Avaya Solution & Interoperability Test Lab

Avaya Aura™ Session Manager Survivable SIP Gateway Solution using the Juniper SRX210 Services Gateway in a Distributed Trunking Configuration – Issue 1.0

Abstract

These Application Notes present a sample configuration of the Avaya Aura™ Session Manager 5.2.1.1 Survivable SIP Gateway Solution using the Juniper SRX210 Services Gateway in a Distributed Trunking configuration.

This solution addresses the risk of service disruption for SIP endpoints deployed at remote branch locations if connectivity to the Avaya SIP call control platform (i.e. Avaya Aura™ Session Manager) located at the main site is lost. Connectivity loss can be caused by WAN access problems being experienced at the branch or by network problems at the main site blocking access to the Avaya SIP call control platform, or by Avaya Aura™ Session Manager going out of service.

The Avaya Aura™ Session Manager Survivable SIP Gateway Solution monitors the connectivity health from the remote branch to the Avaya SIP call control platform at the main site. When connectivity loss is detected, the Avaya one-X™ Deskphone SIP 9600 Series IP Telephones at the branch, as well as the Juniper SRX210 Services Gateway, dynamically switch to Survivability Mode, restoring telephony services to the branch for intra-branch and PSTN calling.

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 present a sample configuration of the Avaya Aura™ Session Manager 5.2.1.1 Survivable SIP Gateway Solution using the Juniper SRX210 SIP Services Gateway in a Distributed Trunking configuration.

SIP endpoints deployed at remote branch locations risk a loss of service if a break in connectivity to the SIP call control platform (i.e. Avaya Aura™ Session Manager) at the main site occurs. Connectivity loss can be caused by WAN access problems being experienced at the branch or by network problems at the main site blocking access to the Avaya SIP call control platform, or by Avaya Aura™ Session Manager going out of service. The survivable SIP gateway solution monitors connectivity health from the remote branch to the Avaya SIP call control platform at the main site. When connectivity loss is detected, SIP endpoints and SIP gateway components within the branch dynamically switch to survivability mode restoring basic telephony services to the branch for intra-branch and PSTN calling. When connectivity from the branch to the Avaya SIP call control platform at the main site is restored, SIP components in the branch dynamically switch back to normal operations.

The primary components of this solution are the Avaya one-X™ Deskphone SIP 9600 Series IP Telephones, the Juniper SRX210 Services Gateway, as well as Avaya Aura™ Session Manager, which provides the centralized SIP control platform with SIP registrar and proxy functions in Normal Mode. The sample configuration shown in these Application Notes utilizes the Juniper Services Gateway model SRX210; however, these configuration steps can also be applied to the Juniper SRX240 Services Gateway using the Juniper firmware version specified in **Section 3**.

1.1. Interoperability Testing

The interoperability testing focused on the dynamic switch from Normal Mode (where the network connectivity between the main site and the branch site is intact) to Survivable Mode (where the network connectivity between the main site and the branch site is broken) and vice versa. The testing also verified interoperability between the Avaya 9600 Series SIP Phones and the Juniper SRX210 Services Gateway in Survivable Mode.

1.1.1. Avaya Aura™ Session Manager and Avaya Aura ™ Communication Manager

The Avaya Aura™ Session Manger is a routing hub for SIP calls among connected SIP telephony system components. The Avaya Aura™ System Manager provides management functions for the Avaya Aura™ Session Manager. Starting with release 5.2, Avaya Aura™ Session Manager also includes onboard SIP Registrar and Proxy functionality for SIP call control. In the test configuration, all Avaya 9600 Series SIP Phones at the central location register to the Avaya Aura™ Session Manager. All Avaya 9600 Series SIP Phones at the branch site register simultaneously to the Avaya Aura™ Session Manager at the main location and the Juniper SRX210 Services Gateway at the branch. The Avaya Aura™ Session Manager provides centralized SIP call control in Normal Mode; the branch Juniper SRX210 provides local SIP control in Survivable Mode. In Normal Mode, the phone calling features are supported by Avaya

Aura™ Communication Manager, which serves as a Feature Server within the Avaya Aura™ architecture. The Avaya 9600 Series SIP Phones are configured on Communication Manger as Off-PBX-Stations (OPS) and acquire advanced call features from Avaya Aura™ Communication Manger.

1.1.2. Juniper SRX210 Services Gateway

The Juniper SRX210 Services Gateway, referred to as Juniper SRX210 (or SRX210) throughout the remainder of this document, takes on various roles based on call flows and network conditions. The following lists these roles:

- SIP PSTN Media Gateway (FXO / T1 interfaces to PSTN)
- SIP Analog Terminal Adapter (FXS interfaces to analog endpoints)
- SIP Registrar and Proxy (dynamically activated on detection of lost connectivity to the SIP control platform at the main site)
- SIP Trunk Edge Point

The SRX210 includes on-board IP router functionality with PoE (Power on Ethernet). With 1 IP port used for the WAN connection, there are 7 ports remaining for direct connections to branch IP phones and/or other IP devices. The SRX210 also provides 2 FXS ports (for analog phone connections) and 2 FXO ports (for analog line connections to the PSTN).

1.1.3. Avaya one-X™ Deskphone SIP 9600 Series IP Telephone

The Avaya one-X™ Deskphone SIP 9600 Series IP Telephone, referred to as Avaya 9600 SIP Phone throughout the remainder of this document, is a key component of the survivable SIP gateway solution. The 2.5 firmware release of the Avaya 9600 SIP Phone tested with the sample configuration includes feature capabilities specific to SIP survivability, enabling the phone to monitor connectivity to Avaya Aura™ Session Manager and dynamically failover to the local Juniper SRX210 as a survivable SIP server. See reference **[7]** for additional information on the Avaya 9600 SIP Phone.

1.1.4. Network Modes

Normal Mode: In Normal Mode, the branch has WAN connectivity to the main site and the Avaya SIP call control platform is being used for all branch calls.

Survivable Mode: In Survivable Mode, the branch has lost WAN connectivity to the main site. The local branch Juniper SRX210 is used for all calls at that branch. Note that if the Avaya Aura™ Session Manager, which provides the centralized SIP call control, loses connectivity to the WAN, all branches will go into Survivable Mode simultaneously.

1.1.5. PSTN Trunking Configurations

The Avaya Aura™ Session Manager Survivable SIP Gateway Solution can interface with the PSTN in either a Centralized Trunking or a Distributed Trunking configuration. These trunking options determine how branch calls to and from the PSTN will be routed over the corporate network. Consider an enterprise consisting of a main Headquarters/Datacenter location and multiple branch locations that are all inter-connected over a corporate WAN. The following descriptions define Centralized Trunking and Distributed Trunking as related to this survivable SIP gateway solution:

Centralized Trunking: In Normal Mode, all PSTN calls, inbound to the enterprise and outbound from the enterprise, are routed from/to the PSTN connection configured on the Avaya Media Gateway (located at the main site). In Survivable Mode, PSTN calls to/from the branch phones are routed through the analog trunks from the Service Provider connected to the FXO interface ports on the branch Juniper SRX210 Services Gateway.

Distributed Trunking: Outgoing PSTN calls are routed based on the originating source location via Avaya Aura™ Session Manager. Local calls from branch locations are routed back to the same branch location and terminate on the FXO interface of the local Juniper SRX210 Services Gateway. This solution has the potential benefits of saving bandwidth on the branch access network, off-loading the WAN and centralized media gateway resources, avoiding Toll Charges, and reducing latency.

Note that with the sample configuration:

1. In both Normal and Survivable Mode, 911 emergency calls from the branch should always be routed through the FXO interfaces on the branch SRX210 to the local Emergency Response Center (regardless of whether Centralized or Distributed Trunking is being used).

