Avaya Solution & Interoperability Test Lab

Application Notes for Med-Pat D2200IP with Avaya Aura® Session Manager R6.3 and Avaya Aura® Communication Manager R6.3 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Med-Pat D2200IP to interoperate with Avaya Aura® Session Manager R6.3 and Avaya Aura® Communication Manager R6.3. The Med-Pat D2200IP is a SIP twin handset telephone that can register with Avaya Aura® Session Manager as a SIP endpoint in support of voice communications.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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 Med-Pat D2200IP to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager Release 6.3. The Med-Pat D2200IP (D2200IP) is a SIP twin handset telephone that can register with Avaya Aura® Session Manager as a SIP endpoint.

The Med-Pat D2200IP is a dual handset telephone for use in areas where telephonic interpretation may be necessary. In conjunction with a 3rd party interpreter service, the D2200IP allows discrete conversations between two on-site parties and an off-site interpreter. This endpoint is typically deployed in hospital patient rooms, reception desks, pharmacy counters or anywhere else there is a need to overcome a language barrier.

2. General Test Approach and Test Results

The general test approach was to place calls to and from the D2200IP and exercise basic telephone operations. The main objectives were to verify the following:

- Registration
- Codecs (G.711, G.722, iLBC and G.729)
- Inbound calls
- Outbound calls
- Hold/Resume, Call Transfer and Conferencing
- Call termination (origination/destination)
- Avaya Features using FAC
    - Call Park
    - Call Pickup
    - Call Forward (Unconditional, Busy/No Answer)
    - Find Me
- Message Waiting Indicator (MWI)
- Voicemail
- Serviceability

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 included features and serviceability. The focus of interoperability compliance testing was primarily on verifying call establishment on the D2200IP. The scope of testing included operations such as inbound calls, outbound calls, hold/resume, transfer, conference, Facility Access Codes, and its interactions with Session Manager, Communication Manager, and other Avaya SIP, and H.323 phones. The serviceability testing introduced failure scenarios to see if D2200IP can recover from failures.

2.2. Test Results/Observations

The test objectives were verified. For serviceability testing, D2200IP operated properly after recovering from failures such as network disconnects, and resets of D2200IP.

Testing was successful with the following observations:

- The following features are not supported by the D2200IP:
  - Call Hold and Resume
  - Call Transfer
  - Conference Call
  - Long Hold Recall Timer
  - Call Park
- A delay of a couple of seconds was noted when an inbound call was picked up on D2200IP. This delay does not happen if shuffling is disabled. Med-Pat will fix this issue in a future release.
- When the call is terminated at far-end, a busy tone is heard on D220IP handset for three to five seconds. As per the signaling, the call terminates properly. Med-Pat will fix this issue in a future release.
- When Originating and Terminating sequences were enabled on Session Manager (**Section 5.6**), it was noted that the calls originating from Avaya SIP endpoints to D2200IP received a Request time out (408) error. These sequences need to be enabled in order for Facility Access Codes to work properly. This issue was noted in firmware release **D-59-201405120** and addressed in the latest firmware release **D-59-201506300** listed in **Section 4**.
- Message Waiting Indication (MWI) – D2200IP uses a stutter tone to indicate MWI
- iLBC Codec is supported only between the D2200IP endpoints
- At least one hardware-supported codec needs to be listed on D2200IP for iLBC or G.722 to work

2.3. Support

For Technical Support

- Avaya products described in these Application Notes visit http://support.avaya.com
- Med-Pat D2200IP please visit http://www.med-pat.com

3. Reference Configuration

Once D2200IP registers as a SIP endpoint with Session Manager, it can place and receive voice calls with various supported features as listed above in **Section 2.1** with exceptions noted in **Section 2.2**. The reference configuration used for the compliance test is shown in **Figure 1** below.

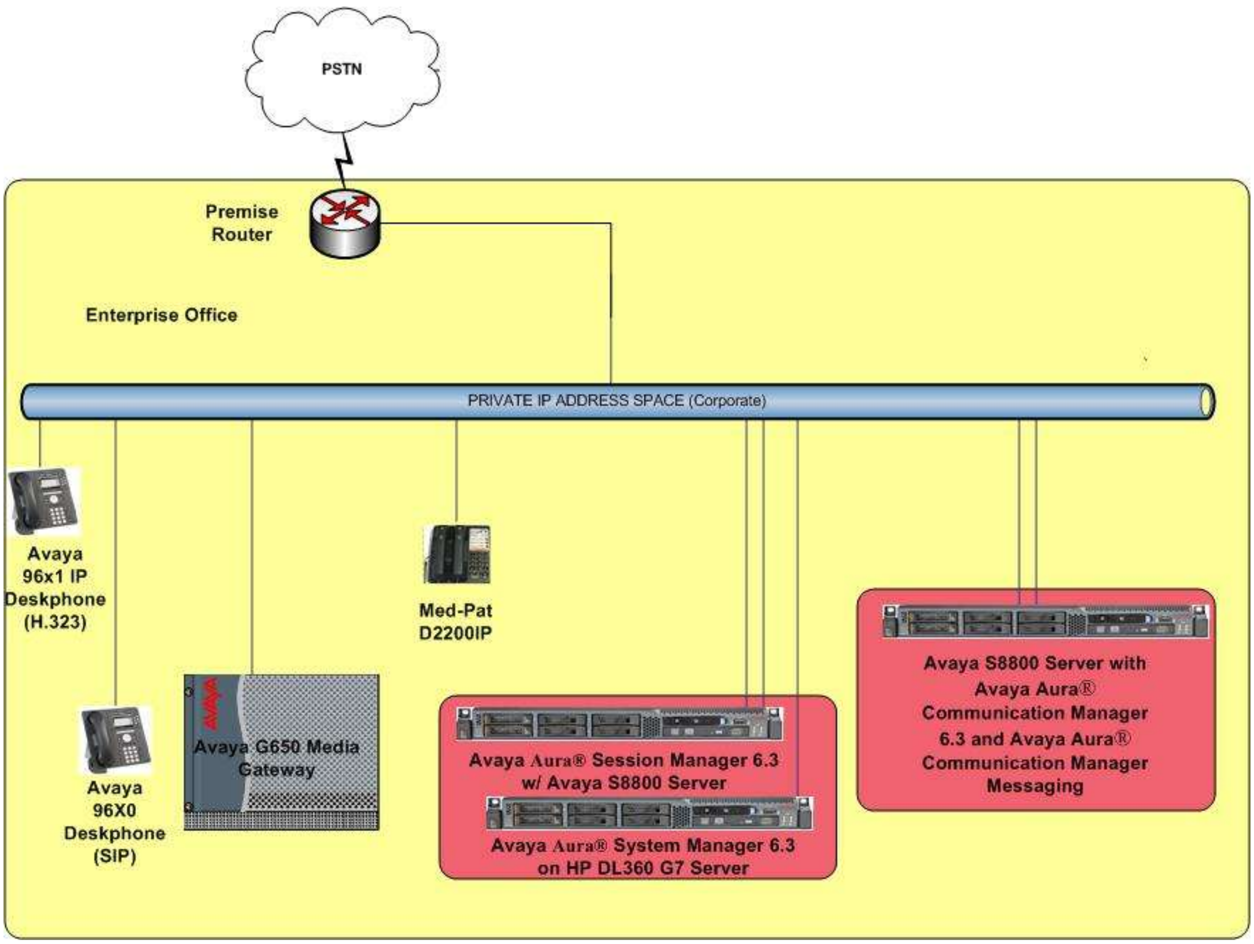


Figure 1: Med-Pat D2200IP with Avaya Aura® Session Manager and Avaya Aura® Communication Manager

4. Equipment and Software Validated

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

Equipment	Software
Avaya Aura® System Manager running on an Avaya HP DL360/G7 Server	R6.3.12.9.3022 – SP12
Avaya Aura® Session Manager running on an Avaya S8800 Server	R6.3.12.0.631208 – SP12
Avaya Aura® Communication Manager running on Avaya S8800 Server and G650 Media Gateway	R016x.03.0.124.0 – R6.3, SP10
Avaya 96x1 IP Deskphone (H323)	R6.2.2313
Avaya 96x0 IP Deskphone (SIP)	R2.6.12.1
Med-Pat D2200IP	D-59-201506300[1]

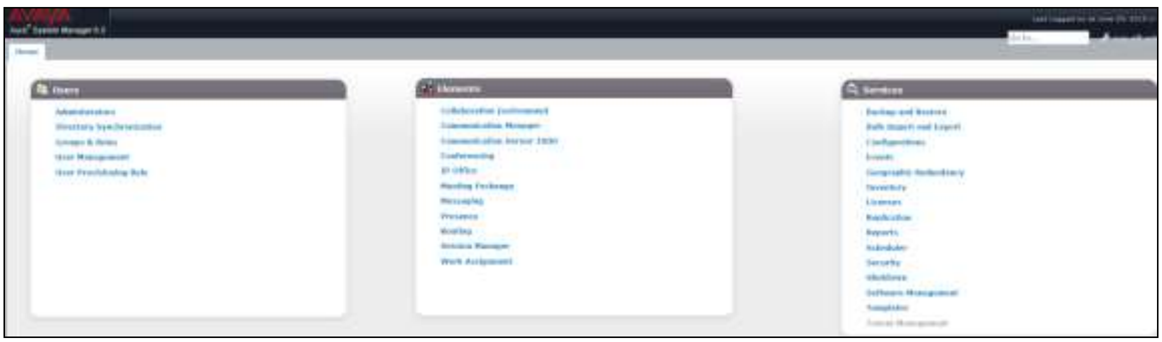
[1] All testing was done with D2200IP firmware release **D-59-201405120**. An issue was observed as noted in **Section 2.2** which was fixed in firmware release **D-59-201506300**. Sanity testing was done with the latest release of the firmware.

