Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Allworx 6x System with Allworx IP phones to interoperate via a SIP Trunk with Avaya Aura® Session Manager 6.1 and Avaya Aura® Communication Manager 6.0.1 - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring Allworx 6x System and Allworx IP Phones to interoperate via a SIP Trunk with Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

The overall objective of the interoperability compliance testing is to verify Allworx's functionalities in an environment comprised of Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and various Avaya endpoints including SIP, H.323 and Digital.

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 for the Allworx 6x system with Allworx IP phones to interoperate via a SIP Trunk with Aura® Session Manager and Avaya Aura® Communication Manager.

Designed for companies with up to 60 users, the Allworx 6x system is an all-in-one communication system with IP phones. Key features of the 6x system include:

- Supports VoIP (SIP) trunks and six (6) traditional phone lines
- PBX and/or Key system features
- Built-in nine (9) unique Auto Attendants
- Fully supports every Allworx IP phone and two (2) traditional phone handsets
- Built-in 8 port voicemail with Unified Communication
- Presence management
- One (1) eight (8) seat conference bridge
- Automatic Call Distribution Option
- Advanced software feature support

2. General Test Approach and Test Results

The compliance testing focused on verifying the ability of the Allworx 6x system with Allworx IP phones to interoperate with an Avaya SIP-enabled IP Telephony Environment comprised of Session Manager, Communication Manager, and various Avaya phones including SIP, H.323 and Digital.

Avaya Aura® Messaging provided voicemail coverage for the Avaya subscribers and the Allworx 6x system provided voicemail coverage for the Allworx subscribers.

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

2.1. Interoperability Compliance Testing

The interoperability compliance test plan included feature and serviceability test cases. The feature testing focused on the following areas:

- Verify basic network connectivity
  - SIP Trunk using UDP between Allworx 6x and Avaya System Manager
  - Allworx IP Phone connectivity to POE Switch and Allworx 6x System
- Basic calls
  - Verify proper set up and tear down of the calls
  - Verify phones display information (e.g., Caller ID)
  - Verify voice paths/quality
- Audio codec negotiation using G.711 and G.729 codecs
- Direct IP-IP Audio Connections (media shuffling)
- DTMF transmission using RFC 2833
- Voicemail with message waiting indicators (MWI)
  - Verify Avaya Aura® Messaging sends appropriate MWI message and verify message lamp indicator for voicemail leave or retrieve messages for Avaya subscribers.
  - Verify message lamp indicator for voicemail leave or retrieve messages for Allworx subscribers on the Allworx 6x System.
- Voice Features
  - Call Transfer
  - Call Conference
  - Call Hold/Resume

Serviceability testing focused on verifying the ability of Allworx 6x system and Allworx IP phones to recover from adverse conditions such as network and server (e.g., Allworx 6x, Session Manager, and Communication Manager) outages.

2.2. Test Results

- The Allworx phones do not update display information for various call scenarios (e.g., call forwarding, transfers, and conferences). Instead of updating the display information to indicate the Allworx phone is now in a conference or connected to a new party (e.g., after the call has been forwarded or transferred), the Allworx phone continues to display the original connected party information.
- Bridging between Allworx phones and Avaya phones is not currently supported.
- For calls from Allworx phones to enterprise Avaya phones, leading digits (e.g., *8) had to be dialed first to indicate that the call would be an enterprise call and should be routed to Session Manager.
- Performing a call transfer, if the Allworx phone displays ‘announcing transfer’ and rings the other party the other end must answer before the Allworx phone can complete the transfer and hang up. If not, then no audio is observed when the other two parties are joined on the call.

2.3. Support

Technical support on the Allworx 6x system and Allworx IP phones can be obtained through the following:

- **Phone:** 1-866-ALLWORX, option 1, option 3
- **Web:** http://www.allworx.com/support/support_overview.aspx
- **Email:** support@allworx.com

3. Reference Configuration

As shown in **Figure 1**, a simulated enterprise site was configured consisting of the following:

- Avaya Aura® Session Manager (configured using Avaya Aura® System Manager)
- Avaya Aura® Communication Manager with an Avaya G430 Media Gateway
- Avaya Aura® Messaging (provided voicemail for Avaya subscribers). The provisioning of Aura® Messaging is beyond the scope of this document
- Avaya SIP and non-SIP phones (extensions 4*xxxx*)
- Allworx 6x system
- Allworx IP Phones (extensions 7*xxx*)

The Allworx 6x system's LAN interface was used to establish a SIP trunk to Session Manager. The Allworx IP Phones were connected via POE switch. Note, the Allworx IP Phones registered with the Allworx 6x system, not with Session Manager or Communication Manager.

The administration routing and basic connectivity between Communication Manager and Session Manager is not the focus of these Application Notes; however, some details are provided only for reference and completeness.

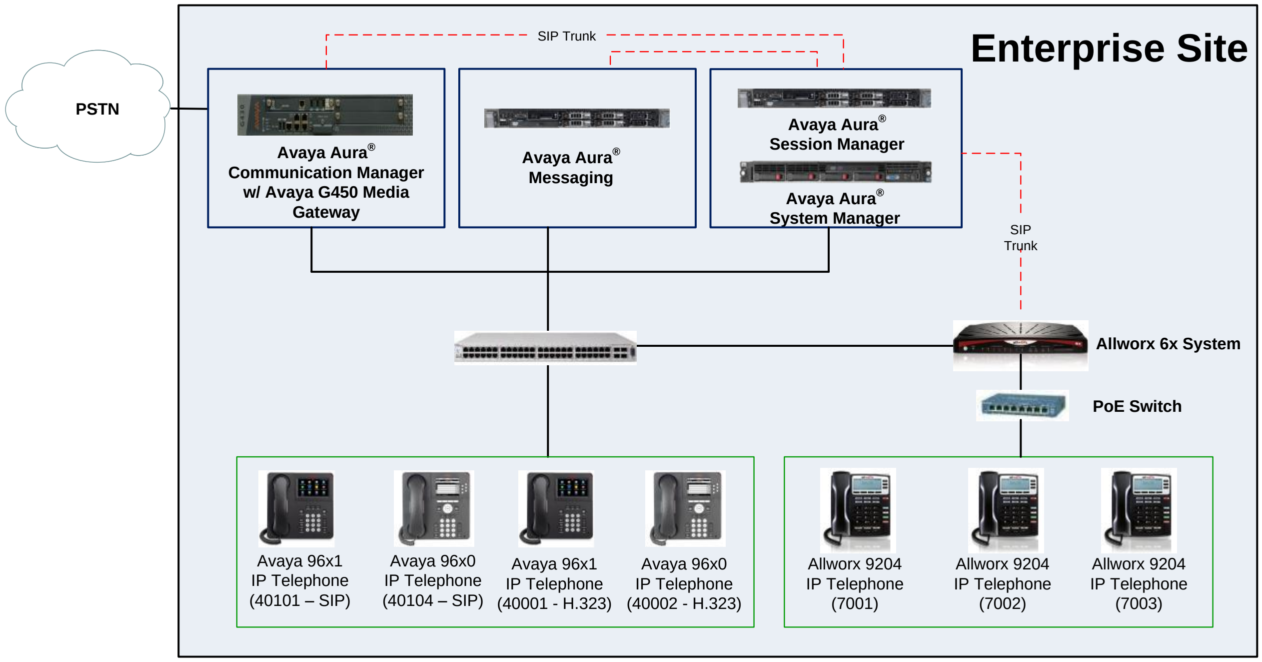


Figure 1: Allworx connecting to Avaya

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager - Avaya S8300 Server with an Avaya G430 Media Gateway	6.0.1 SP7
Avaya Aura® System Manager HP ProLiant DL360 G7 Server	6.1 SP8
Avaya Aura® Session Manager HP ProLiant DL360 G7 Server	6.1 SP7
Avaya Aura® Messaging	6.1 SP2
Avaya 96x0 Series IP Telephones (SIP) • 9650 Avaya 96x0 Series IP Telephones (H.323) • 9630	2.6 SP7 3.1 SP4
Avaya 96x1 Series IP Telephones (SIP) • 9611 • 9621 • 9641 Avaya 96x1 Series IP Telephones (H.323) • 9608 • 9641	6.0 SP4 6.2 SP1
Avaya 1416 Digital Phone	
Allworx 6x System	7.4.4.7
Allworx IP Phones • 9204	2.4.4.1

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- Verify Communication Manager License
- IP Codec Set
- IP Network Region
- IP Node Names
- SIP Signaling Group
- SIP Trunk Group
- Route Pattern
- Private Numbering
- AAR Analysis
- Configure Aura® Messaging Hunt Group and Coverage Path

