'Trusted Hosts'. The main content area is titled 'View System Properties' and contains the following information:

- SES Version: SES-5.0.0.0-825.31
- System Configuration: simplex
- Host Type: SES combined home-edge
- SIP Domain*:
- Note that the DNS domain is avaya.com
- If you are unsure about this field, most often the SIP domain should be the root level DNS domain. For example, for a DNS domain of eastcoast.example.com, the SIP domain would likely be configured to example.com. This allows SIP calls and instant messages to users with handles of the format handle@example.com
- SIP License Host*:
- DiffServ/TOS Parameters**
 - Call Control PHB Value*:
- 802.1 Parameters**
 - Priority Value*:
 - Management System Access Login:
 - Management System Access Password:
 - DB Log Level:

At the bottom of the main content area, there is an 'Update' button. The footer of the page contains the text '© 2006 Avaya Inc. All Rights Reserved.'

Figure 16: Avaya SES Web Interface

To enable secure SIP trunking between Avaya SES and Avaya Communication Manager, add a media server interface corresponding to Avaya Communication Manager. In the **Add Media Server Interface** screen shown in **Figure 17**, enter the following information:

- A descriptive name in the **Media Server Interface Name** field (e.g., S8710-CLAN).
- Select the IP address of Avaya SES in the **Host** field.
- Select *TLS* (Transport Link Security) for the **Link Type**. TLS provides encryption at the transport layer.
- Enter the IP address of the C-LAN board in the Avaya G650 Media Gateway in the **SIP Trunk IP Address** field.

After completing the **Add Media Server** screen, click on the **Add** button.

The screenshot shows the 'Add Media Server Interface' configuration page in the Avaya Integrated Management SIP Server Management interface. The page includes a navigation menu on the left with categories like Users, Adjunct Systems, Certificate Management, Conferences, Emergency Contacts, Export/Import to ProVision, Hosts, IM logs, Media Servers, Media Server Extensions, Server Configuration, SIP Phone Settings, Survivable Call Processors, System Status, Trace Logger, and Trusted Hosts. The main content area contains the following fields and options:

- Media Server Interface Name***: Text input field containing 'S8710-CLAN'.
- Host**: Dropdown menu showing '10.1.1.50'.
- SIP Trunk Link Type**: Radio buttons for TCP and TLS (selected).
- SIP Trunk IP Address***: Text input field containing '10.1.1.112'.
- Media Server Admin Address (see Help)**: Text input field containing '10.1.1.102'.
- Media Server Admin Port**: Text input field containing '5022'.
- Media Server Admin Login**: Text input field containing 'sesadmin'.
- Media Server Admin Password**: Text input field containing '*****'.
- Media Server Admin Password Confirm**: Text input field containing '*****'.
- SMS Connection Type**: Radio buttons for SSH (selected), Telnet, and Not Available.

Below the fields, there is a note: "Note: Changing connection type to SSH resets media server admin port to 5022 if the port has not changed. Changing connection type to Telnet resets media server admin port to 5023 if the port has not changed." At the bottom of the form, there is a note: "Fields marked * are required." and an **Add** button.

© 2006 Avaya Inc. All Rights Reserved.

Figure 17: Add Media Server Interface

Incoming calls originated from the DiVitas Clients (e.g., Nokia N95) on the DiVitas UC Server are routed through Avaya Communication Manager. **Media Server Address Maps** are required to route calls to the PSTN and other stations on Avaya Communication Manager. Three media server address maps are used, two for calls destined to the 650 and 732 area codes (see **Figure 18** and **Figure 19**), and one for calls destined to other stations on Avaya Communication Manager (see **Figure 20**). These stations have 5-digit extensions beginning with '6'. For the address maps used to route calls to the 650 and 732 area codes, the leading digit '9' in the **Pattern** field maps to the ARS feature access code required for public network routing. After configuring the address maps, click on the **Add** button.

The screenshot shows the Avaya Integrated Management SIP Server Management interface. The top header includes the Avaya logo, the title 'Integrated Management SIP Server Management', and the server IP '10.1.1.50'. A navigation menu on the left lists various system management options. The main content area is titled 'Add Media Server Address Map' and contains the following form fields:

- Name***: PSTN-650AreaCode
- Pattern***: ^sip:91650[0-9]{7}
- Replace URI**:

Below the fields is a note: 'Fields marked * are required.' and an **Add** button.

Figure 18: Media Server Address Map for the 650 Area Code

The screenshot shows the Avaya Integrated Management SIP Server Management interface, similar to Figure 18. The main content area is titled 'Add Media Server Address Map' and contains the following form fields:

- Name***: PSTN-732AreaCode
- Pattern***: ^sip:91732[0-9]{7}
- Replace URI**:

Below the fields is a note: 'Fields marked * are required.' and an **Add** button.

