Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the Vocera Communications System with Avaya Aura^{TM} SIP Enablement Services and Avaya Aura^{TM} Communication Manager - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring the Vocera Communications System to interoperate with Avaya Aura^{TM} SIP Enablement Services and Avaya Aura^{TM} Communication Manager.

The overall objective of the interoperability compliance testing is to verify Vocera Communications System functionalities in an environment comprised of Avaya Aura^{TM} Communication Manager, Avaya Aura^{TM} SIP Enablement Services, and various SIP IP Telephones.

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 compliance-tested configuration comprised of the wireless communication features of Vocera Communications System with Avaya Aura^{TM} Communication Manager and Avaya Aura^{TM} SIP Enablement Services.

Vocera Communications System is comprised of three main components:

- Vocera Badges
- Vocera Server
- Vocera SIP Telephony Gateway

The Vocera Badges are wireless 802.11b/g devices that serve as communicators in a wireless environment. By pressing the call button on a badge, a user can interface with the Vocera Server to start the call process.

The Vocera Server acts as a communication server to service calls between the badges. The Vocera Server stores the user and Badge information, and has the speech access interface that allows users to place and receive calls.

The Vocera SIP Telephony Gateway provides connectivity to Avaya Aura^{TM} Communication Manager. The Vocera SIP Telephony Gateway was utilized for the test to setup a SIP trunk between the Vocera SIP Telephony Gateway and Avaya Aura^{TM} SIP Enablement Services. The Vocera SIP Telephony Gateway allows the Vocera Server to connect Badges to Avaya Aura^{TM} Communication Manager users and extensions, as well as route calls to the public network through Avaya Aura^{TM} Communication Manager.

The two server applications, Vocera Server and Vocera SIP Telephony Gateway, can reside in the same physical server platform. Vocera recommends using multiple Vocera SIP Telephony Gateway servers, and array for redundancy, especially if the Vocera SIP Telephony Gateway will be hosted on a VM.

For additional information on Vocera Communication System, please refer to Vocera documentation [3].

1.1. Interoperability Compliance Testing

The interoperability compliance test included features and serviceability. The focus of the interoperability compliance testing was primarily on verifying call establishment on the Vocera Communications System. Vocera Communications System operations such as inbound calls, outbound calls, call transfer, DTMF, and Vocera Communications System interactions with SIP Enablement Services, Communication Manager, and Avaya SIP and H.323 IP telephones were verified. The serviceability testing introduced failure scenarios to see if Vocera Communications System can recover from failures.

1.2. Support

For technical support on the Vocera Communications System solution can be obtained by contacting Vocera Commuications System:

- URL – support@Vocera.com
- Phone – (800) 473-3971

2. Reference Configuration

Figure 1 illustrates a sample configuration consisting of Avaya S8720 Servers, an Avaya G650 Media Gateway, an Avaya Aura^{TM} SIP Enablement Services server, and Vocera Communications System. The solution described herein is also extensible to other Avaya Servers and Media Gateways. Avaya S8300 Server with an Avaya G450 Media Gateway were included in the test to provide an inter-switch scenario. For completeness, Avaya 4600 Series H.323 IP Telephones, Avaya 9600 Series SIP IP Telephones, and Avaya 9600 Series H.323 IP Telephones are included in **Figure 1** to verify calls between the SIP-based Vocera Communications System and Avaya SIP, H.323, and digital telephones.