5. Configure Avaya Aura® Session Manager

This section provides the steps for configuring Session Manager. Note that in all the configuration steps, only the fields which were configured are mentioned. For the remaining fields default values were used for this reference configuration. The steps include adding the following items:

- SIP domain
- Logical/physical Locations that can be occupied by SIP Entities
- SIP Entities and corresponding Entity Links for Session Manager and Communication Manager
- Routing Policy for call routing
- Dial Pattern to be used by Routing Policy
- Define Communication Manager as Administrable Entity (i.e., Managed Element)
- Application Sequence
- Add SIP Users

Configuration is accomplished by accessing the browser-based GUI of System Manager using the URL "**https://<*ip-address*>/SMGR**", where <*ip-address*> is the IP address of System Manager. Log in with the appropriate credentials and the following screen will be displayed:



5.1. Specify SIP Domain

Navigate to **Home→Elements→Routing→Domains** and click the **New** (not shown) button. Configure the screen shown below as follows:

- **Name:** The authoritative domain name (e.g., *avaya.com*)
- **Notes:** Descriptive text (optional)
- Click **Commit**

5.2. Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management. To add a location, navigate to **Home→Elements→Routing→Locations** and click on the **New** button (not shown). Configure the screen shown below as follows:

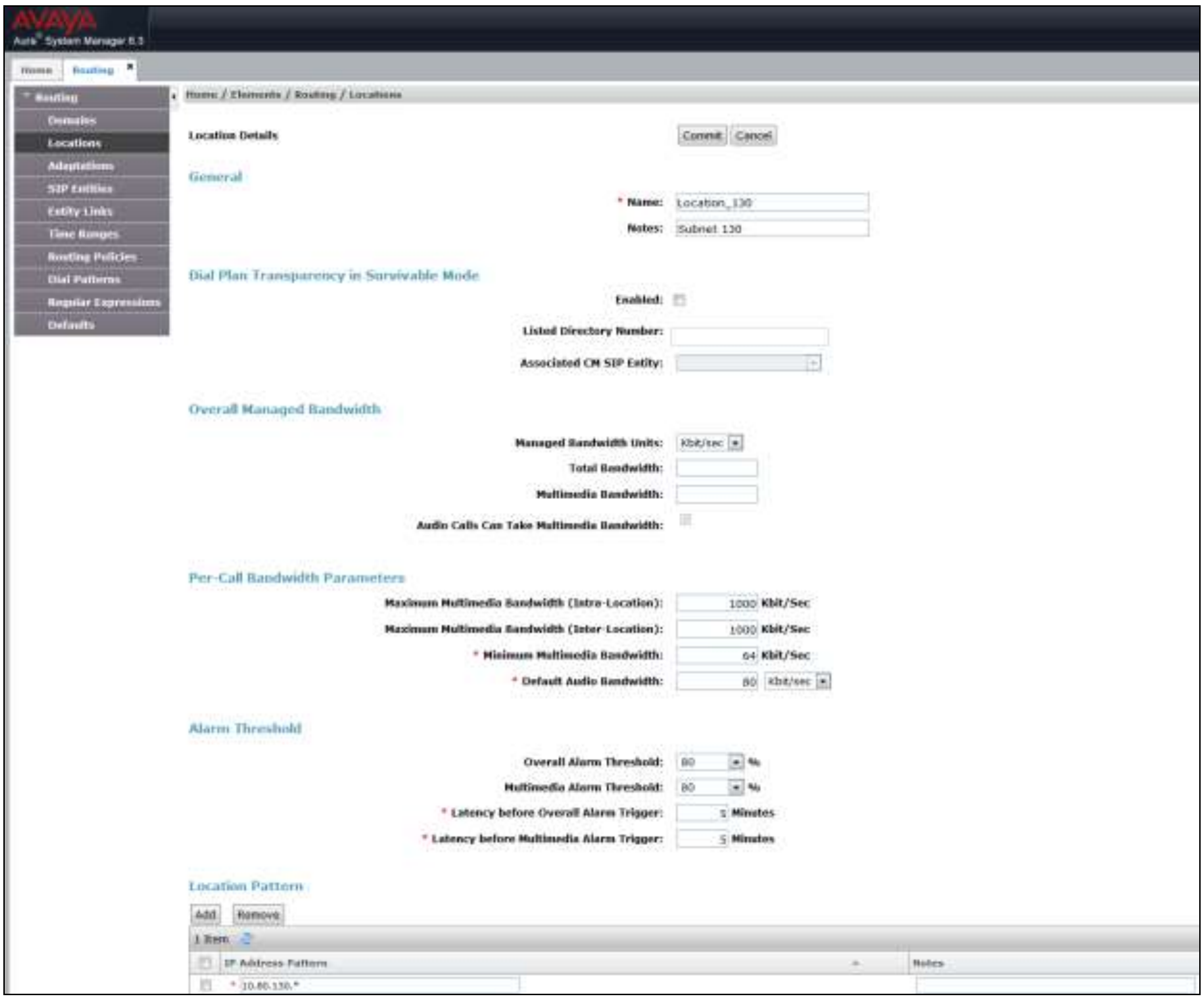
Under **General**:

- **Name**: Any descriptive name.
- **Notes**: Any Descriptive text (optional).

Under **Location Pattern**:

- **IP Address Pattern**: A pattern used to logically identify the location
- **Notes**: Any Descriptive text (optional)
- Click **Commit**

The screen below shows addition of the *Location_130* location for Communication Manager. Similarly a location was defined for Session Manager.



5.3. Add SIP Entities

In the sample configuration, a SIP Entity is added for Session Manager and Communication Manager. The screens below also show the corresponding Entity Links.

5.3.1. Session Manager Entity

Navigate to **Home→Elements→Routing→SIP Entities**, and click on the **New** (not shown) and configure as follows:

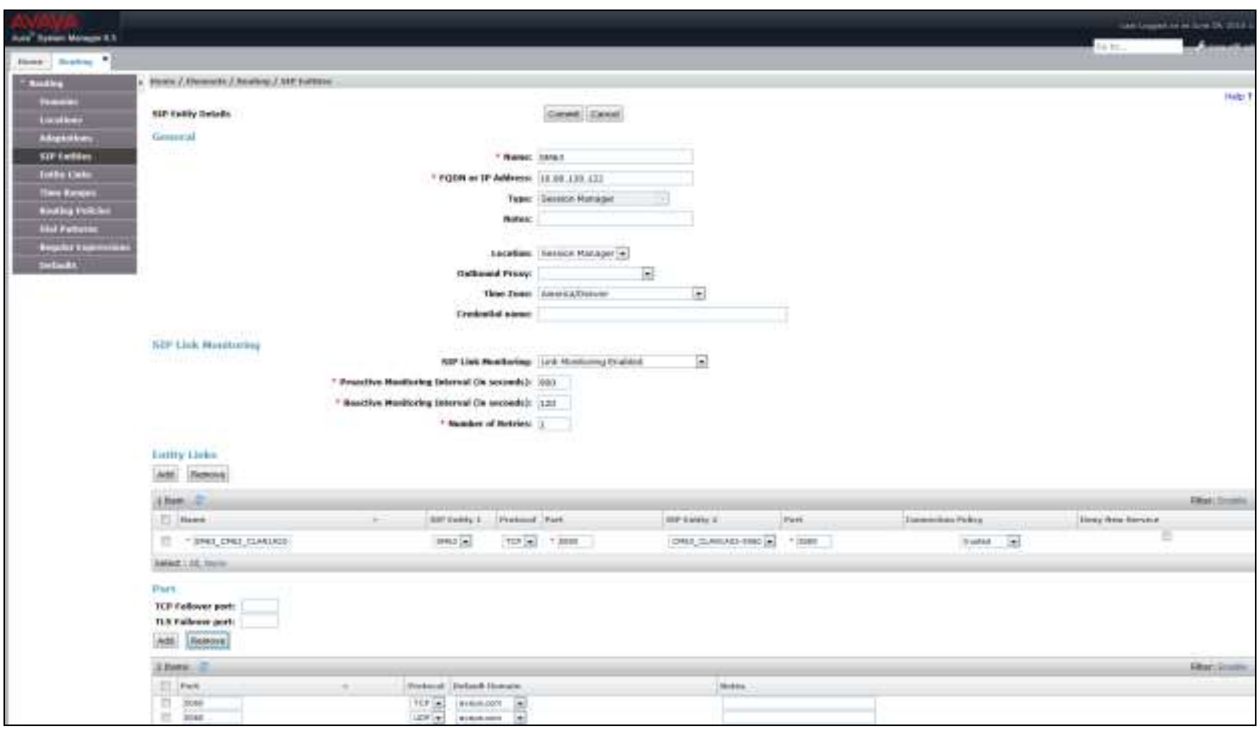
Under **General**:

- **Name**: Any descriptive name
- **FQDN or IP Address**: IP address of the signaling interface on Session Manager
- **Type**: Select *Session Manager*
- **Location**: Select one of the locations defined in **Section 5.2**
- **Time Zone**: Time zone for the current location

Under **Port**, click **Add**, and then edit the fields in the resulting new row as shown below:

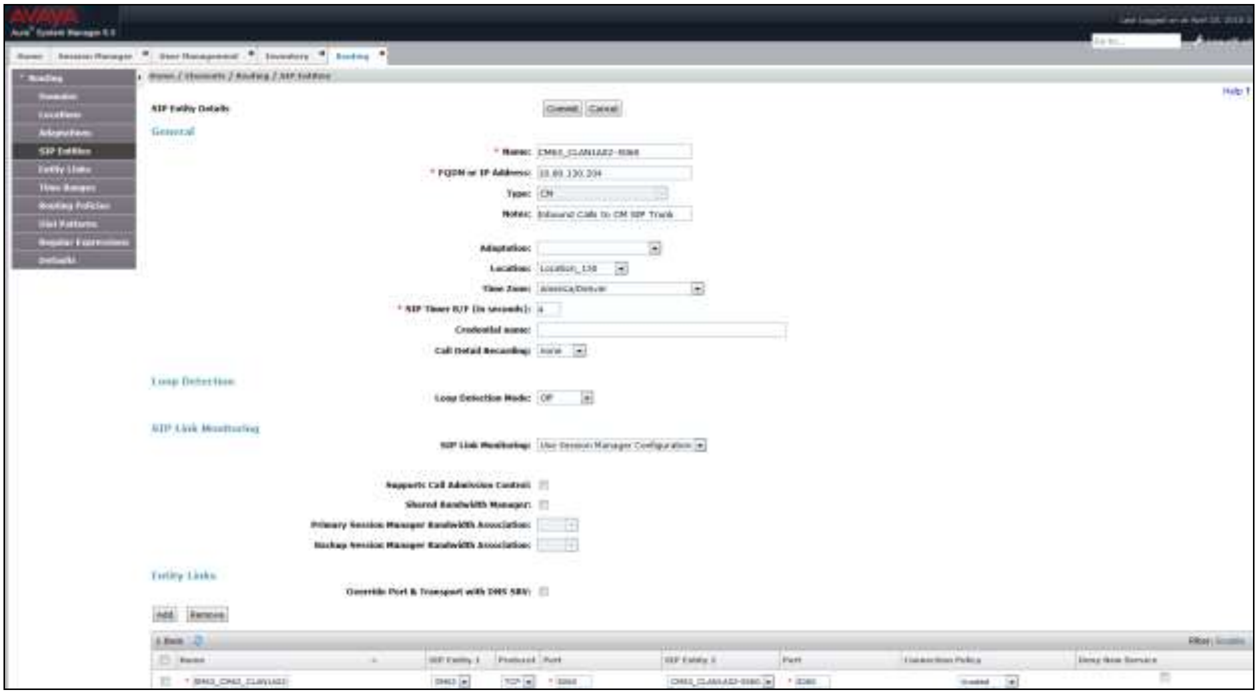
- **Port**: Port number on which the system listens for SIP requests
- **Protocol**: Transport protocol to be used to send SIP requests. Note that D2200IP SIP endpoint uses UDP
- **Default Domain**: The domain used for the enterprise (e.g. *avaya.com*)
- Click **Commit**

Note: D2200IP uses UDP for registration and therefore a UDP port is defined here to facilitate that process.



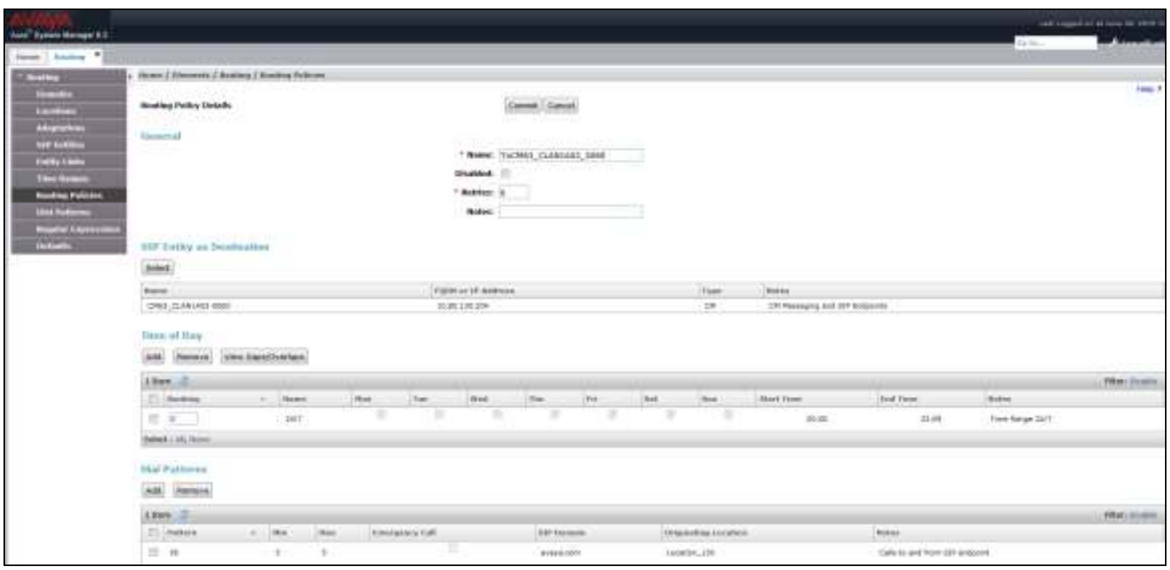
5.3.2. Communication Manager Entity

The following screen displays the Communication Manager entity configured for this reference configuration.



5.3.3. Adding a Route Policy

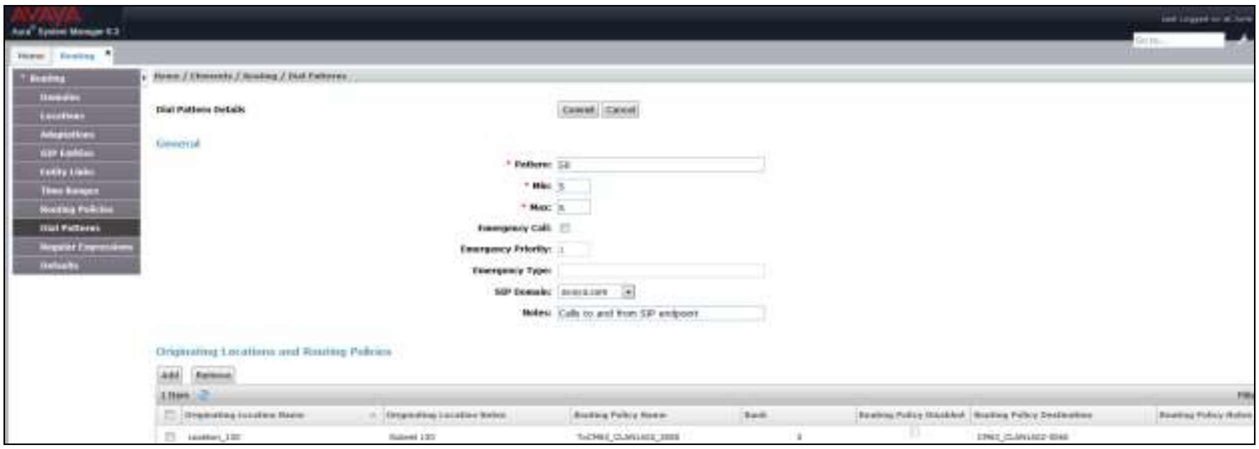
Navigate to **Home→Elements→Routing→Routing Policies**, and click on the **New** (not shown). The user needs to select an existing SIP Entity in the **SIP Entity as Destination** section in a popup window (not shown) and add a dial pattern in the **Dial Patterns** section in another popup window (not shown). In these application notes, the entity used for this Routing Policy is created in **Section 5.3.2** and the dial pattern is created **Section 5.3.4**. Similarly additional routing policies can be created for additional dial patterns and entities.



5.3.4. Adding a Dial Pattern

Navigate to **Home→Elements→Routing→Dial Patterns**, and click on the **New** (not shown) and configure as follows

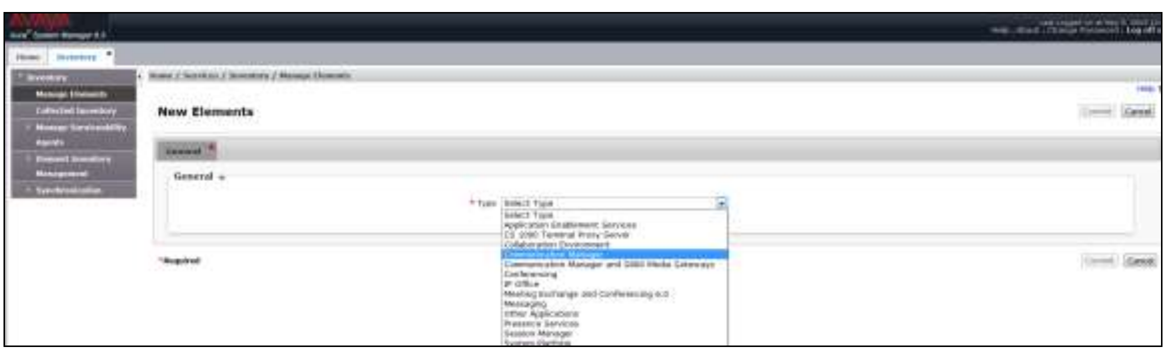
- **Pattern**: Set to any digits for proper routing of the call e.g **50**
- **Min/Max**: Set to the minimum and maximum value of the digit string to be matched
- **SIP Domain**: Set to the domain configured in **Section 5.1**
- In the **Originating Locations and Routing Policies** section, select the routing policy created in **Section 5.3.3** and the location create in **Section 5.2** in the popup window (not shown)