Figure 19: Media Server Address Map for the 732 Area Code

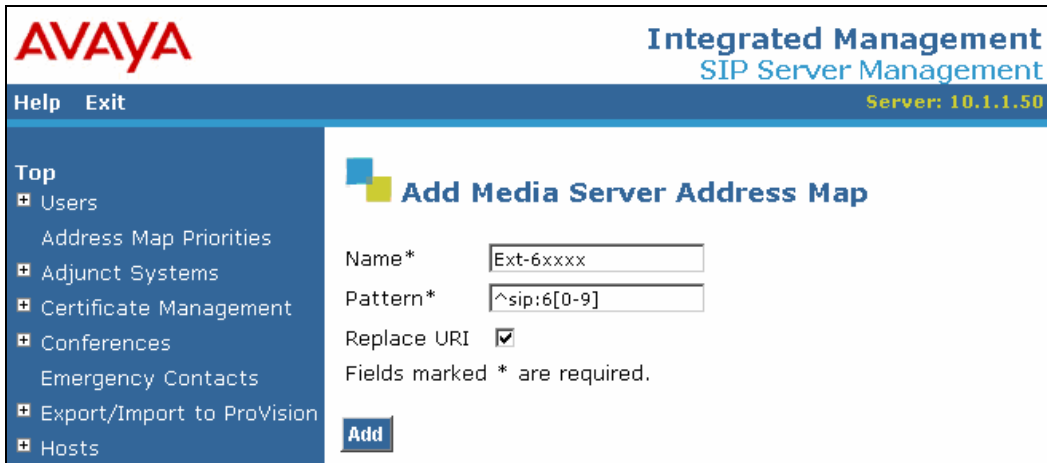


Figure 20: Media Server Address Map for Stations with Extensions starting with ‘6’

The Media Server Address Map is listed in Figure 21.



Figure 21: List Media Server Address Map

A **Host Address Map** is required for routing calls to the DiVitas Clients (i.e., Nokia N95) on the DiVitas UC Server based on the content of the SIP INVITE URI. In this configuration, the DiVitas Clients were assigned 5-digit extensions beginning with '4'. The pattern for the Host Address Map and the Host Contact are shown in **Figure 22** and **Figure 23**, respectively. The **Contact** field includes the IP address of the DiVitas UC Server, the port, and the transport protocol. The **Contact** field in the **Host Contact** was set to `sip:$(user)@10.1.1.123:5060;transport=udp`. After configuring the host address map, click on the **Add** button.

The screenshot shows the Avaya Integrated Management SIP Server Management interface. The top header includes the Avaya logo, the title 'Integrated Management SIP Server Management', and the server IP '10.1.1.50'. A navigation menu on the left lists various management options, with 'Hosts' selected. The main content area is titled 'Add Host Address Map' and contains the following form fields:

- Name***: To-DiVitas
- Pattern***: ^sip:4[0-9]{4}
- Replace URI**:

Below the fields is a note: 'Fields marked * are required.' and an **Add** button.

Figure 22: Host Address Map

The screenshot shows the Avaya Integrated Management SIP Server Management interface. The top header includes the Avaya logo, the title 'Integrated Management SIP Server Management', and the server IP '10.1.1.50'. A navigation menu on the left lists various management options, with 'Hosts' selected. The main content area is titled 'Add Host Contact' and contains the following form fields:

- Handle**: To-DiVitas
- Contact***: sip:\$(user)@10.1.1.123:5060;transport=udp

Below the fields is a note: 'Fields marked * are required.' and an **Add** button.

Figure 23: Host Contact

The **Host Address Map** is listed in **Figure 24**.

The screenshot shows the Avaya Integrated Management SIP Server Management interface. The page title is "List Host Address Map". The host is listed as 10.1.1.50. Below the host information is a table with the following structure:

Commands	Name	Commands	Contact
Add Another Map		Add Another Contact	
Edit	Delete	To-DiVitas	
		Edit	Delete sip:\$(user)@10.1.1.123:5060;transport=udp
Add Another Map		Add Another Contact	Delete Group

Figure 24: List Host Address Map

The IP address of the DiVitas UC Server must be configured as a trusted host on Avaya SES. As a trusted host, Avaya SES will not issue SIP authentication challenges for incoming requests from the DiVitas UC Server. The trusted host was configured as shown in **Figure 25**. After configuring the trusted host, click on the **Add** button.

