Avaya Solution & Interoperability Test Lab

Application Notes for Configuring TeleMatrix 3300IP, 3302IP, 9600IP and 9602IP SIP Telephones with Avaya Aura® Session Manager 6.0 and Avaya Aura® Communication Manager 6.0 - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the TeleMatrix 3300IP, 3302IP, 9600IP and 9602IP SIP Telephones to interoperate with Avaya Aura® Session Manager 6.0 and Avaya Aura® Communication Manager 6.0.

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.

Table of Contents

1. Introduction

These Application Notes describe the steps required to configure TeleMatrix 3300IP, 3302IP, 9600IP and 9602IP SIP Telephones to interoperate with a SIP infrastructure consisting of Avaya Aura® Session Manager 6.0 and Avaya Aura® Communication Manager 6.0. Also described is how Communication Manager features can be made available, in addition to the standard features supported in the TeleMatrix telephones. In this configuration, the Outbound Proxy SIP (OPS) feature set is extended from Communication Manager to the TeleMatrix telephones, providing them with enhanced calling features.

2. General Test Approach and Test Results

To verify interoperability of TeleMatrix 3300IP, 3302IP, 9600IP and 9602IP SIP Telephones with Session Manager and Communication Manager, calls were made between TeleMatrix telephones and Avaya SIP, H.323 and Digital telephones using various codec settings and exercising common PBX features. The telephony features were activated and deactivated using speed-dial buttons. TeleMatrix telephones passed all compliance testing with all scenarios resulting in the expected outcome.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Successful registration of TeleMatrix telephones with Session Manager.
- Calls between TeleMatrix telephones and Avaya SIP, H.323, and digital telephones.
- G.711 and G729 codec support.
- PBX features including Multiple Call Appearances, Hold, Transfer, and Conference.
- Proper system recovery after a TeleMatrix telephone restart and loss of IP connection.
- Correct recovery of TeleMatrix telephones during Session Manager and Communication Manager simulated network failures.
- Failover testing using Alternate and Simultaneous Registration to both Session Managers.

2.2. Test Results

During testing, TeleMatrix telephones completed all scenarios with results in all cases as expected.

2.3. Support

Technical support from TeleMatrix can be obtained through the following:

- Phone: +1 719 638 8821
- E-mail: info@telematrix.net
- Web: http://www.telematrix.net/

3. Reference Configuration

The diagram illustrates an enterprise site with an Avaya SIP-based network, including a pair of Session Managers, an S8800 Server running Communication Manager with a G650 Media Gateway, and Avaya SIP, H.323 and Digital endpoints. The enterprise site also contains four TeleMatrix SIP Telephones (3300IP, 3302IP, 9600IP and 9602IP) used in the compliance testing. The TeleMatrix telephones are registered with the primary Session Manager and are configured as endpoint users.

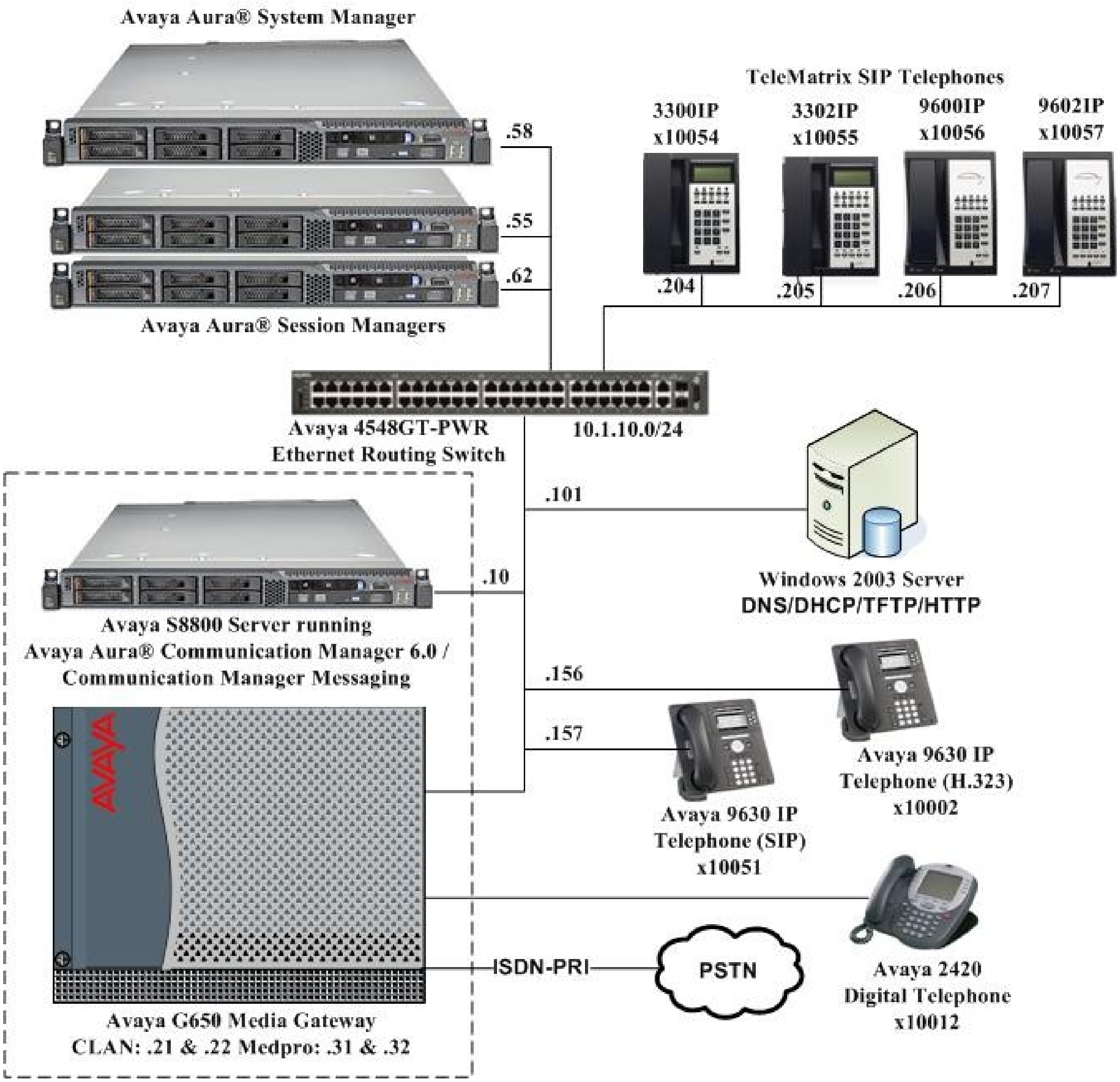


Figure 1: TeleMatrix Telephones with Avaya SIP Solution

4. Equipment and Software Validated

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

Equipment	Software
Avaya S8800 Server with G650 Media Gateway	Avaya Aura® Communication Manager 6.0 (R016x.00.0.345.0, Service Pack 2) / Avaya Aura® Communication Manager Messaging 6.0
Avaya S8800 Servers	Avaya Aura® Session Manager 6.0 Service Pack 2
Avaya S8800 Server	Avaya Aura® System Manager 6.0 Service Pack 2
Avaya 9600 Series IP Telephones	2.6.4.0 (SIP) 3.11 (H.323)
Avaya 2420 Digital Telephone	-
Avaya 4548GT-PWR Ethernet Routing Switch	V5.4.0.008
TeleMatrix 3300IP (single-line)	SC2 V1.8.4-835
TeleMatrix 3302IP (two-line)	SC2 V1.8.4-835
TeleMatrix 9600IP (single-line)	SD1 V1.8.3-782
TeleMatrix 9602IP (two-line)	SD2 V1.8.3-782

5. Configure Avaya Aura® Communication Manager

This section describes the steps for configuring the TeleMatrix telephones as an Outbound Proxy SIP (OPS) station and configuring a SIP trunk between Communication Manager and Session Manager. Use the System Access Terminal (SAT) to configure Communication Manager. Log in using the appropriate credentials.

5.1. Verify System Capacity

Use the **display system-parameters customer-options** command to determine the features activated. On **Page 1**, verify that the **Maximum Off-PBX Telephones** allowed in the system is sufficient. One OPS station is required per TeleMatrix telephone. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative.

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

     G3 Version: V16                             Software Package: Enterprise
       Location: 2                                System ID (SID): 1
       Platform: 28                               Module ID (MID): 1

                                                                USED
                                Platform Maximum Ports: 65000 281
                                      Maximum Stations: 1000  167
                              Maximum XMOBILE Stations: 41000 0
                    Maximum Off-PBX Telephones - EC500: 1000  0
                    Maximum Off-PBX Telephones -   OPS: 1000  15
                    Maximum Off-PBX Telephones - PBFMC: 1000  0
                    Maximum Off-PBX Telephones - PVFMC: 1000  0
                    Maximum Off-PBX Telephones - SCCAN: 0     0
                         Maximum Survivable Processors: 10    1
```

On **Page 2**, verify that the number of **Maximum Administered SIP Trunks** supported by the system is sufficient.

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

IP PORT CAPACITIES                                                      USED
                     Maximum Administered H.323 Trunks: 12000 30
           Maximum Concurrently Registered IP Stations: 18000 15
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 18000 0
                   Maximum Video Capable IP Softphones: 1000  5
                       Maximum Administered SIP Trunks: 24000 40
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   1
                     Maximum Media Gateway VAL Sources: 250   0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   1
   Maximum Number of Expanded Meet-me Conference Ports: 300   0
```

5.2. Define the Dial Plan

Use the **change dialplan analysis** command to define the dial plan used in the system. This includes all telephone extensions, OPS Feature Name Extensions (FNEs), and Feature Access Codes (FACs). A Feature Access Code (FAC) must also be specified for the corresponding FNE feature. In the sample configuration, telephone extensions are five digits long and begin with "1", FNEs are also five digits beginning with "1", and the FACs have formats as indicated with a **Call Type** of "fac".

```
change dialplan analysis                                          Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all           Percent Full: 1

    Dialed   Total  Call      Dialed   Total  Call      Dialed   Total  Call
    String   Length Type      String   Length Type      String   Length Type
   0           1   attd
   1           5   ext
   8           1   fac
   9           1   fac
   *           3   fac
   #           3   dac
```