5.4. Define Communication Manager as a Managed Element

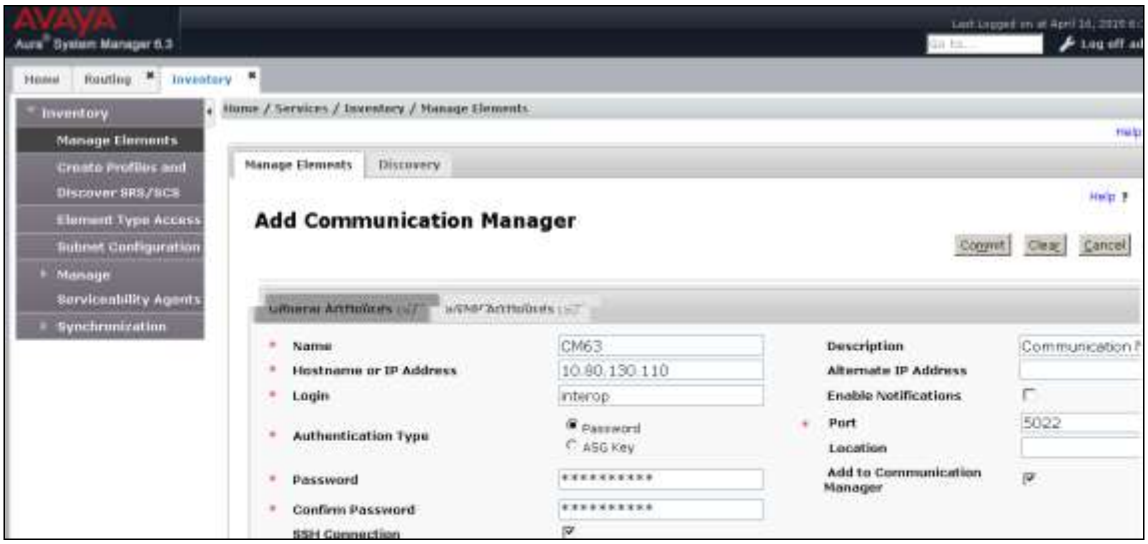
Before adding SIP users, Communication Manager must be added to System Manager as a managed element. This action allows System Manager to access Communication Manager over its administration interface. Using this administration interface, System Manager will notify Communication Manager when new SIP users are added.

To define Communication Manager as a managed element, navigate to **Home→Services→ Inventory→Manage Elements** on the left and click on the **New** (not shown) button on the right. In the **Type** field that is displayed, select *Communication Manager*.



In the **Add Communication Manager** screen, fill in the following fields as follows:
Under **General Attributes**:

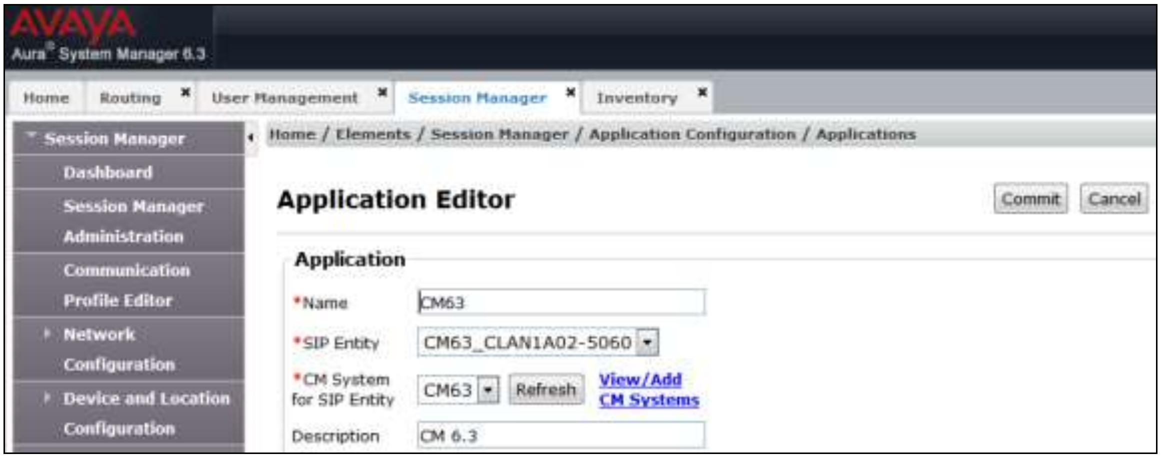
- **Name**: Enter an identifier for Communication Manager
- **Hostname or IP Address**: Enter the IP address of the administration interface for Communication Manager
- **Login**: Enter the login used for administration access to Communication Manager
- **Authentication Type**: Select the **Password** button
- **Password**: Enter a valid password
- **Confirm Password**: This should match the password entered in the **Password** field above
- Click **Commit**



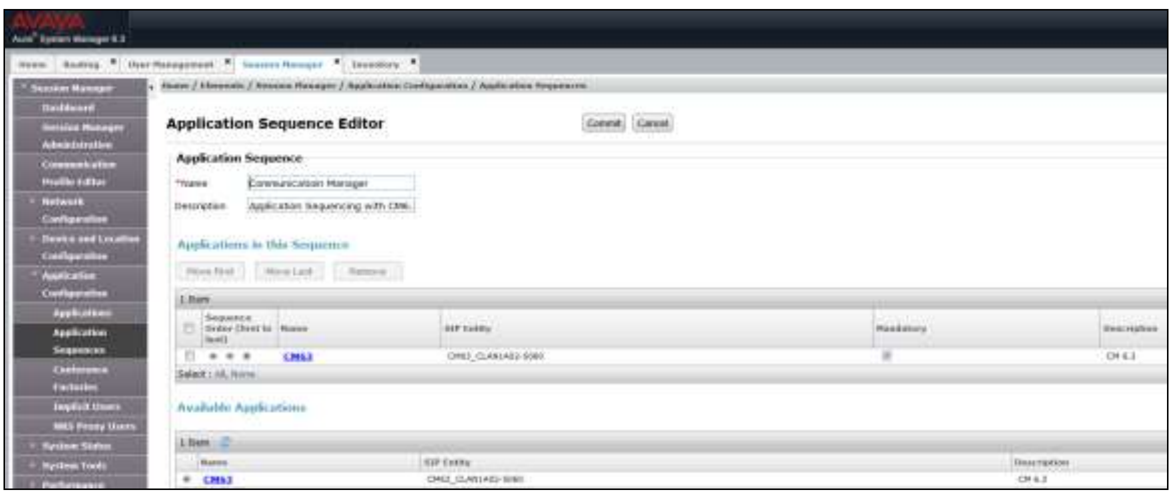
5.5. Add Application Sequence

Navigate to **Home→Elements→Session Manager→Application Configuration→Applications** and configure as follows:

- **Name**: Enter any descriptive name
- **SIP Entity**: Select the Communication Manager SIP Entity configured in **Section 5.3.2**
- **CM System for SIP Entity**: Select the system configured in **Section 5.4**
- Click **Commit**



Next, define the **Application Sequence** for Communication Manager as shown below.

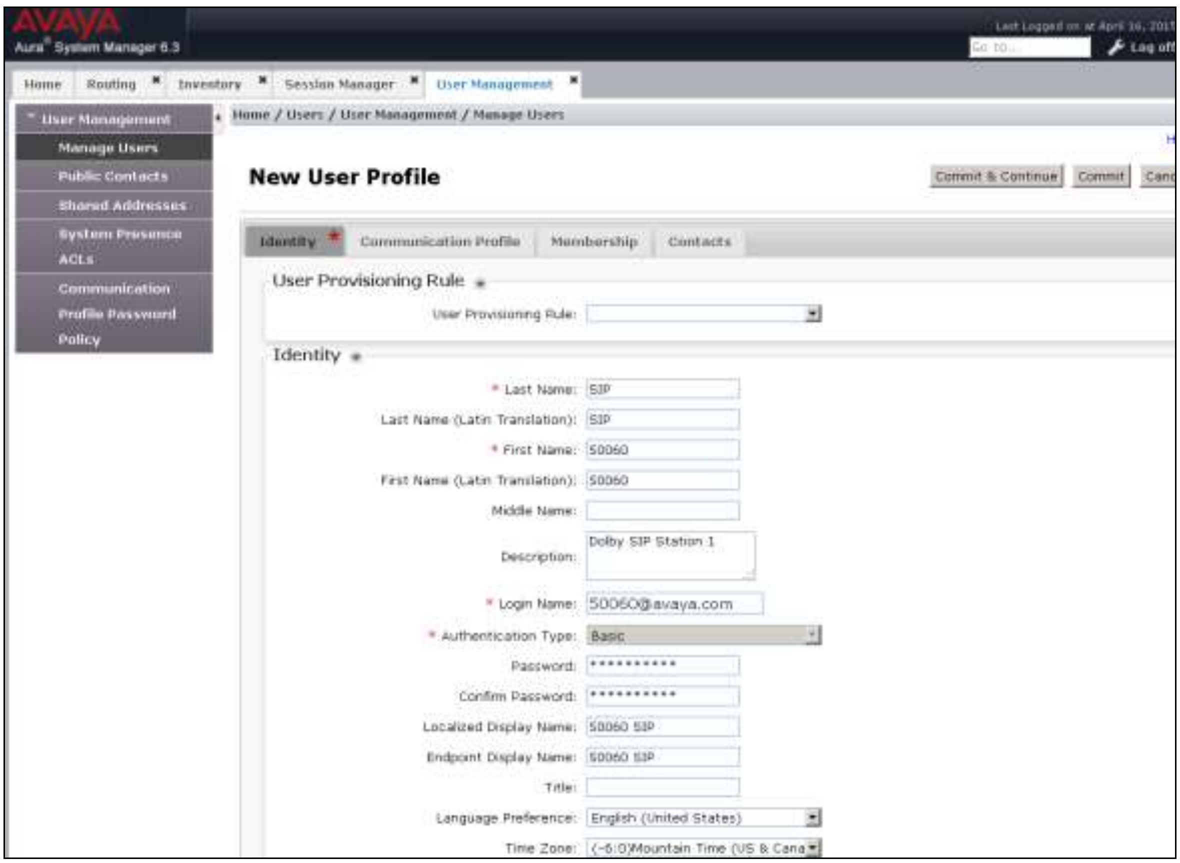


5.6. Add SIP Users

D2200IP was entered as a SIP user on Session Manager using the following steps. This configuration is automatically synchronized with Communication Manager as verified in **Section 6.3**.