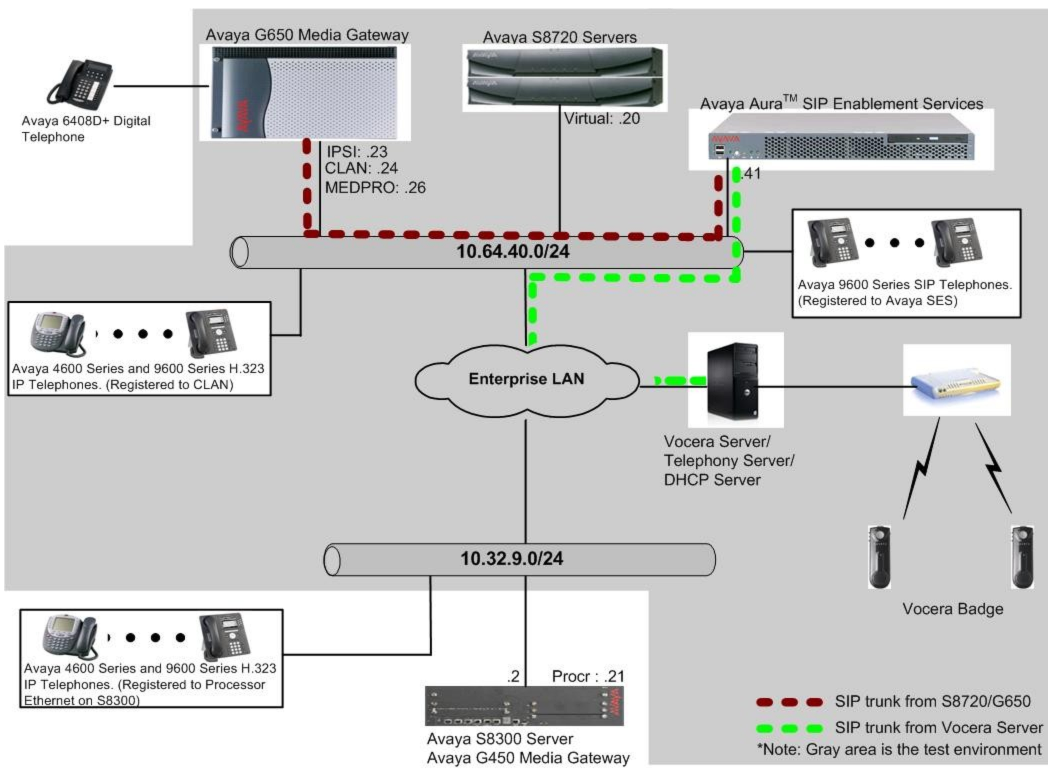


Figure 1: Test Configuration of Vocera Communications System

3. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya S8720 Servers with Avaya G650 Media Gateway		Avaya Aura™ Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya Aura™ SIP Enablement Services		Avaya Aura™ SIP Enablement Services 5.2.1 (SES05.2.1-02.1-016.4)
Avaya S8300 Media Server with Avaya G450 Media Gateway		Avaya Aura™ Communication Manager 6.0 (R016x.00.0.345.0) with Patch 00.0345.0-18246
Avaya 9600 Series SIP Telephones		
	9620 (SIP) 9630 (SIP) 9650 (SIP)	2.5 2.5 2.5
Avaya 4600 and 9600 Series IP Telephones		
	4625 (H.323) 9620 (H.323) 9630 (H.323) 9650 (H.323)	2.9 3.1 3.1 3.1
Avaya 6408D+ Digital Telephone		-
Vocera Communications System	Vocera Server and Vocera SIP Telephony Gateway Vocera Badge Vocera Badge	4.1 SP5 build 1977 B1000 -1977 B2000-345

4. Configure Avaya Aura™ Communication Manager

This section describes the procedure for setting up a SIP trunk between Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services. The steps include setting up an IP codec set, an IP network region, IP node name, a signaling group, a trunk group, route pattern, and aar analysis. Before a trunk can be configured, it is necessary to verify if there is enough capacity to setup an additional trunk. The highlights in the following screens indicate the values used during the compliance test. Default values may be used for all other fields.

These steps are performed from the Avaya Aura™ Communication Manager System Access Terminal (SAT) interface.

4.1. Capacity Verification

Enter the **display system-parameters customer-options** command. Verify that there are sufficient Maximum Off-PBX Telephones – OPS licenses for Avaya SIP endpoints. If not, contact an authorized Avaya account representative to obtain additional licenses. During the compliance test, the Vocera Communications System was not utilized as a SIP endpoint, but did utilize the SIP trunk.

```
display system-parameters customer-options                        Page   1 of  11
                                OPTIONAL FEATURES

     G3 Version: V15                             Software Package: Standard
       Location: 1                            RFA System ID (SID): 1
       Platform: 6                            RFA Module ID (MID): 1

                                                                USED
                                Platform Maximum Ports: 44000 10273
                                      Maximum Stations: 36000 10127
                              Maximum XMOBILE Stations: 0     0
                    Maximum Off-PBX Telephones - EC500: 50    0
                    Maximum Off-PBX Telephones -   OPS: 100   4
                    Maximum Off-PBX Telephones - PBFMC: 0     0
                    Maximum Off-PBX Telephones - PVFMC: 0     0
                    Maximum Off-PBX Telephones - SCCAN: 0     0
```

On **Page 2** of the form, 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.

```
display system-parameters customer-options                        Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 100   39
           Maximum Concurrently Registered IP Stations: 18000 4
             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: 5     0
                   Maximum Video Capable IP Softphones: 5     0
                       Maximum Administered SIP Trunks: 100   50
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                             Maximum TN2501 VAL Boards: 10    1
                     Maximum Media Gateway VAL Sources: 0     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
```

4.2. IP Codec Set

This section describes the steps for administering a codec set in Communication Manager. This codec set is used in the IP network region for communications between Communication Manager and SIP Enablement Services. 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 4.3** for configuring IP network regions to specify which codec sets may be used within and between network regions.

```
change ip-codec-set 1                                          Page   1 of   2

                          IP Codec Set

    Codec Set: 1

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

4.3. Configure IP Network Region

This section describes the steps for administering an IP network region in Communication Manager for communication between Communication Manager and SIP Enablement Services. Enter the **change ip-network-region <n>** command, where **n** is a number between **1** and **250** inclusive, and configure the following:

- Authoritative Domain – Enter the appropriate name for the Authoritative Domain. During the compliance test, the authoritative domain is set to **avaya.com**. This should match the SIP Domain value on SIP Enablement Services, in **Section 5.1**.
- Codec Set – Set the codec set number as provisioned in **Section 4.2**.