5.3. Define Feature Access Codes (FACs)

A FAC (feature access code) should be defined for each feature that will be used via the OPS FNEs. Use **change feature-access-codes** to define the required access codes. The FACs used in the sample configuration are shown in bold.

```
change feature-access-codes                                       Page   1 of   9
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code: *00
         Abbreviated Dialing List2 Access Code: *01
         Abbreviated Dialing List3 Access Code: *02
Abbreviated Dial - Prgm Group List Access Code: *03
                      Announcement Access Code: *04
                       Answer Back Access Code: *05

      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *06    Deactivation: *07
Call Forwarding Activation Busy/DA: *08    All: *09    Deactivation: *10
   Call Forwarding Enhanced Status: *11    Act: *12    Deactivation: *13
                         Call Park Access Code: *14
                       Call Pickup Access Code: *15
CAS Remote Hold/Answer Hold-Unhold Access Code:
                   CDR Account Code Access Code: *16
                         Change COR Access Code:
                    Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code:
```

```
change feature-access-codes                                     Page   2 of   9
                              FEATURE ACCESS CODE (FAC)
                  Contact Closure  Pulse Code:

                 Data Origination Access Code:
                     Data Privacy Access Code: *27
             Directed Call Pickup Access Code: *17
       Directed Group Call Pickup  Access Code: *18
     Emergency Access to Attendant Access Code:
        EC500 Self-Administration Access Codes: *19
                    Enhanced EC500 Activation: *20    Deactivation: *21
           Enterprise Mobility User Activation: *22    Deactivation: *23
  Extended Call Fwd Activate Busy D/A *24  All: *25    Deactivation: *26
        Extended Group Call Pickup Access Code:
               Facility Test Calls Access Code: *28
                             Flash Access Code: *29
             Group Control Restrict Activation: *90    Deactivation: *91
                   Hunt Group Busy Activation: *30    Deactivation: *31
                              ISDN Access Code:
               Last Number Dialed Access Code: *32
     Leave Word Calling Message Retrieval Lock: *33
   Leave Word Calling Message Retrieval Unlock: *34
```

```
change feature-access-codes                                     Page   3 of   9
                              FEATURE ACCESS CODE (FAC)
             Leave Word Calling Send A Message: *35
           Leave Word Calling Cancel A Message: *36
   Limit Number of Concurrent Calls Activation: *37    Deactivation: *38
               Malicious Call Trace Activation: *39    Deactivation: *40
         Meet-me Conference Access Code Change: *41
          Message Sequence Trace (MST) Disable:

 PASTE (Display PBX data on Phone) Access Code: *42
  Personal Station Access (PSA) Associate Code: *43    Dissociate Code: *44
        Per Call CPN Blocking Code Access Code: *45
      Per Call CPN Unblocking Code Access Code: *46

                 Priority Calling Access Code: *47
                          Program Access Code:

      Refresh Terminal Parameters Access Code:
            Remote Send All Calls Activation: *48    Deactivation: *49
              Self Station Display Activation: *50
                     Send All Calls Activation: *51    Deactivation: *52
         Station Firmware Download Access Code: *53
```

5.4. Define Feature Name Extensions (FNEs)

The OPS FNEs can be defined using the **change off-pbx-telephone feature-name-extensions set 1** command. The following screens show the FNEs defined for use with the sample configuration.

```
change off-pbx-telephone feature-name-extensions set 1          Page   1 of   2
     EXTENSIONS TO CALL WHICH ACTIVATE FEATURES BY NAME
                     Set Name: SIP Phones

        Active Appearance Select: 12001
             Automatic Call Back: 12002
      Automatic Call-Back Cancel: 12003
                Call Forward All: 12004
     Call Forward Busy/No Answer: 12005
             Call Forward Cancel: 12006
                       Call Park: 12007
           Call Park Answer Back: 12008
                    Call Pick-Up: 12009
            Calling Number Block: 12010
          Calling Number Unblock: 12011
   Conditional Call Extend Enable:
  Conditional Call Extend Disable:
             Conference Complete:
            Conference on Answer: 12012
           Directed Call Pick-Up: 12013
           Drop Last Added Party: 12014
```

```
change off-pbx-telephone feature-name-extensions set 1          Page   2 of   2
     EXTENSIONS TO CALL WHICH ACTIVATE FEATURES BY NAME

       Exclusion (Toggle On/Off): 12015
      Extended Group Call Pickup:
          Held Appearance Select: 12017
          Idle Appearance Select: 12018
              Last Number Dialed: 12019
            Malicious Call Trace: 12020
     Malicious Call Trace Cancel: 12021
             Off-Pbx Call Enable: 12022
            Off-Pbx Call Disable: 12023
                   Priority Call: 12024
                          Recall:
                  Send All Calls: 12025
           Send All Calls Cancel: 12026
               Transfer Complete:
             Transfer On Hang-Up: 12027
          Transfer to Voice Mail: 12028
         Whisper Page Activation: 12029
```

5.5. Configure Class of Service (COS)

Use the **change cos** command to set the appropriate service permissions to support OPS features (shown in bold). For the sample configuration a COS of "1" was used.

```
change cos                                                          Page   1 of   2

                                0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
 Auto Callback                  n  y  y  n  y  n  y  n  y  n  y  y  y  n  y  n
 Call Fwd-All Calls             n  y  n  y  y  n  n  y  y  n  n  y  y  n  n  y
 Data Privacy                   n  n  n  n  n  y  y  y  y  n  n  n  n  y  y  y
 Priority Calling               n  y  n  n  n  n  n  n  n  y  y  y  y  y  y  y
 Console Permissions            n  y  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Off-hook Alert                 n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Client Room                    n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Restrict Call Fwd-Off Net      y  n  y  y  y  y  y  y  y  y  y  n  y  y  y  y
 Call Forwarding Busy/DA        n  y  n  n  n  n  n  n  n  n  n  y  n  n  n  n
 Personal Station Access (PSA)  n  y  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Extended Forwarding All        n  y  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Extended Forwarding B/DA       n  y  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Trk-to-Trk Transfer Override   n  y  n  n  n  n  n  n  n  n  n  y  n  n  n  n
 QSIG Call Offer Originations   n  n  n  n  n  n  n  n  n  n  n  y  n  n  n  n
 Contact Closure Activation     n  n  n  n  n  n  n  n  n  n  n  n  n  n  n  n
 Automatic Exclusion            n  y  y  n  n  y  n  n  n  n  n  n  n  n  n  n
```

5.6. Configure Class of Restriction (COR)

Use the **change cor n** command, where **n** is the COR used for the TeleMatrix telephones, to enable applicable calling features. To use the Directed Call Pickup feature, the **Can Be Picked Up By Directed Call Pickup** and **Can Use Directed Call Pickup** fields must be set to **y**. In the sample configuration, the TeleMatrix telephones were assigned to COR "1".

```
change cor 1                                                        Page   1 of  23
                              CLASS OF RESTRICTION

              COR Number: 1
         COR Description: Default

                     FRL: 0                                APLT? y
  Can Be Service Observed? y          Calling Party Restriction: none
Can Be A Service Observer? y           Called Party Restriction: none
 Partitioned Group Number: 1       Forced Entry of Account Codes? n
        Priority Queuing? n                 Direct Agent Calling? n
    Restriction Override: all         Facility Access Trunk Test? n
    Restricted Call List? n                  Can Change Coverage? n

           Access to MCT? y            Fully Restricted Service? n
Group II Category For MFC: 7
         Send ANI for MFE? n
           MF ANI Prefix:              Automatic Charge Display? n
Hear System Music on Hold? y   PASTE (Display PBX Data on Phone)? y
                        Can Be Picked Up By Directed Call Pickup? y
                                    Can Use Directed Call Pickup? y
                                    Group Controlled Restriction: inactive
```

5.7. Add Stations

The station features and button assignments were created during the adding of the SIP Users on System Manager. This method was used in this test configuration and the procedure can be found in **Section 6.9**.

5.8. Configure SIP Trunks

Use the **change node-names ip** command and in the IP NODE NAMES form, assign an IP address and host name for each Session Manager Security Module. The host names will be used throughout the other configuration screens of Communication Manager.

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
Gateway001          10.1.10.1
OfficePC            10.3.10.253
default             0.0.0.0
procr               10.1.10.10
procr6              ::
s8500-clan1         10.1.10.21
s8500-medpro1       10.1.10.31
sm6                 10.1.10.55
sm6sec              10.1.10.62
 ( 16 of 21   administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

Use the **change ip-network-region** command and in the IP NETWORK REGION form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is **sglab.com**. By default, **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** (shuffling) are enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G650 Media Gateway. The form also specifies the **Codec Set** to be used for calls routed over the SIP trunk to Session Manager as **ip-network region 1** is specified in the SIP signaling group.

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: sglab.com
    Name: Local
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: 65535
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 46
        Audio PHB Value: 46
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                        RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Use the **change ip-codec-set** command to specify the audio codec's supported for calls routed over the SIP trunk. Note that IP codec set 1 was specified in IP Network Region 1 shown above. Multiple codecs may be specified in the **IP Codec Set** form in order of preference; the example below includes **G.711A** (a-law), **G.711MU** (mu-law) and **G.729.**

```
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.711A            n         2        20
 2: G.711MU           n         2        20
 3: G.729             n         2        20
 4:
 5:
 6:
 7:

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

Use the **add signaling-group** command to configure the Signaling Group parameters for the SIP trunk group. Configure the Signaling Group form shown as follows:

- Set the **Group Type** field to **sip**
- Set the **Transport Method** to the desired transport method; **tcp** (transport control protocol) or **tls** (Transport Layer Security). **Note:** For better security, the recommended method is tls.
- Specify the node names for the processor Ethernet internet and the first Session Manager node name as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These values are taken from the **IP Node Names** form shown above.
- Ensure that the recommended port value of **5060** for tcp is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields **Note**: If tls is used, then the recommended port value is **5061.**
- The preferred codec for the call will be selected from the IP codec set assigned to the IP network region specified in the **Far-end Network Region** field.
- Enter the domain name of the Session Manager Security Module in the **Far-end Domain** field. In this configuration, the domain name is **sglab.com**. This domain is specified in the Uniform Resource Identifier (URI) of the SIP “To” Address in the INVITE message.
- The **DTMF over IP** field should be set to the default value of **rtp-payload**. Communication Manager supports DTMF transmission using RFC 2833.
- The **Direct IP-IP Audio Connections** field should be set to **y** to allow audio traffic to be sent directly between IP endpoints.

Use the **add signaling-group** command to configure another Signaling Group using appropriate values for the trunk group to the second Session Manager. For this testing, Signaling Groups **6** and **7** were configured.

```
add signaling-group 6                                         Page   1 of   1
                                SIGNALING GROUP

 Group Number: 6              Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n                                              SIP Enabled LSP? n
     IP Video? y          Priority Video? y       Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM



   Near-end Node Name: procr                  Far-end Node Name: sm6
 Near-end Listen Port: 5060                 Far-end Listen Port: 5060
                                         Far-end Network Region: 1

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

Use the **add trunk-group** command to configure the SIP trunk group to the first Session Manager. Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with the dial plan. Set the **Service Type** field to **tie**, specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

```
add trunk-group 6                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 6                   Group Type: sip          CDR Reports: n
  Group Name: SIP Trunk to SM6           COR: 1        TN: 1        TAC: #06
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n
                                              Member Assignment Method: auto
                                                     Signaling Group: 6
                                                   Number of Members: 20
```

On **Page 3** of the trunk group form, set the **Numbering Format** field to **private.** This field specifies the format of the calling party number sent to the far-end.

```
add trunk-group 6                                           Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                       Maintenance Tests? y

                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n

 Show ANSWERED BY on Display? y
```

Use the **add trunk-group** command to configure another SIP trunk group using appropriate values for the second Session Manager. For this testing, Trunk Groups **6** and **7** were configured.

Use the **change private-numbering 0** command to configure the calling party number sent to the far-end over the SIP trunk groups. In this testing, local stations with a 5-digit extension beginning with **1** and whose calls are routed over SIP trunk groups **6** and **7** have their extension number sent to the far-end for display purposes.

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

Ext Ext               Trk        Private          Total
Len Code              Grp(s)     Prefix           Len
 5  1                 6                           5     Total Administered: 2
 5  1                 7                           5        Maximum Entries: 540
```

By default, Communication Manager uses the Auto Alternate Routing (AAR) Analysis table to determine how to route calls to SIP endpoints registered on Session Manager. In this testing, the TeleMatrix SIP telephones were assigned the extensions 10054 to 10057. Use the **change aar analysis 0** command to configure a 5-digit dialed string beginning with **1005** to use Route Pattern **6** to route the calls to Session Manager.