The screenshot shows the Avaya Integrated Management SIP Server Management interface. The page title is "Add Trusted Host". The form contains the following fields:

- IP Address*: 10.1.1.123
- Host*: 10.1.1.50
- Comment: DiVitas UC Server

Fields marked * are required. An **Add** button is located at the bottom of the form.

Figure 25: Add Trusted Host

5. Configure DiVitas Mobile Unified Communications

This section describes the steps for configuring the DiVitas Mobile Unified Communications Server (UC Server) which supports a variety of dual mode (WiFi/Cellular) telephones including Nokia E- and N-Series DiVitas Clients. Refer to [4] and [5] for additional configuration information.

All DiVitas Mobile UC Server configuration and management features are accessed from a Web-based interface. From an Internet browser, enter the IP address of the DiVitas Mobile UC Server in the URL field and log in using the appropriate credentials. The screen shown in **Figure 26** is displayed.

DiVitas Server - Microsoft Internet Explorer

Address: https://10.1.1.123/

Navigation: Server, Clients, Voice, Monitoring, Reporting, Tools, Logout

Sub-navigation: Status, Network Status, IP Config, Admin Users, Images, Licensing, Time, Voice Config, Backup/Restore, Email

Logged in as: richw from 198.152.12.67 at 10:36 am PDT

Server Information

Serial Number	G27LCC1
Kernel Version	2.6.25.4-10.fc8
Kernel Build Date	#1 SMP Thu May 22 23:34:09 EDT 2008
System Memory	1034584 kB
System Uptime	2 days, 21:09
DVOS Uptime	2 days, 21:08
DVOS Status	System Normal
CPU Usage	0%

Active Server Image

Platform	U1000
Version	2.1.0.1
Build	418
Timestamp	Jul 31 2008, 13:04:24

License Information

Customer Name	Glenn Vela Test
Customer ID	GFE001
Expiration	Wed Jan 28 23:59:59 2009

DVOS Version: 2.1.0.1.418 © 2008 DiVitas Networks. All Rights Reserved.

Figure 26: DiVitas Mobile UC Server Web Interface

In the **Server→IP Config** webpage, configure the IP network parameters of the DiVitas Mobile UC Server corresponding to the customer's network, and set the DNS domain and the RTP ports as shown in **Figure 27** and **Figure 28**. The **External IP Configuration** is used by DiVitas Clients when operating in cellular mode.

The screenshot shows the 'Server IP Configuration' page. At the top, there is a navigation bar with 'Server' selected. Below it, a status bar indicates the user is logged in as 'richw' from '198.152.12.67' at '10:36 am PDT'. The main content area is titled 'Server IP Configuration' and contains three sections:

- Ethernet Interface: eth0 Configuration:**
 - IP Address: 10.1.1.123
 - Subnet Mask: 255.255.255.128
 - IP Gateway: 10.1.1.1
 - Buttons: Submit, Clear
- Hostname Configuration:**
 - Hostname: localhost
 - Buttons: Submit, Clear
- DNS Configuration:**
 - DNS Domain: selab.divitas.com
 - Primary DNS Server Address: 10.1.1.20
 - Secondary DNS Server Address: 0.0.0.0
 - Buttons: Submit, Clear
 - Note: *If a valid Secondary DNS Server is entered without a valid Primary DNS Server, the secondary server will be promoted to primary.*

Figure 27: Server IP Configuration - Top

The screenshot shows the bottom portion of the 'Server IP Configuration' page. It contains three sections:

- External IP Configuration:**
 - IP Address: 10.1.1.123
 - Buttons: Submit, Clear
- RTP Media Port Configuration:**
 - MSAP Port: 57342
 - UDP Port Base: 57344
 - Buttons: Submit, Clear
 - Notes:
 - The MSAP Port valid range is: 32000 - 65534*
 - The MSAP Port must be an even number.*
 - The valid UDP Port Base is: 32000 - 57344*
 - The UDP Port Base reserves 8190 ports and the MSAP Port must not be within the defined range.*
- QOS Configuration:**
 - QOS Type: Disabled DSCP TOS
 - DSCP Configuration - Only applicable if QOS type is set to DSCP:
 - Diffserv Codepoint(DSCP): Default
 - TOS Configuration - Only applicable if QOS type is set to TOS:
 - Precedence: Routine
 - Delay: Normal Low
 - Throughput: Normal High
 - Reliability: Normal High
 - Buttons: Submit, Clear

At the bottom, the footer shows 'DVOS Version: 2.1.0.1.418' and '© 2008 DiVitas Networks. All Rights Reserved.'

