Avaya Solution & Interoperability Test Lab

Application Notes for the DiVitas Mobile Convergence Appliance with Avaya Communication Manager and Avaya SIP Enablement Services – Issue 1.1

Abstract

These Application Notes describe a solution comprised of Avaya Communication Manager 4.0.1, Avaya SIP Enablement Services 4.0, and dual mode (WiFi/Cellular) telephones registered with the SIP–based DiVitas Mobile Convergence Appliance. During the compliance test, a SIP trunk was established between Avaya SIP Enablement Services server and the DiVitas Mobile Convergence Appliance. Wireless telephones registered with the DiVitas Mobile Convergence Appliance were used to originate and receive calls to and from SIP and non-SIP telephones, and exercise other telephony features such as transfer and hold. Wireless telephones registered with the DiVitas Mobile Convergence Appliance were also tested for roaming between WiFi and Cellular services. 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 a solution comprised of Avaya Communication Manager 4.0.1, Avaya SIP Enablement Services 4.0, and dual mode (WiFi/Cellular) telephones registered with the SIP–based DiVitas Mobile Convergence Appliance (MCA). During the compliance test, a SIP trunk was established between the Avaya SIP Enablement Services server and the DiVitas MCA. Wireless telephones registered with the DiVitas MCA were used to originate and receive calls to and from SIP and non-SIP telephones, and exercise other telephony features such as transfer and hold. Wireless telephones registered with the DiVitas MCA were also tested for roaming between WiFi and Cellular services. These application notes do not cover configuration of the dual mode telephones registered with the MCA.

Figure 1 illustrates a sample configuration consisting of a pair of Avaya S8710 Servers, an Avaya G650 Media Gateway, an Avaya SIP Enablement Services (SES) server, and dual mode wireless telephones registered with DiVitas MCA. Avaya Communication Manager is installed on the Avaya S8710 Servers. The solution described herein is also extensible to other Avaya Servers and Media Gateways. For completeness, Avaya 4600 Series SIP IP Telephones, Avaya 4600 Series H.323 IP Telephones, and Avaya 6400 and 8400 Series Digital Telephones, are included in **Figure 1** to demonstrate calls between the SIP-based DiVitas MCA and Avaya SIP, H.323, and digital telephones. The analog PSTN telephone is also included to demonstrate calls routed by Avaya Communication Manager between the DiVitas MCA and the PSTN.

A SIP trunk is established between the DiVitas MCA and Avaya SES and the DiVitas MCA is configured as a trusted host in Avaya SES. The DiVitas MCA is configured with G711 codec using RFC2823 for DTMF.

Typical call flows in this configuration between Avaya Communication Manager and Avaya SES, and the DiVitas MCA are as follows:

- Incoming calls into the DiVitas MCA
    - Calls originate from PSTN, H.323 or SIP endpoints to a destination number associated with the DiVitas MCA.
    - Avaya Communication Manager uses Automatic Alternate Routing (AAR) to route the calls to Avaya SES over SIP trunks.
    - Avaya SES matches the dialed string pattern to route the calls to the DiVitas MCA over the SIP trunk between Avaya SES and the DiVitas MCA
    - DiVitas MCA forwards the call to the registered dual mode telephone.
- Outgoing calls from the DiVitas MCA
    - DiVitas MCA receives an outbound call from a dual mode telephone registered with it and forwards it to Avaya SES over the SIP trunk.
    - Avaya SES matches the dialed string pattern and routes the call to Avaya Communication manager over the SIP trunk.
    - Avaya Communication Manager then routes the call to the right telephone or PSTN telephone.

These application notes assume that Avaya Communication Manager and Avaya SES are already installed and basic configuration steps have been performed. Only steps relevant to this compliance test will be described in this document. For further details on configuration steps not covered in this document, consult **[1 - 4]**.

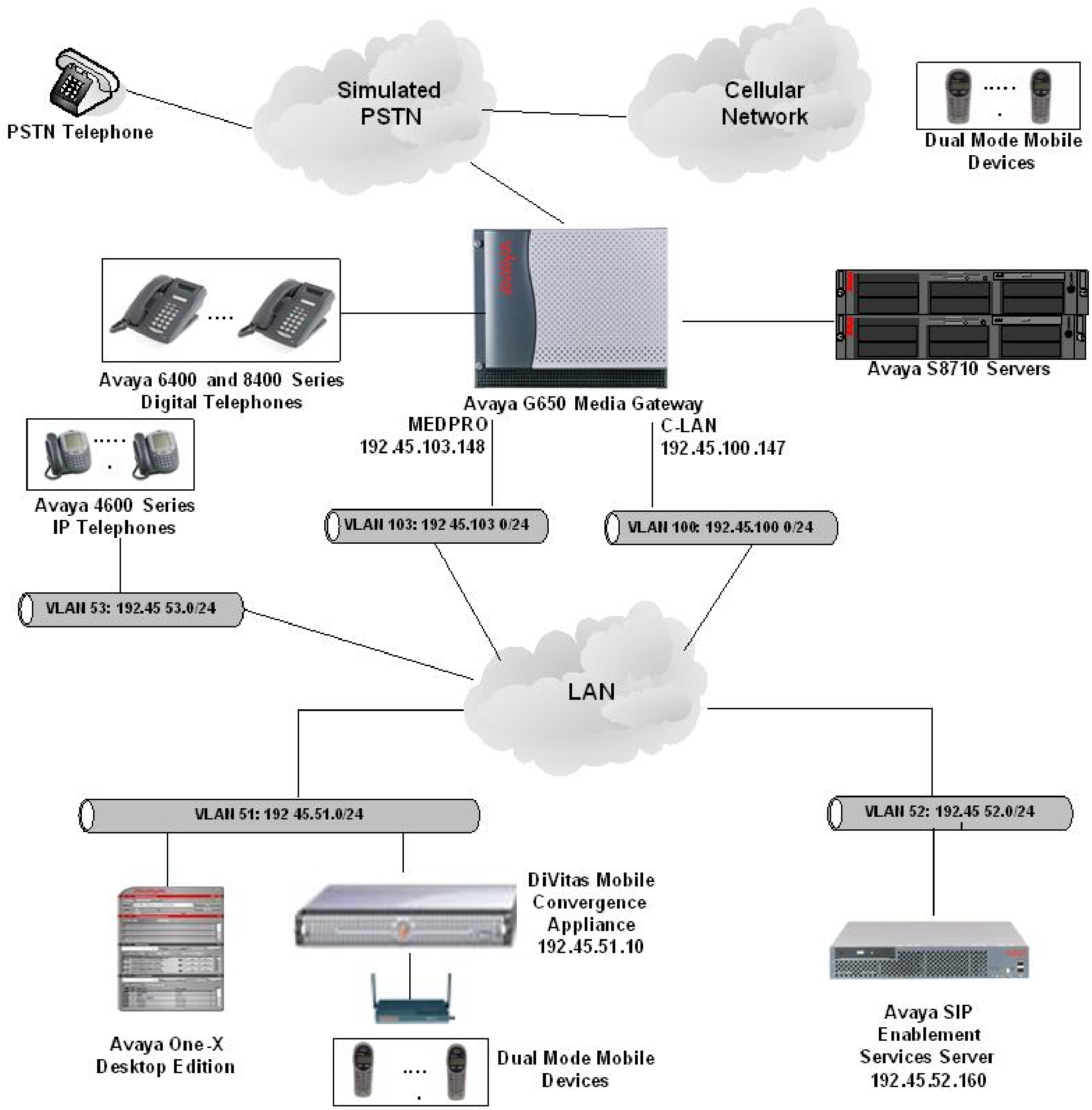


Figure 1: Sample configuration

2. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8710 Media Server	Avaya Communication Manager 4.0.1 (R014x.00.1.731.2)
Avaya G650 Media Gateway	-
TN2312BP IP Server Interface	HW12 FW 40
TN799DP C-LAN Interface	HW01 FW 24
TN2302AP IP Media Processor	HW20 FW 117
Avaya SIP Enablement Services Server	SES 4.0(SES-4.0.0.0-0.33.6)
Avaya 4600 Series IP Telephones	2.2.2 (4610SW SIP) 2.3 (4602SW H.323) 2.6 (4610SW H.323) 2.5 (4625SW H.323)
Avaya 6400 and 8400 Series Digital Telephones	-
Avaya Analog Telephone	-
DiVitas Mobile Convergence Appliance	MMOS v1.3.2
DiVitas Mobile Convergence Client on Dual Mode Wireless Telephones	v1.3.2 and v1.3

3. Configure Avaya Communication Manager

This section describes a procedure for setting up a SIP trunk between Avaya Communication Manager and Avaya SES which includes steps for setting up an IP codec set, an IP network region, a signaling group and its interface. Before a trunk can be configured, it is necessary to verify if there is enough capacity to setup an additional trunk. Configuration in the following sections is only for the fields where a value needs to be entered or modified. Default values are used for all other fields. These steps are performed from the Avaya Communication Manager System Access Terminal (SAT) interface. Refer to [1] for additional details.