```
change aar analysis 0                                          Page   1 of
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all          Percent Full: 0

          Dialed           Total      Route     Call   Node  ANI
          String          Min  Max  Pattern     Type   Num   Reqd
    1005                  5    5      6         unku         n
```

Use the **change route-pattern 6** command to configure the route pattern to use SIP trunk groups **6** and **7** configured above. The **FRL** is set to **0** to be the least restrictive and set **LAR** to **next** so that the next trunk group is used whenever the trunk group is out of service.

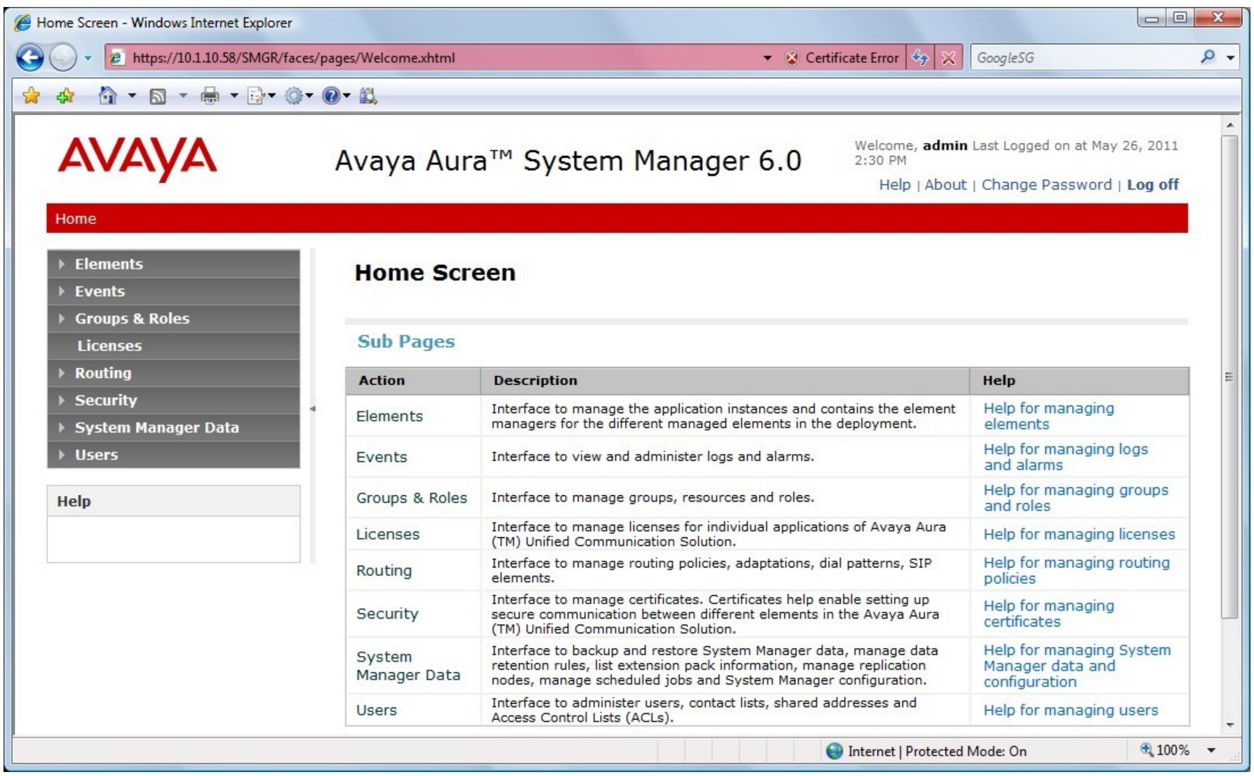
```
change route-pattern 6                                         Page   1 of   3
                    Pattern Number: 6   Pattern Name: non-IMS to SM6
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                            DCS/ IXC
    No          Mrk Lmt List Del  Digits                              QSIG
                             Dgts                                     Intw
 1: 6    0                    0                                        n   user
 2: 7    0                    0                                        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  next
 2: y y y y y n  n            rest                               lev0-pvt  next
 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
```

6. Configure Avaya Aura® Session Manager

This section covers the administration of Session Manager. Session Manager is configured via an internet browser using the System Manager web interface. It is assumed that both System Manager and Session Manager have already been installed. For additional information on installation tasks refer to **Reference [4]**.

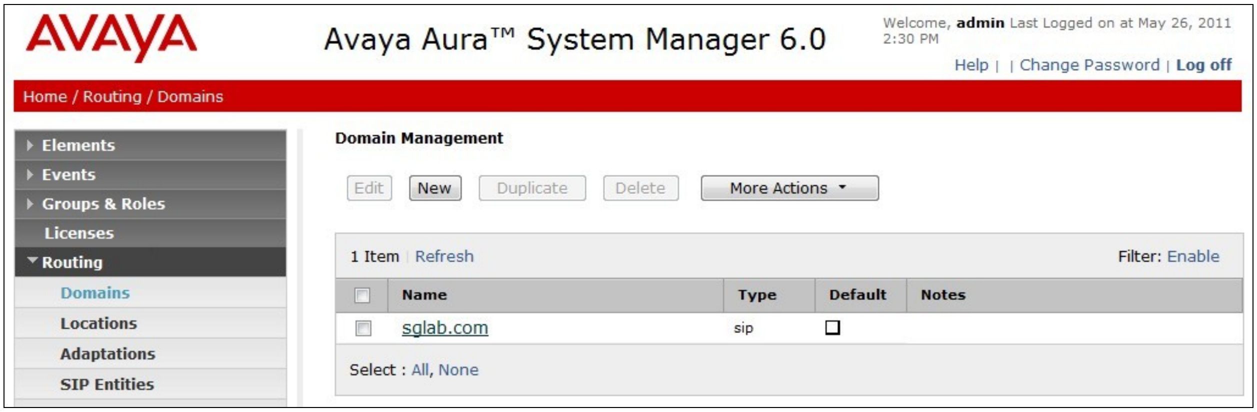
6.1. Logging in to System Manager

To access the web interface, enter "**https://<ip-addr of System Manager>/SMGR**" as the URL in a web browser. Log in using the appropriate credentials. The main screen is displayed, as shown below.



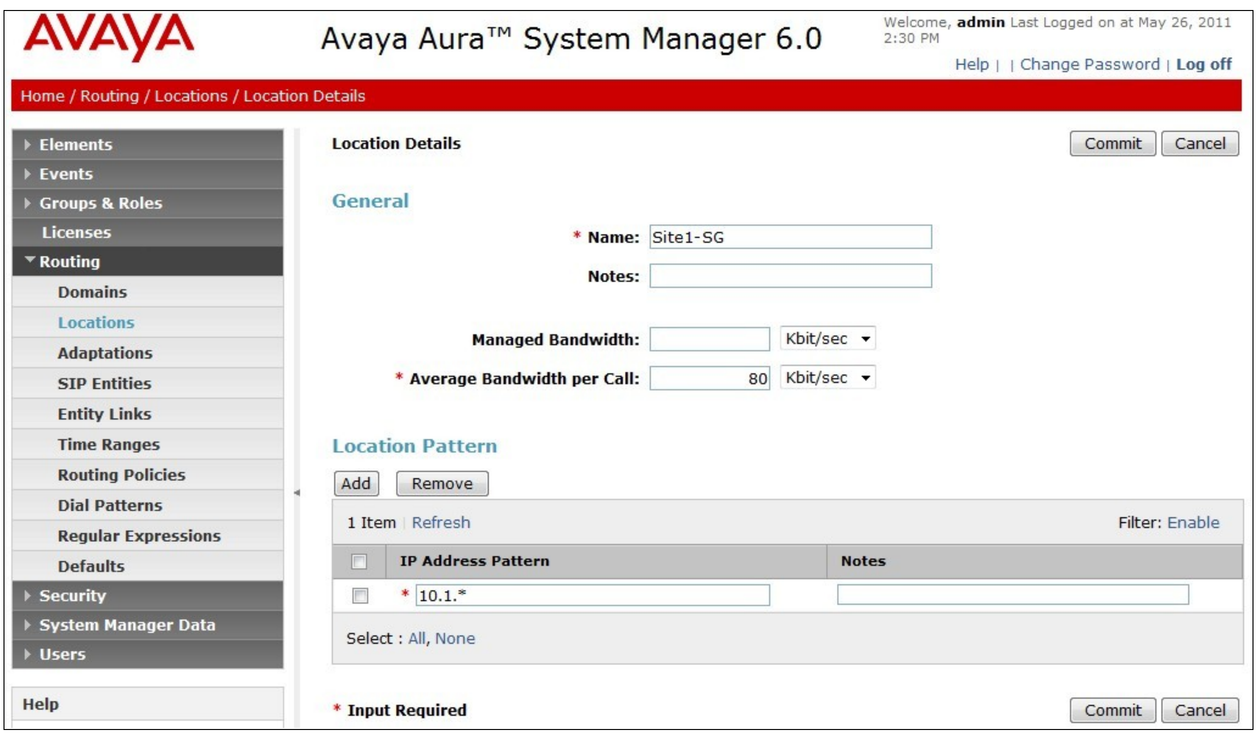
6.2. Domains