```
change ip-network-region 1                                     Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location:          Authoritative Domain: avaya.com
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3029
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? n
        Video PHB Value: 26                   Server IP Address: 10 .64 .44
.101
802.1P/Q PARAMETERS                                 Server Port: 5005
 Call Control 802.1p Priority: 6       RTCP Report Period(secs): 5
        Audio 802.1p Priority: 6
```

4.4. Configure IP Node Name

This section describes the steps for setting the IP node name for SIP Enablement Services in Communication Manager. Enter the **change node-names ip** command, and add a node name for SIP Enablement Services along with its IP address.

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
CLAN                    10.64.40.24
MEDPRO                  10.64.40.26
S8300                   10.64.42.21
SES                     10.64.40.41
```

4.5. Configure SIP Signaling

Enter the **add signaling-group <s>** command, where **s** is an available signaling group and configure the following:

- Group Type – Set to **sip**.
- IMS Enabled – Verify that the field is set to **n**. Setting this filed to **y** will cause Communication Manager to act as a Feature Server.
- Transport Method – Set to **tls** (Transport Layer Security).
- Near-end Node Name – Set to **CLAN** as displayed in **Section 4.4**.
- Far-end Node Name – Set to the SIP Enablement Services name configured in **Section 4.4**.
- Far-end Network Region – Set to the region configured in **Section 4.3**.
- Far-end Domain – Set to **avaya.com**. This should match the SIP Domain value in **Section 4.3**.

```
add signaling-group 201                                           Page   1 of   1
                                SIGNALING GROUP

 Group Number: 201             Group Type: sip
                         Transport Method: tls
  IMS Enabled? n




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

                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload              Direct IP-IP Audio Connections? n
Session Establishment Timer(min): 3                       IP Audio Hairpinning? n
         Enable Layer 3 Test? n
                                                  Alternate Route Timer(sec): 6
```

4.6. Configure Trunk Group

To configure the associated trunk group, enter the **add tunk-group <t>** command, where **t** is an available trunk group and configure the following:

- Group Type – Set the Group Type field to **sip**.

- Group Name – Enter a descriptive name.
- TAC (Trunk Access Code) – Set to any available trunk access code.
- Service Type – Set the Service Type field to **tie**.
- Signaling Group – Set to the Group Number field value configured in **Section 4.4**.
- Number of Members – Allowed value is between 0 and 255. Set to a value large enough to accommodate the number of SIP telephone extensions being used.

```
Add trunk-group 201                                             Page   1 of  21
                                TRUNK GROUP

Group Number: 201                  Group Type: sip          CDR Reports: y
  Group Name: SIP-4-Vocera                 COR: 1        TN: 1          TAC: 116
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                     Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n

                                                      Signaling Group: 201
                                                    Number of Members: 10
```

4.7. Configure Route Pattern

For the trunk group created in **Section 4.6**, define the route pattern by entering the **change route-pattern <r>** command, where **r** is an unused route pattern number. The route pattern consists of a list of trunk groups that can be used to route a call. The following screen shows route-pattern 201 will utilize trunk group 201 to route calls. The default values for the other fields may be used.

```
change route-pattern 201                                        Page   1 of   3
                    Pattern Number: 201 Pattern Name: SIP trunk
                             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: 201  0                                                             n   user
 2:                                                                    n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 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
```

4.8. Configure AAR Analysis

For the AAR Analysis Table, create the dial string that will map calls to the Vocera Communications System via the route pattern created in **Section 4.7**. Enter the **change aar analysis <x>** command, where **x** is a starting digit. The dialed string created in the AAR Digit

Analysis table should contain a map to the Vocera Communications System extensions, which are configured as x28021 – x28025.

```
change aar analysis 2802                                        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
    2802                     5    5      201       aar            n
    303532802                10   10     201       aar            n
```

5. Configure Avaya Aura™ SIP Enablement Services

This section covers the configuration of Avaya Aura™ SIP Enablement Services. Avaya Aura™ SIP Enablement Services is configured via an Internet browser using the administration web interface. It is assumed that the Avaya Aura™ SIP Enablement Services software and the license file have already been installed on the server. During the software installation, an installation script is run from the Linux shell of the server to specify the IP network properties of the server along with other parameters. In addition, it is assumed that the setup screens of the administration web interface have been used to initially configure Avaya Aura™ SIP Enablement Services.

This section is divided into two parts. **Section 5.1** will summarize the user-defined parameters used in the installation procedures that are important to understanding the solution as a whole. This section will not attempt to show the installation procedures in their entirety. It will describe any deviations from the standard procedures, if any. **Section 5.2** will describe procedures beyond the initial SIP installation procedures that are necessary to support Vocera Communications System.