5.1. Verify Avaya Aura® Communication Manager License

Use the **display system-parameters customer-options** command and on **Page 2,** verify that the **Maximum Administered SIP Trunks** value is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that **4000** licenses are available and **30** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity

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

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 4000  36
           Maximum Concurrently Registered IP Stations: 2400  2
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  0
                   Maximum Video Capable IP Softphones: 2400  0
                       Maximum Administered SIP Trunks: 4000  30
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
                             Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 50    0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0

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

5.2. IP Codec Set

This section describes the steps for administering an IP codec set in Communication Manager. This IP codec set is used in the IP network region **(Section 5.3)** for communications between Communication Manager and Session Manager. Use the **change ip-codec-set <c> command**, where **c** is a number between **1** and **7**, inclusive. Enter the audio codec types **G.711MU** and **G.729A** in the **Audio Codec** fields. Refer to Allworx documentation for details on how to configure matching codecs with the Allworx equipment.

```
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
 2: G.729A             n          2        20
 3:
 4:
 5:
 6:
 7:
```

5.3. IP Network Region

This section describes the steps for administering an IP network region in Communication Manager for communication between Communication Manager and Session Manager. Use 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**
- **Intra-region** and **Inter-region IP-IP Direct Audio** (media shuffling) – By default are set to **yes** if supported. This allows audio traffic to be sent directly between IP endpoints to reduce the use of media resources
- **Codec Set** – Enter the IP codec set number as provisioned in **Section 5.2**

```
change ip-network-region 1                                     Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: avaya.com
    Name: Compliance Testing
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: 3329
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                        RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

5.4. IP Node Names

This section describes the steps for setting the IP node name for Session Manager in Communication Manager. Use the **change node-names ip** command, and add a node name for Session Manager signaling. The node name for Session Manager is **sm_60_19** with IP Address **10.64.60.19**. Note: The **procr / 10.64.60.13** entries, which are the node name / IP address for the processor board. It will be used later to configure the SIP Trunk in Session Manager

```
change node-names ip                                           Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
default             0.0.0.0
msgserver           10.64.60.13
procr               10.64.60.13
procr6              ::
sm_60_19            10.64.60.19
```

5.5. SIP Signaling Group

This section describes the steps for administering a SIP signaling group for a new trunk that will be created for the connection between Communication Manager and Session Manager. Use the **add signaling-group <s>** command, where **s** is an available signaling group number. Enter the following values for the specified fields and the default values may be used for the remaining fields.

- **Group Type:** **sip**
- **IMS Enabled:** **n**
- **Transport Method:** **tls**
- **Peer Detection Enabled:** **y**
- **Peer Server:** **SM** (this field will be automatically populated)
- **Near-end Node Name:** Processor node name from **Section 5.4**
- **Near-end Listen Port:** **5061**
- **Far-end Node Name:** Session Manager node name from **Section 5.4**
- **Far-end Listen Port:** **5061**
- **Far-end Network Region**: The IP network region number from **Section 5.3**
- **DTMF over IP:** **rtp-payload**
- **Direct IP-IP Audio Connections:** **y**

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

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n                                                SIP Enabled LSP? n
     IP Video? n                                      Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                   Far-end Node Name: sm_60_19
 Near-end Listen Port: 5061                  Far-end Listen Port: 5061
                                          Far-end Network Region: 1

Far-end Domain:
                                             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? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

5.6. SIP Trunk Group

This section describes the steps for administering a trunk group in Communication Manager for communication between Communication Manager and Session Manager. This SIP trunk was used for SIP telephone and Aura® Messaging traffic.

Use the **add trunk-group <t>** command, where **t** is an available trunk group number.

- **Group Type**: **sip**
- **Group Name**: Enter a descriptive name (e.g., **sm_60_19**)
- **TAC**: Set to any available trunk access code that is valid in the provisioned dial plan (e.g., ***001**)
- **Service Type**: **tie**
- **Signaling Group**: **1** (Signaling group added in **Section 5.5**)
- **Number of Members**: **10** (Enter a desired value for trunk group members)
- **Numbering Format:** **unk-pvt** (page 3)

Note: The number of members determines how many simultaneous calls can be processed by the trunk through Session Manager.

```
add trunk-group 1                                                 Page   1 of  21
                                TRUNK GROUP

Group Number: 1                   Group Type: sip           CDR Reports: y
  Group Name: sm_60_19                   COR: 1        TN: 1        TAC: *001
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n
                                             Member Assignment Method: auto
                                                      Signaling Group: 1
                                                    Number of Members: 10
```

```
add trunk-group 1                                                 Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                        Maintenance Tests? y



                     Numbering Format: unk-pvt
                                               UUI Treatment: service-provider

                                                Replace Restricted Numbers? n
                                               Replace Unavailable Numbers? n


                                Modify Tandem Calling Number: no




 Show ANSWERED BY on Display? y
```

5.7. Route Pattern

Create a route pattern to use for the newly created SIP trunk group. Use the **change route-pattern <r>** command, where **r** is an available route pattern.

- **Pattern Name:** A descriptive name (e.g., **sm_60_19**)
- **Grp No:** The trunk group number from **Section 5.6** (e.g., **1**)
- Set the **FRL:** Enter a level that allows access to this trunk, with **0** being least restrictive

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: sm_60_19
                             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: 1    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 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                lev0-pvt  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
```

5.8. Private Numbering

Use the **change private-numbering 0** command, to define the calling party number to send to Session Manager. In the example shown below, all calls originating from a 5-digit extension beginning with 4 or a 5 will be routed over any trunk group, since the Trk Grp(s) field is blank; will result in a 5-digit calling number. The calling party number will be in the SIP “From” header.

```
change private-numbering 0                                      Page   1 of   2
                           NUMBERING - PRIVATE FORMAT

Ext Ext              Trk        Private          Total
Len Code             Grp(s)     Prefix           Len
 5  4                                            5     Total Administered: 2
 5  5                                            5        Maximum Entries: 540
```

5.9. Automatic Alternate Routing Analysis

This section provides a sample Automatic Alternate Routing (AAR) routing used for routing calls to Session Manager. (See **Section 6.8** for corresponding Session Manager configuration) Note that other methods of routing may be used.

AAR entries will need to be added for 7*xxx* to direct calls to the Allworx 6x System, 4*xxxx* for Avaya stations and 49990 is used for direct coverage calls to Aura® Messaging.

Use the **change aar analysis <n>** command where **n** is the dial string pattern to configure an entry for. Add an entry to specify how to route calls for 7*xxx, 4xxxx and 49990*. In the example shown below, calls with **Dialed String 7**, **Min 4** and **Max 4**, will be routed as an AAR call using **Route Pattern 1** from **Section 5.7**.

```
change aar analysis 7                                          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
    7                     4    4     1        aar          n
```

5.10. Provisioning for Coverage to Aura® Messaging

To provide coverage to Aura® Messaging for Avaya extensions, a hunt group is defined using the Aura® Messaging pilot number (e.g., 49990), as well as a coverage path that is defined to the various stations.

5.10.1. Configure Messaging Hunt Group and Coverage Path

Use the **add hunt-group <h>** command where **h** is an available hunt-group to be assigned, and on **Page 1** of the form enter the following:

- **Group Name** – Enter a descriptive name (e.g., Voicemail AAM)
- **Group Extension** – Enter an available extension (e.g., 49990)
- **ISDN/SIP Caller Display** – Enter **mbr-name**
- Let all other fields default

```
add hunt-group 98                                          Page   1 of  60
                                  HUNT GROUP

            Group Number: 98                           ACD? n
              Group Name: Voicemail AAM              Queue? n
         Group Extension: 49990                     Vector? n
              Group Type: ucd-mia             Coverage Path:
                      TN: 1          Night Service Destination:
                     COR: 1                 MM Early Answer? n
           Security Code:              Local Agent Preference? n
 ISDN/SIP Caller Display: mbr-name
```

Navigate to **Page 2** of the form and enter the following:

- **Message Center** – Enter **sip-adjunct**
- **Voice Mail Number** - Enter the Aura® Messaging pilot number (e.g.,**49990**)
- **Voice Mail Handle** - Enter the Aura® Messaging pilot number (e.g.,**49990**)
- **Routing Digits** - Are only necessary if the number used in the **Voice Mail Number** field require a Feature Access Code (FAC) to access the SIP trunk (e.g., ***8**)

```
add hunt-group 98                                                    Page   2 of  60
                                  HUNT GROUP





                      Message Center: sip-adjunct

     Voice Mail Number         Voice Mail Handle          Routing Digits
                                                   (e.g., AAR/ARS Access Code)
     49990                     49990                      *8
```

After the hunt group is provided, it is associated with a coverage path. Use the **add coverage path <n>** command where **n** is the coverage path to be assigned. Configure a coverage point, using value **hx** where **x** is the hunt group number created above.