Navigate to **Routing > Domains** from the left menu and check that the domain corresponds to that administered in the IP Network Region and Signaling Group forms on Communication Manager in **Section 5.8**.



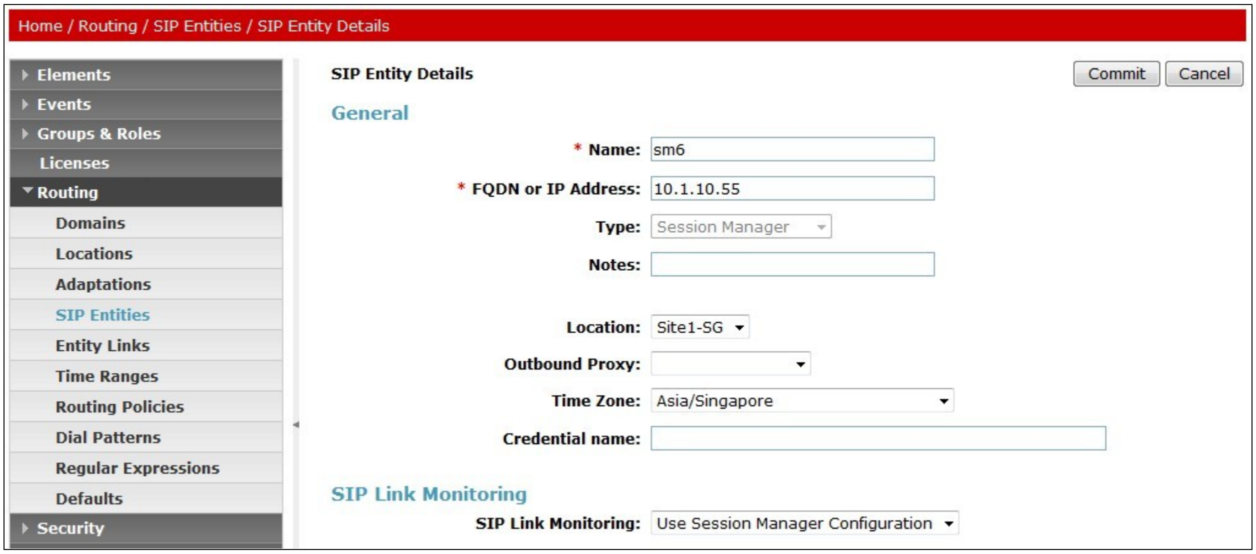
6.3. Add Location

Navigate to **Routing > Locations** from the left menu and click on the **New** button (not shown). Specify the Location **Name** and configure **IP Address Pattern** for the Location in the format shown under **Location Patterns**. Click on the **Commit** button to save.

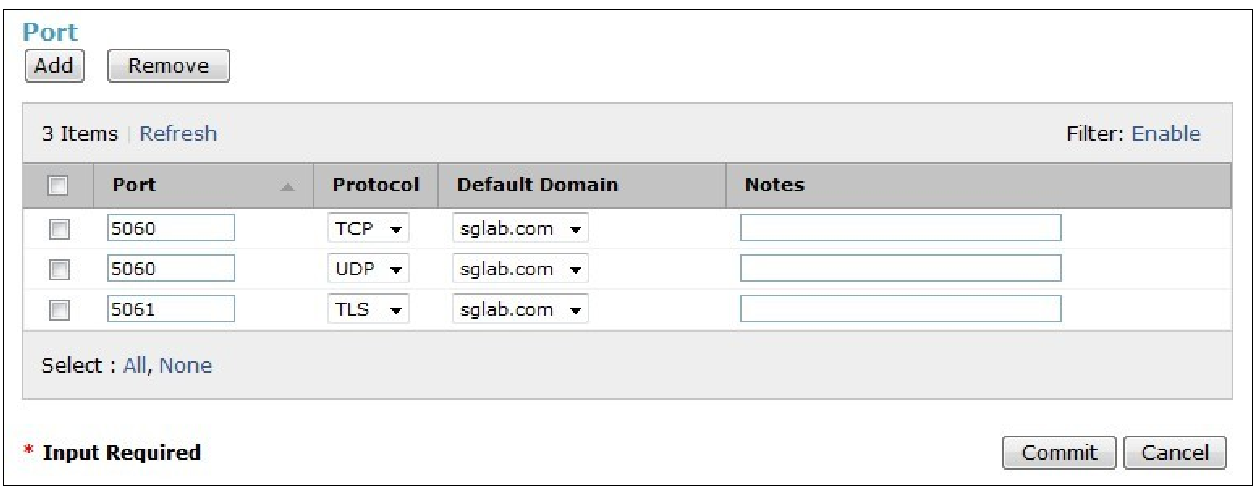


6.4. Create SIP entities

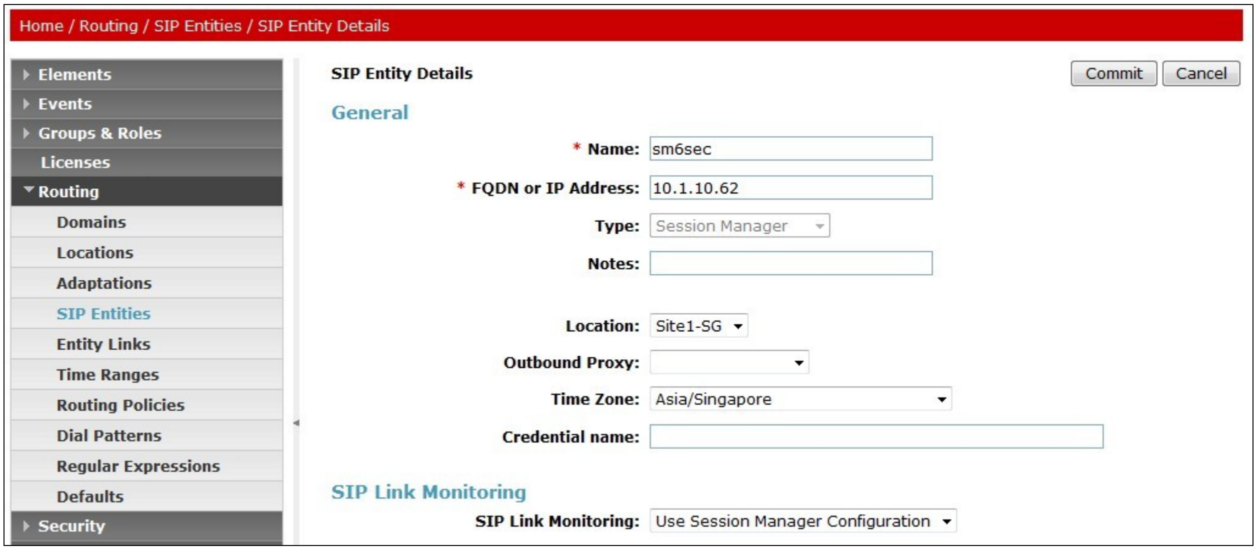
Navigate to **Routing > SIP Entities** from the left menu and click on the **New** button (not shown) to create the SIP Entity for the first Session Manager. Enter a **Name** and **FQDN or IP Address** for the Session Manager Security Module. Select **Type** as **Session Manager** and **Location** as the Session Manager Location created in **Section 6.3**.

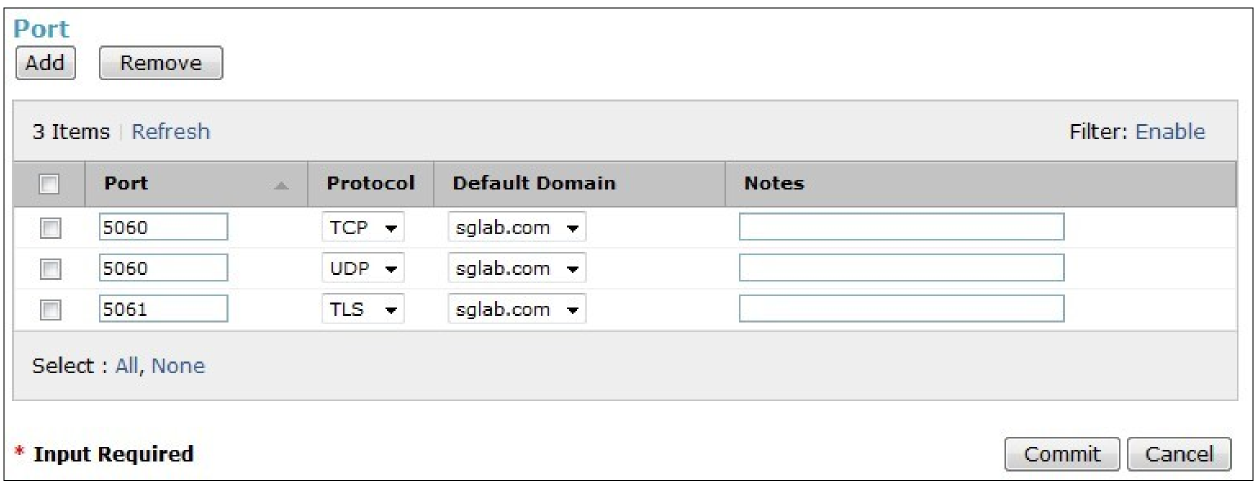


Add the **Port** and **Protocol** information to the **Port** section of the SIP Entity screen as shown below. Set the **Default Domain** to the domain configured in **Section 6.2**. Click **Commit** to save the changes.

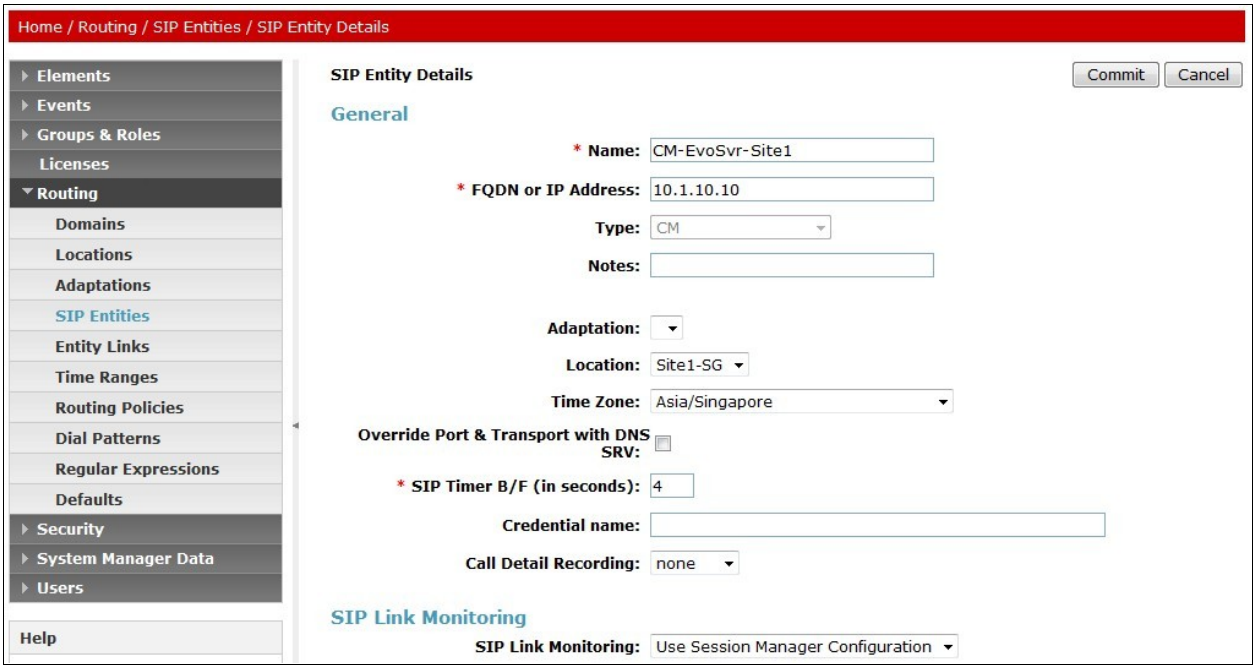


Repeat the step above to configure another SIP Entity for the second Session Manager. The details are as shown below.





A SIP Entity is added for Communication Manager with the details as shown below with an appropriate **Name** and the **FQDN or IP Address** of the processor Ethernet interface configured in **Section 5.8**. Select **Type** as **CM** and **Location** as the Session Manager Location created in **Section 6.3**.

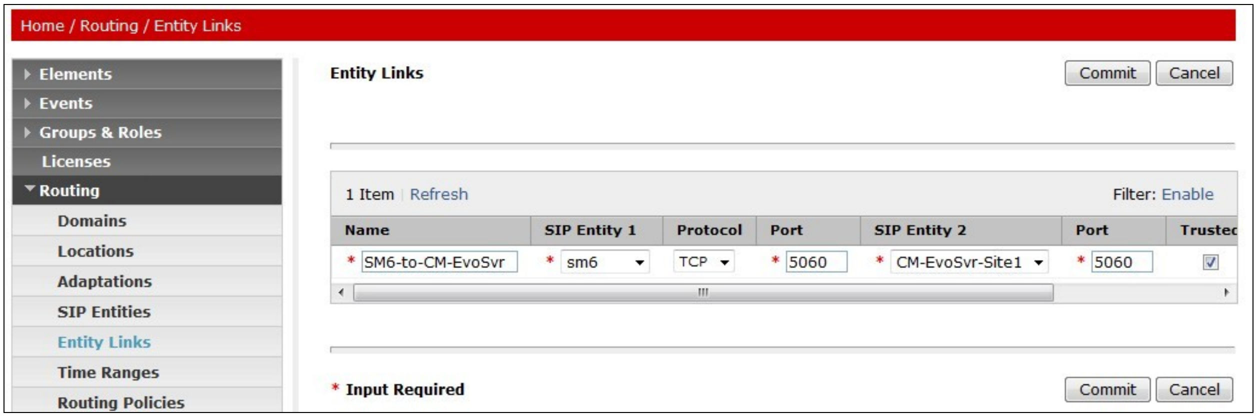


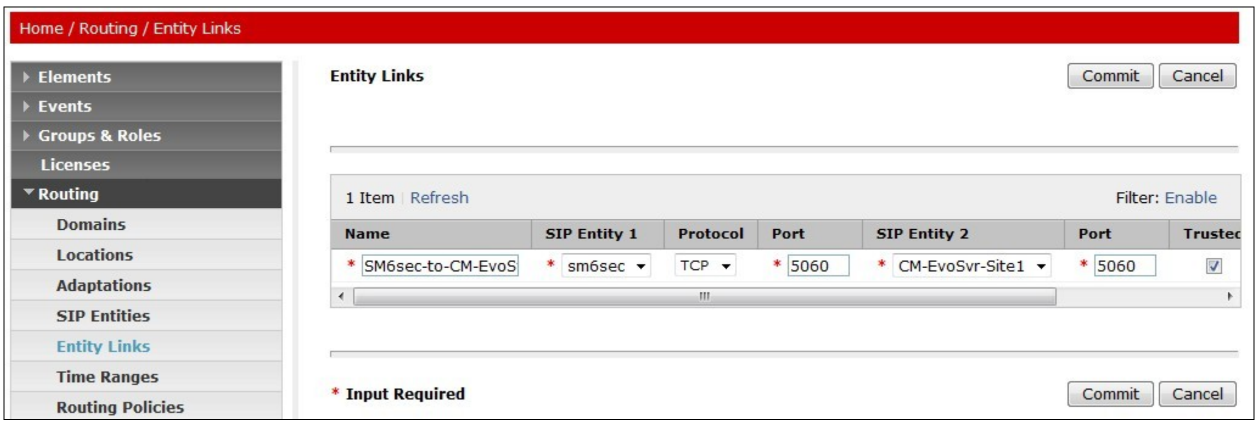
6.5. Add an Entity link

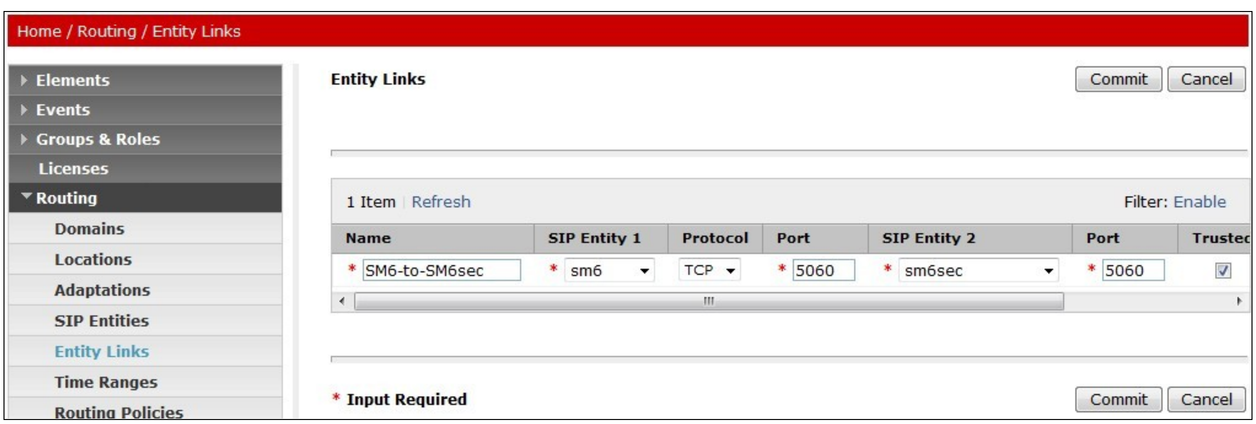
Navigate to **Routing > Entity Links** from the left menu and click on the **New** button (not shown) to create the Entity Links between the SIP Entities. In total, the following three Entity Links were created:

1. First Session Manager to Communication Manager
2. Second Session Manager to Communication Manager
3. First Session Manager to Second Session Manager