3.1. Capacity Verification

Step	Description
1.	Enter the **display system-parameters customer-options** command. Verify that the number of SIP trunks supported by the system is sufficient for the number of SIP trunks needed. If not, contact an authorized Avaya account representative to obtain additional licenses. **Note:** *Each SIP call between two SIP endpoints (whether internal or external) requires two SIP trunks for the duration of the call. The license file installed on the system controls the maximum permitted.*

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

IP PORT CAPACITIES                                           USED
                     Maximum Administered H.323 Trunks: 200   148
           Maximum Concurrently Registered IP Stations: 1000  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: 0     0
                  Maximum Video Capable H.323 Stations: 0     0
                   Maximum Video Capable IP Softphones: 0     0
                       Maximum Administered SIP Trunks: 200   153

   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                             Maximum TN2501 VAL Boards: 1     1
                    Maximum G250/G350/G700 VAL Sources: 0     0
           Maximum TN2602 Boards with 80 VoIP Channels: 2     0
          Maximum TN2602 Boards with 320 VoIP Channels: 2     1
   Maximum Number of Expanded Meet-me Conference Ports: 0     0
        (NOTE: You must logoff & login to effect the permission changes.)
```

3.2. IP Codec Set

This section describes the steps for administering a codec set in Avaya Communication Manager. This codec set is used in the IP network region for communication between Avaya Communication Manager and Avaya SES.

Step	Description
1.	Enter the **change ip-codec-set <c>** command, where **c** is a number between **1** and **7**, inclusive. IP codec sets are used in **Section 3.3** for configuring an IP network region to specify which codec sets may be used within and between network regions. For the compliance testing only **G.711MU** was used and **Media Encryption** was set to **none**.

```
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:
 4:
 5:
 6:
 7:

     Media Encryption
 1: none
 2:
 3:
```

3.3. IP Network Region

This section describes the steps for administering an IP network region in Avaya Communication Manager for communication between Avaya Communication Manager and Avaya SES.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>Enter the change ip-network-region <n> command, where n is a number between 1 and 250 inclusive and configure the following:

Authoritative Domain – Set to devconnect.com in this example. This should match the SIP Domain value in Section 4, Step 2.
Intra-region IP-IP Direct Audio – Set to yes to allow direct IP-to-IP audio connectivity between endpoints registered to Avaya Communication Manager or Avaya SES in the same IP network region.
Codec Set – Set the codec set number as provisioned in Section 3.2.
Inter-region IP-IP Direct Audio – Set to yes to allow direct IP-to-IP audio connectivity between endpoints registered to Avaya Communication Manager or Avaya SES in different IP network regions.

<pre>
change ip-network-region 2   Page 1 of 19
                               IP NETWORK REGION
  Region: 2
Location: Authoritative Domain: devconnect.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: 65535
DIFFSERV/TOS PARAMETERS   RTCP Reporting Enabled? y
 Call Control PHB Value: 46   RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46   Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5   AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS   RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
</pre></td></tr>
</table>

Step	Description
2.	Proceed to **Page 3** of IP network region configuration and enable inter-region connectivity between regions as per below. For this compliance testing, **codec set** was set to the IP codec set configured in **Section 3.2**.

```
Page 3 of 19
                     Inter Network Region Connection Management

 src dst  codec  direct   Total           Video                         Dyn
 rgn rgn   set    WAN  WAN-BW-limits  WAN-BW-limits Intervening-regions CAC IGAR
 2   1     2      y        :NoLimit                                         n
 2   2     2
 2   3
 2   4
 2   5
 2   6
 2   7
 2   8
 2   9
 2   10
 2   11
 2   12
 2   13
 2   14
 2   15
```

3.4. IP Node Names

This section describes the steps for setting an IP node name for Avaya SES in Avaya Communication Manager.

Step	Description
1.	Enter the **change node-names ip** command and add a node name for Avaya SES along with its IP address.

```
change node-names ip                                                Page 1 of 1
                                  IP NODE NAMES
    Name              IP Address
CLAN-1A06           192.45 .100.147
MEDPRO-1A13         192.45 .103.148
SES                 192.45 .52 .160
```

3.5. SIP Signaling

This section describes the steps for administering a signaling group in Avaya Communication Manager for communication between Avaya Communication Manager and Avaya SIP Enablement Services.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td rowspan="3">1.</td><td>Issue the command add signaling-group <s>, where s is an available signaling group and configure the following:

Group Type – Set to sip.
Transport Method – Set to tls.
Near-end Node Name - Set to node name CLAN-1A06 as displayed in Section 3.4.
Far-end Node Name - Set to node name SES configured in Section 3.4.
Far-end Network Region - Set to the region configured in Section 3.3.
Far-end Domain - Set to devconnect.com in this example. This should match the SIP Domain value in Section 4, Step 2.
DTMF over IP – Set to rtp-payload (RFC2833).
Direct IP-IP Audio Connections – Set to y for shuffling.
</td></tr>
<tr><td><pre>
add signaling-group 10   Page   1 of 5
                                SIGNALING GROUP

 Group Number: 10   Group Type: sip
                       Transport Method: tls

   Near-end Node Name: CLAN-1A06   Far-end Node Name: SES
 Near-end Listen Port: 5061   Far-end Listen Port: 5061
                                        Far-end Network Region: 2
       Far-end Domain:devconnect.com

                                             Bypass If IP Threshold Exceeded? n

        DTMF over IP: rtp-payload   Direct IP-IP Audio Connections? y
                                                        IP Audio Hairpinning? n
 Session Establishment Timer(min): 120
</pre></td></tr>
<tr><td></td></tr>
</table>

3.6. SIP Trunking

This section describes the steps for administering a trunk group in Avaya Communication Manager for communication between Avaya Communication Manager and Avaya SES.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>Issue the command add trunk-group <t>, where t is an unallocated trunk group and configure the following:

Group Type – Set to the Group Type field value configured in Section 3.5.
TAC (Trunk Access Code) – Set to any available trunk access code.
Signaling Group – Set to the Group Number field value configured in Section 3.5.
Number of Members – Allowed values are between 0 and 255. Set to a value large enough to accommodate the number of SIP telephone extensions being used.
Group Name – Enter any descriptive name.

Note: Each SIP call between two SIP endpoints (whether internal or external) requires two SIP trunks for the duration of the call. The license file installed on the system controls the maximum permitted.</td></tr>
<tr><td></td><td><pre>add trunk-group 10   Page   1 of 21
                                TRUNK GROUP

Group Number: 10   Group Type: sip   CDR Reports: y
  Group Name: SIP-SES-DevCon1   COR: 1   TN: 1   TAC: 110
   Direction: two-way   Outgoing Display? n
 Dial Access? n   Night Service:
Queue Length: 0
Service Type: tie   Auth Code? n

                                                     Signaling Group: 10
                                                   Number of Members: 150</pre></td></tr>
<tr><td></td><td></td></tr>
</table>

3.7. Dialplan/AAR/Route Pattern

This section describes the steps for setting the Dialplan, AAR digit analysis and Route Pattern in Avaya Communication Manager for proper routing of calls from Avaya Communication Manager to Avaya SES. These calls are ultimately destined for the DiVitas MCA.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>Issue the command change uniform-dialplan <dialstring> where dialstring is the string to match for the dialed number, and configure as follows:

Matching Pattern – Set it to a value for routing calls to Avaya SES for proper AAR digit analysis.
Len – The dialed string length to be analyzed.
Del – Set to 0.
Net – Set to aar.

<pre>
change uniform-dialplan 5   Page 1 of 2
                             UNIFORM DIAL PLAN TABLE
                                                             Percent Full: 02

 Matching   Inserted   Node
 Pattern   Len Del   Digits   Net Conv   Num
 64000   5   0   aar   n
                                           n
                                           n
</pre></td></tr>
<tr><td>2.</td><td>Issue the command change public-unknown-numbering <e>, where e is extension code to be administered.

Ext Len – Set to the length of calling party number.
Ext Code – Extension Code to be administered. Set to 6 in this example.
Trk Grp<s> - Trunk Group/s from Section 3.6, Step 1.
Total CPN Len – Length of the dialed number.

<pre>
change public-unknown-numbering 5   Page   1 of 2
                         NUMBERING - PUBLIC/UNKNOWN FORMAT
                                       Total
Ext Ext   Trk   CPN   CPN
Len Code   Grp<s>   Prefix   Len

5   6   10   5
</pre></td></tr>
</table>

Step	Description
3.	Issue the command **change route-pattern <r>**, where **r** is the number of the route pattern to be administered. • **Grp No –** Set to the Trunk Group provisioned in **Section 3.6**. • **FRL –** Set to **0**.