Figure 28: Server IP Configuration - Bottom

The DiVitas Server and Avaya SES communicate over a SIP trunk. Any call from a DiVitas Client to a number other than another DiVitas Client must use the SIP trunk to reach the dialed number. The SIP trunk is also used to route calls to DiVitas Clients operating in cellular mode. To configure the SIP trunk on the DiVitas Server, navigate to **Voice**→**Configuration** and then click on **Trunks**→**Add Trunk**. The following example shows the SIP trunk after it has been configured.

In the SIP trunk configuration, specify a descriptive name for the **Trunk Name** field. For the Dial Rules, specify the format of the dial patterns that are allowed to be routed over this SIP trunk. In this example, the DiVitas Clients are allowed to dial numbers in the 650 and 732 area codes. The digit '9' and prefix mark '1' is added to the 10-digit number. The '9' corresponds to the ARS feature access code on Avaya Communication Manager. **Figure 29** shows the first half of the SIP trunk configuration.

The screenshot displays the 'Edit SIP Trunk' configuration page in the DiVitas Networks web interface. The top navigation bar includes 'Server', 'Clients', 'Voice' (selected), 'Monitoring', 'Reporting', and 'Tools', with a 'Logout' link. Below this, a secondary bar shows 'Configuration', 'Conferencing', 'Voicemail', and 'Ring Groups'. The left sidebar lists various system components, with 'Trunks' highlighted. The main content area is titled 'Edit SIP Trunk' and includes a 'Delete Trunk T-AvayaSES' link. It shows the trunk is 'In use by 1 route'. Under 'General Settings', the 'Trunk Name' is 'T-AvayaSES', and 'Outbound Caller ID' and 'Maximum channels' are empty. The 'Outgoing Dial Rules' section includes an 'Outbound Dial Prefix' field, a 'Dial rules wizards' dropdown set to '(pick one)', and a list of dial rules: '9+1650NXXXXXX', '9+1732NXXXXXX', '91+650NXXXXXX', and '91+732NXXXXXX'. A 'Clean & Remove duplicates' button is at the bottom of the list. On the right, a 'Trunk SIP/T-AvayaSES' link is visible.

Figure 29: SIP Trunk - Top

Figure 30 displays the second half of the SIP trunk configuration webpage. The **Host Address** field should be set to the Avaya SES IP address, the **Port** field should be set to *5060* since UDP transport is used for the SIP trunk, and *rfc2833* should be used for the **DTMF Mode**.

The screenshot shows the configuration interface for a SIP trunk. It is divided into three main sections: Outgoing Settings, Incoming Settings, and Registration.

Outgoing Settings:

- Connection Type:** Advanced Basic [Change View](#)
- PEER Details:**
- Host Address:**
- Port:**
- User Name:**
- Secret:**
- Type:**
- Context:**
- NAT:** yes no
- Insecure:**
- DTMF Mode:**
- Reinvite:** yes no

Configuration Summary (Text Area):

```
canreinvite=no
context=from-pstn
dtmfmode=rfc2833
host=10.1.1.50
insecure=port,invite
nat=no
port=5060
secret=
type=peer
username=
```

Incoming Settings:

- USER Context:**
- USER Details:**

Registration:

- Register String:**

[Submit Changes](#)

Figure 30: SIP Trunk - Bottom

To properly route incoming calls to the DiVitas Clients, an inbound route was configured. To configure the inbound routes, navigate to **Voice**→**Configuration** and then click on **Inbound Routing**→**Add Incoming Route**. The incoming route shown below was already configured. The route shown in **Figure 31** routes **DID Number 40000** to the user “DV User 40000” configured below in **Figure 34**. The DID number should be set to the dialed string received from Avaya SES. In this example, the 5-digit extension was received by the DiVitas Server as opposed to the 10-digit public number. An inbound route should be added for each DiVitas Client.

The screenshot displays the DiVitas Networks web interface for configuring an inbound route. The top navigation bar includes 'Server', 'Clients', 'Voice' (selected), 'Monitoring', 'Reporting', and 'Tools'. Below this, there are sub-tabs for 'Configuration', 'Conferencing', 'Voicemail', and 'Ring Groups'. A 'Logout' link is visible in the top right corner.

On the left side, there is a vertical menu with the following items: Incoming Calls, Extensions, Digital Receptionist, Trunks, Trunk Profile, Show Registry, Inbound Routing (highlighted), Outbound Routing, System Recordings, and General Settings.