Choose an appropriate **Name** and then choose the entities added in **Section 6.4,** the **Protocol** used (TCP used in this example) and the **Port** the protocol communicates on. Click on the **Commit** button to save.

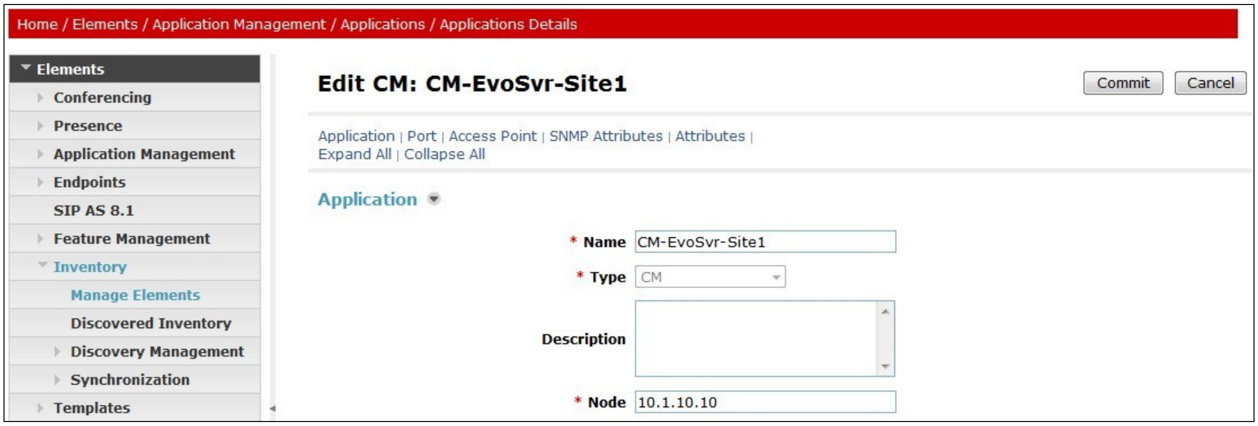




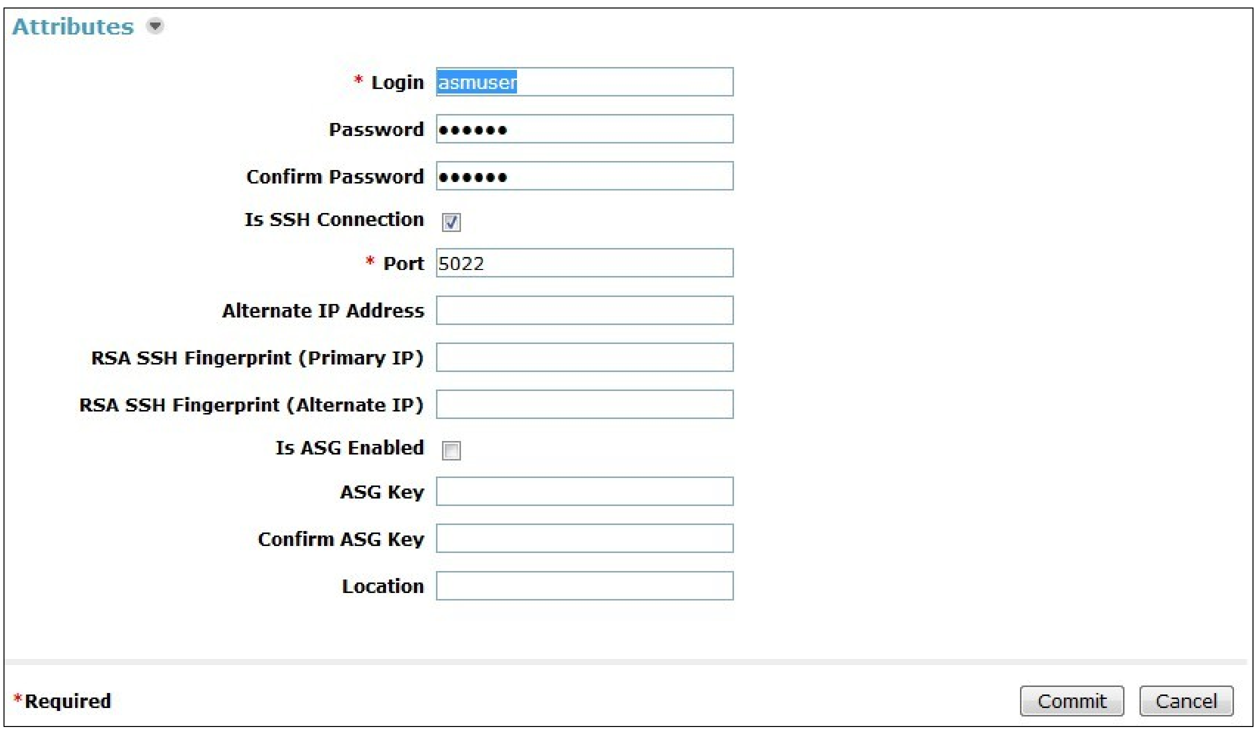


6.6. Add Communication Manager Managed Element

Navigate to **Elements > Inventory > Manage Elements** from the left menu and click on the **New** button (not shown). Enter a valid **Name**, **Type** as **CM** and the SAT IP address in the **Node** field. Click on **Commit** to save.



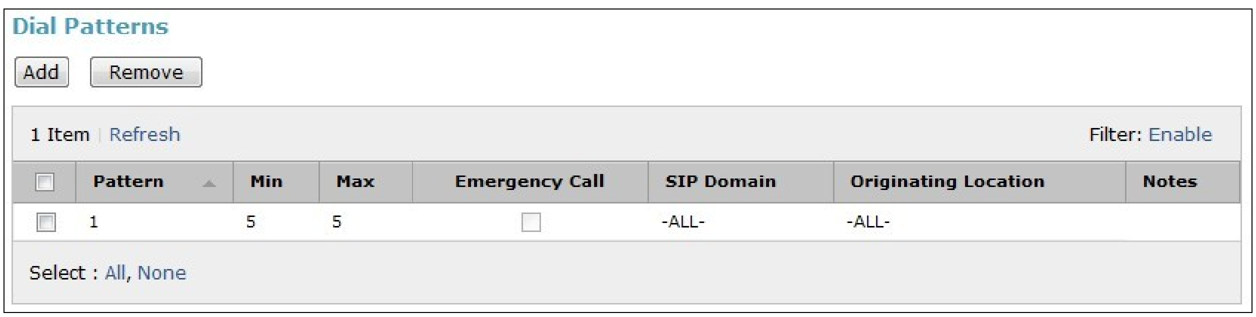
In the Attributes Section, specify a **Login** and **Password** that has permissions to perform administration on Communication Manager. This can be the same credentials used in **Section 5**.



6.7. Add Routing Policy

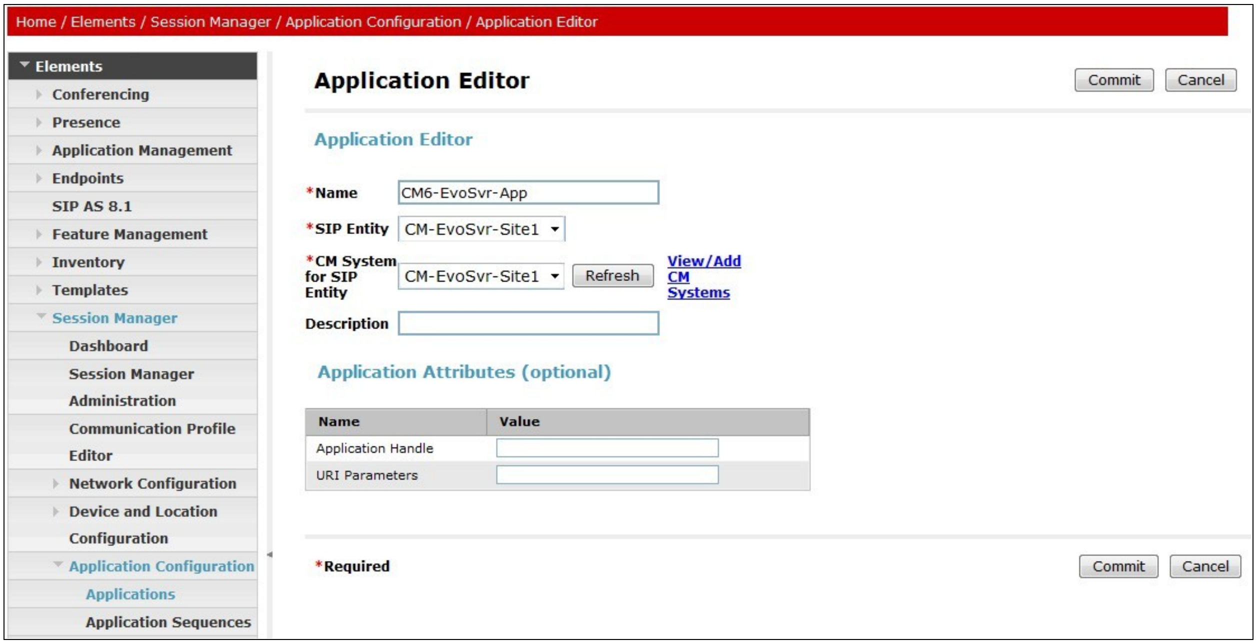
Navigate to **Routing > Routing Policies** from the left menu and click on the **New** button (not shown) to create a Routing Policy to route calls to Communication Manager. Specify the **Name** for the policy and select the Communication Manager entity as the Destination under **SIP Entity as Destination**.

Add the **Dial Patterns** for non SIP stations and PSTN routing. A **Pattern** to be dialed and **Min**, **Max** digits are entered. Click on the **Commit** button to save.

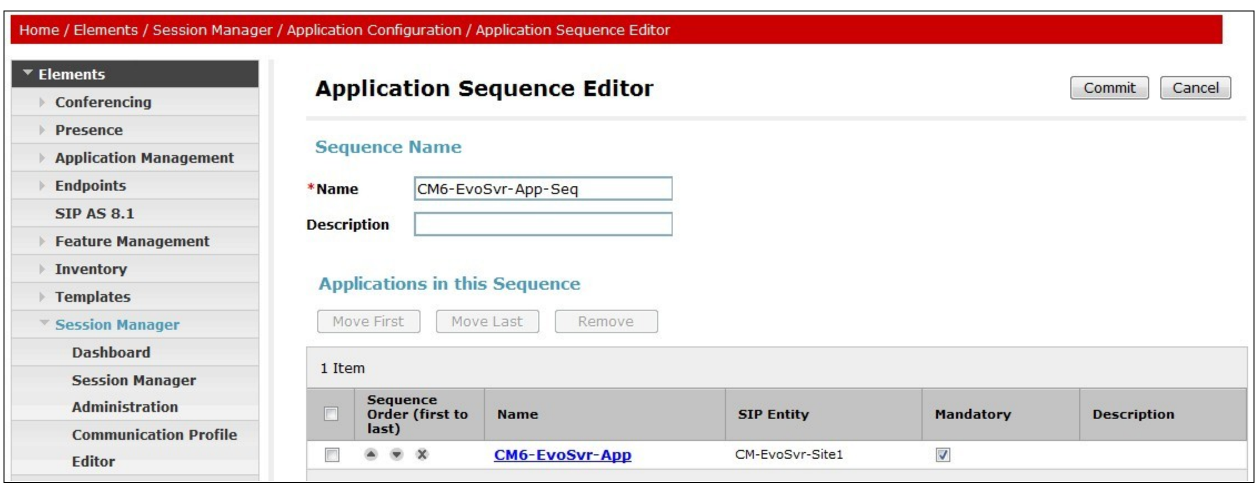


6.8. Add Application and Application Sequence

Navigate to **Elements > Session Manager > Application Configuration > Applications** from the left menu and click on the **New** button (not shown). Enter an appropriate **Name**, Select the Communication Manager **SIP Entity** added in **Section 6.4** and the Communication Manager Managed Element added in **Section 6.6** as **CM System for SIP Entity**. Click on the **Commit** button to save.

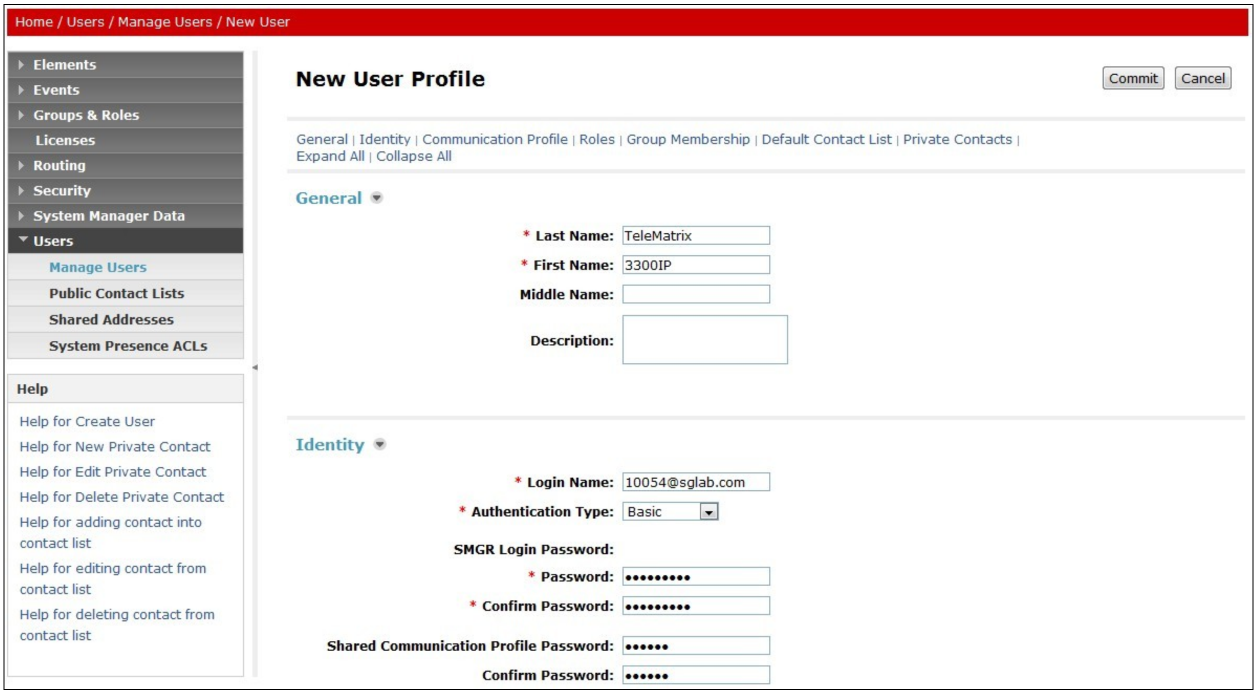


Navigate to **Elements > Session Manager > Application Configuration > Applications** from the left menu and click on the **New** button (not shown). Add a **Name** and select the Application added above to interact with the Communication Manager Entity.

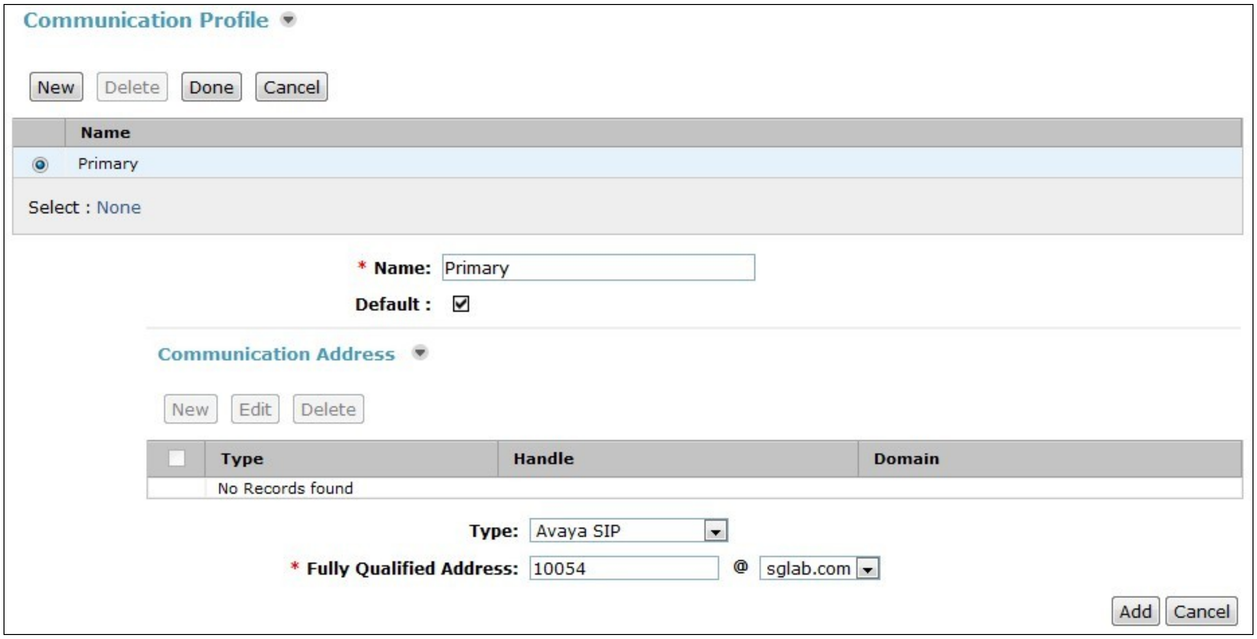