2. In both Centralized Trunking and Distributed Trunking configurations, routing of DID (Direct Inward Dialing) calls from the PSTN to the FXO interfaces on the branch SRX210 is determined by the network mode that the branch is currently operating in:
   - If the branch is in Normal Mode, the DID call will be routed to the Headquarters for further routing decisions. The DID call can terminate either to a Headquarters phone or to a branch phone depending on further digits collected from the calling party.
   - If the branch is in Survivable Mode, the DID call will be terminated to the Auto-Attendant on the SRX210 for onward routing to branch phones on user-provided branch extension numbers.

The two trunking configurations share mostly the same configuration procedures on Avaya Aura™ Communication Manager, Avaya Aura™ Sessions Manager, and the Juniper SRX210. The configuration procedures in this document implement the Distributed Trunking configuration.

1.2. Support

For technical support on the Juniper SRX210, contact Juniper Networks via the support web site http://www.juniper.net/customers/support.

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. In the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support. Customers may also use specific numbers provided on http://support.avaya.com to directly access specific support and consultation services based upon their Avaya support agreements.

2. Reference Configuration

The network implemented for the sample configuration shown in **Figure 1** is modeled after an enterprise consisting of a main Headquarters/Datacenter location and multiple branch locations all inter-connected over a corporate WAN. One sample branch configuration was documented in the ensuing sections of these Application Notes.

The Headquarters location hosts a Session Manager (with its companion System Manager) providing enterprise-wide SIP call control, a Communication Manager as a Feature Server (with an Avaya G430 Media Gateway) providing advanced feature capabilities to Avaya 9600 SIP Phones, and another Communication Manager as an Access Element (with an Avaya G450 Media Gateway) providing trunks to the PSTN. Avaya Modular Messaging is also located at the Headquarters location to provide the voice mail messaging service. In addition, the Headquarters location hosts an Avaya IP Phone Configuration File Server for Avaya 9600 SIP Phones to download configuration information. Session Manager, System Manager, Communication Manager (Feature Server), and Modular Messaging, are connected to the 10.64.20.0/24 subnet. The phone configuration file server, Communication Manager (Access Element), and the Avaya 9600 SIP Phones are connected to the 10.62.21.0/24 subnet.

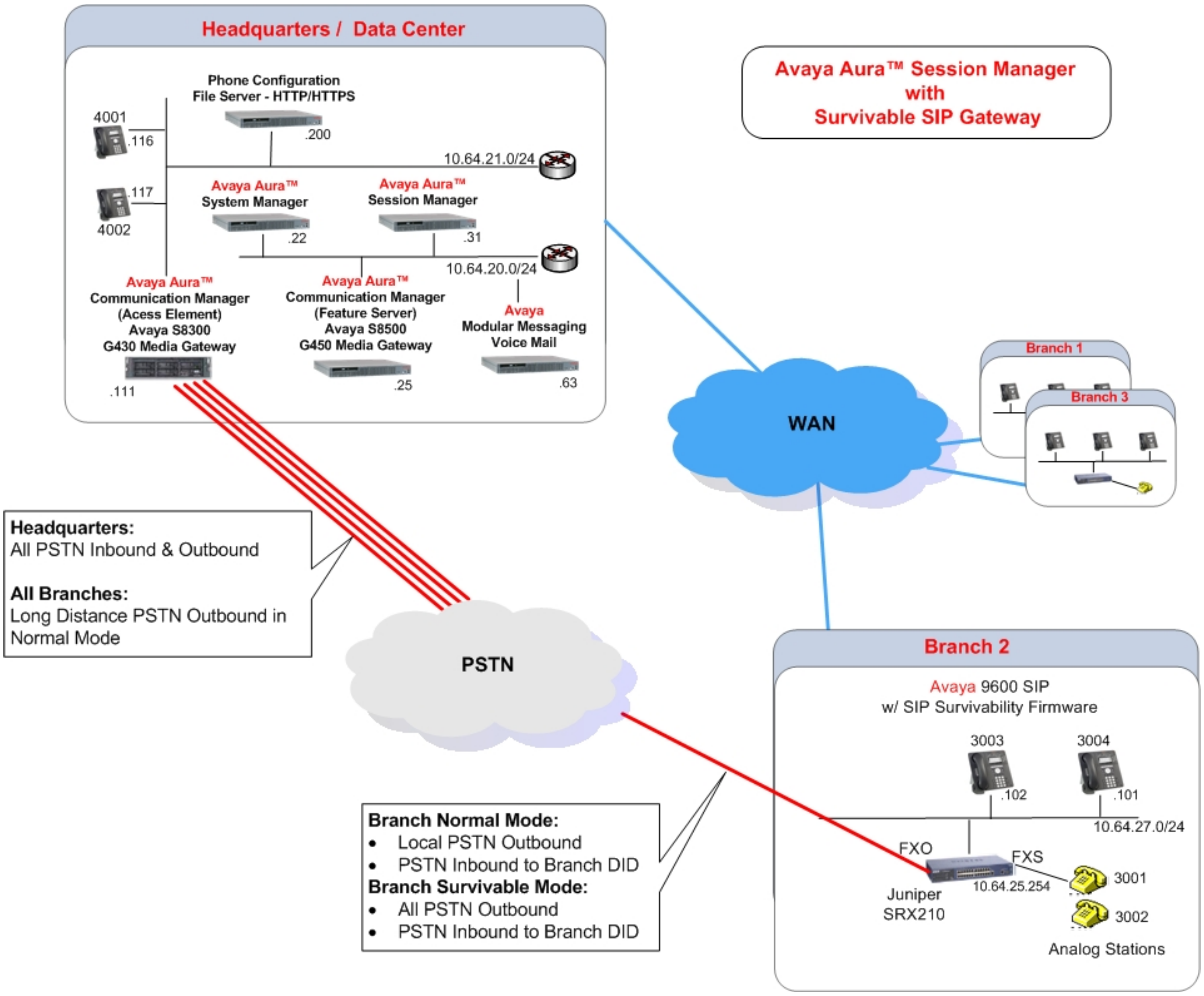


Figure 1 – Network Diagram

The configuration details of the phone configuration file server as well as Modular Messaging are considered outside the scope of these Application Notes and are therefore not included.

The Avaya IP Phone Configuration File Server contains a 46xxsettings.txt file used by Avaya IP phones to set values of the phone configuration parameters. **Section 6** includes the parameters of the 46xxsettings.txt file used by the Avaya 9600 SIP Phones for survivability. Modular Messaging can be reached by dialing the internal extension configured as the voice mail access number, or by dialing a PSTN number that also terminates to the voice messaging application. The internal extension is configured in the 46xxsettings.txt file as the default voice mail access number to dial when the Message button of the Avaya 9600 SIP Phone is pressed while the phone is in Normal Mode. The external PSTN number is configured in the 46xxsettings.txt file as an alternate voice mail access number to dial when the Message button of the Avaya 9600 SIP Phone is pressed while the branch phone is in Survivable Mode. This enables branch users to continue to access the centralized voice mail service while in Survivable Mode.

The branch locations consist of two Avaya 9600 SIP Phones, a Juniper SRX210 Services Gateway with PSTN analog trunks connected to the FXO interface ports, and two analog phones on the FXS interfaces.

Note that there are two Communication Managers in the test configuration. One serves as a Feature Server and one serves as an Access Element. Release 5.x of Session Manager and Communication Manager does not support inter-working between SIP phones and non-SIP phones (H.323 and other Avaya digital and/or analog telephone sets) configured on the same Communication Manager[1]. This restriction was lifted in Release 6 of Session Manager and Communication Manager (Release 6 was not yet Generally Available at the time of compliance testing). In the sample configuration, all phones at both the main and branch sites are SIP phones (branch analog sets are adapted by the Juniper SRX210 as SIP phones too).

[1] See reference **[10]** for application notes on configuring Communication Manager as an Access Element to support H.323 and digital / analog telephones.

The configuration details throughout this document utilize the network information as listed in **Table 1**.