```
change route-pattern 10                                           Page   1  of  3
                    Pattern Number: 1   Pattern Name: SES SIP
                             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: 10   0                                                                 n   user
 2:                                                                        n   user
 3:                                                                        n   user
 4:                                                                        n   user
 5:                                                                        n   user
 6:                                                                        n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 3 4 W     Request                                Dgts Format
                                                        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
```

Step	Description
4.	Issue the command **change aar analysis 6** and configure as follows: • **Dialed String –** Set it to the same value as **Matching Pattern** in **Step 1**. • **Total Min and Max –** Set it to the same value as **Len** in **Step 1.** • **Route Pattern –** Set a value for a route pattern defined in **Step 3**. • **Call Type –** Set to **aar**

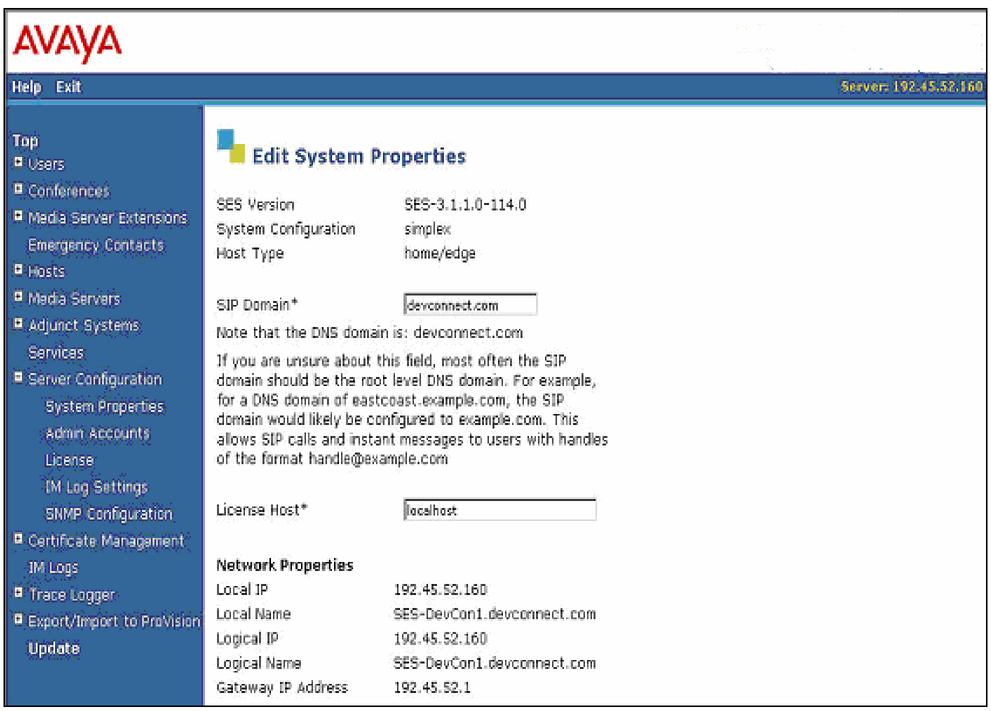
```
Change aar analysis 6                                                 Page 1 of 2
                             AAR DIGIT ANALYSIS TABLE
                                                               Percent Full:    2