6.9. Add User

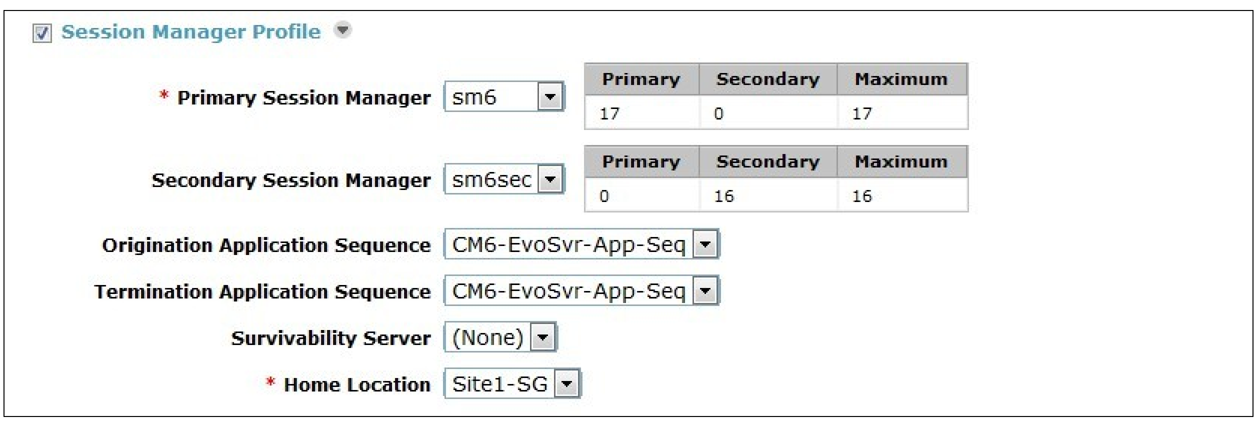
Navigate to **Users > Manage Users** from the left menu and click on the **New** button (not shown). Specify the **Last Name** and **First Name. E**nter the fully qualified name in the form <user>@<sip domain> for **Login Name** and specify the **SMGR Login Password**. Specify also the **Shared Communication Profile Password**, which is used by the TeleMatrix SIP telephone to log in to Session Manager.



In the **Communication Profile** Section, move to **Communication Address** and click on the **New** button. Select **Avaya SIP** as **Type** and enter the **Fully Qualified Address** the same as on the Identity tab. Select **Add** to continue.

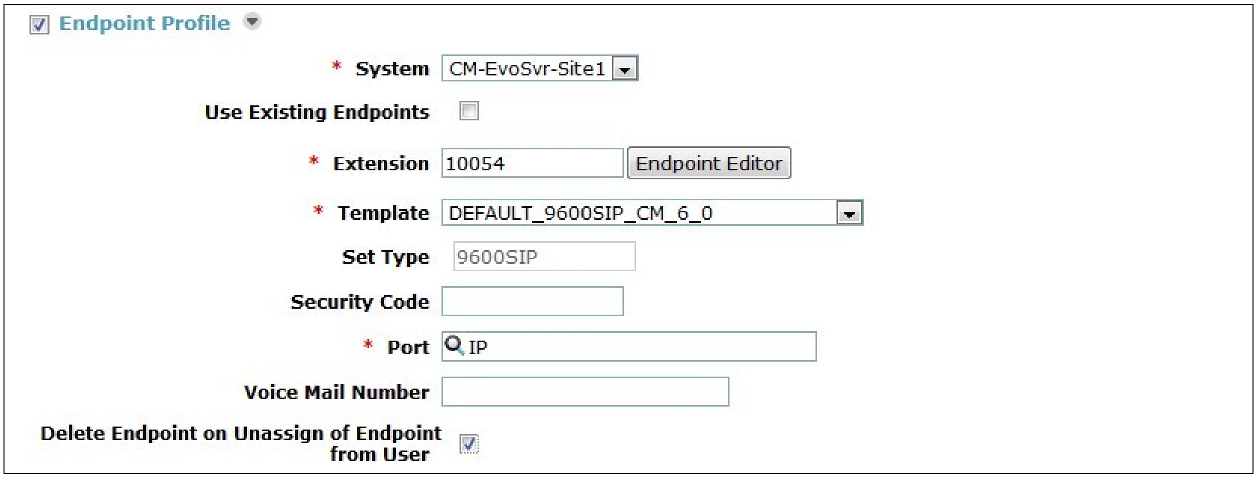


Move down and select **Session Manager Profile.** Fill in the details with the **Primary Session Manager** and **Secondary Session Manager** as the SIP entities added in **Section 6.4.** Fill in the **Application Sequences** as the Application Sequence added in **Section 6.8**. Fill in the **Home Location** as the Location added in **Section 6.3**.



Move down and select **Endpoint Profile**. Fill in the **System** as the Communication Manager Managed Element added in **Section 6.6**. Select an appropriate **Template** for SIP telephones. In this testing, the **DEFAULT_9600SIP_CM_6_0** template was used. Specify the **Extension** assigned to this user, select **IP** for **Port**, and tick the **Delete Endpoint on Unassign of Endpont from User or on Delete User**.

Note: Endpoint Editor can be used to administer COS, COR, features and buttons for the extension.



7. Configure TeleMatrix SIP Telephones

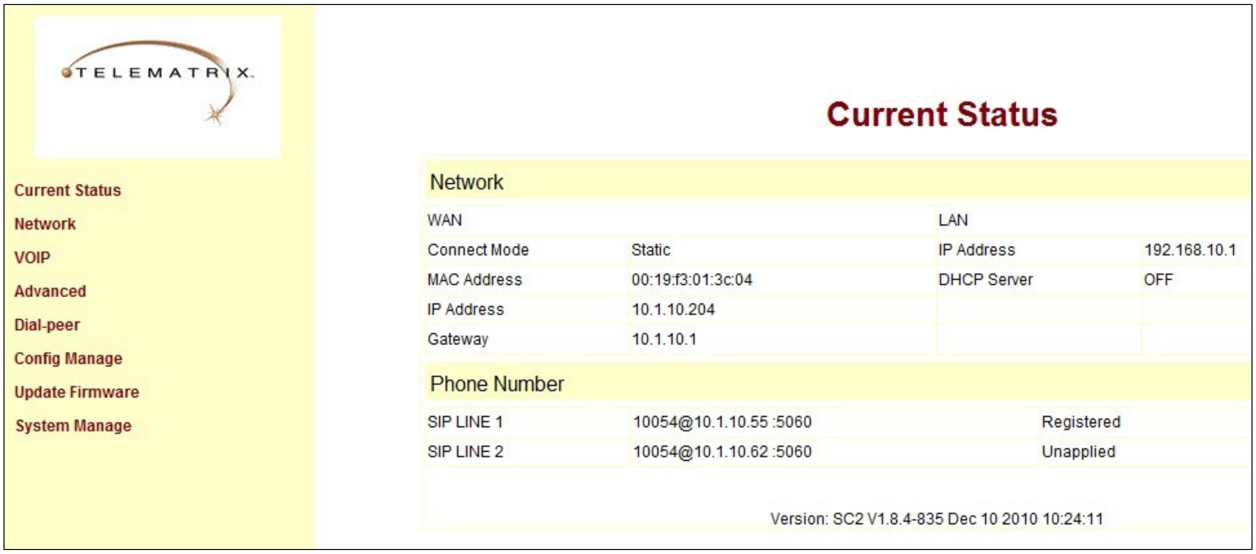
This section covers the administration of the TeleMatrix SIP Telephones. The TeleMatrix SIP Telephones were configured via a web browser. To access the web interface, enter the IP address of the telephone in the browser URL. All the TeleMatrix SIP phones being tested are configured in the same way.

7.1. Determining IP Address

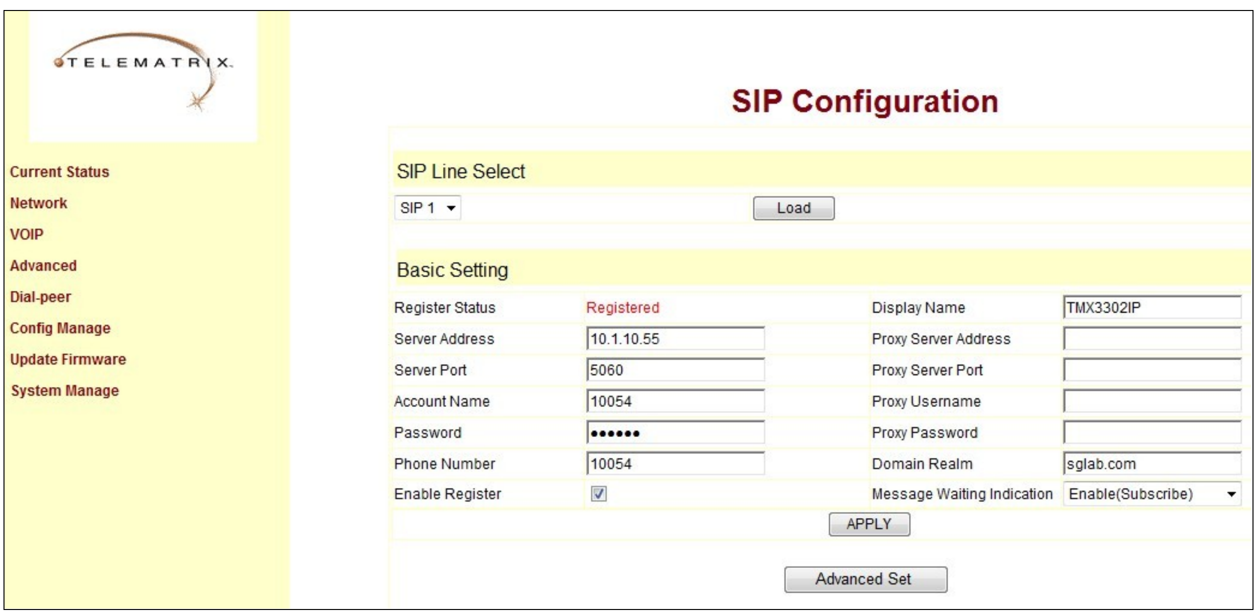
Press “**47#” on the keypad of the telephone and it will read out the IP address currently assigned.