IP Network	**IP Network Region** on Communication Manager	**Location** on Session Manager	**Area Code**	**Juniper SRX210 IP Address**
10.64.20.0/24 10.64.21.0/24	1	10.64.20/21.0	303	
10.64.25.0/24 10.64.26.0/24 10.64.27.0/24	1	Juniper SRX210	732	10.64.25.254 (assigned to port 7 to provide connectivity to the WAN)

Table 1 – Network Information

3. Equipment and Software Validated

The following components were used for the sample configuration:

Component	Software/Firmware
Avaya S8800 Server	Avaya Aura™ Session Manager 5.2.1.1
Avaya S8800 Server	Avaya Aura™ System Manager 5.2.1.1,
Avaya S8800 Server with an Avaya G430 Media Gateway (Feature Server)	Avaya Aura™ Communication Manager 5.2.1 (R015x.02.1.016.4-17959)
Avaya S8300 Server in a Avaya G450 Media Gateway (Access Element)	Avaya Aura™ Communication Manager 5.2.1 (R015x.02.1.016.4-17959)
Avaya S8800 Server	Avaya Modular Messaging Application Server 5.2, Avaya Modular Messaging Storage Server 5.2
Avaya 9600 Series IP Telephones Model: 9620 and 9630	Avaya one-X™ Deskphone Edition SIP 2.5.0
Avaya 6210 Analog Telephone	-
HTTPS/HTTP Phone Configuration File Server	Windows Server 2003 SP2
Juniper SRX210	10.1-20100504.0

Table 3 – Software/Hardware Version Information

4. Configure Avaya Aura^{TM} Communication Manager

This section shows the necessary steps to configure Communication Manager as a Feature Server to support the survivable SIP gateway solution. It is assumed that the basic configuration on Communication Manager, the required licensing, as well as the configuration required for accessing Modular Messaging, has already been administered. See the reference documents in **Section 11** for additional information.

All commands discussed in this section are executed on Communication Manager using the System Access Terminal (SAT).

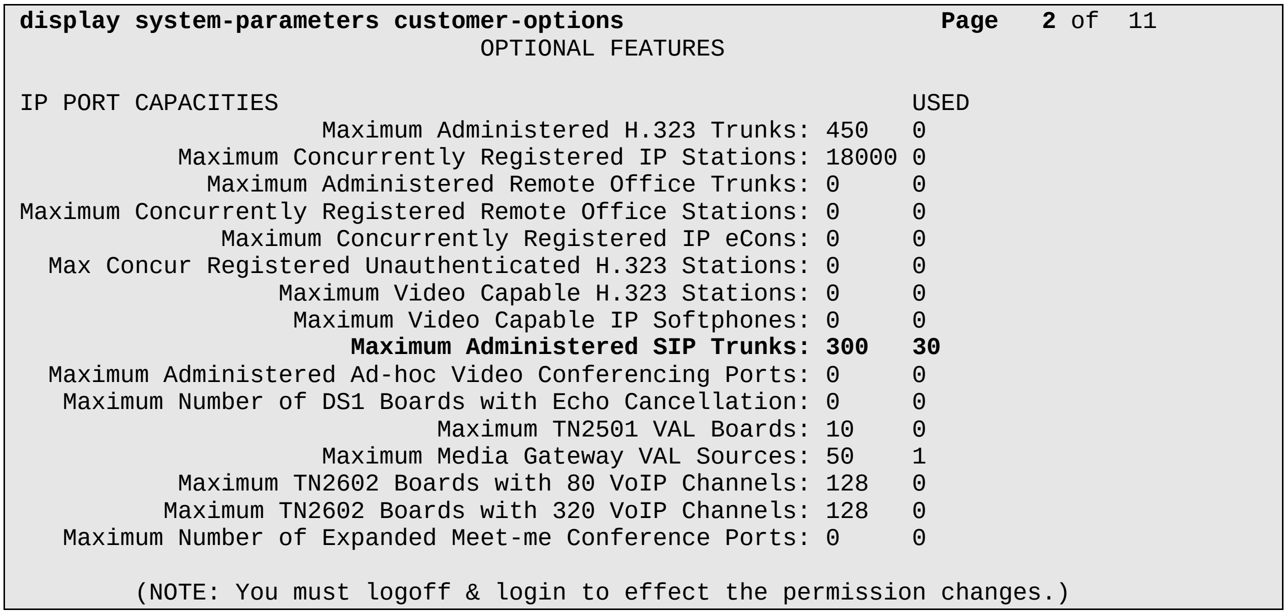
The administration procedures in this section include the following areas. Some administration screens have been abbreviated for clarity.

- Verify Avaya Aura^{TM} Communication Manager license
- Configure System parameters features
- Configure IP node names
- Configure IP codec set
- Configure IP network regions
- Add Stations
- Configure SIP signaling group and trunk group
- Configure Route pattern
- Configure Private numbering
- Configure Automatic Alternate Routing (AAR)
- Configure Automatic Route Selection (ARS)

4.1. Verify Avaya Aura^{TM} Communication Manger License

Log into the System Access Terminal (SAT) to verify that the Communication Manager license has proper permissions for features illustrated in these Application Notes. Use the “display system-parameters customer-options” command. Navigate to **Page 2**, and verify that there is sufficient remaining capacity for SIP trunks by comparing the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections.

The license file installed on the system controls the maximum capacities permitted. If there is insufficient capacity or a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.



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

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 450   0
           Maximum Concurrently Registered IP Stations: 18000 0
             Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
              Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 0     0
                  Maximum Video Capable H.323 Stations: 0     0
                   Maximum Video Capable IP Softphones: 0     0
                       Maximum Administered SIP Trunks: 300   30
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                             Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 50    1
           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: 0     0

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

4.2. Configure System Parameters Features

Use the “change system-parameters features” command to allow for trunk-to-trunk transfers. This feature is needed to be able to transfer an incoming/outgoing call from/to the remote switch back out to the same or another switch. For simplicity, the **Trunk-to-Trunk Transfer** field was set to “all” to enable all trunk-to-trunk transfers on a system-wide basis.

Note: This feature poses security risks, and must be used with caution. As an alternative, the trunk-to-trunk transfer feature can be implemented using Class Of Restriction or Class Of Service levels. Refer to the appropriate documentation in **Section 11** for more details.

```
change system-parameters features                               Page   1 of  18
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? n
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 10
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y
                             Music/Tone on Hold: music Type: ext   4500
              Music (or Silence) on Transferred Trunk Calls? no
                       DID/Tie/ISDN/SIP Intercept Treatment: attd
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n




             Abbreviated Dial Programming by Assigned Lists? n
       Auto Abbreviated/Delayed Transition Interval (rings): 2
                    Protocol for Caller ID Analog Terminals: Bellcore
    Display Calling Number for Room to Room Caller ID Calls? n
```

4.3. Configure IP Node Names

Use the “change node-names ip” command to add an entry for the Session Manager that the Communication Manager will connect to. The **Name** “SM01” and **IP Address** “10.64.20.31” are entered for the Session Manager Security Module (SM-100) interface. The configured node-name “SM01” will be used later in the SIP Signaling Group administration (**Section 4.7.1**).

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
SM-Chung            10.64.40.42
SM01                10.64.20.31
default             0.0.0.0
procr               10.64.20.25
```

4.4. Configure IP Codec Set

Configure the IP codec set to use for SIP calls. Use the “change ip-codec-set n” command, where “n” is the codec set number to be used for interoperability. Enter the desired audio codec type in the **Audio Codec** field. Retain the default values for the remaining fields.

In the sample configuration, IP codec set 1 was used for the IP network regions assigned to the Headquarters and Branch locations.