- **Point1** – Specify the hunt group defined in the previous section (e.g., **h98**)
- **Number of Rings** – Enter the number of rings before the stations go to coverage (e.g., **2**)

```
add coverage path 98                                                     Page   1 of   1
                            COVERAGE PATH

                   Coverage Path Number: 99
     Cvg Enabled for VDN Route-To Party? n        Hunt after Coverage? n
                       Next Path Number:          Linkage

COVERAGE CRITERIA
    Station/Group Status    Inside Call     Outside Call
             Active?             n               n
               Busy?             y               y
       Don't Answer?             y               y        Number of Rings: 2
                All?             n               n
 DND/SAC/Goto Cover?             y               y
   Holiday Coverage?             n               n


COVERAGE POINTS
    Terminate to Coverage Pts. with Bridged Appearances? n
  Point1: h98             Rng:    Point2:
  Point3:                         Point4:
  Point5:                         Point6:
```

5.10.2. Station Coverage Path to Avaya Aura® Messaging

The coverage path configured in the previous section is then defined on the stations.

Enter the command **change station xxxxx**, where **xxxxx** is a previously defined station or agent extension (e.g., station 40101), and on **Page 1** of the form enter the following:

- **Coverage path** – Specify the coverage path defined on the previous page (e.g., **98**).

```
change station 40101                                          Page   1 of   5
                                     STATION

Extension: 40101                         Lock Messages? n             BCC: 0
     Type: 9641                          Security Code: 123456         TN: 1
     Port: S00005                      Coverage Path 1: 98            COR: 1
     Name: 40101, Station 9641G        Coverage Path 2:               COS: 1
                                       Hunt-to Station:
STATION OPTIONS
                                           Time of Day Lock Table:
              Loss Group: 19         Personalized Ringing Pattern: 1
                                                 Message Lamp Ext: 40101
            Speakerphone: 2-way                Mute Button Enabled? y
        Display Language: english                  Button Modules: 0
 Survivable GK Node Name:
          Survivable COR: internal               Media Complex Ext:
   Survivable Trunk Dest? y                           IP SoftPhone? n

                                                          IP Video? n
                              Short/Prefixed Registration Allowed: default

                                              Customizable Labels? y
```

Navigate to **Page 2** and set the **MWI Served User Type** to **sip-adjunct.**

```
change station 40101                                          Page   2 of   5
                                     STATION
FEATURE OPTIONS
           LWC Reception: spe           Auto Select Any Idle Appearance? n
          LWC Activation? y                      Coverage Msg Retrieval? y
  LWC Log External Calls? n                                 Auto Answer: none
             CDR Privacy? n                            Data Restriction? n
   Redirect Notification? y                  Idle Appearance Preference? n
 Per Button Ring Control? n                Bridged Idle Line Preference? n
   Bridged Call Alerting? n                    Restrict Last Appearance? y
  Active Station Ringing: single
                                                          EMU Login Allowed? n
        H.320 Conversion? n          Per Station CPN - Send Calling Number?
       Service Link Mode: as-needed                        EC500 State: enabled
         Multimedia Mode: enhanced               Audible Message Waiting? n
    MWI Served User Type: sip-adjunct         Display Client Redirection? n
                                             Select Last Used Appearance? n
                                               Coverage After Forwarding? s
                                                 Multimedia Early Answer? n
                                             Direct IP-IP Audio Connections? y
  Emergency Location Ext: 40101         Always Use? n IP Audio Hairpinning? N
```

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager to receive calls from and route calls to the SIP trunk between Communication Manager and Session Manager, and the SIP trunk between Session Manager and the Allworx 6x system. In addition, provisioning for calls to Aura® Messaging is described.

All provisioning for Session Manager is performed via the System Manager web interface. System Manager delivers a set of shared, secure management services and a common console across multiple products in the Avaya network, including the central administration of routing policies, and a common format for logs and alarms.

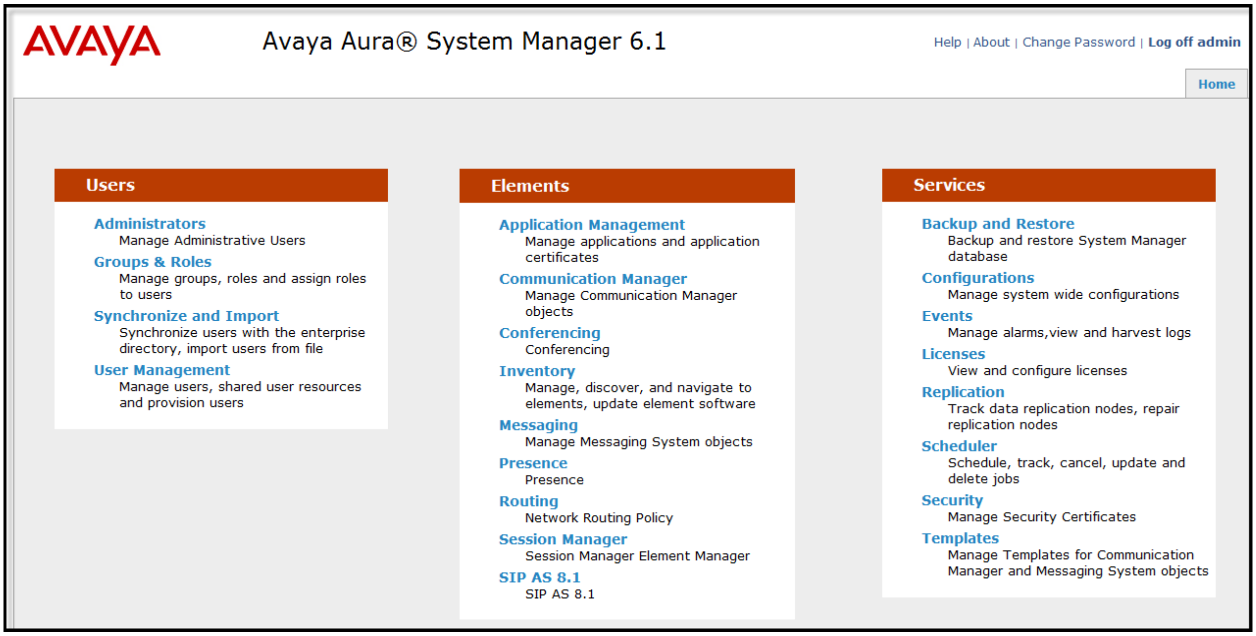
The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

The procedures described in this section include configurations for the following:

- **SIP Domains** - SIP Domains are the domains for which Session Manager is authoritative in routing SIP calls. In other words, for calls to such domains, Session Manager applies Network Routing Policies to route those calls to SIP Entities. For calls to other domains, Session Manager routes those calls to another SIP proxy (either a pre-defined default SIP proxy or one discovered through DNS)
- **Locations** – Logical/physical areas that may be occupied by SIP Entities
- **Adaptations** – Adaptations are used to apply any necessary protocol adaptations, to modify SIP headers, and apply any necessary digit conversions for the purpose of interworking with specific SIP Entities
- **SIP Entities** – Typically SIP Entities represent SIP network elements such as Session Manager instances, Communication Manager Systems, Session Border Controllers, SIP gateways, SIP trunks, and other SIP network devices.
- **Entity Links** – Connection information which define the SIP trunk parameters used by Session Manager when routing calls to/from other SIP Entities. (e.g., ports, protocol (UDP/TCP/TLS), and trust relationship)
- **Time Ranges** – Specified windows during which SIP call processing is permitted for a particular Routing Policies
- **Routing Policies** - Policies that determine which control call routing between the SIP Entities based on applicable Dial Patterns
- **Dial Patterns** – Matching digit patterns which govern to which SIP Entity a call is routed

Session Manager is managed via System Manager. Using a web browser, access ***https://<ip-addr of System Manager>/SMGR***.

Log in using appropriate credentials. The main page for the administrative interface is shown below.