7.2. Configuring using the Web Browser

Enter the IP address of the TeleMatrix telephone into the address bar of web browser and log in using a valid account. The **Current Status** screen is displayed.

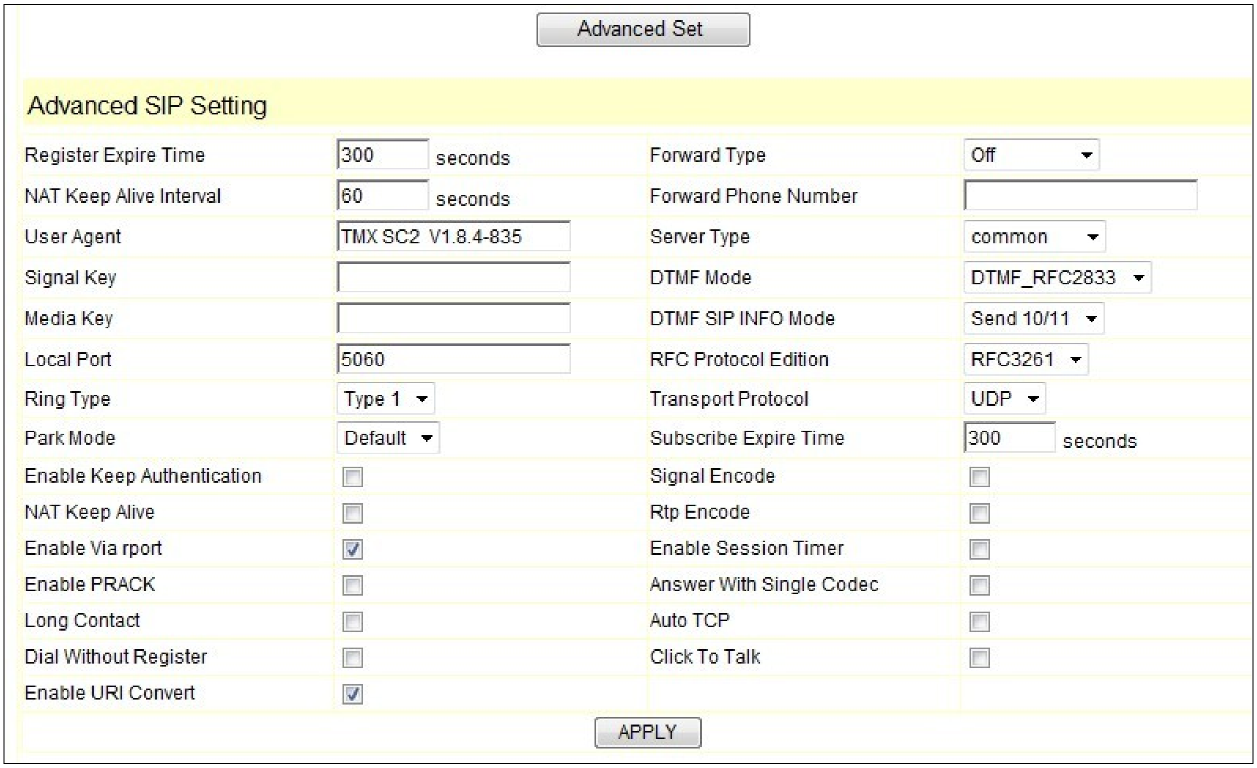


Select **VOIP** from the left menu. Enter the account details as shown below to match the settings in the Session Manager added in **Section 6.9**. Select **Enable(Subscribe)** for **Message Waiting Indication**. Click **APPLY** to save the changes. If the details have been entered correctly, the **Register Status** will change to **Registered** as shown below.

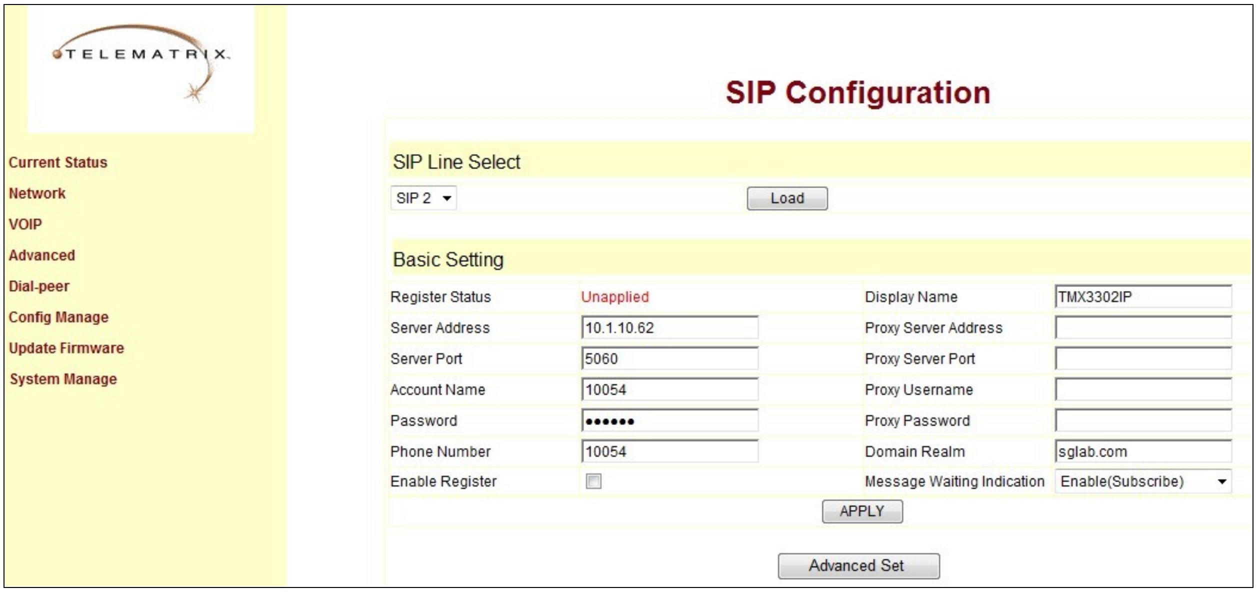


Click **Advanced Set** to display the Advanced SIP Setting section as shown below. The following values were used during compliance testing. For **DTMF Mode**, Select **DTMF_RFC2833**. **Register Expire Time** and **Subscribe Expire Time** are both set to **300** seconds for this testing. The values can be increased to reduce the frequency of the Register and Subscribe SIP messages. For **Transport Protocol**, select either **UDP** to **TCP**.

Note: Most test cases were completed using UDP transport protocol.

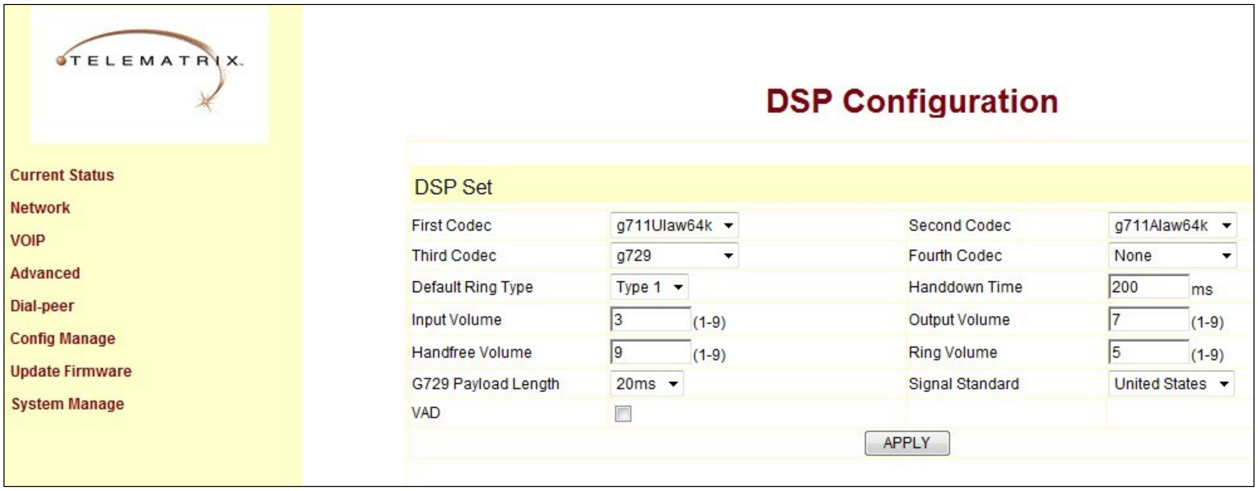


To configure the account details to register to the second Session Manager, select **SIP 2** from the **SIP Line Select** section and click **Load**. Enter the same account details as shown below and enter the IP address of the second Session Manager in **Server Address**. Click **APPLY** to save the changes. The **Register Status** will show as **Unapplied** as shown below. This is because the default behavior of the TeleMatrix SIP phone is to use the Alternate Registration strategy for failover. The phone will register to the second Session Manager only when it loses connection to the first. Click on Advanced Set to configure the Advanced SIP setting as described above.



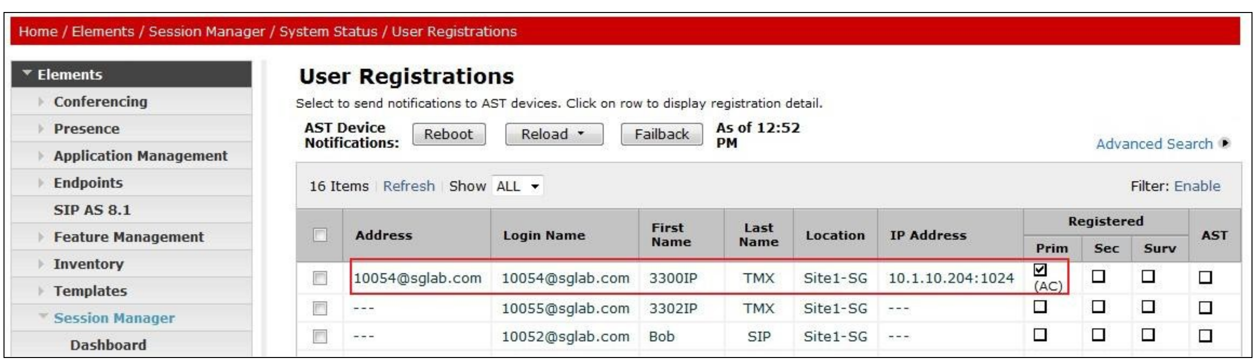
Note: To configure the TeleMatrix SIP telephone to use the Simultaneous Registration strategy requires the phone to be configured using a configuration file. As such, it will not be discussed in these application notes. For further information, refer to **Reference [08]**.