```
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:
```

4.5. Configure IP Network Regions

For simplicity, IP network region 1 was used for the phones and servers at the Headquarters and Branch locations. Other configurations are possible. An IP address map can be used for network region assignment if required.

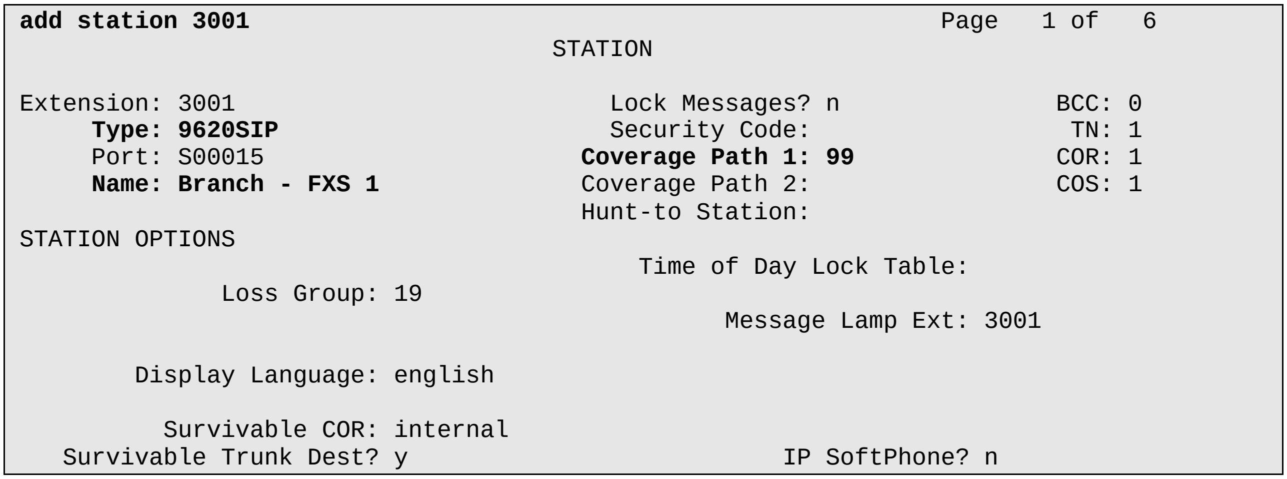
The **Authoritative Domain** “avaya.com” matches the SIP domain configured in the Session Manager (**Section 5.1**). The **Codec Set** for intra-region calls is set to the codec set “1” as configured in **Section 4.4**. The **IP-IP Direct Audio** parameters retain the default “yes” allowing direct IP media paths both within the region and between regions to minimize the use of media resources in the Avaya Media Gateway.

```
display ip-network-region 1                                       Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                  RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
           Keep-Alive Count: 5
```

4.6. Add Stations

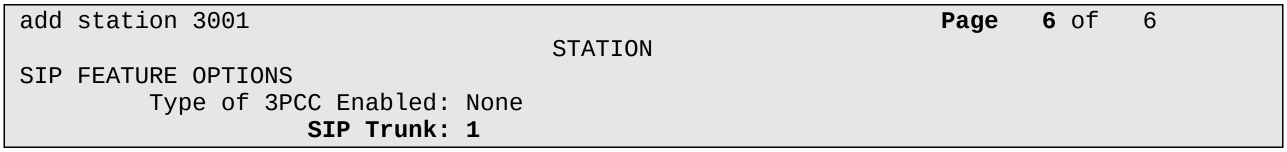
A station must be created on Communication Manager for each SIP User account to be created in Session Manager which includes a provisioned Communication Manager Extension. The extension assigned to the Communication Manager station must match the Communication Manager Extension assignment in Session Manager (see **Section 5.10**).

Use the “add station” command to add a station to Communication Manager. The “add station” command for an Avaya 9620 SIP Phone located in the sample branch, and assigned to extension 3001, is shown below. Because this is a SIP station, only the **Type** and **Name** fields are required to be populated as highlighted in bold. All remaining fields can be left at default values.   Feature programming for each station can vary.



```
add station 3001                                              Page   1 of   6
                                     STATION

Extension: 3001                           Lock Messages? n             BCC: 0
     Type: 9620SIP                        Security Code:                TN: 1
     Port: S00015                       Coverage Path 1: 99            COR: 1
     Name: Branch - FXS 1               Coverage Path 2:               COS: 1
                                        Hunt-to Station:
STATION OPTIONS
                                            Time of Day Lock Table:
              Loss Group: 19
                                                  Message Lamp Ext: 3001

        Display Language: english

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

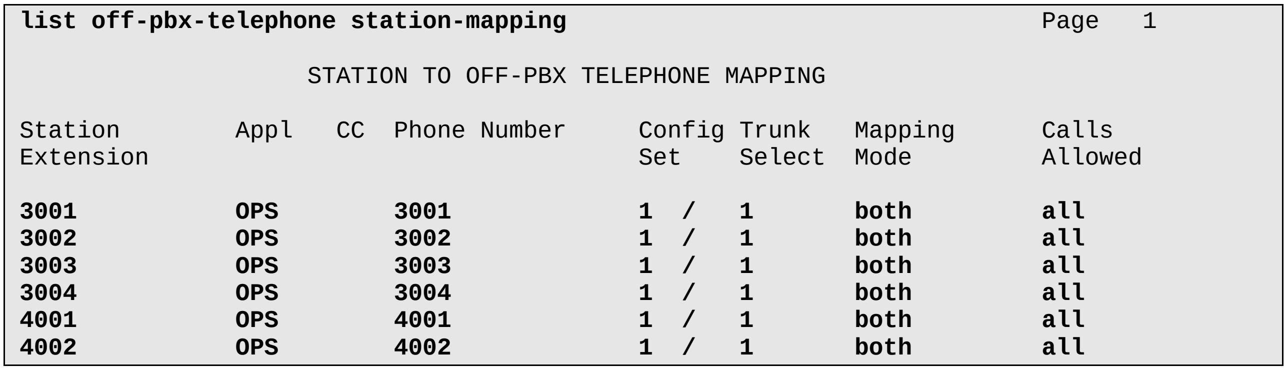
On **Page 6** of the station form, specify “1” for **SIP Trunk**. The is the SIP trunk administered in **Section 4.7**.



```
add station 3001                                              Page   6 of   6
                                     STATION
SIP FEATURE OPTIONS
         Type of 3PCC Enabled: None
                    SIP Trunk: 1
```

Repeat the above procedures to add each SIP phone located at both the main site and the branch sites, including the branch analog stations. Note that a phone type of “9620SIP” should be used for the branch analog stations.

After all the stations have been added, use the “list off-pbx-telephone station-mapping” command to verify that all the stations have been automatically designated as OPS (Off-PBX Station) sets. In the screen shown below, extensions 4001 and 4002 are SIP phones at the main site; extensions 3003 and 3004 are SIP phones at the sample branch; and extensions 3001 and 3002 are analog phones at the sample branch.



```
list off-pbx-telephone station-mapping                          Page   1

                    STATION TO OFF-PBX TELEPHONE MAPPING

Station         Appl   CC  Phone Number     Config Trunk   Mapping      Calls
Extension                                   Set    Select  Mode         Allowed

3001            OPS        3001             1  /   1       both         all
3002            OPS        3002             1  /   1       both         all
3003            OPS        3003             1  /   1       both         all
3004            OPS        3004             1  /   1       both         all
4001            OPS        4001             1  /   1       both         all
4002            OPS        4002             1  /   1       both         all
```

4.7. Configure SIP Signaling Group and Trunk Group

A SIP signaling group and an associated trunk group was configured between Communication Manager and Session Manager in the sample configuration. The signaling and trunk groups were used for call signaling and media transport to/from SIP phones registered to Session Manager including phones in the branch location (when in Normal Mode).

4.7.1. SIP Signaling Groups

In the sample configuration, Communication Manager acts as a Feature Server supporting the Avaya 9600 SIP Phones. An IMS-enabled SIP trunk to Session Manager is required for this purpose. Use the “add signaling-group n” command, where “n” is an available signaling group number. Enter the following values for the specified fields, and retain the default values for all remaining fields.