Enter values for the following required attributes for a new SIP user in the **New User Profile** screen:

- **Last Name**: Enter the last name of the user
- **First Name**: Enter the first name of the user
- **Login Name**: Enter *<extension>@<sip domain>* of the user (e.g., *50060@avaya.com*)
- **Password**: Enter the password which will be used to log into System Manager
- **Confirm Password**: Re-enter the password from above



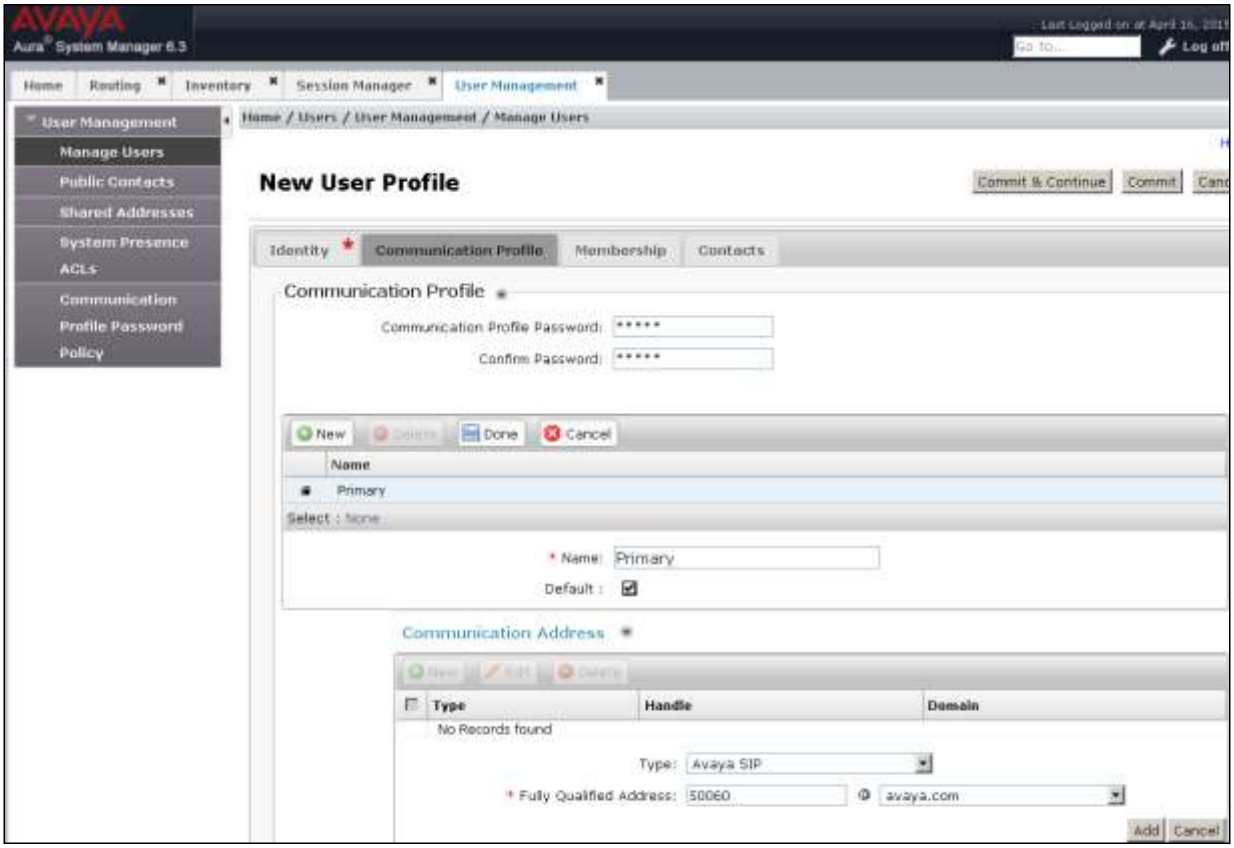
Click the **Communication Profile** tab and select **New** (not shown) to define a **Communication Profile** for a new SIP user and configure as follows:

- **Communication Profile Password**: Enter a valid password
- **Confirm Password**: Make sure that it matches the password entered above
- **Name**: Enter name of the communication profile
- **Default**: Check box to indicate that it is the default profile

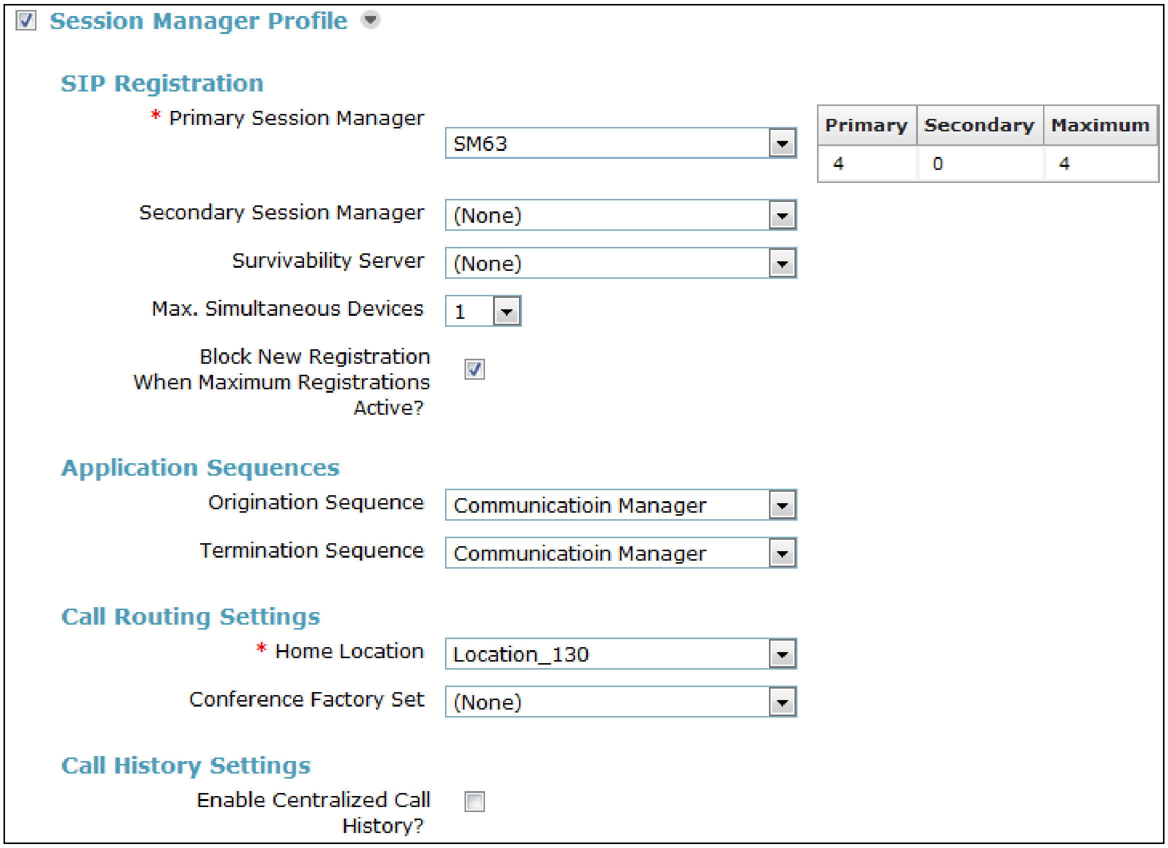
Click **New** to define a **Communication Address** for the new SIP user. Enter values for the following required fields:

- **Type**: Select *Avaya SIP*
- **Fully Qualified Address**: Enter extension number and SIP domain
- Click **Add**

The screen below shows the information when adding a new SIP user to the sample configuration.