Navigate to **Advanced > DSP** from the left menu. The audio codecs configured for this testing are as shown below. This should match the codecs configured on Communication Manager shown in **Section 5.8**.

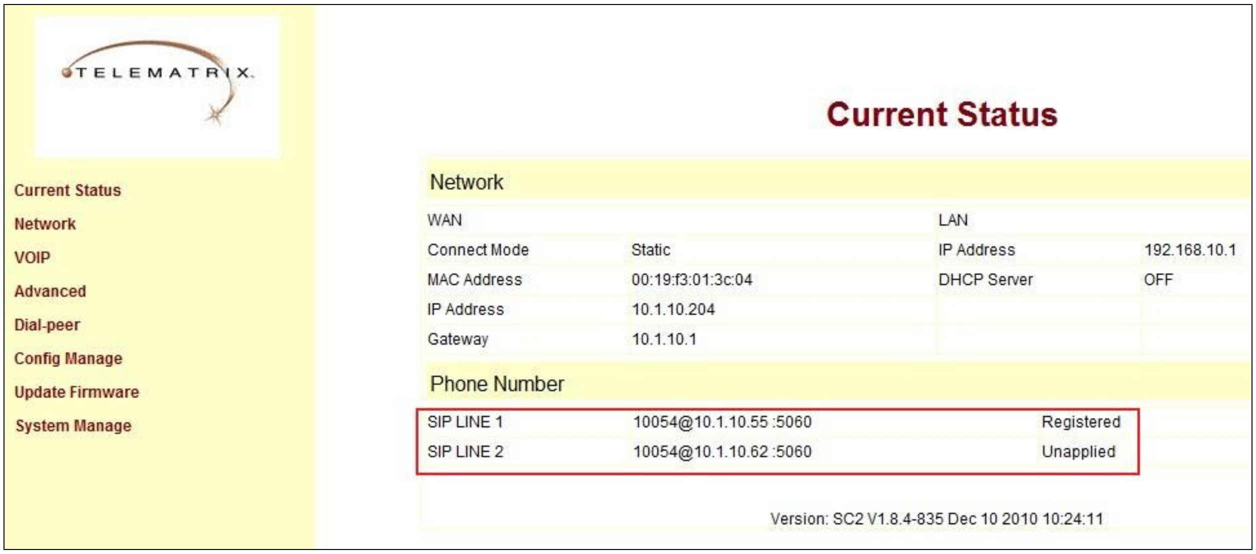


8. Verification Steps

The following steps can be used to verify and/or troubleshoot installations in the field. Verify that the TeleMatrix phones have successfully registered with Session Manager. From the System Manager web interface, navigate to **Elements > Session Manager > System Status > User Registrations** to display a list of registered users on Session Manager as shown below. The **Address** and **IP Address** fields are populated and the box is checked in the **Registered** column when the phone has successfully registered.



From the web interface of the TeleMatrix phones, click Current Status from the left menu. Verify that the status for either **SIP LINE 1** or **SIP LINE 2** shows as **Registered**.



9. Conclusion

These Application Notes described the administration steps required to configure TeleMatrix 3300IP, 3302IP, 9600IP and 9602IP SIP Telephones with Avaya Aura® Session Manager 6.0 and Avaya Aura® Communication Manager 6.0. The test cases described in **Section 2** passed successfully.

10. Additional References

This section references documentation relevant to these Application Notes. Avaya product documentation is available at http://support.avaya.com.

[1] *Installing and Configuring Avaya Aura® Communication Manager*, Doc ID 03-603558, Release 6.0 June, 2010.
[2] *Administering Avaya Aura® Communication Manager*, Doc ID 03-300509, Issue 6.0 June 2010.
[3] *Administering Avaya Aura® Session Manager*, Doc ID 03-603324, Release 6.0, June 2010.
[4] *Installing and Configuring Avaya Aura® Session Manager,* Doc ID 03-603473 Release 6.0, June 2010.
[5] *Maintaining and Troubleshooting Avaya Aura® Session Manager,* Doc ID 03-603325, Release 6.0, June 2010.
[6] TeleMatrix EN10107 Step-by-Step Deployment.
[7] TeleMatrix EN10107 Reference – 1.8.3 Quick Keys – SL010.
[8] TeleMatrix EN10107 SIP Configuration File Parameters 1.8 – SL016.

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.