The main content area is titled 'Route: 40000/'. It contains the following sections:

- Delete Route 40000/**: A link to delete the route.
- Edit Incoming Route**: The main configuration section.
 - DID Number:** Input field containing '40000'.
 - Caller ID Number:** Empty input field.
 - Fax Handling**:
 - Fax Extension:** Dropdown menu set to 'AMP default'.
 - Fax Email:** Empty input field.
 - Options**:
 - Immediate Answer:** Dropdown menu set to 'No'.
 - Pause after answer:** Input field containing '0'.
 - Privacy Manager:** Dropdown menu set to 'No'.
 - Set Destination**:
 - Digital Receptionist:** Dropdown menu.
 - Extension:** Radio button selected, dropdown menu set to 'DV User 40000 <40000>'.
 - Voicemail:** Radio button unselected, dropdown menu set to '"DV User 40000" <40000>'.
 - Ring Group:** Radio button unselected, dropdown menu.
 - Queue:** Radio button unselected, dropdown menu.
 - Custom App:** Radio button unselected, input field.
 - Use 'Incoming Calls' settings:** Radio button unselected.

At the bottom of the configuration area, there is a 'Submit' button.

On the right side of the interface, there is a table titled 'Add Incoming Route' with the following entries:

Add Incoming Route
12512430179/
12512437731/
40000/
40001/
40002/

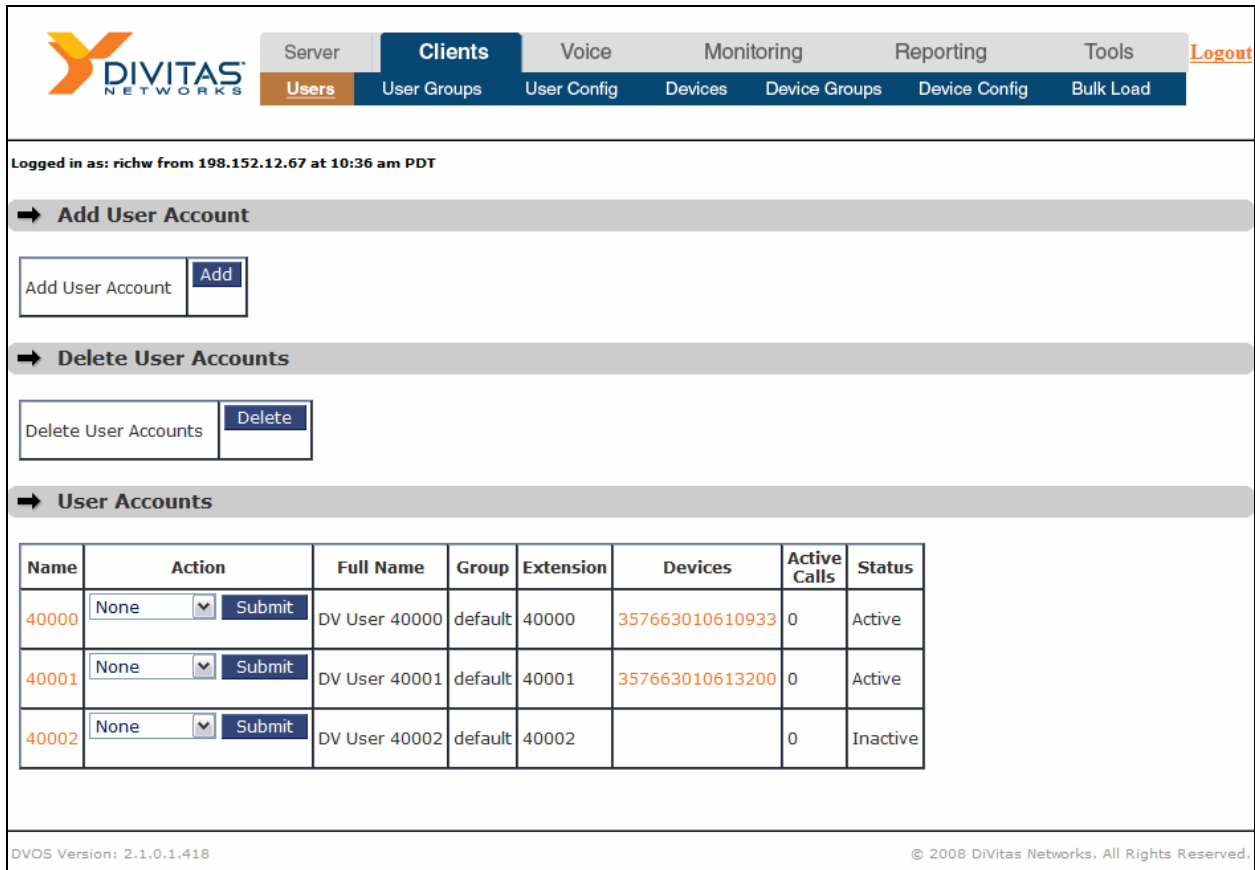
Figure 31: Inbound Routing

To properly route calls to stations on Avaya Communication Manager or the PSTN, a generic route was defined. The **Route Name** was set to a descriptive name. The **Dial Pattern** was set to X which matches any digit and the **Insert** field is set to commonly used dial patterns. The **Trunk Sequence** specifies the trunk(s) for routing outbound calls. In this example, the calls are routed over the SIP trunk configured in **Figure 29** and **Figure 30**.