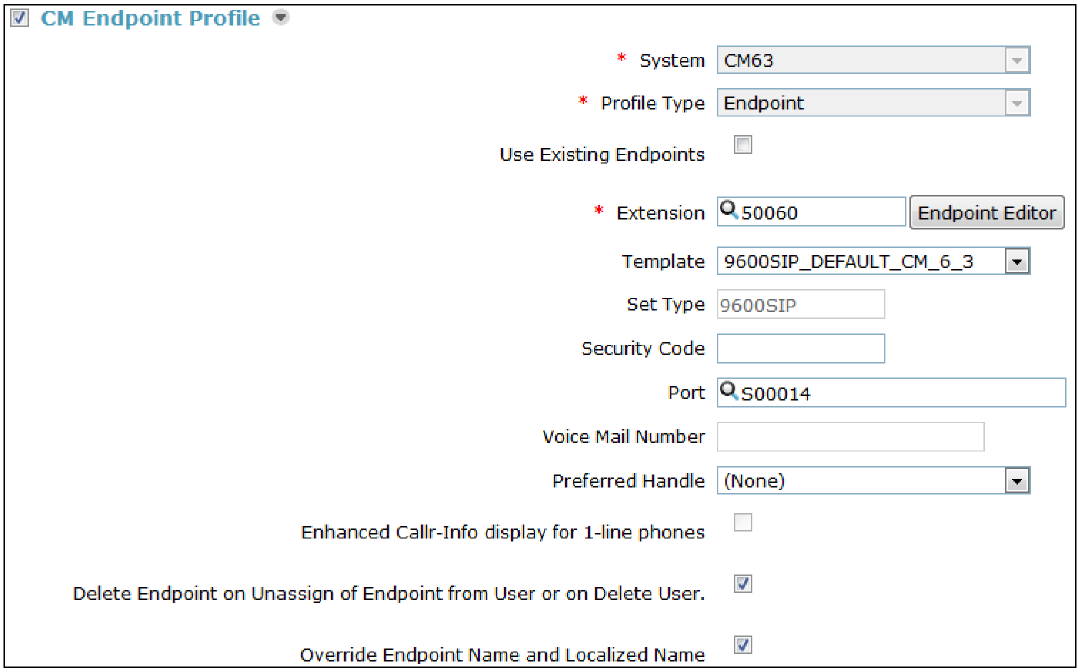


In the **Session Manager Profile** section, specify the Session Manager entity configured in **Section 5.3.1** and assign the **Application Sequence** defined in **Section 5.5** to both the **Originating Sequence** and **Termination Sequence** fields. Additionally, set **Home Location** field to **Location_130** configured in **Section 5.2**.



In the **CM Endpoint Profile** section, fill in the following fields:

- **System**: Select the managed element corresponding to Communication Manager in **Section 5.4**
- **Profile Type**: Select *Endpoint*
- **Use Existing Stations**: If field is not selected, the station will automatically be added in Communication Manager
- **Extension**: Enter extension number of SIP user
- **Template**: Select template for type of SIP phone which is set to **9600SIP_DEFAULT_CM_6_3** for **D2200IP**
- Click **Commit** (not shown)



6. Configure Avaya Aura® Communication Manager

This section describes the steps for configuring the D2200IP as an Off-PBX Station (OPS) and configuring a SIP trunk between Communication Manager and Session Manager. Use the System Access Terminal (SAT) to configure Communication Manager and log in with the appropriate credentials. These configuration steps illustrate only the field values changed for this reference configuration. Default values were used for all the other fields.

6.1. Verify OPS and SIP Trunk Capacity

Using the SAT, verify that the Off-PBX Telephones (OPS) and SIP Trunks features are enabled on the **system-parameters customer-options** form. The license file installed on the system controls these options. If a required feature is not enabled, contact an authorized Avaya sales representative. On **Page 1**, verify that the number of OPS stations allowed in the system is sufficient for the number of SIP endpoints that will be deployed.

```
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: 6400  25
                                      Maximum Stations: 2400  10
                              Maximum XMOBILE Stations: 2400  0
                    Maximum Off-PBX Telephones - EC500: 9600  0
                    Maximum Off-PBX Telephones -   OPS: 9600  5
                    Maximum Off-PBX Telephones - PBFMC: 9600  0
                    Maximum Off-PBX Telephones - PVFMC: 9600  0
                    Maximum Off-PBX Telephones - SCCAN: 0     0
                         Maximum Survivable Processors: 313   0

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

On **Page 2** of the **system-parameters customer-options** form, verify that the number of 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: 4000  0
           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  15
  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.)
```

6.2. Configure SIP Trunk

In the **IP Node Names** form, assign an IP address and host name for Session Manager (ASM63) and Communication Manager (CLAN_1A02). 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
    Name              IP Address
default             0.0.0.0
ASM63               10.80.130.122
CLAN_1A02           10.80.130.204
procr               10.80.130.110
procr6              ::

( 4 of 4   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
```

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 *avaya.com*. By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G650 Media Processor. The **IP Network Region** form also specifies the **Codec Set** to be used for calls routed over the SIP trunk to Session Manager. This codec set is used when its corresponding network region (i.e., IP Network Region *2*) is specified in the SIP signaling group.

```
change ip-network-region 2                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 2
Location: 1       Authoritative Domain: avaya.com
    Name: Main Network Region
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 2              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? 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
```

In the **IP Codec Set** form, select the audio codec type supported for calls routed over the SIP trunk to the D2200IP. The form is accessed via the **change ip-codec-set 2** command. Note that IP codec set **2** was specified in IP Network Region *2* shown above. The following form shows the list of codecs tested. The order of these codecs was changed to support the some of the codecs for reasons listed in **Section 2.2**.

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

                          IP Codec Set

    Codec Set: 2

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2: G.711A            n         2        20
 3: G.722-64K                   2        20
 4: iLBC                        1        20-30
 5: G.729A            n         1        20
 6:
 7:
```

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the Signaling Group form as follows:

- Set the **Group Type** field to *sip*
- Set the **IMS Enabled** field to *n*
- The **Transport Method** field was set to *tcp*
- Specify the C-LAN board and the Session Manager as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These field values are taken from the **IP Node Names** form in the beginning of this section
- Ensure that the recommended TCP port value of *5060* is configured for the **Near-end Listen Port** and the **Far-end Listen Port** fields
- 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 Session Manager in the **Far-end Domain** field. In this configuration, the domain name is *avaya.com*
- Set **Direct IP-IP Audio Connections** field to *y*
- Verify that **DTMF over IP** field is set to the default value of *rtp-payload*. Communication Manager supports DTMF transmission using RFC 2833

```
add signaling-group 2                                          Page   1 of   1
                                 SIGNALING GROUP

Group Number: 2             Group Type: sip
  IMS Enabled? n        Transport Method: tcp
        Q-SIP? n
     IP Video? n                                   Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n


   Near-end Node Name: CLAN_1A02              Far-end Node Name: ASM63
 Near-end Listen Port: 5060                 Far-end Listen Port: 5060
                                         Far-end Network Region: 2
                                    Far-end Secondary Node Name:
Far-end Domain: avaya.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                 RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? 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
```

Configure the **Trunk Group** form as shown below. This trunk group is used for calls to the SIP Phones. Set the **Group Type** field to *sip*, set the **Service Type** field to *tie*, specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Configure the other fields in bold and accept the default values for the remaining fields.

```
add trunk-group 2                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 2                    Group Type: sip          CDR Reports: y
  Group Name: SIP Endpoints/CM Messaging  COR: 1        TN: 1        TAC: 102
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                             Member Assignment Method: auto
                                                      Signaling Group: 2
                                                    Number of Members: 15
```

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 2                                           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

                                Modify Tandem Calling Number: no
 Show ANSWERED BY on Display? y
 DSN Term? n
```

Configure the **Private Numbering Format** form to send the calling party number to the far-end. Add an entry so that call from a 5-digit local extension beginning with *5* is routed using SIP trunk group *2*, and the number is 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  33               10                          5     Total Administered: 4
 5  58               10                          5        Maximum Entries: 540
 5  5                2                           5
 5  600              10                          5
```

6.3. Verify SIP Stations

Use the **display station** command to view each D2200IP SIP endpoint configured in **Section 5.6**.

```
display station 50060                                          Page   1 of   6
                                     STATION

Extension: 40012                        Lock Messages? n               BCC: 0
     Type: 9620SIP                      Security Code:                  TN: 1
     Port: S00003                     Coverage Path 1: 1               COR: 1
     Name: 50060 SIP                  Coverage Path 2:                 COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
              Loss Group: 19
                                                Message Lamp Ext: 40012

        Display Language: english

          Survivable COR: internal
   Survivable Trunk Dest? y                         IP SoftPhone? n

                                                        IP Video? n
```

Use the **display off-pbx-telephone station-mapping** to verify proper entry of D2200IP SIP station in Communication Manager.

```
display off-pbx-telephone station-mapping 50060                Page   1 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Application Dial   CC  Phone Number    Trunk       Config  Dual
 Extension                 Prefix                     Selection   Set     Mode
 50060            OPS           -       50060          aar        1
```

On **Page 2**, verify that the **Call Limit** matches the number of *call-appr* entries in the station form.

```
display off-pbx-telephone station-mapping 50060                Page   2 of   3
                  STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

 Station       Appl    Call        Mapping    Calls       Bridged       Location
 Extension     Name    Limit       Mode       Allowed     Calls
 50060         OPS     3           both       all         none
```