          Dialed            Total      Route    Call   Node   ANI
          String           Min  Max  Pattern   Type   Num    Reqd
    64000                  5    5     10       aar           n
    2                      5    5     15       aar           n
    2                      7    7     999      aar           n
    245                    5    5     33       aar           n
```

4. Configure Avaya SIP Enablement Services

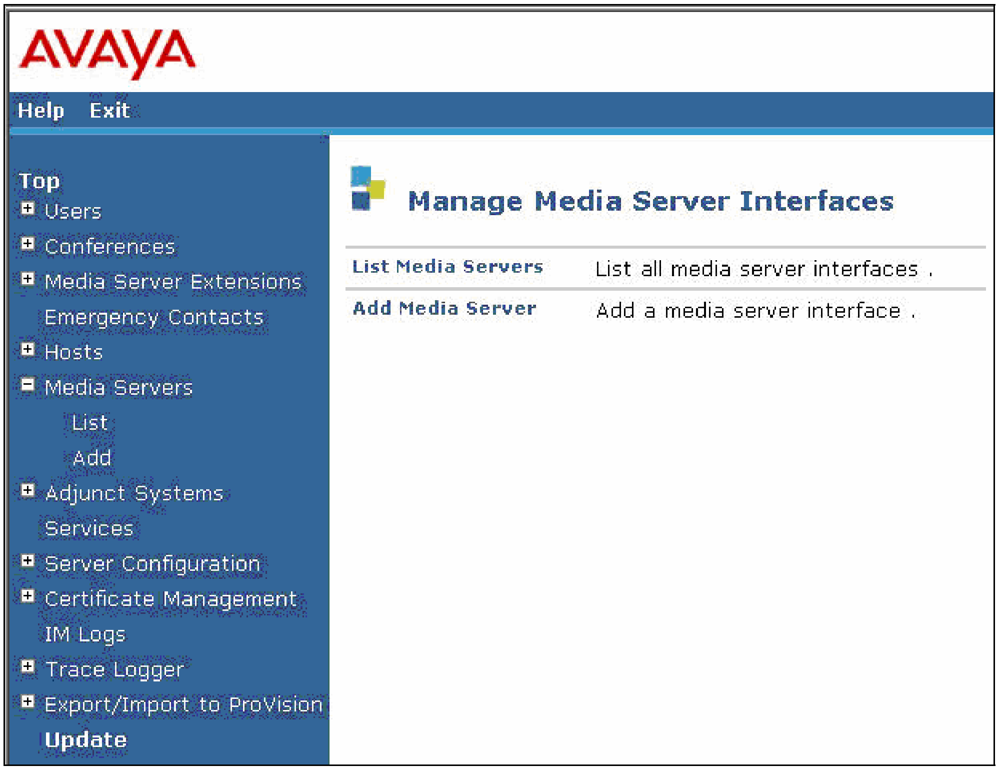
This section describes the steps for configuring Avaya SES to communicate with Avaya Communication Manager and the DiVitas MCA. The DiVitas MCA will be configured as a trusted host with Avaya SES and a host map will be created in Avaya SES for all the calls destined for the DiVitas MCA. Additionally, a Media Server Map needs to be created from Avaya SES to Avaya Communication Manager for the calls originating from the DiVitas MCA. Refer to [3, 4] for additional details.

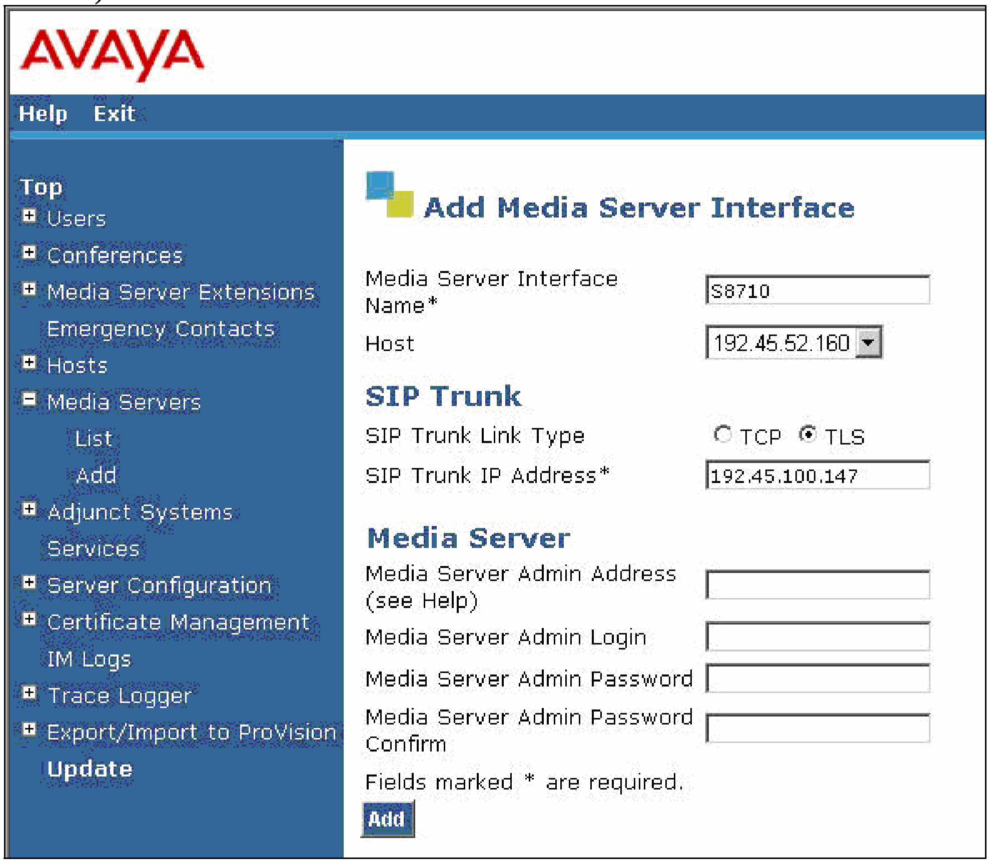
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>Open a web browser, enter http://<IP address of Avaya SES server>/admin for the URL, and log in with the appropriate credentials. Click on the Launch Administration Web Interface link upon successful login.</td></tr>
<tr><td>2.</td><td>On the SIP Server Management page:

Click the + sign to expand the options under Server Configuration.
Click System Properties.
Verify the SIP Domain matches the Far-end Domain field value configured for the signaling group on Avaya Communication Manager in Section 3.5.



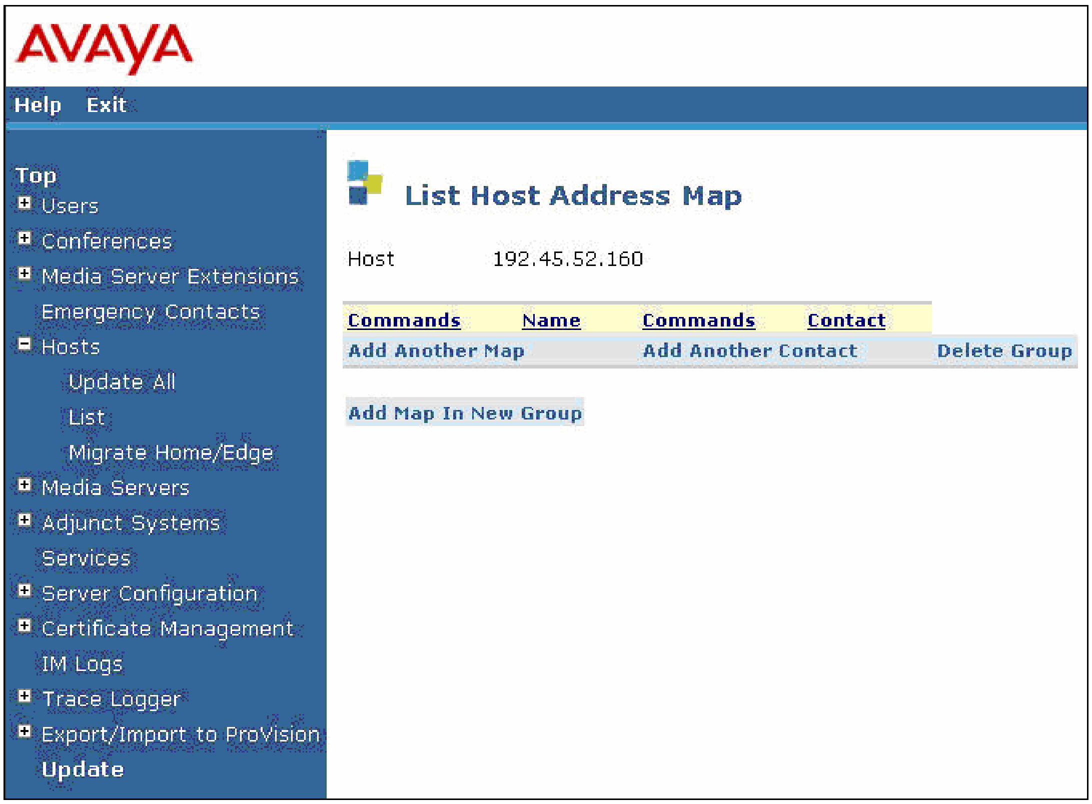
</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>3.</td><td>To enable secure SIP trunking between Avaya SES and Avaya Communication Manager, add a media server corresponding to Avaya Communication Manager from the SIP Server Management page:
• Click the + sign to expand the options under Media Servers.
• Click Add.

</td></tr>
</table>

Step	Description
4.	At the **Add Media Server Interface** page, provision **SIP Trunk** parameters as follows for connectivity to Avaya Communication Manager: • **SIP Trunk Link Type** - Set to the **Transport Method** field value in **Section 3.5**. • **SIP Trunk IP Address** - Set to the CLAN IP address as displayed in **Section 3.4**. • Click **Add** when finished and then click **Continue** on the confirmation page (not shown). 

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>5.</td><td>
A Host Address Map is required on Avaya SES to direct outbound calls from Avaya Communication Manager to the DiVitas MCA. An Address Map is used to route the calls based on the contents of the SIP INVITE URI. To configure the Host Address Map, do the following:

- Click the **+** sign to expand the options under **Hosts**.
- Click **Add Another Map**.

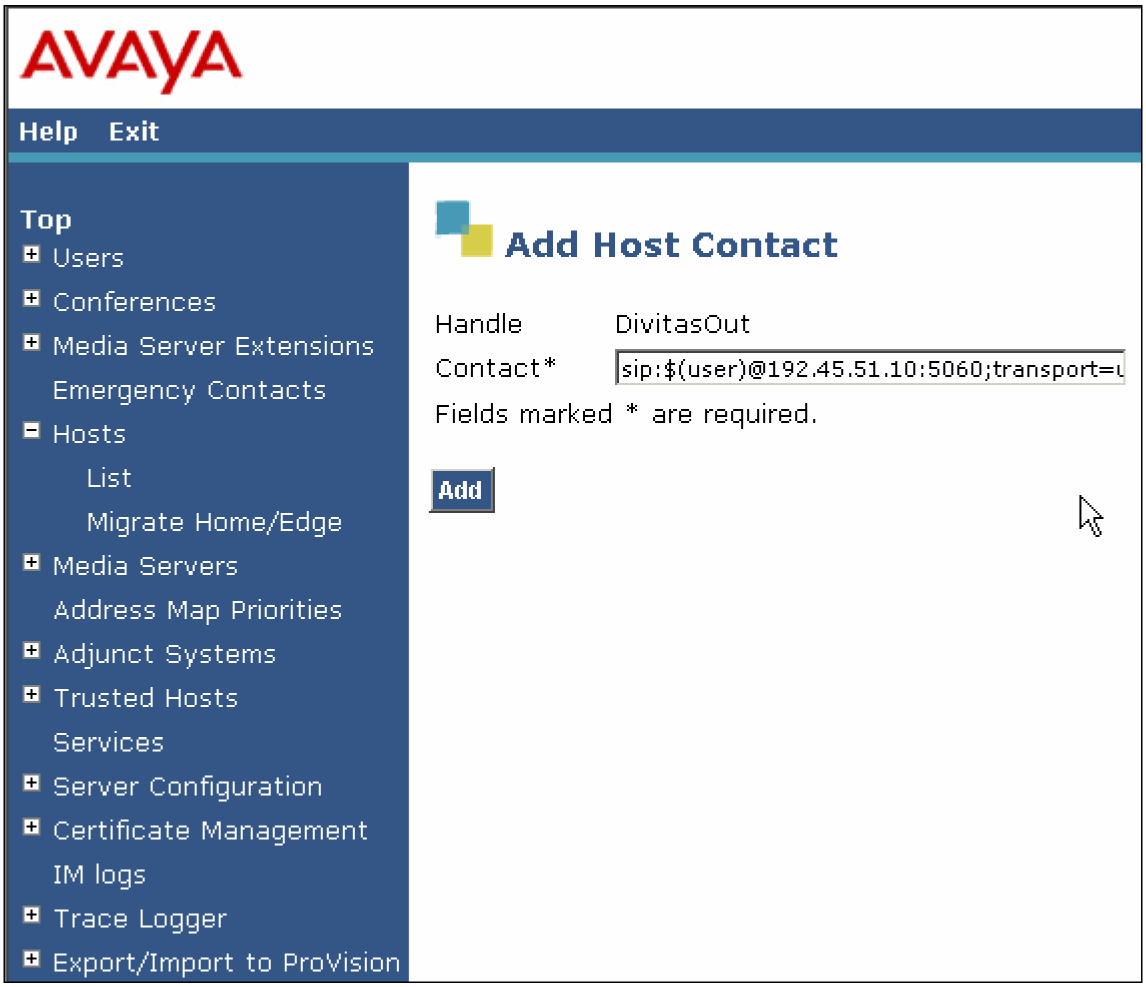


</td></tr>
</table>

Step	Description