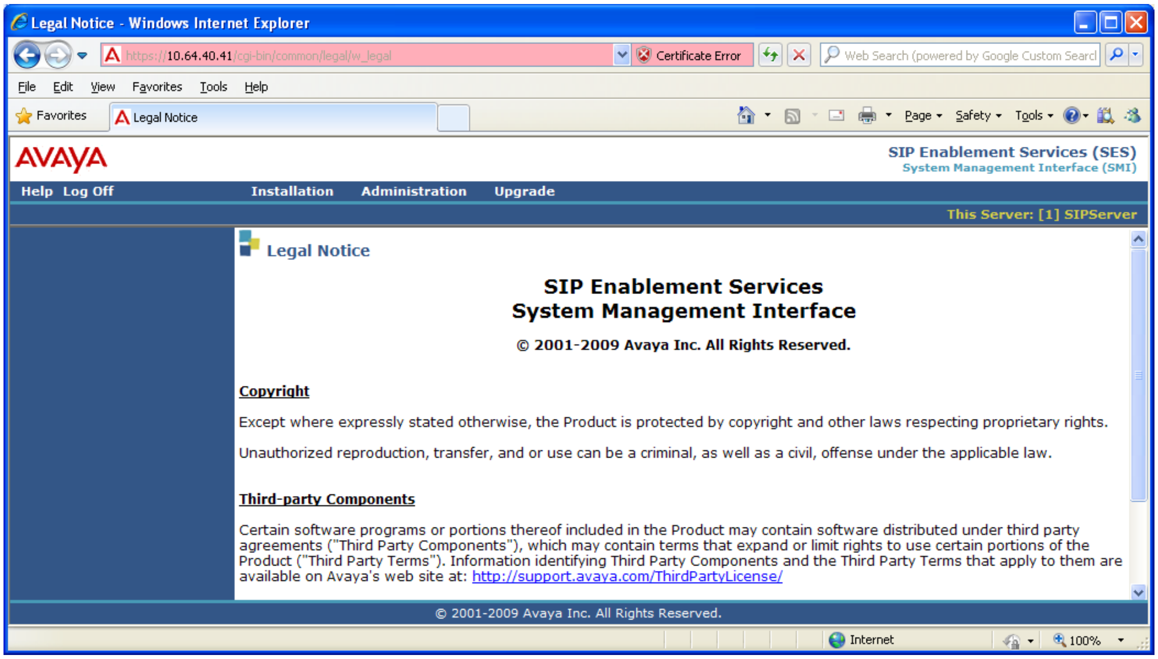
5.1. Summarize Initial Configuration Parameters

This section summarizes the applicable user-defined parameters used during the SIP installation procedures.

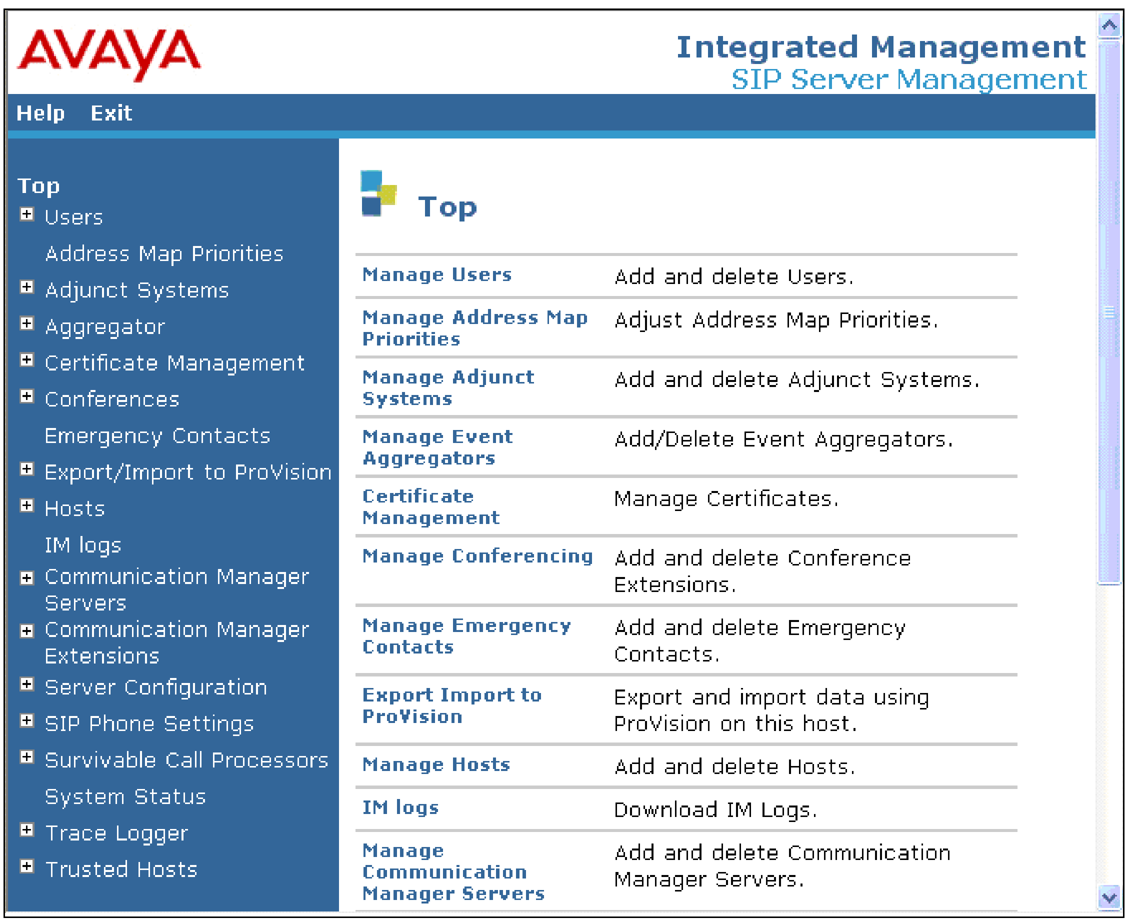
5.1.1. Login

Access the SIP Enablement Services administration web interface by entering http://<*ip-addr*>/admin as the URL in an Internet browser, where <*ip-addr*> is the IP address of the SIP Enablement Services.

Log in with the appropriate credentials and then navigate to the **Administration→ SIP Enablement Services** link from the main page shown below.



The SIP Enablement Services **Top** page will be displayed as shown below.