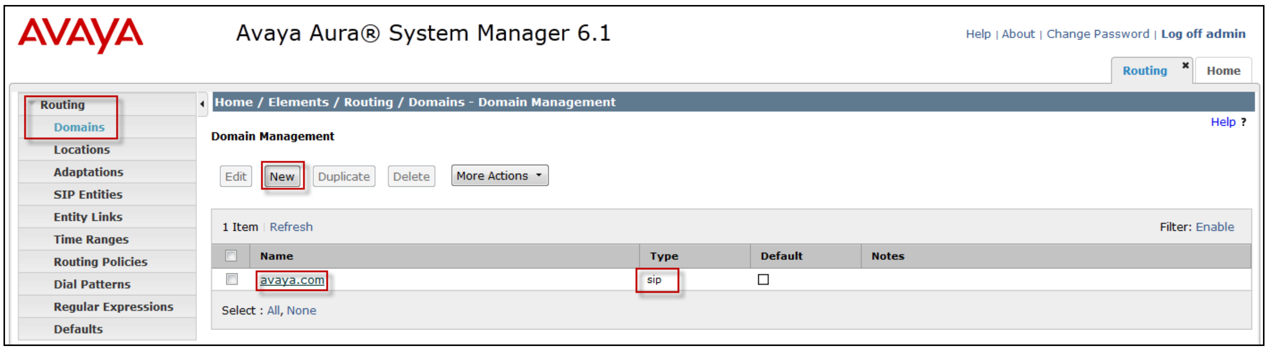


6.1. SIP Domains

In the reference configuration, one SIP domain was used; **avaya.com**.
Navigate to **Element** → **Routing** → **Domains** and click the **New** to add a new SIP domain with the following:

- Enter the SIP Domain (**avaya.com**) in the **Name** field
- **Type** : **sip**
- Enter a description in the **Notes** field if desired

Click on the **Commit** button.



6.2. Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside, by specifying the IP addressing for the locations as well as for purposes of bandwidth management if required.

Navigate to **Routing** → **Locations** and click the **New** button (not shown) to add the Location. Enter the following information:

Section **General:**

- Enter a descriptive Location name in the **Name** field (e.g., **.60 & .101 subnets**)
- Enter a description in the **Notes** field if desired

Section **Location Pattern** heading, click on **Add**

- Enter the IP address information for the Location (e.g., **10.64.60.*** & **10.64.101***)
- Enter a description in the **Notes** field if desired
- Repeat steps in the Location Pattern section if the Location has multiple IP segments.
- Modify the remaining values on the form, if necessary; otherwise, use all the default values

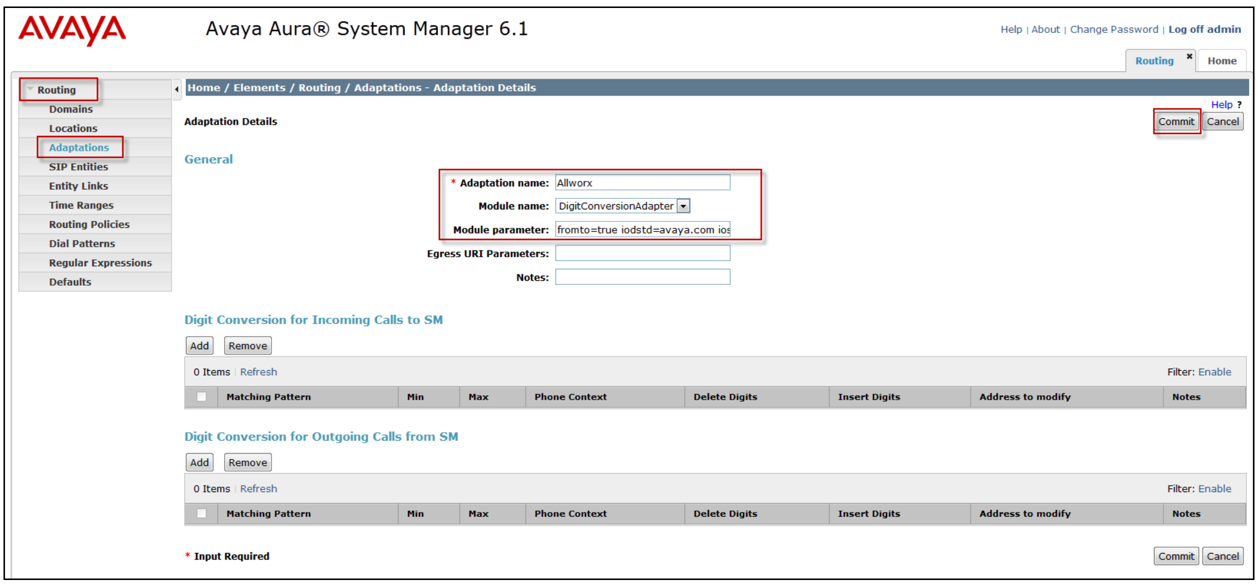
Click on the **Commit** button.

6.3. Add Allworx Adaptation

For calls from an Allworx IP Phone towards Communication Manager, an adaptation was created to change the domain in the From header from the Allworx 6x IP address to ***avaya.com***. To create an adaptation, navigate to **Routing** → **Adaptations** and click the **New** button (not shown). Enter the following information:

- **Adaptation name**: a descriptive name
- **Module name**: select from the drop-down menu or enter **DigitConversionAdapter**
- **Module parameter**: enter **fromto=true iodstd=avaya.com ioscrd=avaya.com**
- **Notes**: optional descriptive text

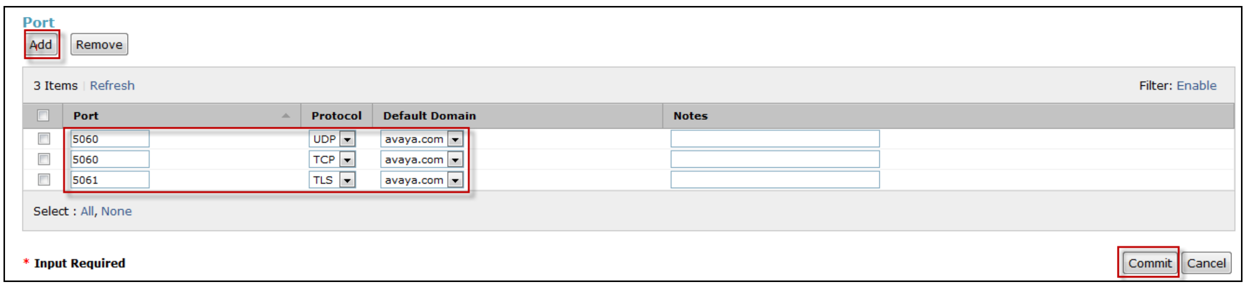
Click the **Commit** button.



6.4. SIP Entities

A SIP Entity must be added for the Session Manager and for each SIP-based telephony system supported by it using SIP trunks. In the sample configuration, a SIP Entity is added for Session Manager, Communication Manager, Aura® Messaging and the Allworx 6x system.

Note, the Session Manager SIP Entity is assumed to have already been configured. Navigate to **Routing→ SIP Entities**; check the checkbox for the Session Manager SIP Entity, and click the Edit button (not shown). Under the **Ports** section, verify the required Session Manager listening port for communication with Allworx is configured (e.g., **Port 5060** and **Protocol UDP**). If necessary, click the **Add** button to add the listening port and then click the **Commit** button when done to save the changes.



To add a SIP Entity, navigate to **Routing** → **SIP Entities** and click the **New** button (not shown).

The configuration details for the SIP Entity defined for the Communication Manager are below:

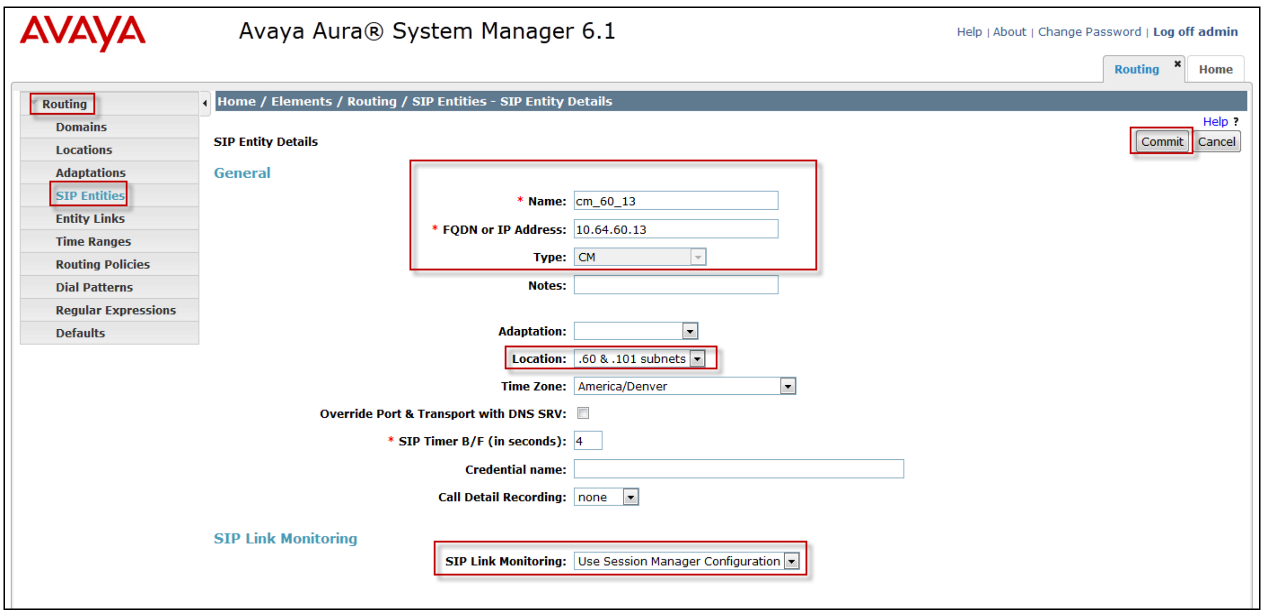
Section **General**:

- **Name**: Enter an descriptive name
- **FQDN or IP Address**: Enter the IP address of the SIP Entity (e.g., **10.64.60.13**)
- **Type:** Select best match for the SIP entity (e.g. ,**CM**)
- **Location :** Select the appropriate location (Configured in **Section 6.2**) from the drop down menu (e.g., **.60 & .101 subnets)**

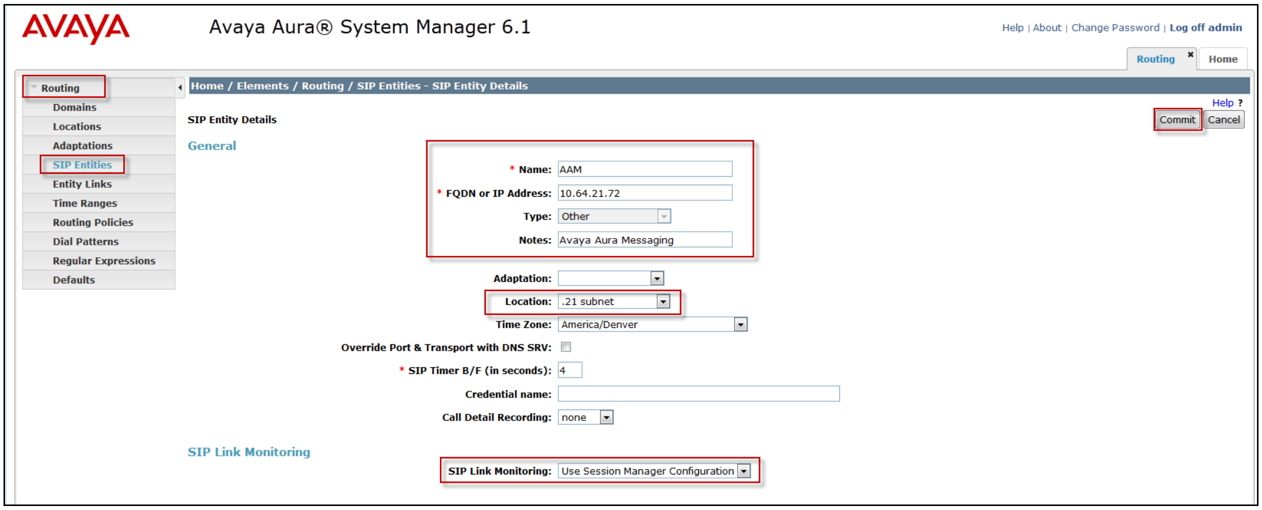
Section **SIP Link Monitoring**:

- Select desired option

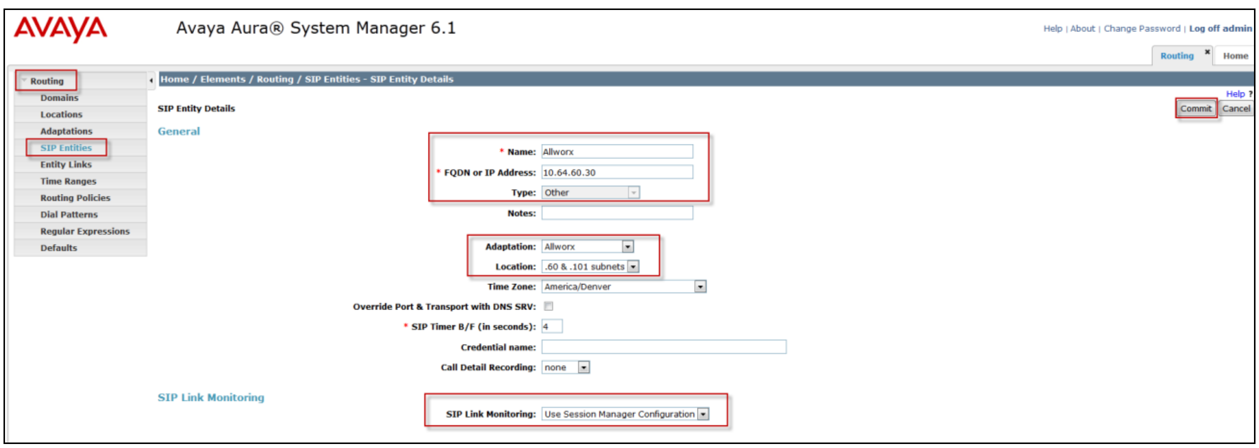
Default settings can be used for the remaining fields. Click **Commit** to save the SIP Entity definition.



The following two screens show the addition of the Aura® Messaging and the Allworx 6x SIP Entity. Note the selection of **Other** for the **Type**.



Note the selection of **Allworx** for the **Adaptation** (**Section 6.3**).



6.5. Entity Links

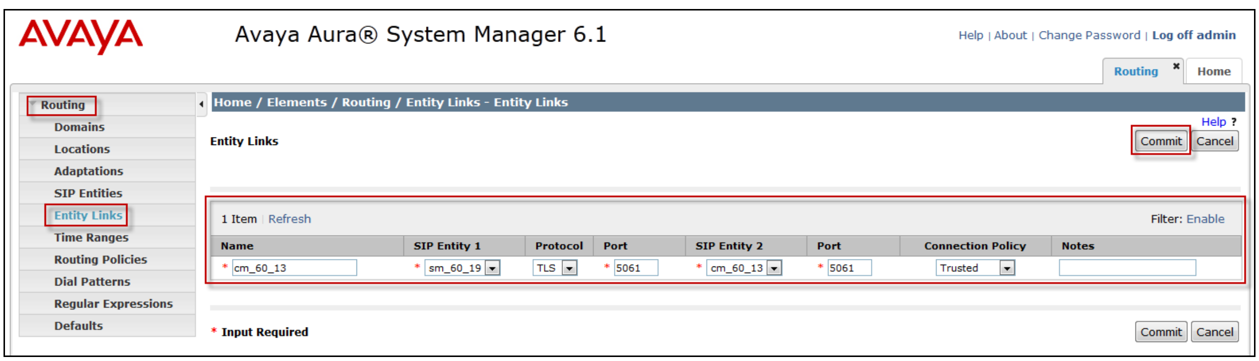
A SIP trunk between Session Manager and a telephony system is described by an Entity link. Three Entity Links were created:

- Session Manager <-> Communication Manger
- Session Manager <-> Aura® Messaging
- Session Manager <-> Allworx 6x

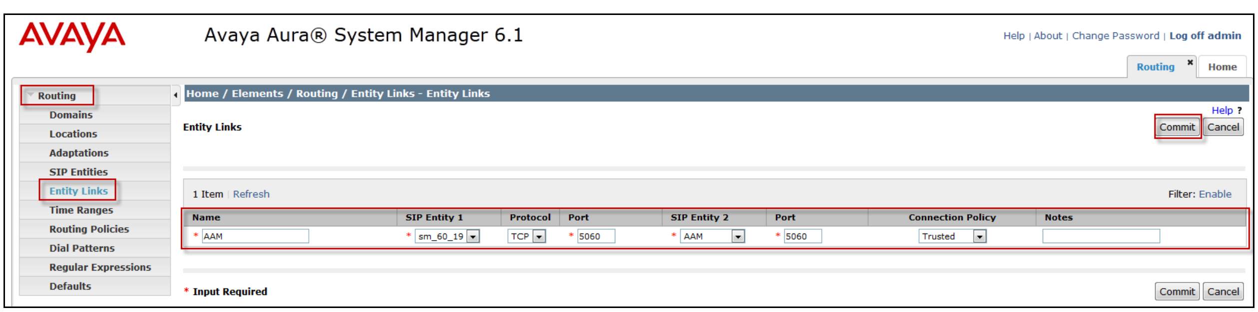
Navigate to **Routing** → **Entity Links**, and click the **New** button (not shown) to add a new Entity Link. The screen below shows the configuration details for the Entity Link connecting Session Manager with Communication Manager.