6.	On the **Add Host Address Map** page configure as follows: • **Name** – Any descriptive name. • **Pattern** – Expression to match the beginning of the SIP URI. • Click **Add** and then **Continue** on the next page (not shown). 

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>7.</td><td>
The host contact must be entered for the Address Map defined in Step 6 and is configured as follows:

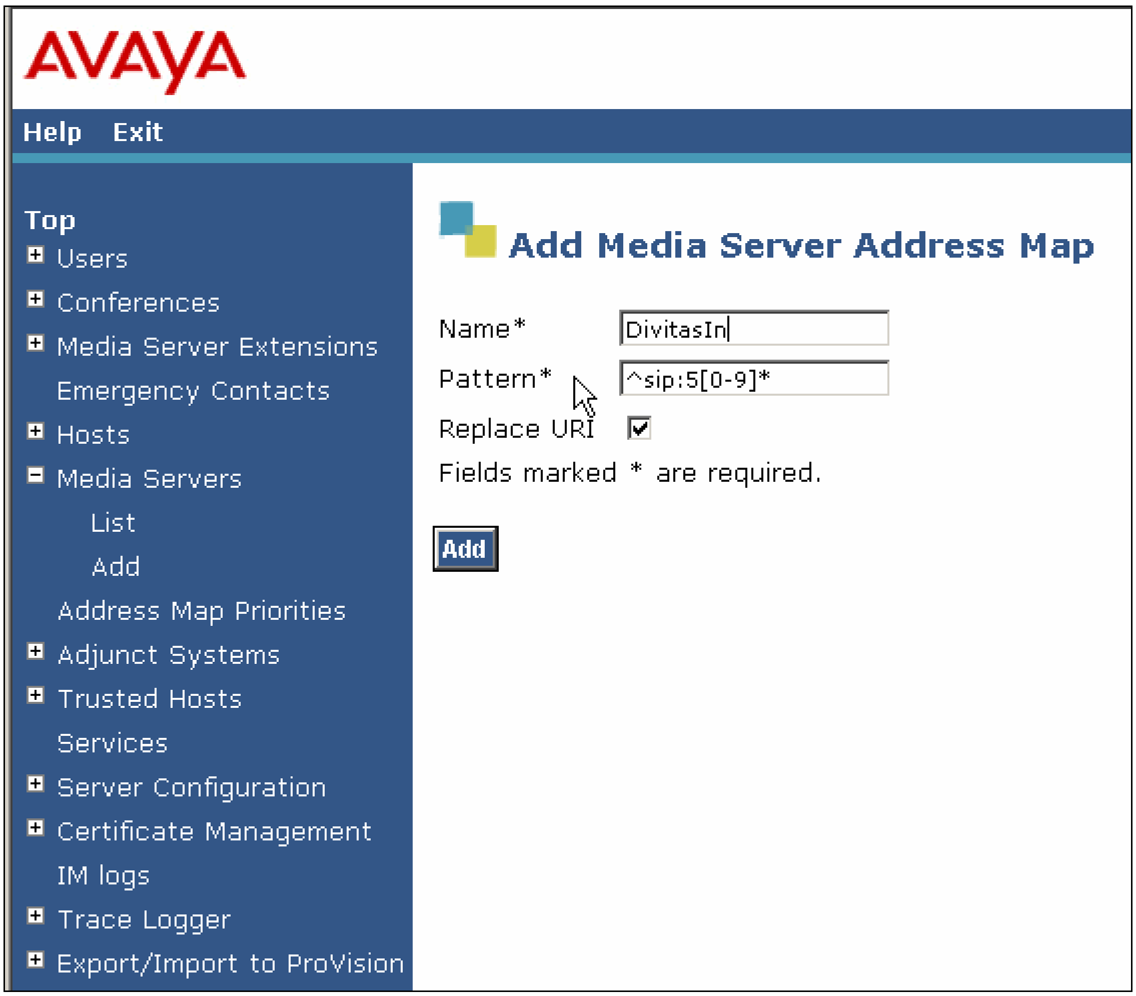
Click Add Another Contact on the List Host Address Map screen. [not shown]
Contact – Enter the destination IP address (ip_addr), port number (port) and transport protocol (protocol) as follows:
sip:$(user)@ip_addr:port;transport=protocol.
In this example sip:$(user)@192.45.51.10:5060;transport=udp is entered. The IP address corresponds to the DiVitas MCA IP address.
Click on Add and then click Continue on the next page (not shown).

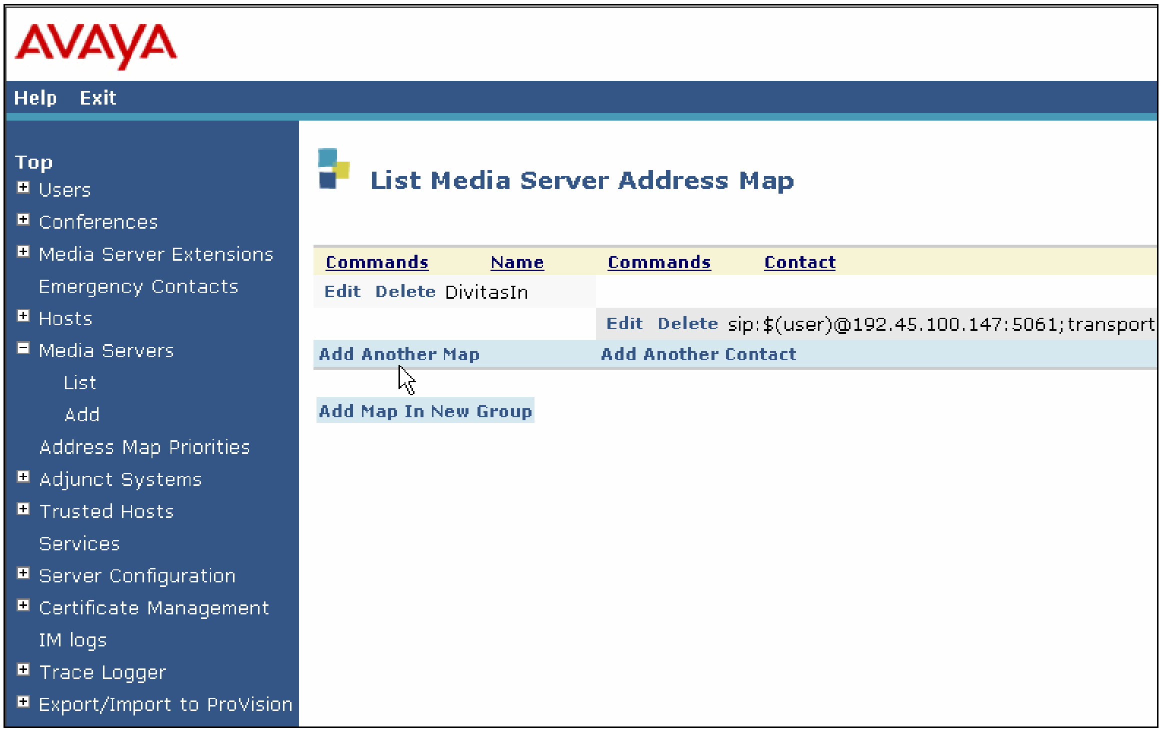


</td></tr>
</table>

Step	Description
8.	The IP Address of the DiVitas MCA 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 IP address of the DiVitas MCA. Configure as follows: • IP Address – IP Address of the DiVitas MCA. • Host – Select the IP address of the appropriate SES. • Comment – Any descriptive comment. • Click **Add**. 

Step	Description
9.	To add a map back to Avaya Communication Manager, configure as follows: • Click the **+** sign next to **Media Servers** and select **List**. • At the next screen [not shown], click **Add Another Map** to display the screen below. • **Name** – Any Descriptive Name • **Pattern** – Pattern to match for calls originating from the DiVitas MCA for proper routing back to Avaya Communication Manager. • Click **Add**.



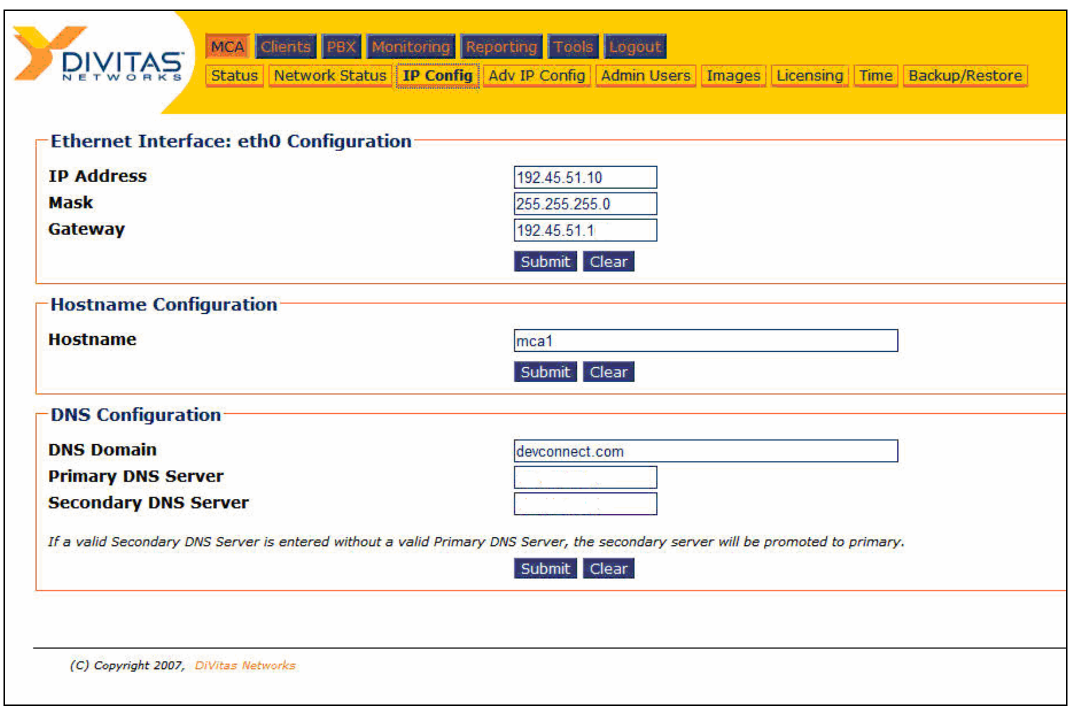
Step	Description
10.	Confirmation screen indicating a route back to Avaya Communication Manager. 
11.	Click Update at the bottom of left pane [not shown] to accept all the changes.

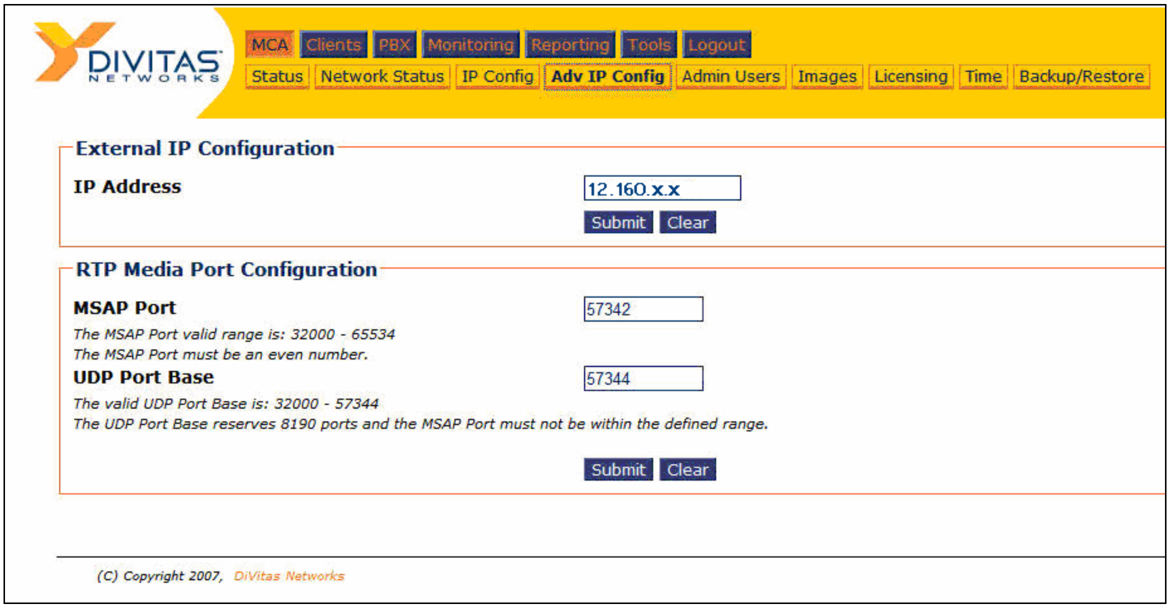
5. Configure DiVitas Mobile Convergence Appliance

This section describes the steps for configuring the DiVitas MCA which supports a variety of dual mode (WiFi/Cellular) telephones including Nokia E61i and Nokia E65 running the DiVitas Mobile Convergence Client. Steps described here apply only to the fields where a value needs to be entered or modified. Default values are used for all other fields. Refer to [5, 6] for additional information.

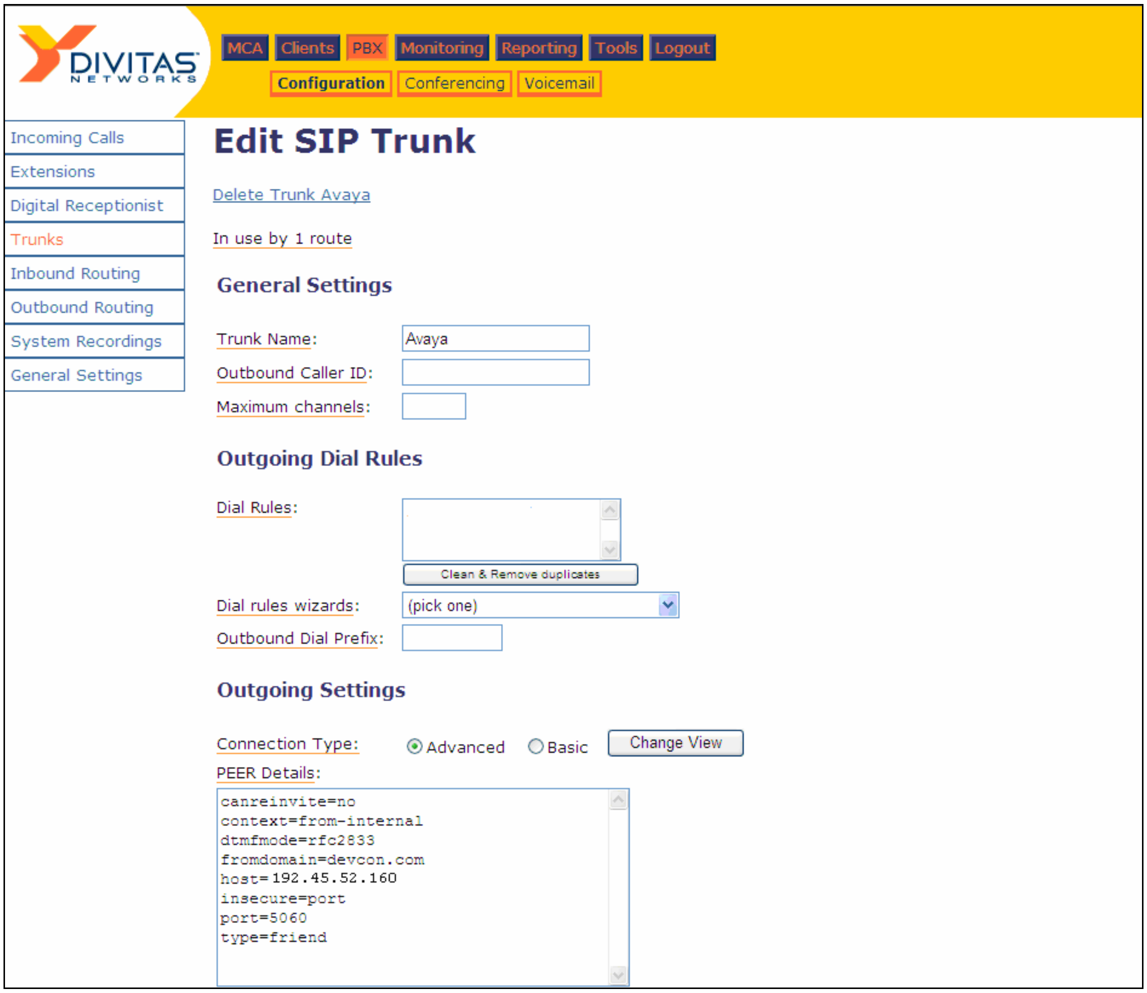
Table 1 - DiVitas MCA Configuration Sequence

Step	Description
1	Configure the MCA network parameters: IP address, Net mask, DNS, etc…
2	Configure the MCA External IP address and RPT port addresses
3	Define and configure SIP trunk
4	Define trunk advanced configuration features
5	Define the routing for the non-MCA hosted extensions
6	Define MCA Extensions
7	Complete the extension profile
8	Create and configure each User account