7. Configure Med-Pat D2200IP

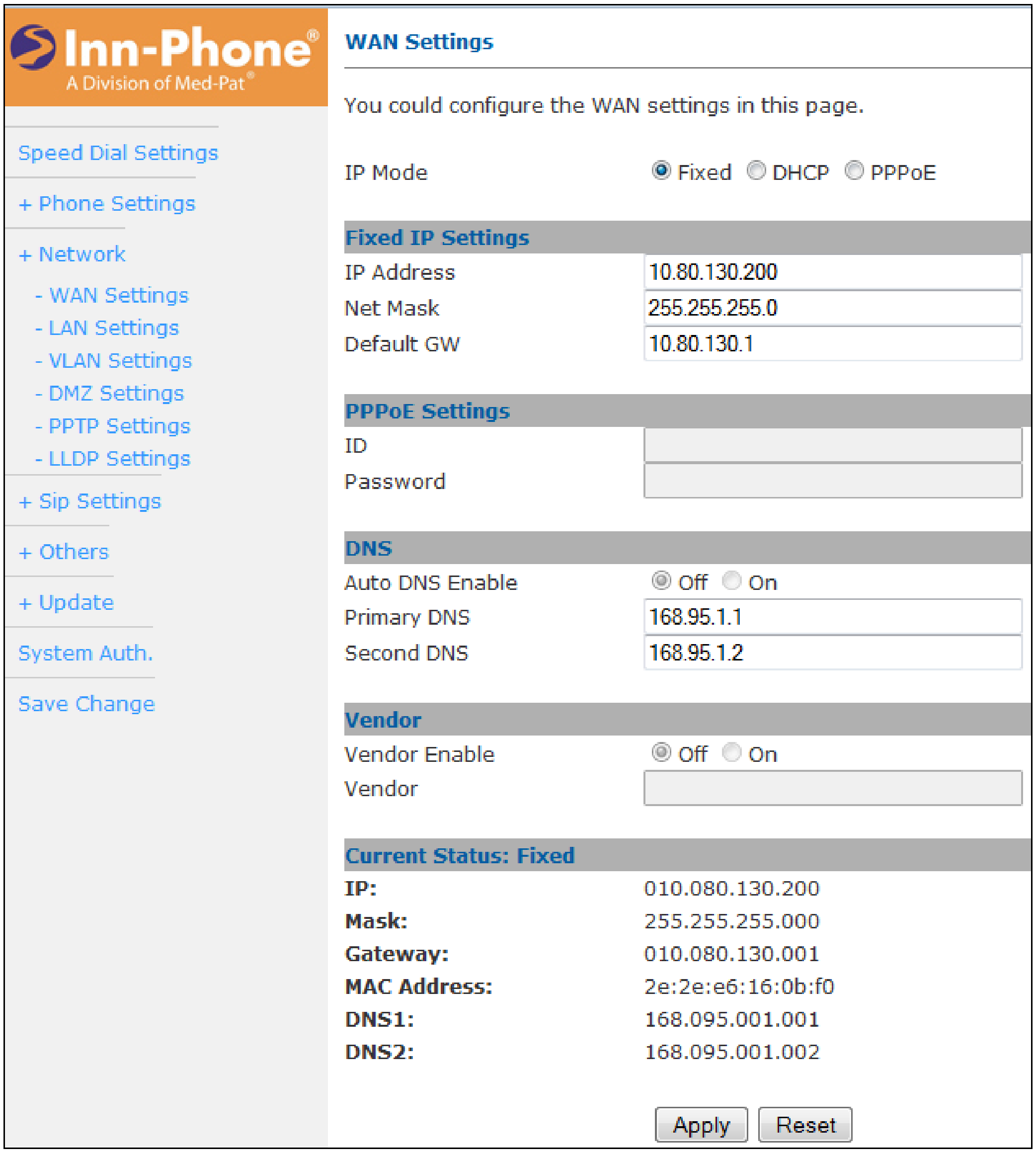
This section provides the steps for configuring the D2200IP. **Note** that D2200IP only uses **UDP** for registration and a corresponding UDP port was configured in **Section 5.3.1** for this purpose. The following configuration steps illustrate the field values changed for this reference configuration. Defaults were used for all the other fields.

- Configure IP Address of D2200IP
- Launch Web Interface
- Verify/Modify Port Settings
- Modify Codec Settings
- Modify Other Settings

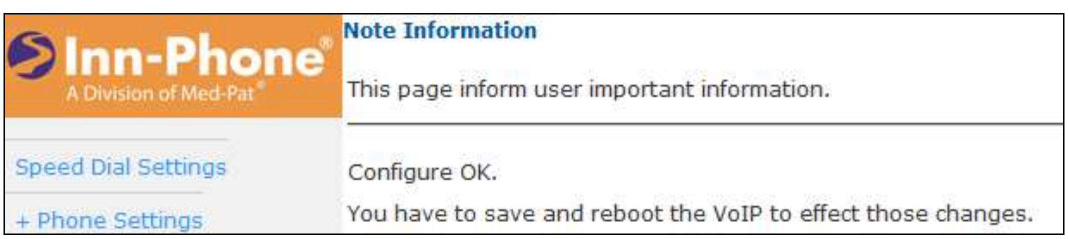
7.1. Configure IP Address of D2200IP

- Connect the WAN port of the D2200IP to a Power over Ethernet (PoE) switch
- Connect the LAN port to any desktop which has a default address of **192.168.2.1**
- Change the IP address on the desktop to an IP address matching the **192.168.2.*** range
- Access the URL for the D2200IP phone from the desktop as shown below and login

- Navigate to **Network→WAN Settings** and set the **IP Address**, **Net Mask** and **Default GW** fields as shown below and click **Apply**.



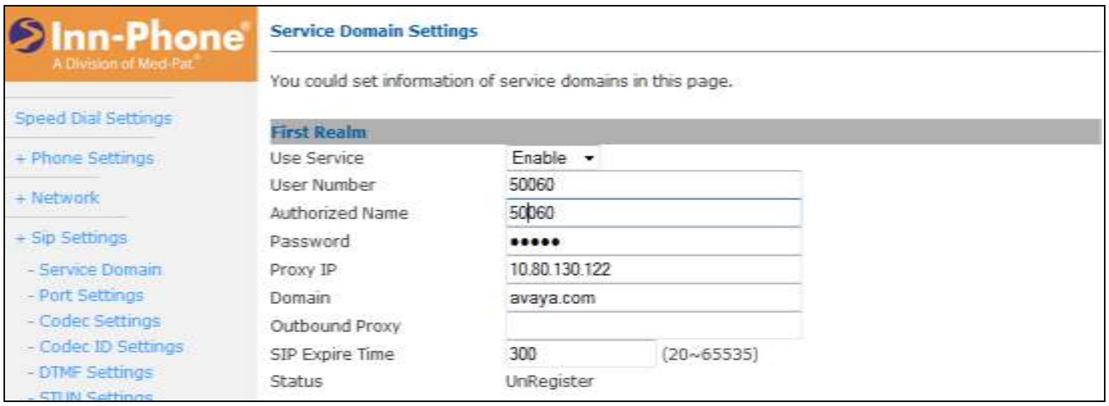
- The following screen appears. Click on **Save Change** and user will be prompted to **Reboot** (now shown)



7.2. Launch Web Interface

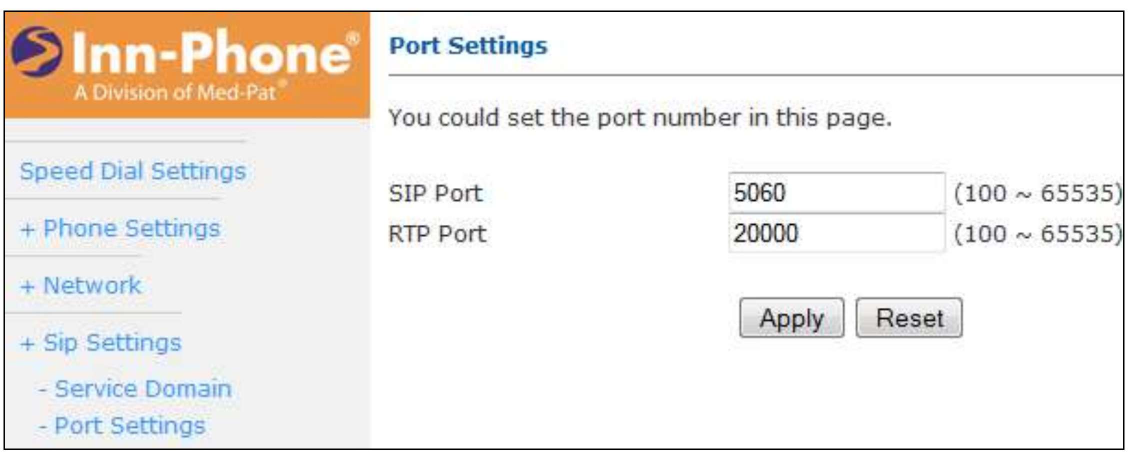
After the system reboots, access the D2200IP using the WAN port configured in **Section 7.1** and navigate to **Sip Settings→Service Domain** and configure as follows:

- **Use Service** – Set **Enable**
- **User Number** – Set to the extension configured in **Section 5.6**
- **Authorized Name** - Set to the extension configured in **Section 5.6**
- **Password** – Set to the same value as **Communication Profile password** created in **Section 5.6**
- **Proxy IP** – Set to the IP address of the Session Manager Signaling interface from **Section 5.3.1**
- **Domain** – Set to domain name configured in **Section 5.1**
- Click **Apply** (not shown)