- **Name**: a descriptive name
- **SIP Entity 1**: select the Session Manager SIP Entity
- **Protocol**: select **TLS** as the transport protocol
- **Port: 5061**. This is the port number to which the other system sends SIP requests
- **SIP Entity 2**: select the Communication Manager SIP Entity
- **Port: 5061**. This is the port number on which the other system receives SIP requests
- **Connection Policy**: select **Trusted**
- **Notes**: optional descriptive text

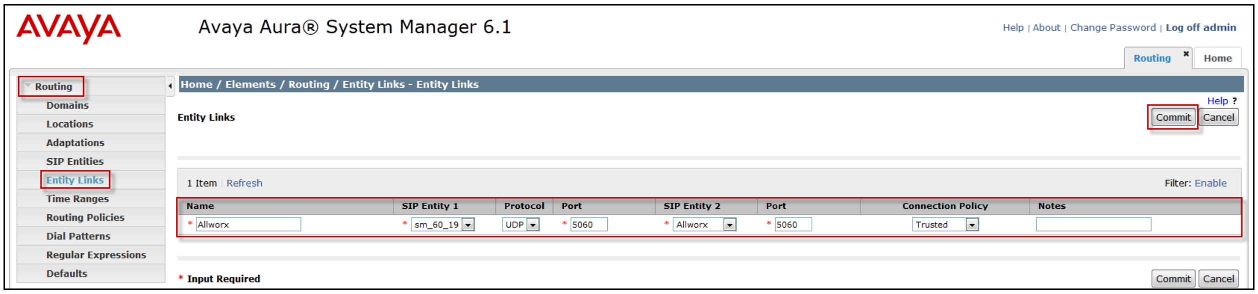
Click **Commit** to save the configuration



The Entity Link for connecting Session Manager with Aura® Messaging was similarly defined as shown in the screen below. Note the use of **TCP** and port **5060**.



The Entity Link for connecting Session Manager with Allworx 6X was similarly defined as shown in the screen below. Note the use of **UDP** and port **5060**.



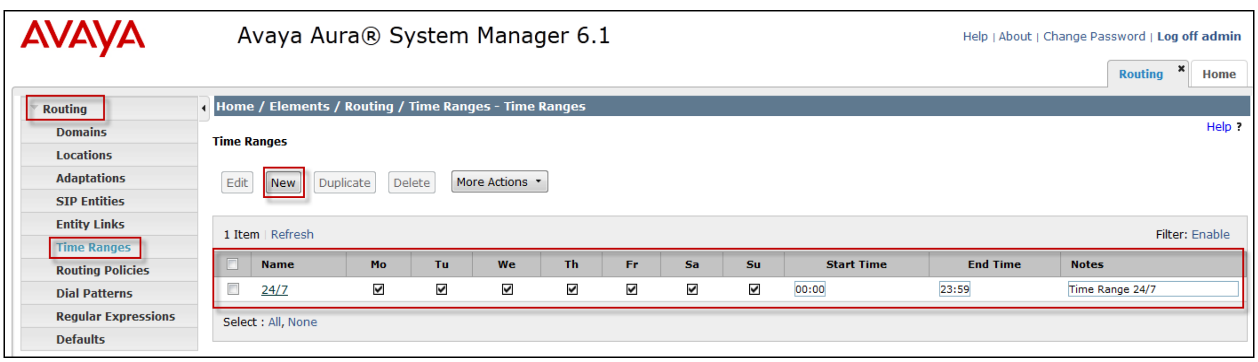
6.6. Time Ranges

The **Time Ranges** form allows admission control criteria to be specified for **Routing Policies** (**Section 6.7**). In the reference configuration, no restrictions were used.

To add a **Time Range**, navigate to **Routing** → **Time Ranges** and click the **New** button to add a new Time Range. Enter the following information:

- **Name:** Enter an descriptive name
- **Mo** through **Su**: check the box under each of these headings
- **Start Time:** enter **00:00**
- **End Time:** enter **23:59**
- **Notes:** Enter a description if desired

Click the **Commit** button. The following screen shows the Time Range page used during the compliance test.



6.7. Routing Policies

Routing Policies associate destination SIP Entities (**Section 6.4**) with Time of Day admission control parameters (**Section 6.6**) and Dial Patterns (**Section 6.8**). In the reference configuration, Routing Policies are defined for:

- Inbound calls to Communication Manager
- Outbound calls to the Allworx 6x System
- Call coverage to Aura® Messaging

To add a Routing Policy, navigate to **Routing → Routing Policies**, and click on the **New** button (not shown) on the right. Provide the following information:

Section **General:**

- **Name**: Enter an descriptive name
- **Notes**: Add a brief description (optional)

Section **SIP Entity as Destination:**

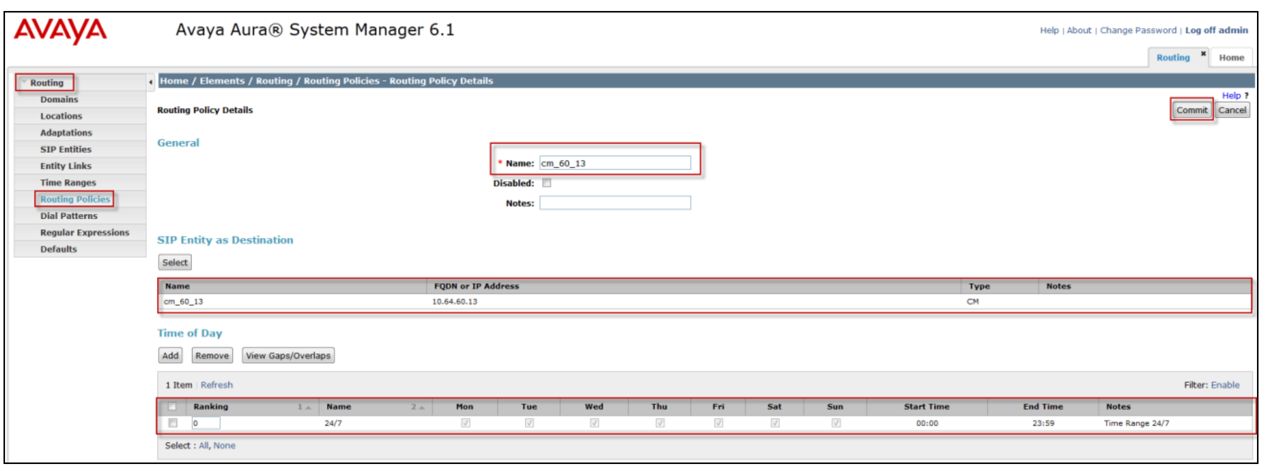
- Click **Select**, and then select the appropriate SIP Entity to which this routing policy applies

Section **Time of Day:**

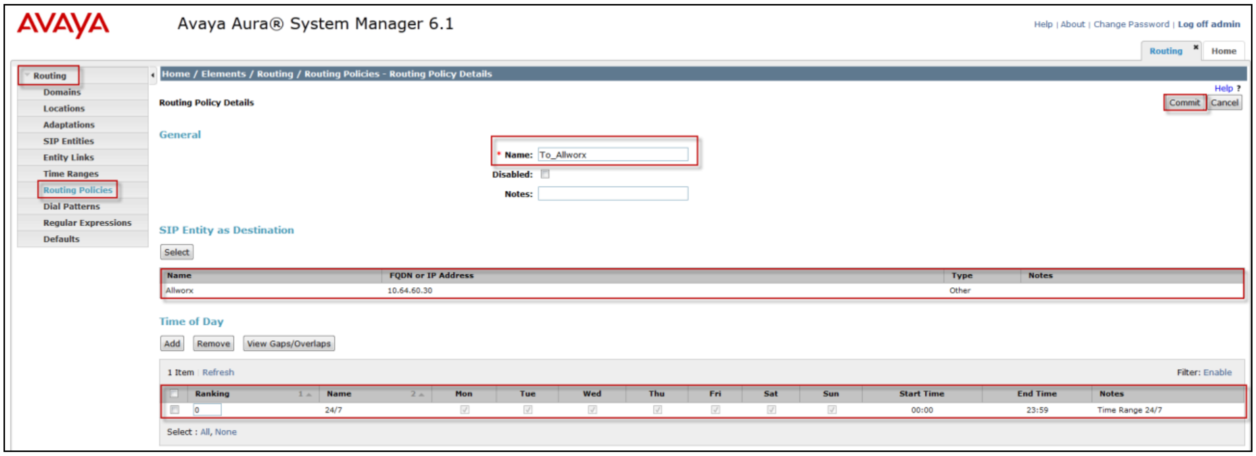
- Click **Add**, and select the time range configured from **Section 6.6**

Defaults can be used for the remaining fields. Click **Commit** to save each **Routing Policy** definition.