Step	Description
1.	Configure the MCA-1000 network addresses to be conformant to the hosting network scheme. Screen below is the main network dialog box for setting the MCA IP parameters. 

Step	Description
2.	The dialog box below is where any valid public IP address must be configured. This is used by the Mobile Convergence Client (MCC) for accessing the MCA from a cellular data network. The two ports defaulting on this screen are necessary to traverse the NAT or firewall from off campus. 

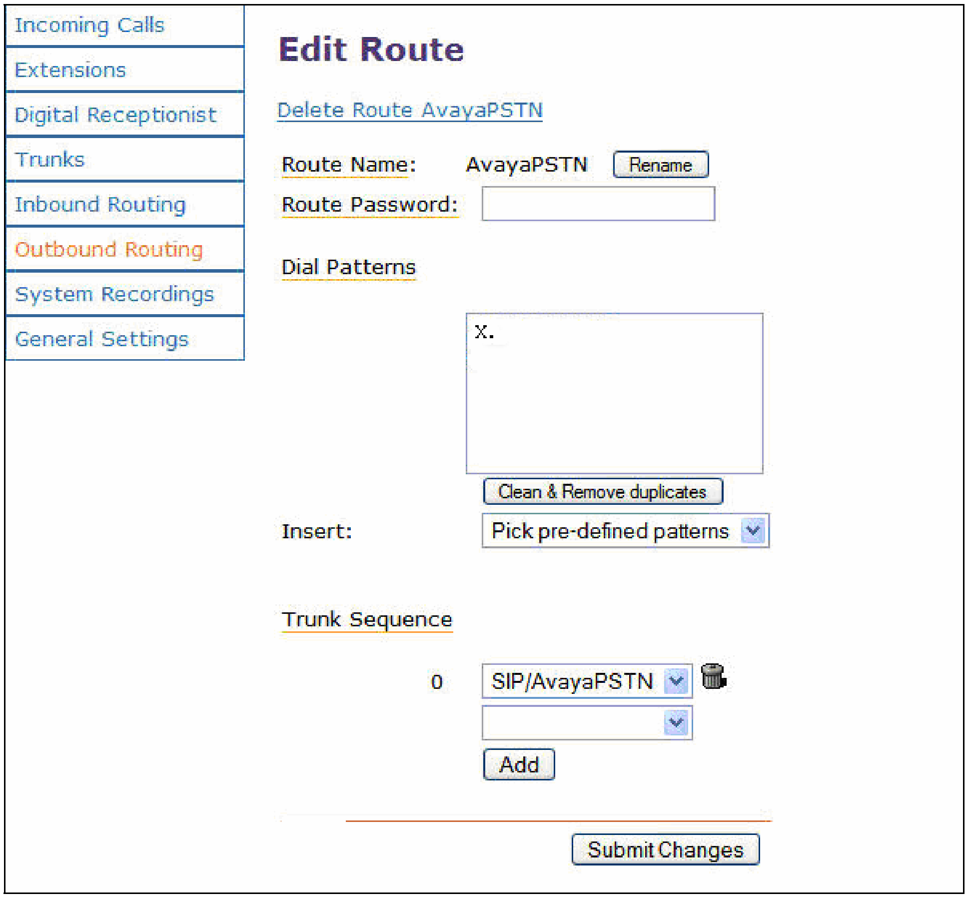
Step	Description
3.	The interface to the Avaya SES is via definition of a SIP trunk (see below) for example.



Step	Description
4.	Advanced trunk configuration information is provided below. canreinvite=yes context=from-internal dtmfmode=rfc2833 fromdomain=devconnect.com host=192.45.52.160 (Should match the IP address of the Avaya SES) insecure=port port=5060 type=friend

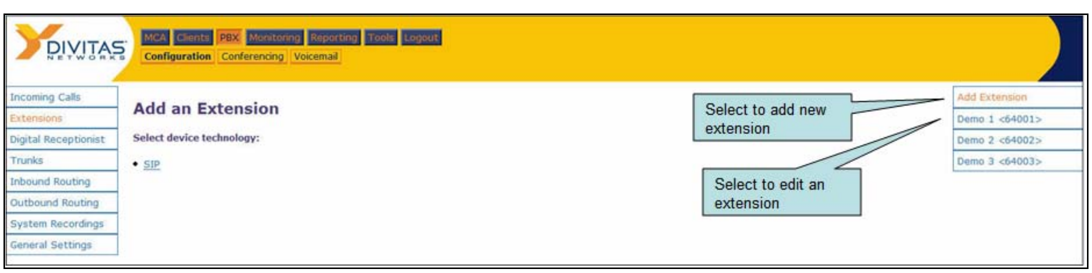
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>5.</td><td>

To properly route non-MCA hosted extension or PSTN calls, outbound dial plans must be defined. The figure below provides an example of how such dial plans are defined to route calls to the SES/Avaya system. **X.** in **Dial Patterns** field will allow any number of digits to be dialed.

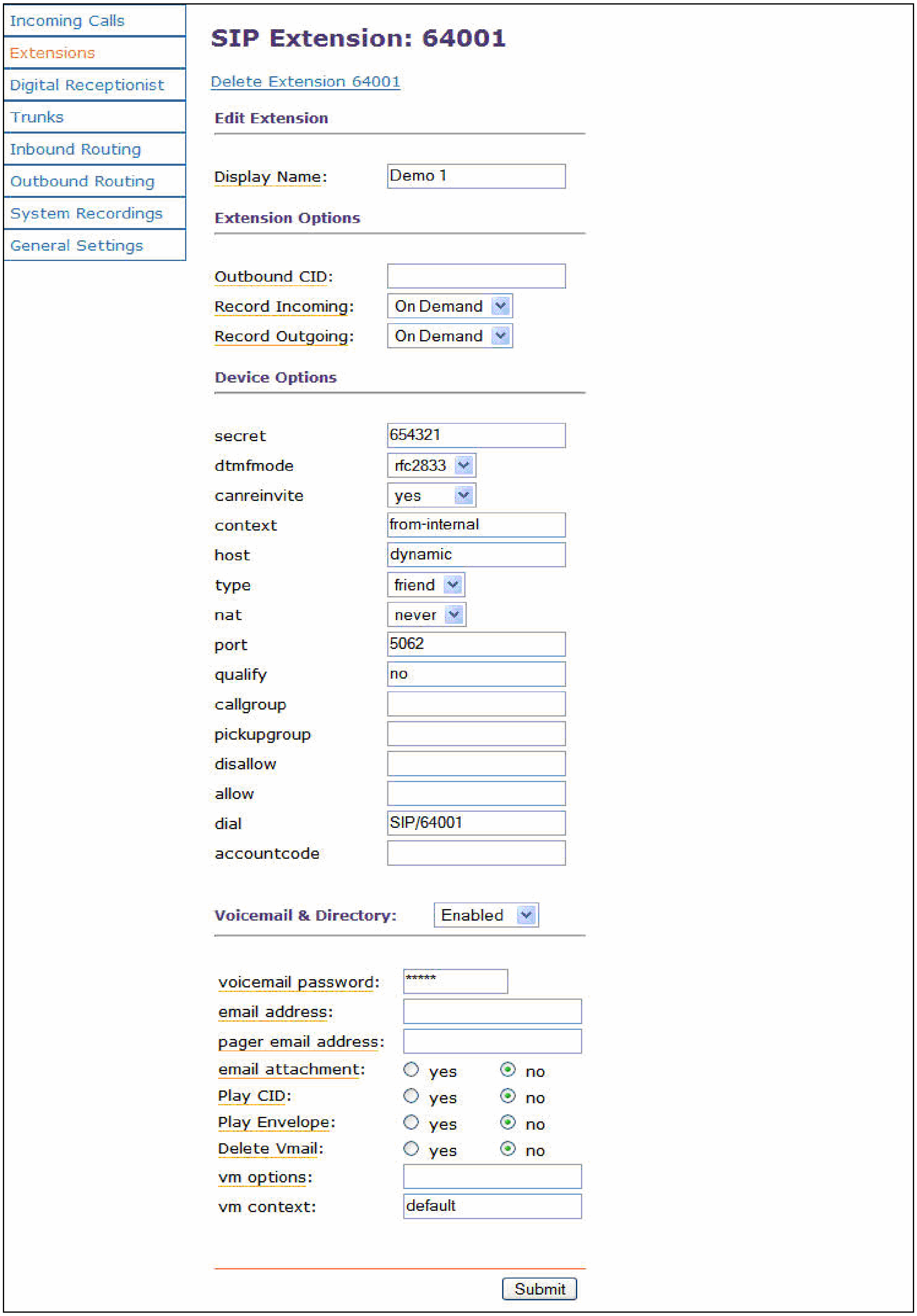


</td></tr>
<tr><td>6.</td><td>

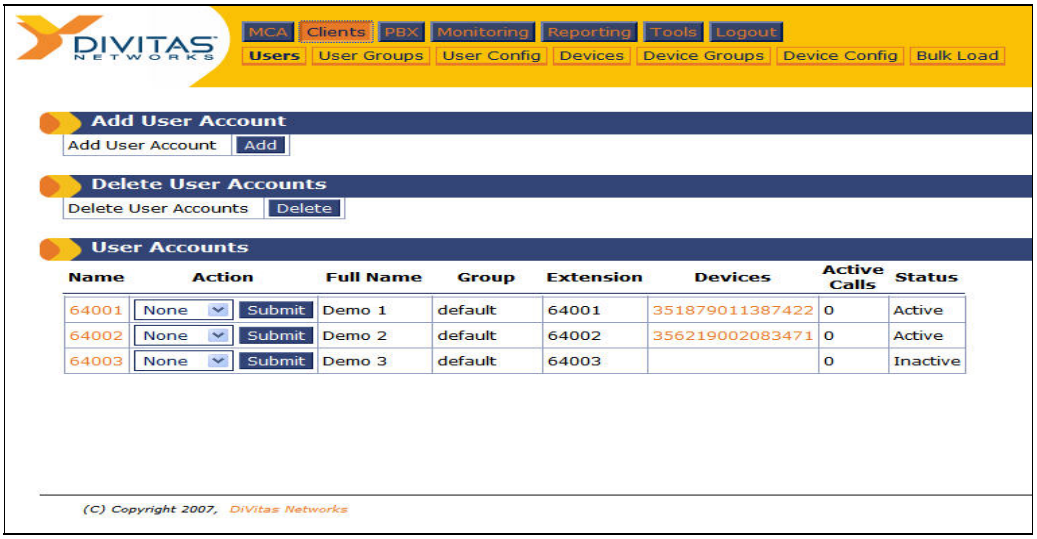
MCA extensions must be added that have extension numbers assigned that are not in conflict with the hosting Avaya Communication Manager extension range. The screen below is the initial screen invoked to add extension profiles to the MCA. Extension profile must be defined for each supported extension.



</td></tr>
</table>

Step	Description
7.	The SIP Extension dialog box is used to complete the extension profile. 

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>8.</td><td>Configure Users with assigned extensions (name) that do not conflict with the hosting Avaya Communication Manager extension ranges. These will be configured as Off Premise Extension (OPE). Creation of new User Accounts can be invoked by pressing the Add in the Add User Account section.



</td></tr>
</table>

6. Interoperability Compliance Testing

The focus of the interoperability compliance testing was primarily on verifying call establishment using the DiVitas MCA and operations such as dialing methods (manual, re-dial, and telephone book), hold, mute, transfer and conference. Tests were done to verify DiVitas MCA interactions with Avaya SES, Avaya Communication Manager, and Avaya SIP, H.323, and digital telephones.

6.1. General Test Approach

The general test approach was to place calls to and from the DiVitas MCA handsets and exercise basic telephone operations. The main objectives were as follows:

- Successfully establish calls between the DiVitas MCA and Avaya SIP, H.323, and digital telephones registered to Avaya SES or Avaya Communication Manager.
- Successfully establish calls between the DiVitas MCA and PSTN telephone through Avaya Communication Manager.
- The DiVitas MCA successfully negotiates the right codec.
- The DiVitas MCA successfully shuffles the VoIP calls.
- The DiVitas MCA successfully transmits DTMF during a call.
- The DiVitas MCA successfully holds a call, transfers a call, establishes a three party conference call, and displays calling party number.
- The DiVitas MCA successfully handles layer-3 (DiffServ) QoS for Audio.

For serviceability testing, failures such as cable pulls and hardware resets were applied. For performance testing, a conference call involving two devices registered with DiVitas MCAs and two Avaya telephones was formed as follows.

6.2. Test Results

The test objectives of **Section 6.1** were verified. For serviceability testing, the DiVitas MCA operated properly after recovering from failures such as cable disconnects, and resets of the DiVitas MCA, the Avaya SES server, and Avaya Communication Manager. For performance testing, the conference call was successfully maintained for approximately two hours. The DiVitas MCA successfully shuffles to communicate directly with the other endpoints.

The following observations were made during testing:

- The DiVitas MCA cannot negotiate with Avaya Communication Manager for the correct codec when establishing a conference call if the codec used during negotiation is not the top priority codec for the DiVitas MCA. After the conference setup, the other two parties cannot hear audio from the last party added.
- The DiVitas MCA cannot negotiate with Avaya Communication Manager for the correct codec when a held call is retrieved. This happens if the codec used during negotiation is not the top priority codec for the DiVitas MCA and hence no audio for the call when the call is put off hold.

DiVitas will address and resolve all the above observations with future firmware releases. Contact DiVitas (www.divitas.com) for further updates.

7. Verification Steps

The following steps may be used to verify the configuration:

- Place calls to and from the DiVitas MCA handset and verify that the calls are successfully established with two-way talk path.
- From the Avaya Communication Manager System Access Terminal (SAT) interface, perform the following steps to verify:
    - Audio codec used between two telephones
    - Shuffling between two telephones

Step	Description
1.	Enter **status trunk <t>** command, where **t** is the SIP trunk configured in **Section 3.6**. Note the **Member** with **Service State** set to **in-service/active**. In this example, **0010/002** and **0010/006** are active and either member can be used to verify whether calls shuffled and which codec was used.