5.1.2. Initial Configuration Parameters

As part of the SIP Enablement Services installation and initial configuration procedures, the following parameters were defined. Although these procedures are out of the scope of these Application Notes, the values used in the compliance test are shown below for reference. After each group of parameters is a brief description of how to view the values for that group from the SIP Enablement Services administration home page shown in the previous step.

- SIP Domain: ***testroom.avaya.com***
  (To view, navigate to **Server Configuration→System Parameters**)

- Host IP Address (SES IP address): ***10.64.40.41***
- Host Type: ***SES combined home-edge***
  (To view, navigate to **Host→List**; click **Edit**)

- Communication Manager Server Interface Name: ***S8720***
- SIP Trunk Link Type: ***TLS***
- SIP Trunk IP Address (procr IP address): ***10.64.40.24***
  (To view, navigate to **Communication Manager Servers→List**; click **Edit**)

5.2. Vocera Specific Configuration

This section describes additional SIP Enablement Services configuration necessary for supporting Vocera Communications System.

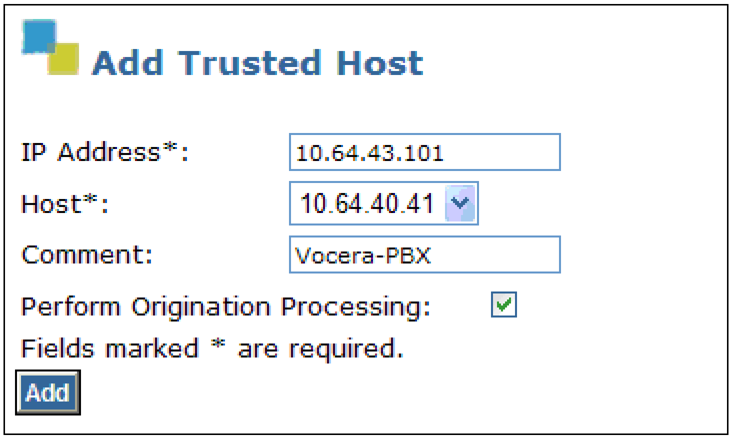
5.2.1. Trusted Host

Define Vocera Communications System to be a trusted host. Navigate to **Trusted Hosts→Add** in the left pane (see **Section 5.1.1**). In the **Add Trusted Host** window that appears, configure the following:

- **IP Address**: Enter the IP address of Vocera Communications System (Vocera SIP Telephony Gateway).
- **Host**: Select the SIP Enablement Services IP address from the drop-down menu.
- **Comment**: Enter a description of the trusted host being added.

Click the **Add** button.

Repeat this step as necessary to configure additional trusted hosts if needed. During the Vocera DevConnect Compliance test, two trusted hosts were utilized (NBS-East and NBS-West), as shown in **Figure 1**.



5.2.2. Communication Manager Address Map

A Communication Manager Address map is needed to route calls from the Vocera Communications System, via the SIP trunk, to the enterprise (Communication Manager). This is necessary because neither the caller nor the called party is a registered user with SIP Enablement Services with a Communication Manager extension assigned to them. As a result, SIP Enablement Services does not know to route this call to Communication Manager. Thus to accomplish this task, a Communication Manager address map is needed.

Each map defines a call matching criteria based on the contents of the SIP Request-URI of the call. If a call matches the map, then the call is directed to the specified destination or contact. The URI usually takes the form of *sip:user@domain*, where *user* is the destination number and *domain* is a domain name or an IP address.

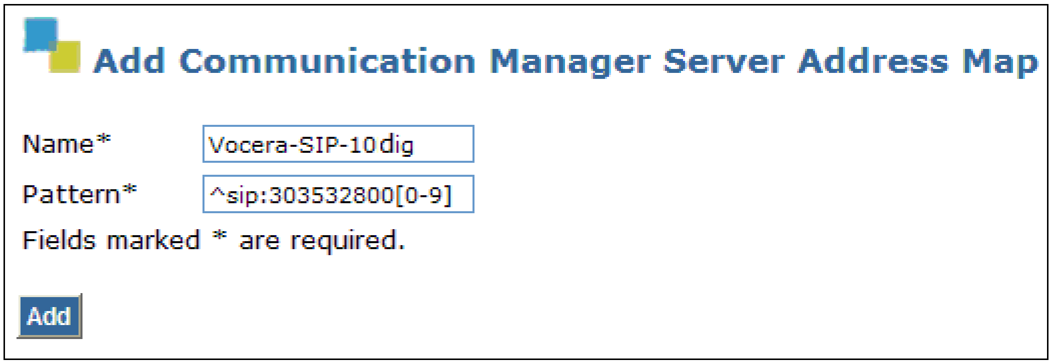
To configure a **Communication Manager Server Address Map**:

- Navigate to **Communication Manager Servers→List** in the left pane of the Administration web interface.
- Click on the **Map** link associated with the appropriate server.
- Click on the **Add Map In New Group** link. If other maps exist that point to the correct destination (contact) then click on **Add Another Map**.

In either case, the **Add Communication Manager Server Address Map** window appears as shown below. Configure the address map as follows:

- **Name**: Enter any descriptive name.
- **Pattern**: Enter an expression to define the matching criteria for calls to be routed from the Vocera Communications System to Communication Manager. For the address map named ***Vocera-SIP-10Dig***, the expression will match any URI that begins with ***sip:303532800*** followed by any digit between ***0-9*** for the next digit.