The screenshot shows the 'Edit Route' configuration page in the Divitas Networks web interface. The page is titled 'Edit Route' and is for a route named 'GenericOUT'. The interface includes a navigation menu on the left with options like 'Incoming Calls', 'Extensions', 'Digital Receptionist', 'Trunks', 'Trunk Profile', 'Show Registry', 'Inbound Routing', 'Outbound Routing', 'System Recordings', and 'General Settings'. The main content area has several sections: 'Route Name' (GenericOUT), 'Route Password' (empty), 'Intra Company Route' (checkbox), 'Dial Patterns' (a list containing 'X.'), 'Insert' (a dropdown menu set to 'Pick pre-defined patterns'), and 'Trunk Sequence' (a list with one entry '0' and 'SIP/T-AvayaSES'). A 'Submit Changes' button is at the bottom.

Figure 32: Outbound Routing

To view and add users to the DiVitas Server, navigate to **Clients**→**Users**. To view the details of the configured user accounts, click on the **Name** and **Devices** link in the **User Accounts** section. To add a **User**, click on the **Add** button under **Add User Account**.



Logged in as: richw from 198.152.12.67 at 10:36 am PDT

➔ **Add User Account**

Add User Account

➔ **Delete User Accounts**

Delete User Accounts

➔ **User Accounts**

Name	Action	Full Name	Group	Extension	Devices	Active Calls	Status
40000	None <input type="button" value="Submit"/>	DV User 40000	default	40000	357663010610933	0	Active
40001	None <input type="button" value="Submit"/>	DV User 40001	default	40001	357663010613200	0	Active
40002	None <input type="button" value="Submit"/>	DV User 40002	default	40002		0	Inactive

DVOS Version: 2.1.0.1.418 © 2008 DiVitas Networks. All Rights Reserved.

Figure 33: User Accounts

When adding a **User**, specify the user's **Full Name**, **Extension**, and **Outbound Caller ID** as shown in **Figure 34**. The figure below shows the user account after it has been configured. The **Add User Account** webpage will appear slightly different, but contain similar fields.

The screenshot shows the Divitas Networks web interface. At the top, there is a navigation menu with tabs for Server, Clients, Voice, Monitoring, Reporting, and Tools. The 'Clients' tab is active, and it contains sub-tabs for Users, User Groups, User Config, Devices, Device Groups, Device Config, and Bulk Load. The 'Users' sub-tab is selected. Below the navigation, there is a login status message: 'Logged in as: richw from 198.152.12.67 at 10:36 am PDT'. A 'Refresh' button is visible. The main content area is titled 'Configuration Details for User: 40000'. It contains a table with the following data:

Attribute	Value
Full Name	DV User 40000
Extension	40000
Outbound CallerId	7328522746
Email ID	
Service Provider Email ID	
Email Status	Not Sent
User Group	default
User Admin State	Enabled
License Status	Valid
Voicemail Configuration	Enabled
Play Caller ID	No
Play Envelope	No
VM Redirect Number	
VM Access Number	

Below this table is another section titled 'Status Details for User: 40000', which contains another table with the following data:

Attribute	Value
Status	Active
Associated Device ID(s)	357663010610933
Wifi Voice Availability	Available
Cell Voice Availability	Available
User Active	Yes
Number of Active Calls	0
User Registered	Yes
Invalid Password Count	0
Account Login Status	Login Enabled

At the bottom of the page, there is a footer with the text 'DVOS Version: 2.1.0.1.418' on the left and '© 2008 DiVitas Networks. All Rights Reserved.' on the right.

Figure 34: User

6. Interoperability Compliance Testing

This section describes the interoperability compliance testing used to verify the DiVitas Mobile Unified Communications solution with Avaya Communication Manager and Avaya SIP Enablement Services. This section covers the general test approach and the test results.