- **Group Type**: “sip”
- **Transport Method**: “tcp”
- **IMS Enabled?**: “y”
- **Near-end Node Name**: “procr” node name from **Section 4.3**
- **Far-end Node Name**: “SM01” Session Manager node name from **Section 4.3**
- **Near-end Listen Port**: “5060”
- **Far-end Listen Port**: “5060”
- **Far-end Network Region**: Network region number “1” from **Section 4.5**
- **Far-end Domain**: SIP domain name from **Section 4.5** and **Section 5.1**
- **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
                        Transport Method: tcp
  IMS Enabled? y





   Near-end Node Name: procr                 Far-end Node Name: SM01
 Near-end Listen Port: 5060                Far-end Listen Port: 5060
                                        Far-end Network Region: 1
Far-end Domain: avaya.com

                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                     Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n            Alternate Route Timer(sec): 6
```

4.7.2. SIP Trunk Groups

Use the “add trunk-group n” command, where “n” is an available trunk group number, to add SIP trunk groups. Enter the following values for the specified fields, and retain the default values for the remaining fields.

Group Type:	“sip”
Group Name:	Descriptive text
TAC:	An available trunk access code as per dialplan
Service Type:	“tie”
Signaling Group:	The signaling group number as configured in **Section 4.7.1**
Number of Members:	Equal to the maximum number of concurrent calls supported

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

Group Number: 1                    Group Type: sip          CDR Reports: y
  Group Name: to SM (avaya.com)            COR: 1        TN: 1        TAC: *001
   Direction: two-way       Outgoing Display? y
 Dial Access? n                                Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                    Signaling Group: 1
                                                  Number of Members: 10
```

Navigate to **Page 3**, and enter “private” for the **Numbering Format** field as shown below. Use the default values for all other fields.

```
add trunk-group 1                                              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
```

4.8. Configure Route Patterns

Configure a route pattern to route calls through the added SIP trunk group. Use the "change route-pattern n" command, where "n" is an available route pattern. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Pattern Name**: A descriptive name
- **Grp No**: The trunk group number configured in **Section 4.7.2**
- **FRL**: Facility Restriction Level that allows access to this trunk, "0" being the least restrictive

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: to SM
                             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                    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                                          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
```

4.9. Configure Private Numbering

Use the “change private-numbering 0” command to define the calling party number to be sent. Add an entry for the trunk group defined in **Section 4.7.2**. In the example shown below, all calls originating from a 4-digit extension beginning with “3” (branch extensions) or “4” (Headquarters extensions) and routed across trunk group 1 will result in a 4-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  2                11                          5     Total Administered: 4
 4  3                1                           4        Maximum Entries: 540
 4  4                1                           4
 5  5                1-2                         5
```

4.10. Configure Automatic Alternate Routing (AAR)

Use the “change aar analysis” command to add an entry for the extension range corresponding to the SIP telephones as configured in **Section 4.6** (required for feature server Off-PBX-Station support). Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **Dialed String**: Dialed prefix digits to match on
- **Total Min**: Minimum number of digits
- **Total Max**: Maximum number of digits
- **Route Pattern**: The route pattern number from **Section 4.8**
- **Call Type**: “aar”

```
change aar analysis 0                                              Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location:  all          Percent Full:    1

          Dialed            Total     Route     Call   Node  ANI
          String           Min  Max  Pattern    Type   Num   Reqd
    10                     4    4     1         aar          n
    22                     5    5     11        aar          n
    230                    5    5     1         aar          n
    3                      4    4     1         aar          n
    4                      4    4     1         aar          n
    530                    5    5     1         aar          n
    6                      5    5     1         aar          n
    7                      5    5     1         aar          n
    8                      5    5     1         aar          n
```

4.11. Configure Automatic Route Selection (ARS)

The ARS entries highlighted in the section focus on the local and long distance dialing from branch locations.

4.11.1. ARS Access Code

The sample configuration designates ‘9’ as the ARS Access Code as shown below on **Page 1** of the **change feature-access-codes** form. Calls with a leading 9 will be directed to the ARS routing table.

```
change feature-access-codes                                    Page   1 of   6
                               FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialing List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: 08
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: *008
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA:        All:        Deactivation:
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code:
                       Call Pickup Access Code:
CAS Remote Hold/Answer Hold-Unhold Access Code:
                  CDR Account Code Access Code:
                        Change COR Access Code:
                   Change Coverage Access Code:
            Conditional Call Extend Activation:        Deactivation:
                   Contact Closure   Open Code:          Close Code:
```

4.11.2. ARS Digit Analysis

The “change ars analysis y” command is used to make routing entries where the y is the dialed digit string to match. The ARS Digit Analysis Table used in the sample configuration is shown below. Calls to the PSTN with area code 303 (1 + 10 digits) will match the **Dialed String** of “130” with “11” digits and select **Route Pattern** “1”. Calls to the PSTN with area code “732” will match the **Dialed String** of “173” with “11” digits and select **Route Pattern** “1” too. **Route Pattern** “1” as configured in **Section 4.8** routes calls on trunk group 1 to the Session Manager for onward routing to the PSTN (in the setup used for the sample configuration, Session Manager routes these calls either to a separate Communications Manager for termination to the PSTN via the T1/E1 facilities in an Avaya G-Series Media Gateway[2], or routes the local PSTN calls from the branch phones back to the branch SRX210 for termination to the PSTN via the FXO interfaces on the SRX210). Note that in a real deployment environment, calls with other area

[2] The configuration of the Route Pattern and the associated PSTN Trunk Group on this separate Communication Manager and the Avaya G-Series Media Gateway are outside the scope of these Application Notes, and are therefore not included.

codes or with no area code restrictions (i.e., **Dialed String** “1xxxxxxxxxx”) can be specified to fit specific business policies.

```
change ars analysis 173                                         Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location:  all          Percent Full:    1

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    173                   11   11    1        fnpa         n
```

```
change ars analysis 130                                         Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location:  all          Percent Full:    1

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    130                   11   11    1        fnpa         n
```

The routing of E-911 calls is outside the scope of these Application notes. However, an ARS Digit Analysis entry should be created to route the E-911 calls to the Session Manager for onward routing to the PSTN. Routing policies would be defined on the Session Manager to

- Route E-911 calls originated from the branch in the Normal Mode to go out to the PSTN through the FXO interfaces on the branch Juniper SRX210
- Route E-911 calls originated from the Headquarters to go out to the PSTN through the E1/T1 facilities at the central site

This assures the E-911 calls from both Headquarters and branch sites would be received by the local Emergency Response Center.

5. Configure Avaya Aura^{TM} Session Manager

This section provides the procedures for configuring Session Manager as provisioned in the sample configuration. Session Manager is comprised of two functional components: the Session Manager server and the System Manager management server. All SIP call provisioning for Session Manager is performed via the System Manager Web interface and are then downloaded into Session Manager.