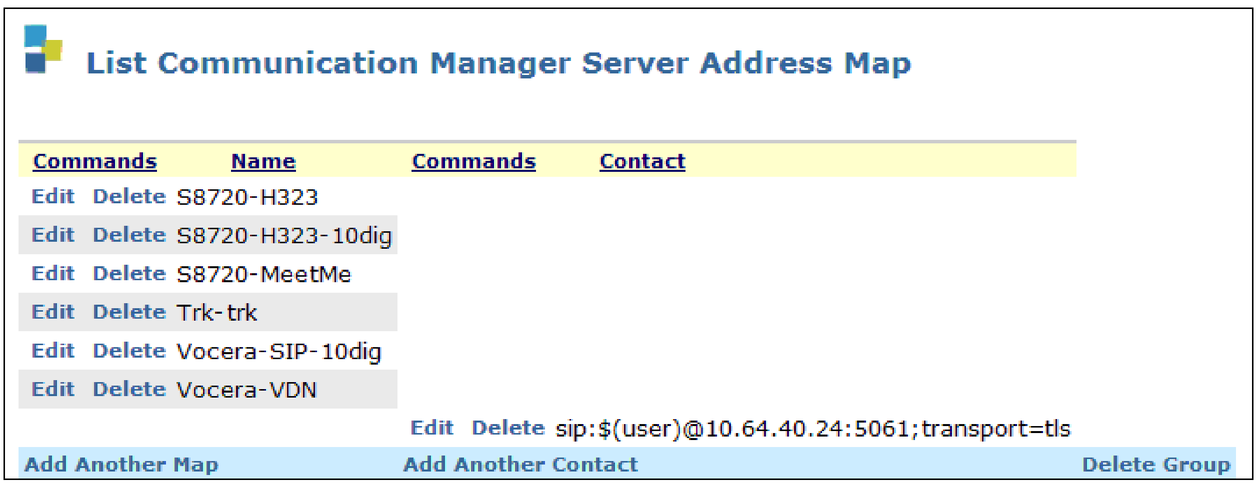
Click **Add**.



After adding the address map, the **List Communication Manager Server Address Map** screen will appear, as shown below. When the first **Communication Manager Server Address Map** is added, a **Contact** is created automatically. For the **Communication Manager Server Address Map** previously added, the following contact was created:

sip:$(user)@10.64.40.24:5061;transport=tls

This contact directs the calls to Communication Manager via IP address (***10.64.40.24***) using port ***5061*** and ***TLS*** as the transport protocol. The incoming DID number sent in the user part of the original request URI is substituted for **$(user)** in the **Contact** expression.



5.2.3. Host Address Map

A Host Address map is needed to route calls from Communication Manager via the SIP trunk to Vocera Communications System. This is necessary because neither the caller nor the called party is a registered user with SIP Enablement Services with a Communication Manager extension assigned to it. As a result, SIP Enablement Services does not know to route this call to Vocera Communications System. Thus, to accomplish this task, a Host Address map is needed.

Each map defines a call matching criteria based on the contents of the SIP Request-URI of the call. If a call matches the map, then the call is directed to the specified destination or contact. The URI usually takes the form of *sip:user@domain*, where *user* is the destination number and *domain* is a domain name or an IP address.

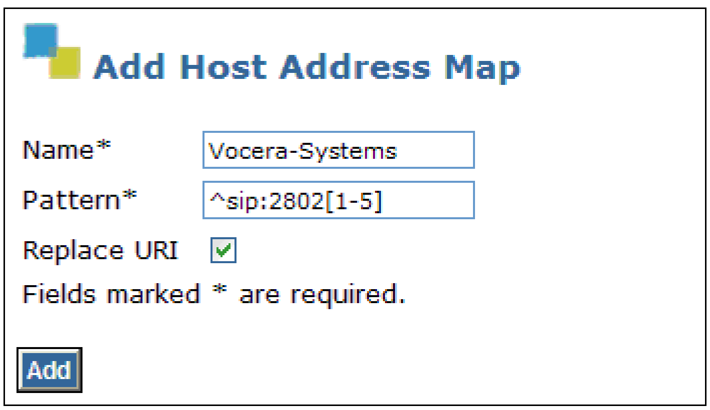
To configure a **Host Address Map**:

- Navigate to **Hosts→List** in the left pane of the Administration web interface.
- Click on the **Map** link associated with the appropriate server.
- Click on the **Add Map In New Group** link. If other maps exist that point to the correct destination (contact) then click on **Add Another Map**.

In either case, the **Add Host Address Map** window appears as shown below. Configure the address map as follows:

- **Name**: Enter any descriptive name.
- **Pattern**: Enter an expression to define the matching criteria for calls to be routed from the Vocera Communications System to Communication Manager. For the address map named ***Vocera-Systems***, the expression will match any URI that begins with ***sip:2802*** followed by any digit between ***0-5*** for the next digit.