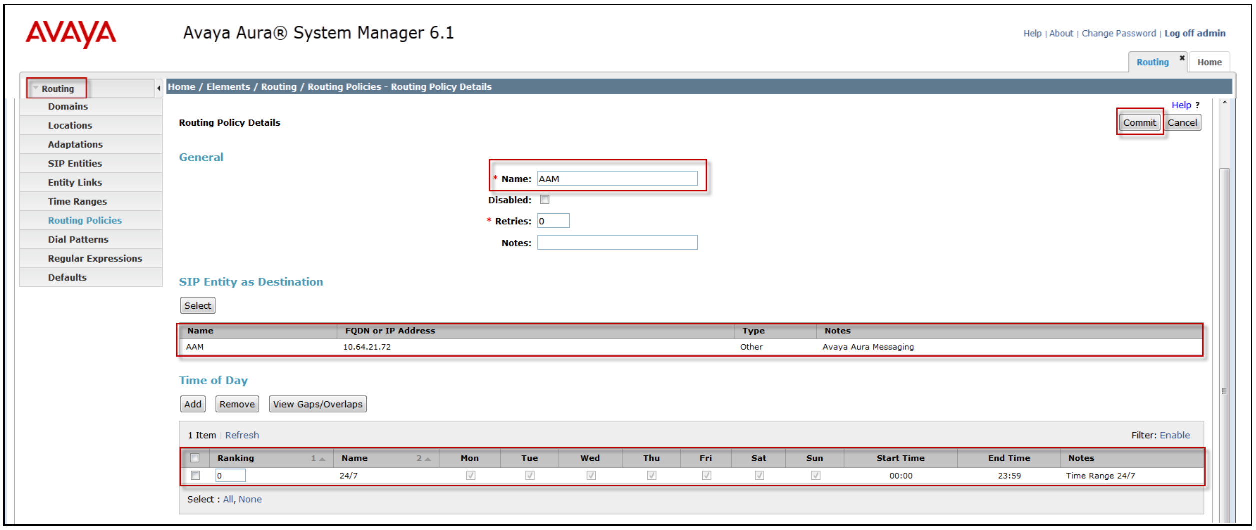
The following screen shows the Routing Policy for Communication Manager.



The following screen shows the Routing Policy for routing calls to the Allworx 6x system.



The following screen shows the routing policy used for Call Coverage to Aura® Messaging



6.8. Dial Patterns

Session Manager uses dial pattern to route calls to appropriate SIP Entity for processing. A dial pattern specifies which routing policy or routing policies are used to route a call based on the digits dialed by a user which match that pattern.

Navigate to **Routing →Dial Patterns**, and click the **New** button (not shown) to add a new Dial Pattern.

Section **General**:

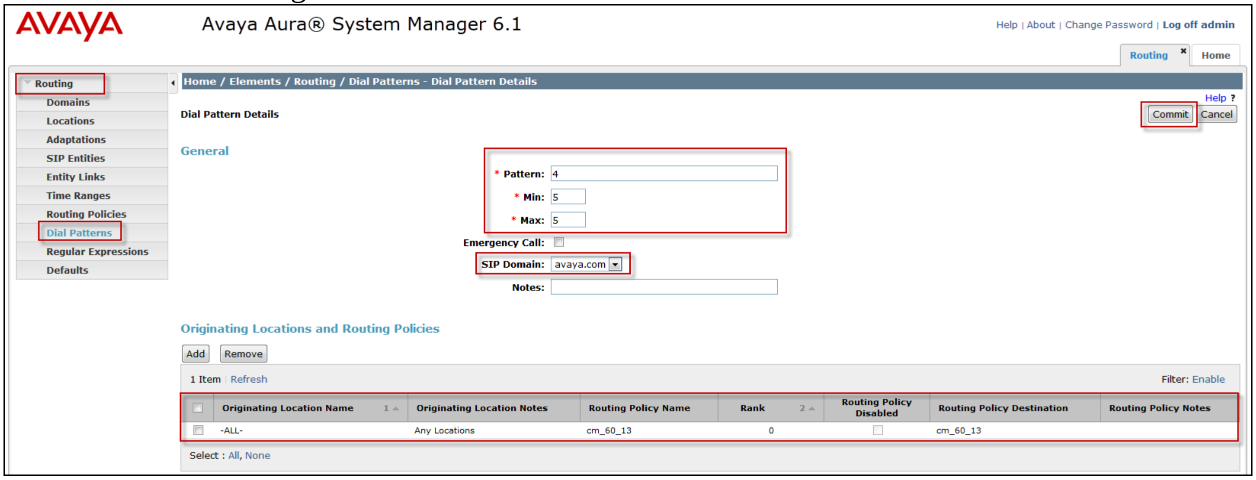
- **Pattern**: dialed number or prefix
- **Min**: minimum length of dialed number
- **Max**: maximum length of dialed number
- **SIP Domain**: select the SIP Domain created in **Section 6.1** (or select **–ALL,**to be less restrictive)
- **Notes**: optional descriptive text

Section **Originating Locations and Routing Policies**

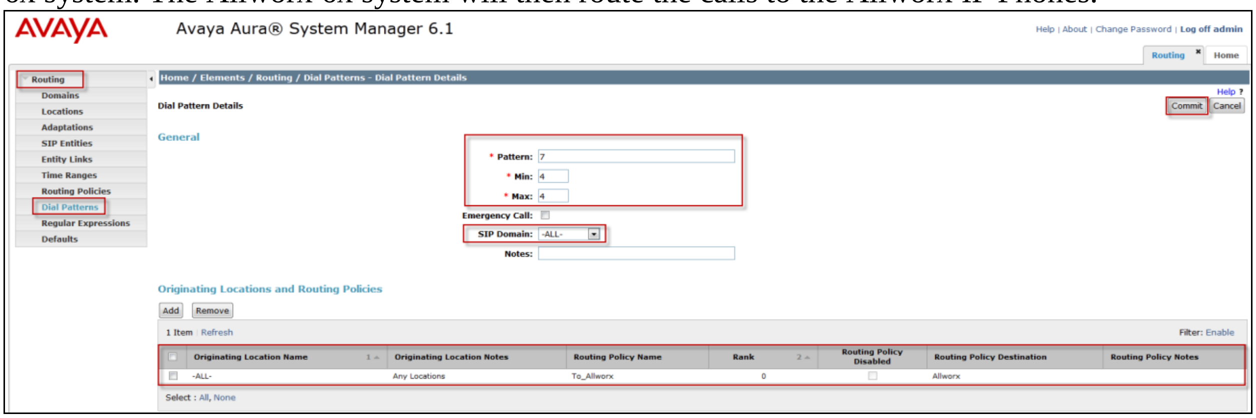
Click **Add** to select the appropriate originating Location and Routing Policy from the list (not shown).

Default settings can be used for the remaining fields. Click **Commit** to save the configuration.

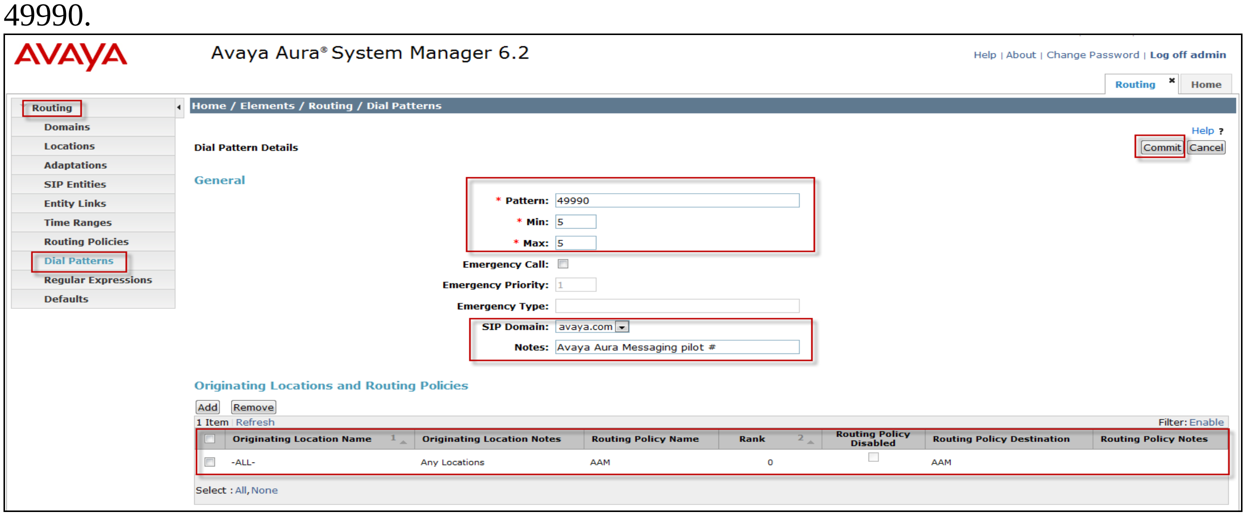
The following is an example of routing to route calls that match the pattern ***4xxxx*** to Communication Manager.