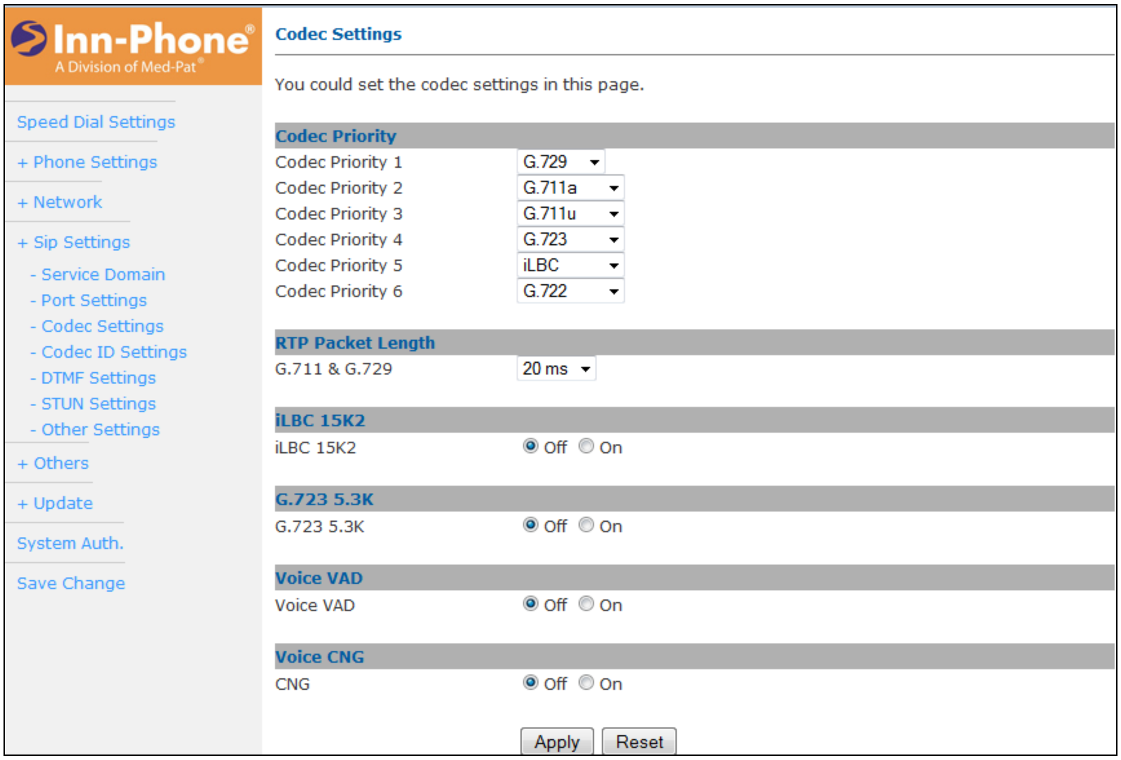
7.3. Verify/Modify Port Settings

Navigate to **SIP Settings→Port Settings** from the menu on the left and verify/enter the following values for the specified fields and click **Apply**.



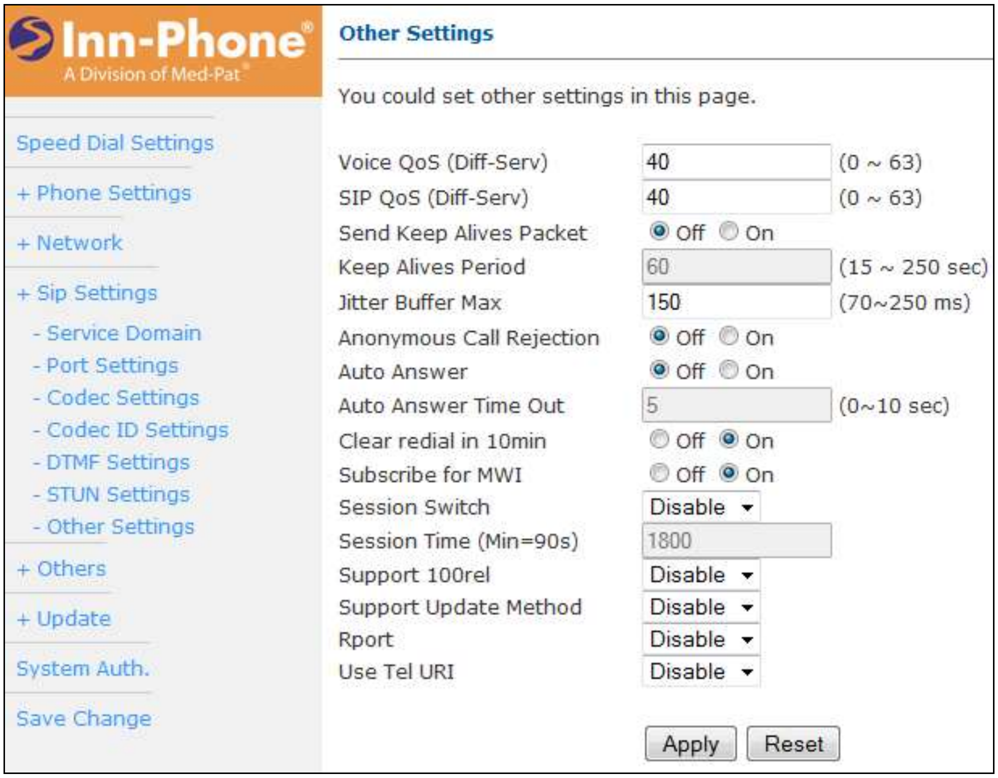
7.4. Modify Codec Settings

Navigate to **SIP Settings→Codec Settings** from the menu on the left and modify the priority order of codecs as desired and click **Apply**.



7.5. Modify Other Settings

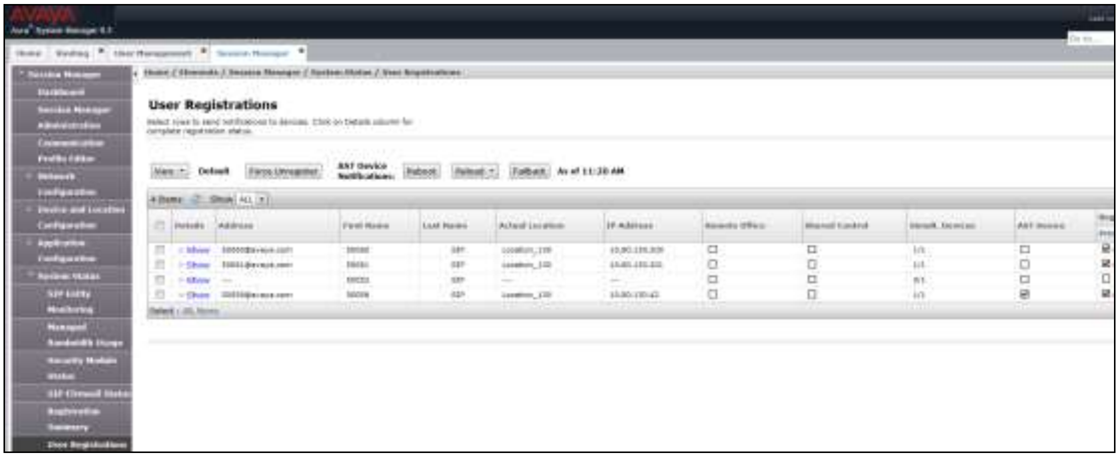
Navigate to **SIP Settings→Other Settings** from the menu on the left and set **Rport** to **Disable** and click **Apply**.



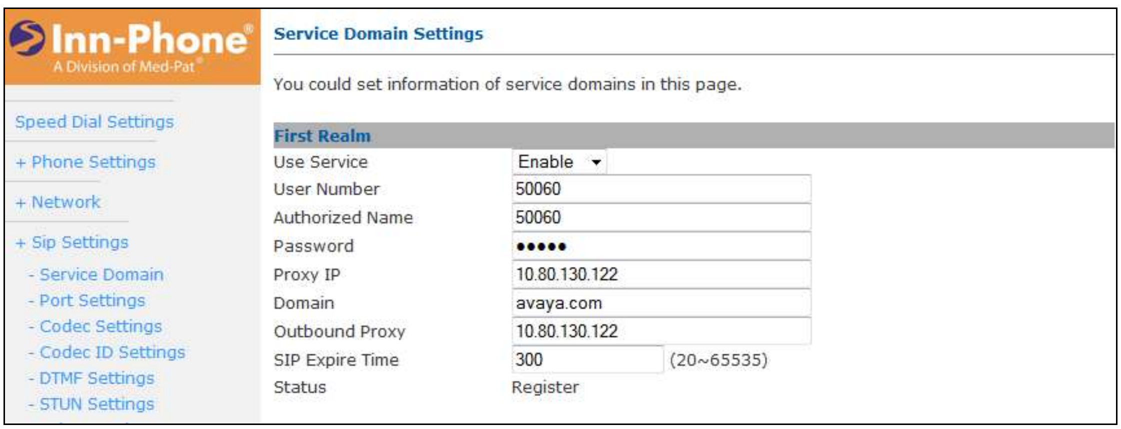
8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Session Manager and Communication Manager with D2200IP.

- Verify that D2200IP (**50060** and **50061**) is registered with Session Manager. The following screen shows the registered SIP users with their corresponding IP Address:



- The following screen shows that D2200IP is successfully registered with Session Manager. If the registration was not successful, the **Status** field is set to **UnRegister**



- Verify that basic calls can be made from and to D2200IP and another telephone registered with Communication Manager.

9. Conclusion

These Application Notes describe the configuration steps required for Med-Pat D2200IP SIP twin handset telephone to successfully interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager. All feature and serviceability test cases were completed with exceptions noted in **Section 2.2**.

10. Additional References

This section references the product documentation available at support.avaya.com relevant to these Application Notes.

1. Administering Avaya Aura® Session Manager, Release 6.3, Issue 7, September 2014
2. Maintaining and Troubleshooting Avaya Aura® Session Manager, Release 6.3, Issue 7, March 2015
3. Administering Avaya Aura® System Manager, Release 6.3, Issue 8, July 2015
4. Administering Avaya Aura® Communication Manager, Issue 10, August 2015