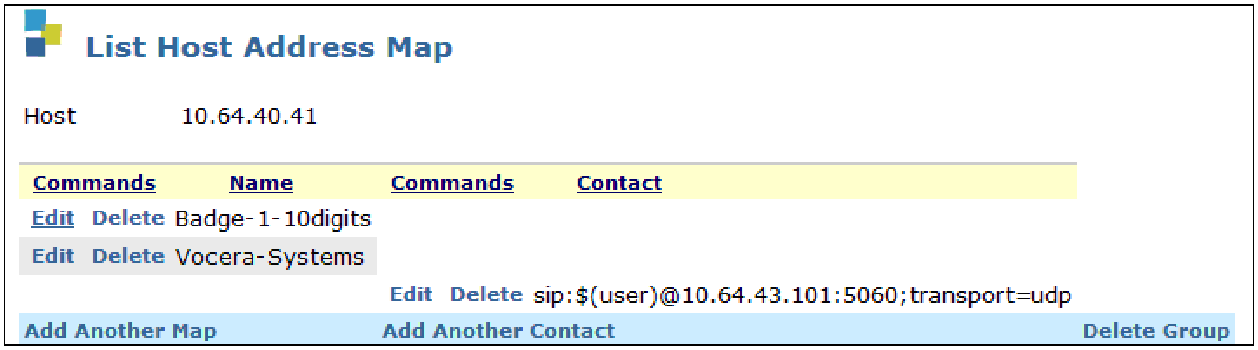
Click **Add**.



After adding the address map, the **List Host Address Map** screen will appear, as shown below. When the first **Host Address Map** is added, a **Contact** is created automatically. For the **Host Server Address Map** previously added, the following contact was created:

sip:$(user)@10.64.43.101:5060;transport=udp

This contact directs the calls to Vocera Communications System (Vocera SIP Telephony Gateway) via IP address (***10.64.43.101***) using port ***5060*** and ***UDP*** as the transport protocol. The incoming DID number sent in the user part of the original request URI is substituted for **$(user)** in the **Contact** expression.



6. Configure Vocera Communications System

This section will only describe the basic configuration to interface with Avaya Aura™ SIP Enablement Services. Configuration steps for Vocera Communication System, refer to [3]. The Vocera Communications System is configured using a web based console interface using appropriate credentials.

There are two ways that an inbound call can reach an individual badge.

- A caller calls the Guest Access or Direct Access Number. In this case, the user is greeted by the voice interface, and prompted for a badge user to contact.
- A user calls a Direct Inward Dialing (DID) number for a badge user. In this case, the call will be directly connected to the badge user without a greeting.

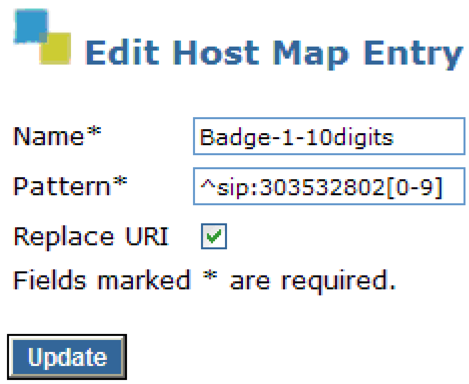
During the compliance test, 5 digit and 10 digit dialing plans were utilized. The first test was executed utilizing 5 digits. The second test utilized 10 digits. For 10 digit calling, the following modifications have to be implemented.

- Modification in Communication Manager (uniform-dialplan and aar analysis forms):

```
display uniform-dialplan 303                                        Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                                  Percent Full: 0

  Matching                          Insert                  Node
  Pattern           Len Del         Digits          Net Conv Num
 30353               10  0                          aar   n
```