```
status trunk 10

                          TRUNK GROUP STATUS

Member   Port    Service State      Mtce Connected Ports
                                    Busy

0010/001 T00046  in-service/idle    no
0010/002 T00047  in-service/active  no   T0051
0010/003 T00048  in-service/idle    no
0010/004 T00049  in-service/idle    no
0010/005 T00050  in-service/idle    no
0010/006 T00051  in-service/active  no   T0047
0010/007 T00052  in-service/idle    no
0010/008 T00053  in-service/idle    no
0010/009 T00054  in-service/idle    no
0010/010 T00055  in-service/idle    no
```

Step	Description
2.	Enter **status trunk** <m>**,** where **m** is the member in the active state as noted in the previous step for verification of codec used and shuffling status: • Codec – The codec used for Audio is **G.711MU** in this example. • Shuffling - If the **Near-end IP Addr** and **Far-end IP Addr** for **Audio** are using the same port and the **Audio Connection Type** is **ip-direct**, it signifies that shuffling was successful. In this example, shuffling was successful.

```
status trunk 10/2                                              Page 1 of 2

                            TRUNK STATUS

 Trunk Group/Member: 0010/002           Service State: in-service/active
               Port: T00047          Maintenance Busy? No
Signalling Group ID:



   Connected Ports: T0051

           Port     Near-end IP Addr  : Port    Far-end IP Addr  : Port
Signaling: 01A0617  192. 45.100.147   : 5061    192. 45. 52.160  : 5061

G.711MU   Audio:    192. 45. 53.101   : 34008   192. 45. 53.102  : 34008
          Video:
    Video Codec:
                                   Authentication Type: None
  Audio Connection Type: ip-direct
```

8. Support

For technical support on the DiVitas MCA 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: 1-866-857-6087
- E-mail: support@divitas.com

9. Conclusion

These Application Notes describe a solution comprised of Avaya Communication Manager 4.0.1, Avaya SIP Enablement Services 4.0, and dual mode (WiFi/Cellular) telephones registered with the SIP–based DiVitas Mobile Convergence Appliance (MCA). The compliance testing was successful with the exception of the issues noted in **Section 6.2**.

10. Additional References

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

[1] *Administrator Guide for Avaya Communication Manager*, Issue 3.1, February 2007, Document Number 03-300509

[2] *Administration for Network Connectivity for Avaya Communication Manager*, Issue 12, February 2007, Document Number 555-233-504

[3] *SIP Support in Release 3.1 of Avaya Communication Manager*, Issue 7, May 2007, Document Number 555-245-206

[4] *Installing and Administering SIP Enablement Services R3.1.2*, Issue 4, May 2007, Document Number 03-600768

Product documentation for DiVitas products may be found at http://www.divitas.com.

[5] DiVitas Mobile Convergence Appliance Administration Guide, v1.3 P/N: DOC-MCA-AG-008

[6] DiVitas Mobile Convergence Client User Guide, v1.3 P/N: DOC-MCC-UG-004

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.