The following is an example of routing to route calls that match the pattern ***7xxx*** to the Allworx 6x system. The Allworx 6x system will then route the calls to the Allworx IP Phones.



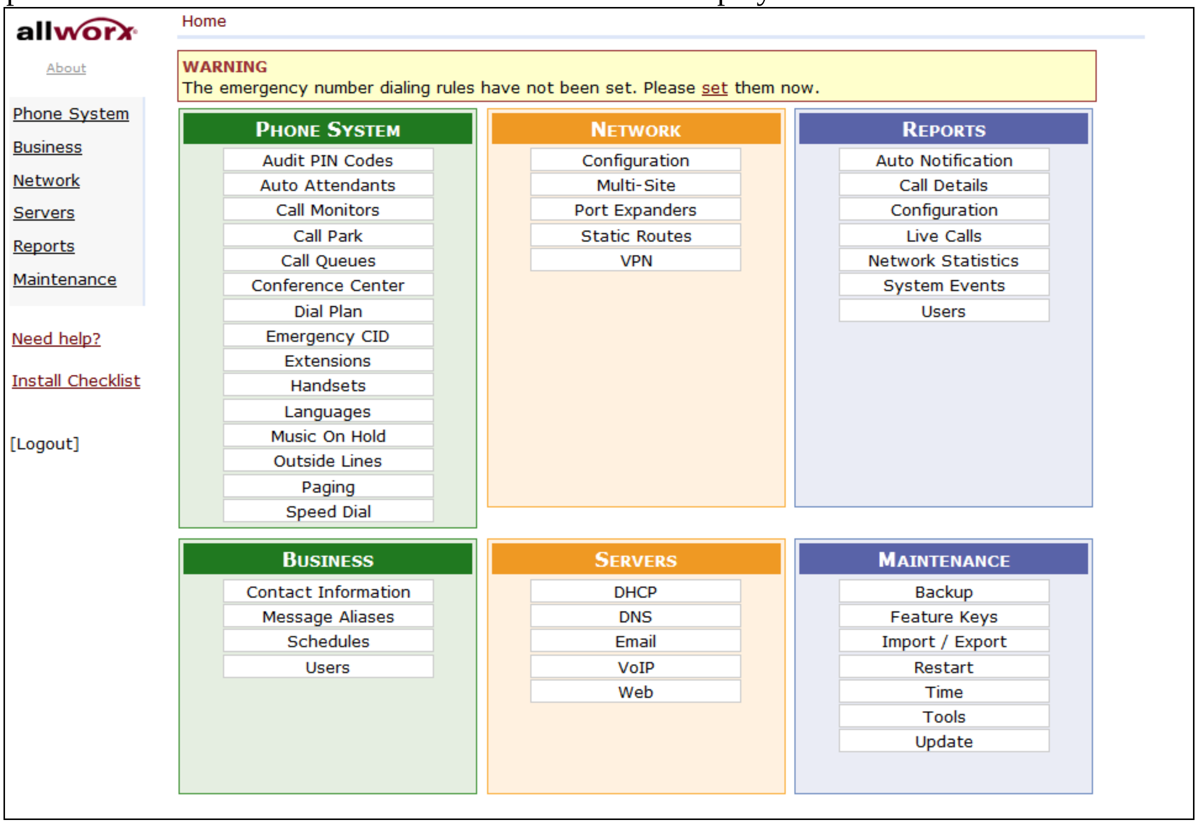
The following screen is examples of routing calls to Aura® Messaging via the pilot number 49990.



7. Configure Allworx 6x System and Allworx IP Phones

Allworx 6x System was configured by Allworx but not provided. Please contact Allworx for configuring the Allworx 6x system and Allworx IP Phones as shown in the reference configuration (**Section 3**).

A picture of the Allworx 6x administrative interface is displayed below.



8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager, Session Manager, Allworx 6x System and Allworx IP Phones.

8.1. Verify Avaya Aura ® Communication Manager

On Communication Manager, verify the status of the SIP signaling group by using the **status signaling-group <s>** command, where **s** is the signaling group number administered in **Section 5.5**. Verify that the signaling group is **in-service** as indicated in the Group State field shown below.

```
status signaling-group 1
                         STATUS SIGNALING GROUP

        Group ID: 1
      Group Type: sip

     Group State: in-service
```

Verify the status of the local SIP trunk group by using the **status trunk <t>** command, where **t** is the trunk group number administered in **Section 5.6**. Verify **Service State** displays all trunks are in the **in-service/idle** state as shown below.

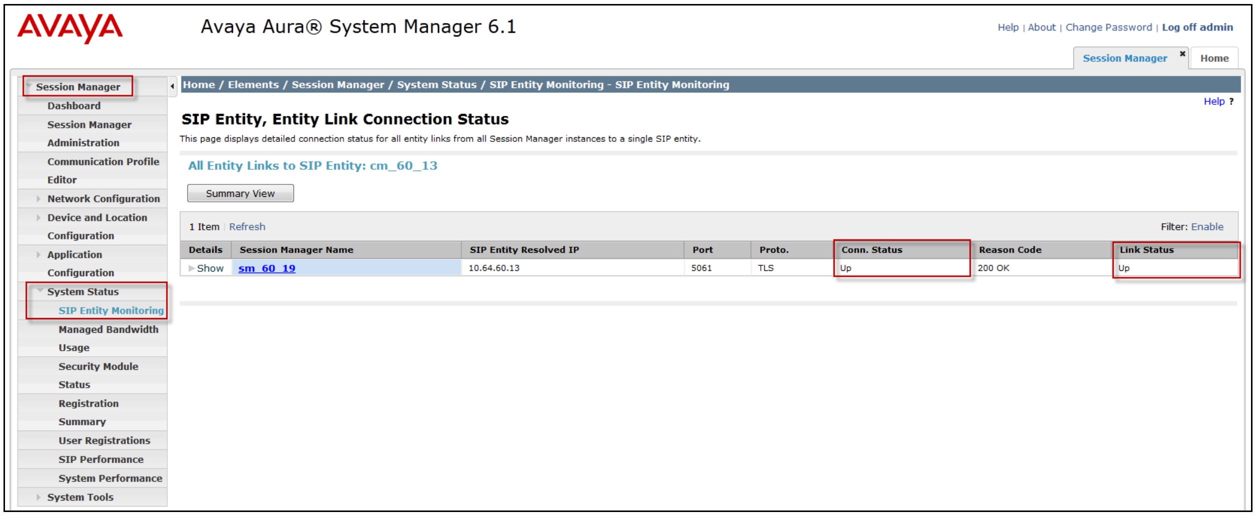
```
status trunk 1

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0001/001 T00001   in-service/idle    no
0001/002 T00002   in-service/idle    no
0001/003 T00003   in-service/idle    no
0001/004 T00004   in-service/idle    no
0001/005 T00005   in-service/idle    no
0001/006 T00006   in-service/idle    no
0001/007 T00007   in-service/idle    no
0001/008 T00008   in-service/idle    no
0001/009 T00009   in-service/idle    no
0001/010 T00010   in-service/idle    no
```

While calls are established, **Enter status trunk <t/r>** command, where **t** is the SIP trunk group configured in **Section 5.6**, and **r** is the trunk group member used for a call. Verify **Service State** is **in-service/active.**

```
status trunk 0001/001                                            Page   1 of   3
                              TRUNK STATUS

 Trunk Group/Member: 0001/001             Service State: in-service/active
              Port: T00001             Maintenance Busy? no
 Signaling Group ID: 1

   IGAR Connection? no

    Connected Ports: T00003
```

8.2. Verify Avaya Aura® Session Manager

Navigate to **Home** → **Elements** → **Session Manager** → **System Status** → **SIP Entity Monitoring** and select the Communication Manager SIP Entity (not shown). Verify the **Conn. Status** and **Link Status** are **Up.**



Repeat the procedure above selecting the Allworx SIP Entity, and verify the **Conn. Status** and **Link Status** are **Up.**

8.3. Verify Allworx 6x System and Allworx IP Phones

Make the following calls and verify the calls are set up properly, there is two-way audio with good audio quality, and the calls are torn down properly after completing the calls.

- Place a call from an Allworx IP Phone to an enterprise Avaya phone
- Place a call from an enterprise Avaya phone to an Allworx IP phone
- Place a call from an Allworx IP Phone to the PSTN
- Verify message lamp indicator for voicemail leave or retrieve messages for Allworx subscribers on the Allworx 6x System

9. Conclusion

These Application Notes describe the configuration steps required for the Allworx 6x system with Allworx IP phones to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager via a SIP trunk.   All feature and serviceability test cases were completed and passed with the exceptions/observations noted in **Section 2.2**.

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) *Administering Avaya Aura® Session Manager, Document 03-603324, Issue 1.1, Release 6.1, November 2010*

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 Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com