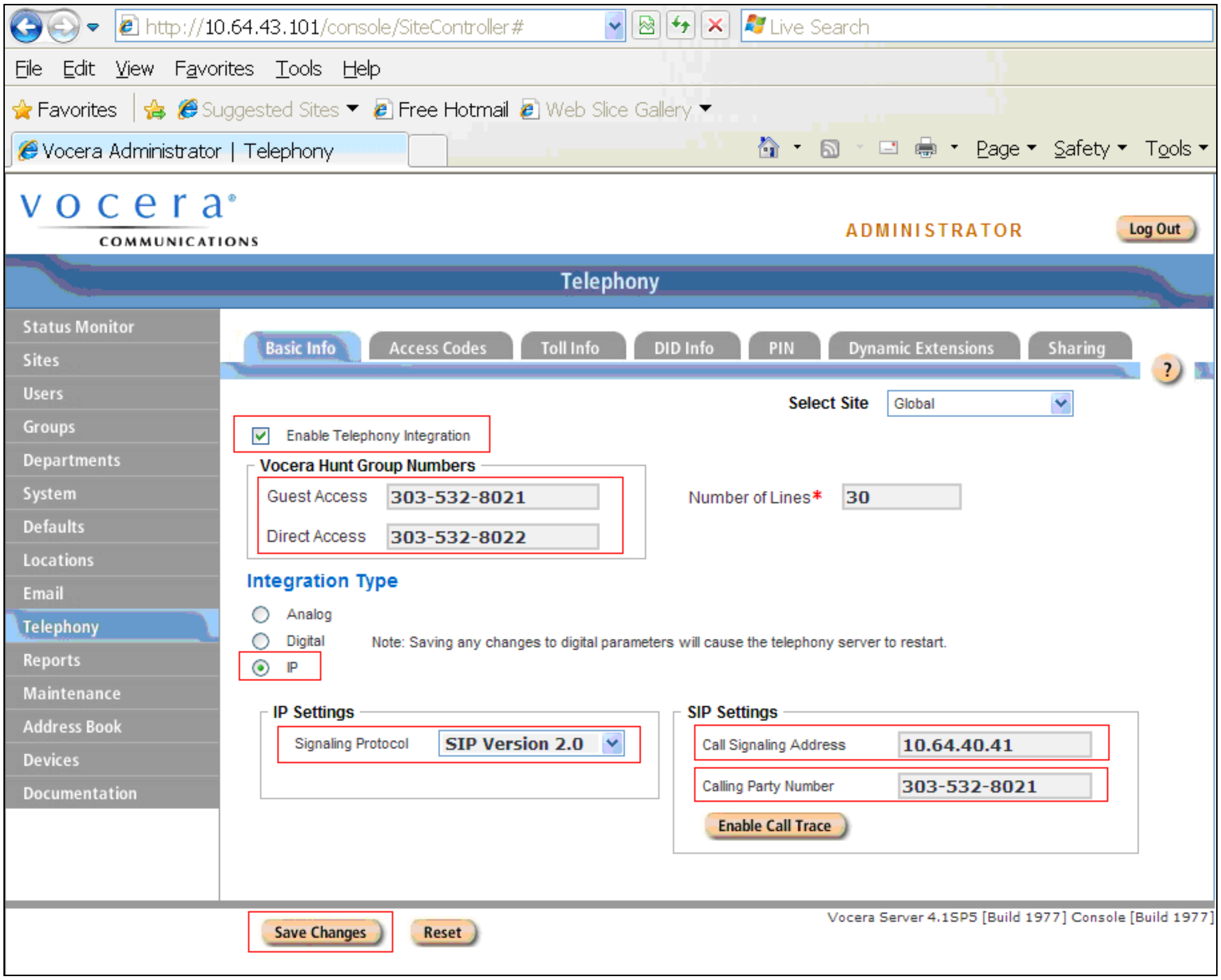
```
display aar analysis 303                                            Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all                Percent Full: 3

          Dialed                Total       Route     Call     Node    ANI
          String              Min   Max   Pattern     Type     Num     Reqd
    30353                      10    10     201       aar              n
```

- Modification in SIP Enablement Services to send 10 digit calls to Vocera.



Launch a web browser, enter **http://<IP address of Vocera Server>/console/AdminController** in the URL, and log in with the appropriate credentials. In the Administrator page, select the Basic Info tab and provide the following information:

- Check the Enable Telephony Integration check box.
- Enter the Guest access and Direct Access numbers. During the preparation phase of the compliance test, the following extensions were provided:
  - Guest Access Number – x28021
  - Direct Access Number – x28022
  - Three user extensions: x28023, x28024, x28025
- Set the Integration Type to **IP**.
- Using the drop-down menu, select **SIP Version 2.0** for Signaling Protocol field under the IP Settings section.
- Enter the SIP Enablement Services IP address for the Call Signaling Address field under the SIP Settings section. During the compliance test, IP address, **10.64.40.41**, was utilized
- Enter the Call Party extension Number. During the compliance test, Calling Party Number, **x28021**, was utilized.
- Click on the **Save Change**s button.



7. General Test Approach and Test Results

The general test approach was to place calls to and from the Vocera Communications System and exercise basic telephone operations. The main objectives were to verify that:

- Calls can be successfully established between Vocera Communications System and Avaya SIP and H.323 telephones.
- Calls were able to Hold /unHold.
- Vocera Communications System successfully negotiates the right codec (G.711MU, G.711A).
- Vocera Communications System successfully blind transfers a call.
- Vocera Communications System successfully consult transfers a call.
- Vocera Communications System successfully conferences three party calls.
- Successfully tested DTMF using the vector steps.

For serviceability testing, failures such as cable pulls and hardware resets were applied.

The test objectives were verified. For serviceability testing, the Vocera Communications System operated properly after recovering from failures such as cable disconnects, and resets of the Vocera Communications System and the Avaya Aura™ SIP Enablement Services.

8. Verification Steps

The following steps may be used to verify the configuration:

- Verify the SIP trace, using traceSES from Avaya Aura™ SIP Enablement Services.
- Place calls to and from the Vocera Communications System and verify that the calls are successfully established with two-way talk path.
- While calls are established, Enter **status trunk <t/r>** command, where **t** is the SIP trunk group configured in **Section 4.6**, and **r** is the trunk group member used for a call.

9. Conclusion

Vocera Communications System was compliance tested with Avaya Aura™ Communication Manager (Version 5.2.1) and Avaya Aura™ SIP Enablement Services (Version 5.2.1). Vocera Communications System (Vocera Server and SIP Telephony Gateway Version 4.1 SP5 – build 1977) functioned properly for features and serviceability. During compliance testing, Vocera Communications System successfully placed and received calls to and from SIP and non-SIP telephones, and executed other telephony features like transfer, conference and DTMF.

10. Additional References

The following Avaya product documentation can be found at http://support.avaya.com

[1] *Administering Avaya Aura™ Communication Manager* Release 6.0, Issue 6.0, June 2010, Document Number 03-300509.

[2] *SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers*, Issue 9, May 2009, Document Number 555-245-206.

The following document was provided by Vocera.

[3] *Vocera Communications System Quick Start Guide*, Document Version 1.2, October 2009.

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.