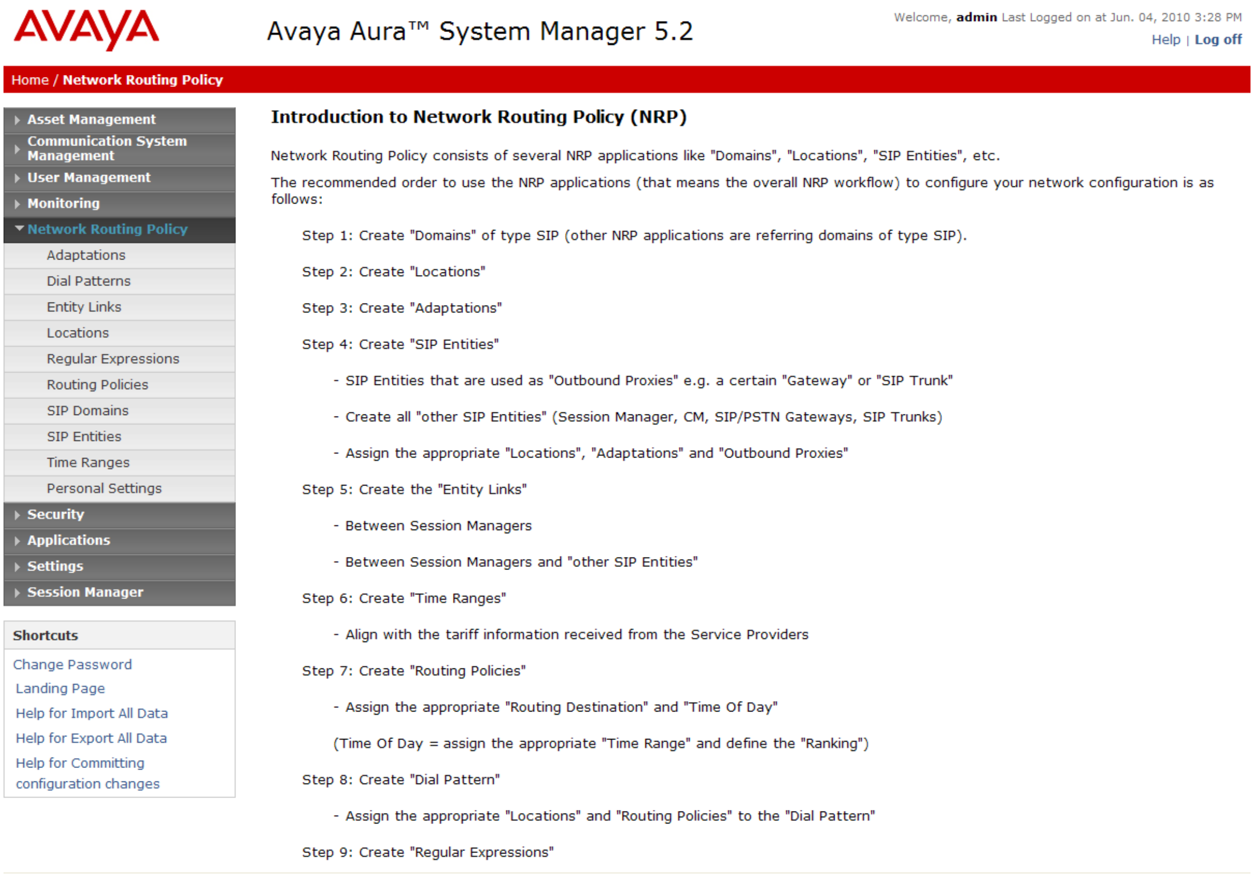
The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two servers.

The Session Manager server contains an SM-100 security module that provides the network interface for all inbound and outbound SIP signaling and media transport to all provisioned SIP entities. For the Session Manager used in the sample configuration, the IP address assigned to the SM-100 interface is 10.64.20.31 as shown in **Figure 1**. The Session Manager server has a separate network interface used for connectivity to System Manager for managing/provisioning Session Manager. For the sample configuration, the IP address assigned to the Session Manager management interface is 10.64.20.30. In the sample configuration, the SM-100 interface and the management interface were both connected to the same IP network. If desired, the SM-100 interface for real-time SIP traffic can be configured to use a different network than the management interface. For more information on Session Manager and System Manager, see references **[1]** and **[2]**.

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

- **SIP domain**
- Logical/physical **Locations** that can be occupied by SIP Entities
- **Adaptations** to convert digits
- **SIP Entities** corresponding to the SIP telephony systems including Communication Manager, branch Juniper SRX210 and Session Manager itself
- **Entity Links** which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- **Routing Policies** which control call routing between the SIP Entities
- **Dial Patterns** which govern to which SIP Entity a call is routed
- **Session Manager** corresponding to the Session Manager Servers managed by System Manager
- Add Communication Manger as a Feature Server
- **User Management** for SIP telephone users

Configuration of Session Manager 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 click on **OK** in the subsequent confirmation screen. The menu shown below is then displayed. Expand the **Network Routing Policy** link on the left side as shown. The sub-menus displayed in the left column will be used to configure the first seven of the above items (**Sections 5.1** through **5.7**).



Introduction to Network Routing Policy (NRP)

Network Routing Policy consists of several NRP applications like "Domains", "Locations", "SIP Entities", etc.

The recommended order to use the NRP applications (that means the overall NRP workflow) to configure your network configuration is as follows:

Step 1: Create "Domains" of type SIP (other NRP applications are referring domains of type SIP).

Step 2: Create "Locations"

Step 3: Create "Adaptations"

Step 4: Create "SIP Entities"

- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"

Step 5: Create the "Entity Links"

- Between Session Managers
- Between Session Managers and "other SIP Entities"

Step 6: Create "Time Ranges"

- Align with the tariff information received from the Service Providers

Step 7: Create "Routing Policies"

- Assign the appropriate "Routing Destination" and "Time Of Day"

(Time Of Day = assign the appropriate "Time Range" and define the "Ranking")

Step 8: Create "Dial Pattern"

- Assign the appropriate "Locations" and "Routing Policies" to the "Dial Pattern"

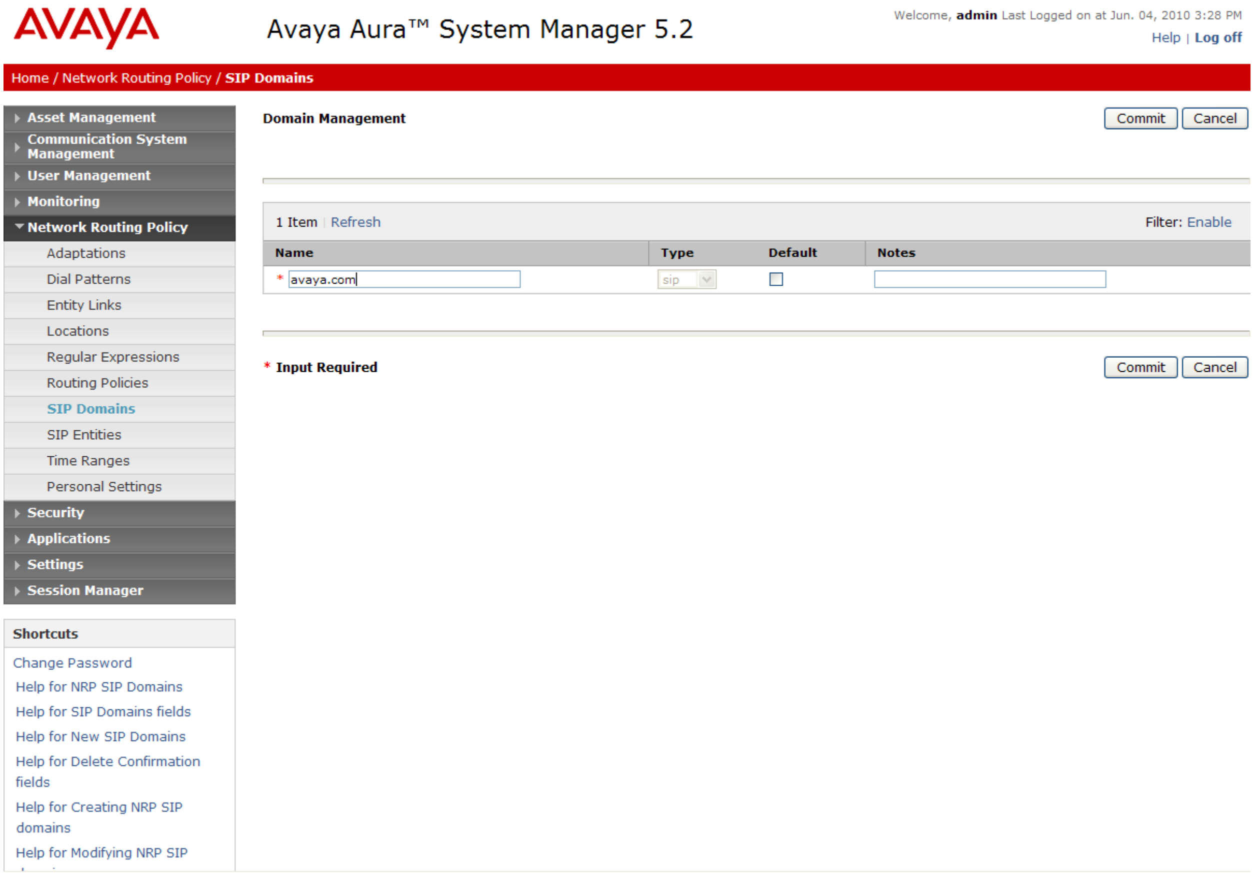
Step 9: Create "Regular Expressions"

5.1. Specify SIP Domain

Add the SIP domain for which the communications infrastructure will be authoritative. Select **SIP Domains** on the left and click the **New** button (not shown) on the right. Fill in the following:

- **Name**: The authoritative domain name matching the domain configuration on Communication Manager (see **Section 4.5**)
- **Notes**: Descriptive text (optional)

Click **Commit**.