6.1. General Test Approach

The focus of the interoperability compliance testing was primarily on verifying call establishment using the DiVitas Server and the DiVitas Clients in WiFi and cell modes to the PSTN and stations on Avaya Communication Manager and Avaya SES. The general test approach was to verify the following functionality:

- Establishing calls between DiVitas Clients in WiFi and cell modes and SIP, H.323, digital, and analog stations on Avaya Communication Manager and Avaya SES while the DiVitas Clients were in WiFi and cell modes.
- Establishing calls between the DiVitas Clients in WiFi and cell modes and the PSTN.
- Ability to hold a call, transfer a call, and establish a 3-party conference.
- Displaying the calling party number on the DiVitas Clients.
- Simultaneous ringing on a desktop IP phone and DiVitas client when an incoming call is received.
- The DiVitas Clients' ability to roam between the WiFi and cell networks.
- Call establishment using G.711mu-law codec.

The serviceability testing focused on verifying the ability of the DiVitas Server to recover from adverse conditions, such as power failures and disconnecting cables to the IP network. In addition, the ability of the solution to recover from Avaya S8710 Server interchange and from cycling power on Avaya Communication Manager and Avaya SES was also verified.

6.2. Test Results

All tests passed.

7. Verification Steps

This section provides the verification steps that may be performed to verify that DiVitas Clients registered with the DiVitas Mobile UC server can place calls to the PSTN or stations on Avaya Communication Manager.

1. From the Avaya Communication Manager SAT, verify that the SIP signaling group and trunk group are in-service using the **status signaling-group** and **status trunk** commands, respectively.
2. From the DiVitas web interface, navigate to the **Clients**→**Users** webpage shown in **Figure 33**. From that webpage, click on the **Devices** link to verify that the DiVitas Client is registered with the DiVitas Server. The screen shown in **Figure 35** will be displayed with information provided by the DiVitas Client.

The screenshot displays the DiVitas web interface. The top navigation bar includes 'Server', 'Clients', 'Voice', 'Monitoring', 'Reporting', and 'Tools'. The 'Clients' section is expanded to show 'Users', 'User Groups', 'User Config', 'Devices', 'Device Groups', 'Device Config', and 'Bulk Load'. The 'Logout' link is visible in the top right corner.

The main content area is titled 'Configuration Details for Client Device: 357663010610933'. It contains a table with the following data:

Attribute	Value
Device Name	357663010610933
Device Type	Dual Mode
Device Group	default
Serial Number (Type)	357663010610933 (IMEI)
Debug Level	force high

Below this is the 'Status Details for Client Device: 357663010610933' section, which contains a larger table with the following data:

Attribute	Value
Current User	40000
Image Version	2.1.0.1.418
Image Status	OK
Device Type	smart
OS Type	s6031
Registration Status	WiFi
Incoming Call Medium	VOIP
Outgoing Call Medium	VOIP
WiFi Voice Presence	Online
Cellular Voice Presence	Online
WiFi Voice Availability	Available
Cellular Voice Availability	Available
WiFi Voice Network Status	Up
Cell Voice Network Status	Up
DND State	DND Disabled
Current IP:Port	64.186.163.2:54993
Current Local IP	172.18.16.79
Cellular Number	1111111111
Number of Active Calls	0
Device State	Active
NAT-T	External
Log Download Status	Idle
Provisioning Type	Auto-Provisioned
Client Type	DiVitas Client
Last Change Time	2008-08-04 08:35:44 (PDT)
Client Logs	No Logs

Figure 35: Status Details for Client Device

- Place a call from the DiVitas Client to a SIP phone on Avaya Communication Manager. Verify that the call completes successfully. From the DiVitas Web interface, navigate to **Monitoring**→**Active Calls** to view the call summary as shown in **Figure 36**.

Logged in as: richw from 12.160.179.101 at 12:50 pm PDT

Pause Auto Refresh

→ Active Calls Summary

Call Ref	Action	User	Type	Index	From	To	Call State	Hold State	Handoff State	Toggle State	Network	Paired Call Ref
219	Delete	40001	Incoming	1	60004	40001	CALL_CONNECTED	NO	NONE	IDLE	Wifi	
225	Delete	40000	Outgoing	0	40000	61003	CALL_CONNECTED	NO	NONE	IDLE	Cell	

DVOS Version: 2.1.0.1.418 © 2008 DiVitas Networks. All Rights Reserved.

Figure 36: Call Summary – Call from DiVitas Client to Avaya Communication Manager

- Place a call from a DiVitas Client in WiFi mode to a DiVitas Client in cell mode. The call is routed through the PSTN. Verify that the call completes successfully. From the DiVitas Web interface, navigate to **Monitoring**→**Active Calls** to view the call summary as shown in **Figure 37**.