Name	Type	Default	Notes
* avaya.com	sip	□	

5.2. Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of location-based routing as well as bandwidth management and call admission control. To add a location, select **Locations** on the left and click on the **New** button (not shown) on the right. Under *General*, enter:

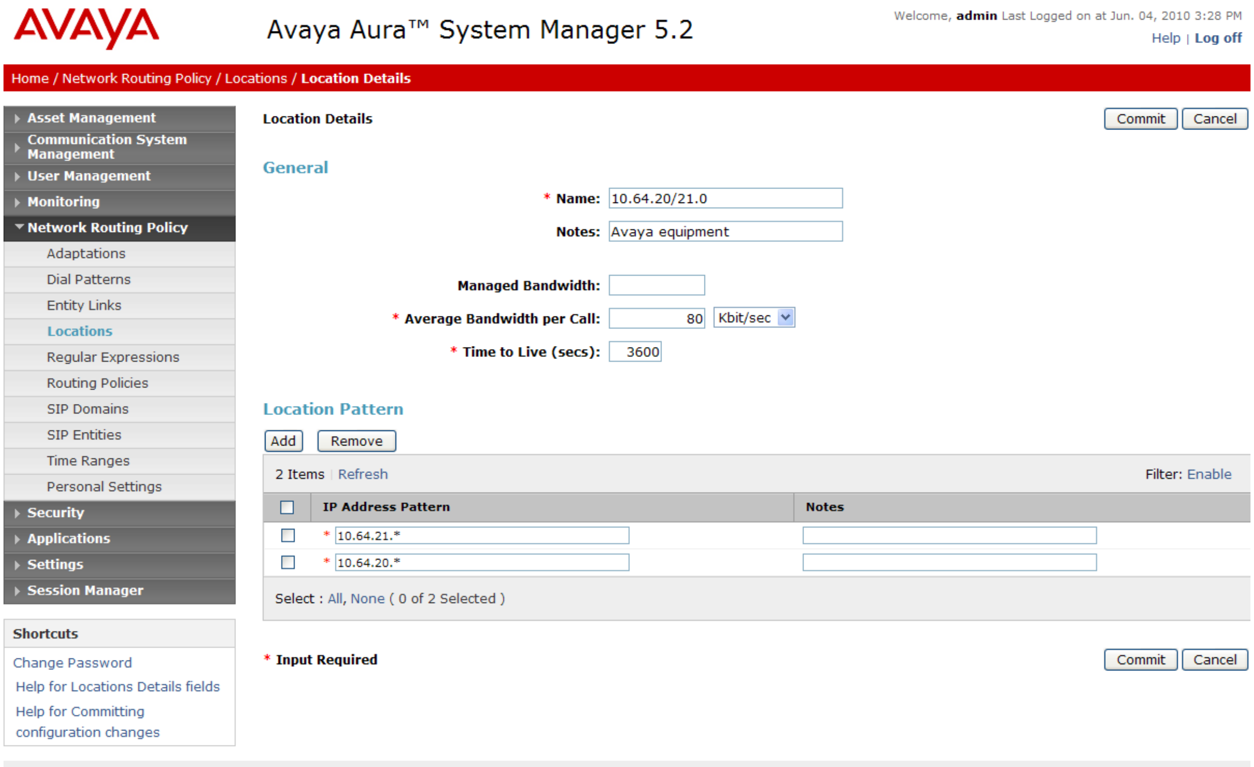
- **Name**: A descriptive name
- **Notes**: Descriptive text (optional)

The remaining fields under *General* can be filled in to specify bandwidth management parameters between Session Manager and this location. These were not used in the sample configuration, and reflect default values. Note also that routing policies can be defined based on Locations. The location-based routing was used in the sample configuration to route local PSTN calls originated from the branch to go out to the PSTN via the FXO interfaces on the branch SRX210 (see **Sections 5.6** and **5.7**).

Under *Location Pattern*:

- **IP Address Pattern**: An IP address pattern used to identify the location
- **Notes**: Descriptive text (optional)

The screen below shows addition of the “10.64.20/21.0” Location for the Headquarters site, which includes the 10.64.20.0/24 and 10.64.21.0/24 subnets. Click **Commit** to save the **Location Details** definition.



Location Details

General

* Name:	10.64.20/21.0
Notes:	Avaya equipment
Managed Bandwidth:	
* Average Bandwidth per Call:	80 Kbit/sec
* Time to Live (secs):	3600

Location Pattern

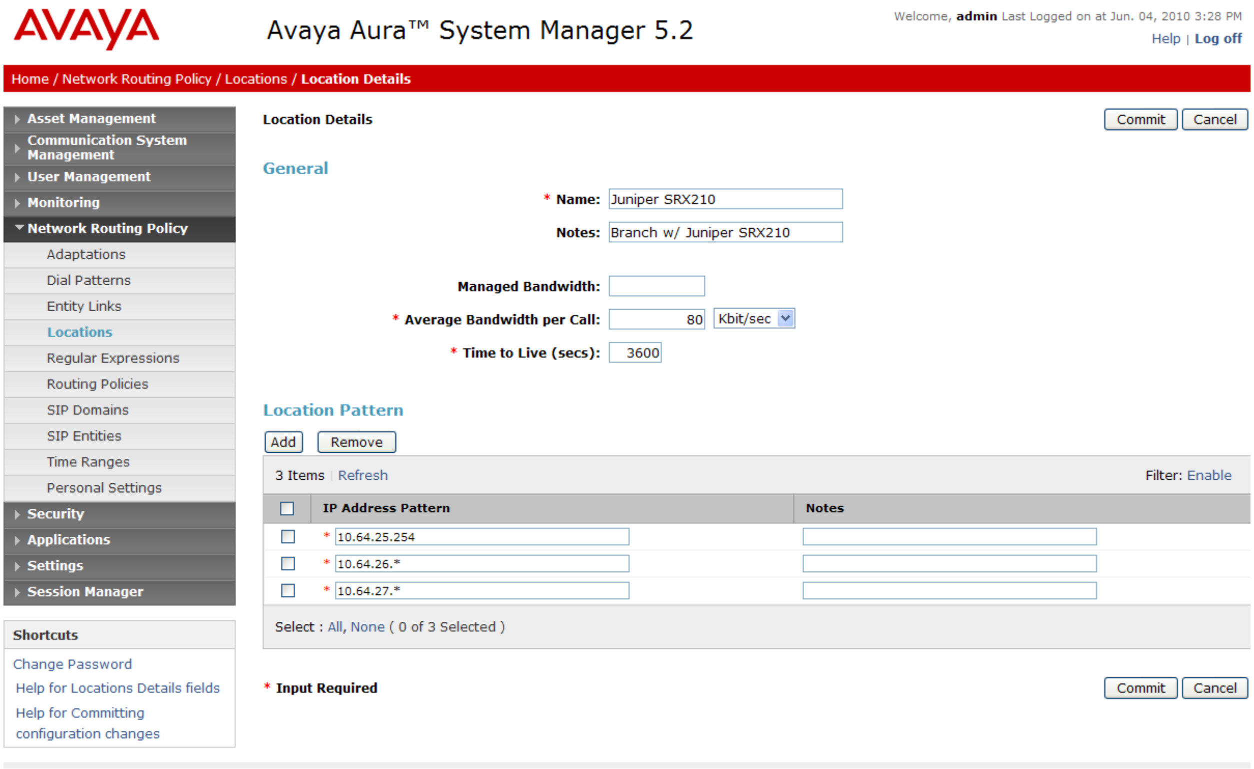
2 Items

□	IP Address Pattern	Notes
□	* 10.64.21.*	
□	* 10.64.20.*	

Select : All, None (0 of 2 Selected)

* Input Required

In addition to the Location created for the Headquarters site, each branch needs to have its own Location defined. Each branch Location is similarly configured as shown below with its own **Name** and **IP Address Patterns**. The IP addresses 10.64.25.254, 10.64.26.*, and 10.64.27.* were specified for the sample branch.