Logged in as: richw from 12.160.179.101 at 8:47 am PDT

Resume Auto Refresh

→ Active Calls Summary

Call Ref	Action	User	Type	Index	From	To	Call State	Hold State	Handoff State	Toggle State	Network	Paired Call Ref
77	Delete	40000	Outgoing	2	40000	7328522747	CALL_CONNECTED	NO	NONE	IDLE	Wifi	
78	Delete	40001	Incoming	1	7328522746	40001	CALL_CONNECTED	NO	COMPLETED	IDLE	Cell	

DVOS Version: 2.1.0.1.418 © 2008 DiVitas Networks. All Rights Reserved.

Figure 37: Call Summary – Call from DiVitas Client to PSTN

5. While a call is active on a Nokia N95 with the DiVitas Client, the connected number is shown on the phone's display as shown in **Figure 38** and **Figure 39**.

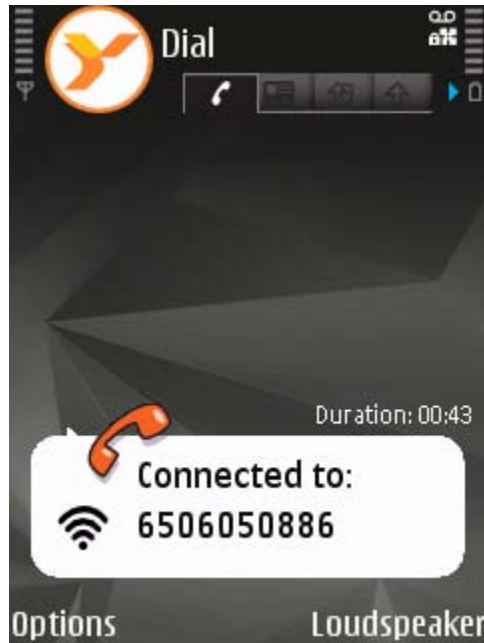


Figure 38: Active Call to DiVitas Client in Cell Mode

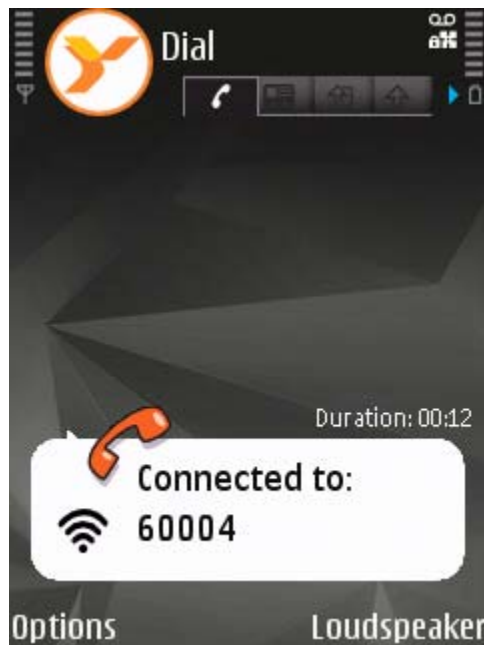


Figure 39: Active Call to an Avaya SIP Telephone

After the call is completed, calls are maintained in the phone's call log as shown in **Figure 40**.



Figure 40: Call Log

8. Support

For technical support on the DiVitas Mobile Unified Communications Solution and how to configure dual mode handsets connected to it, consult the support pages at <http://www.divitas.com/support.html> or contact technical support at:

- Telephone: (866) 857-6087
- E-mail: support@divitas.com

9. Conclusion

These Application Notes describe the configuration steps required to integrate the DiVitas Mobile Unified Communications solution with Avaya Communication Manager and Avaya SIP Enablement Services. The DiVitas Clients were able to register with the DiVitas Server and originate and terminate calls to the PSTN and stations on Avaya Communication Manager.

10. References

This section references the product documentation that is relevant to these Application Notes.

- [1] *Administrator Guide for Avaya Communication Manager*, Document 03-300509, Issue 4, January 2008, available at <http://support.avaya.com>.
- [2] *Feature Description and Implementation for Avaya Communication Manager*, Document 555-245-205, Issue 6, January 2008, available at <http://support.avaya.com>.
- [3] *SIP Support in Avaya Communication Manager*, Issue 8, January 2008, Document Number 555-245-206, available at <http://support.avaya.com>.
- [4] *DiVitas Server Administration Guide*, Version 2.1.0.1, Part Number: DOC-DVOS-AG-202.
- [5] *DiVitas Client User Guide for Nokia E- and N-Series*, Version 2.1.0.1, Part Number: DOC-CLIENT-UG-202.

©2008 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.