Location Details

General

* Name:	Juniper SRX210
Notes:	Branch w/ Juniper SRX210
Managed Bandwidth:	
* Average Bandwidth per Call:	80 Kbit/sec
* Time to Live (secs):	3600

Location Pattern

3 Items

□	IP Address Pattern	Notes
□	* 10.64.25.254	
□	* 10.64.26.*	
□	* 10.64.27.*	

Select : All, None (0 of 3 Selected)

* Input Required

5.3. Add Adaptation

The *DigitConversionAdapter* allows Session Manager to convert inbound and/or outbound digits in the SIP Request-URI, History-Info header, P-Asserted-Identity header, and Notify messages, based on the SIP Entities to which this adaptation is defined. This functionality is similar to the Communication Manager public-unknown-numbering and incoming-call-handling-treatment capabilities.

Session Manager will perform digit conversion based on whether the digits are being received (incoming) or sent (outgoing) by Session Manager with another SIP Entity. For example, on a call between the branch (with the SRX210) and Session Manager, a call from the branch to Session Manager is considered to be incoming, while a call from Session Manager to the branch is considered to be outgoing.

In Normal Mode, the Juniper SRX210 was configured to route calls from Session Manager that match route pattern “91732XXXXXXX” to the PSTN via an SRX210 FXO port. However, due to the configuration of Session Manager and Communication manager, if a branch caller dials a local number “91732XXXXXXX”, the leading two digits “91” are stripped off the dialed number before Session Manager routes the call back to the SRX210. Therefore, in order for Juniper to route the call properly to the PSTN, the leading “91” are added back in using an adaptation. Routing configuration and the use of Adaptations can vary per deployment, and aren’t necessarily required for this solution. The example Adaptation shown below is what was used during compliance testing.

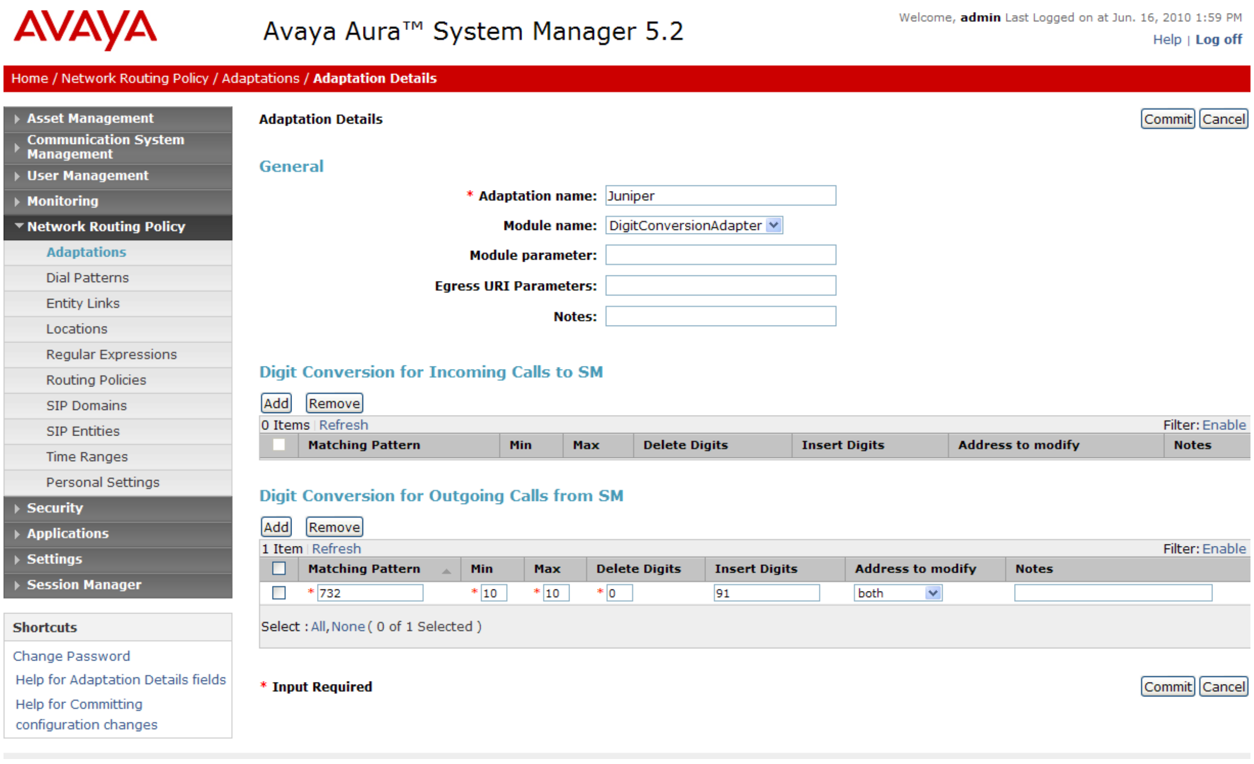
Select **Adaptations** from the menu.

1. Select **New**.
   - Enter a descriptive name (e.g. **Juniper**).
   - Specify **DigitConversionAdapter** in the Adaptation Module field.
   - Enter a description in the **Notes** field if desired.

2. Click the **Add** button under *Digit Conversion for Outgoing Calls from SM* and enter:
   - **Matching Pattern** – The digit string to match → **732**
   - **Min** – The minimum number of digits → **10**
   - **Max** – The maximum number of digits → **10**
   - **Delete Digits** – The number of digits to delete → **0**
   - **Insert Digits** – The digits to be inserted → **91**
   - **Address to Modify** – Associated headers to be monitored for matching digits (origination/destination/both) → **both**
   - **Notes** - Enter a description in the **Notes** field if desired.

   With this Adaptation, the number 732XXXXXXX is converted to 91732XXXXXXX for calls going from Session Manager to the Juniper SRX210.

3. Click on the **Commit** button.



Adaptation Details

General

* Adaptation name: Juniper

Module name: DigitConversionAdapter

Module parameter:

Egress URI Parameters:

Notes:

Digit Conversion for Incoming Calls to SM

0 Items

□	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes

Digit Conversion for Outgoing Calls from SM

1 Item

□	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
□	* 732	* 10	* 10	* 0	91	both	

* Input Required

5.4. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP-based telephony system supported by it using SIP trunks. In the sample configuration, a SIP Entity was added for the Session Manager itself and the Communications Managers at the Headquarters, and the Juniper SRX210 for the branch.

Select **SIP Entities** on the left and click on the **New** button (not shown) on the right.

Under *General*:

- **Name** A descriptive name
- **FQDN or IP Address**: FQDN or IP address of the Session Manager or the signaling interface on the telephony system
- **Type**: "Session Manager" for Session Manager; "CM" for Communication Manager; "Other" for SRX210
- **Adaptation**: Leave blank (except for the Juniper-SRX210 Entity)
- **Location:** Select the Location configured in **Section 5.2**
- **Time Zone:** Select the proper time zone for this installation

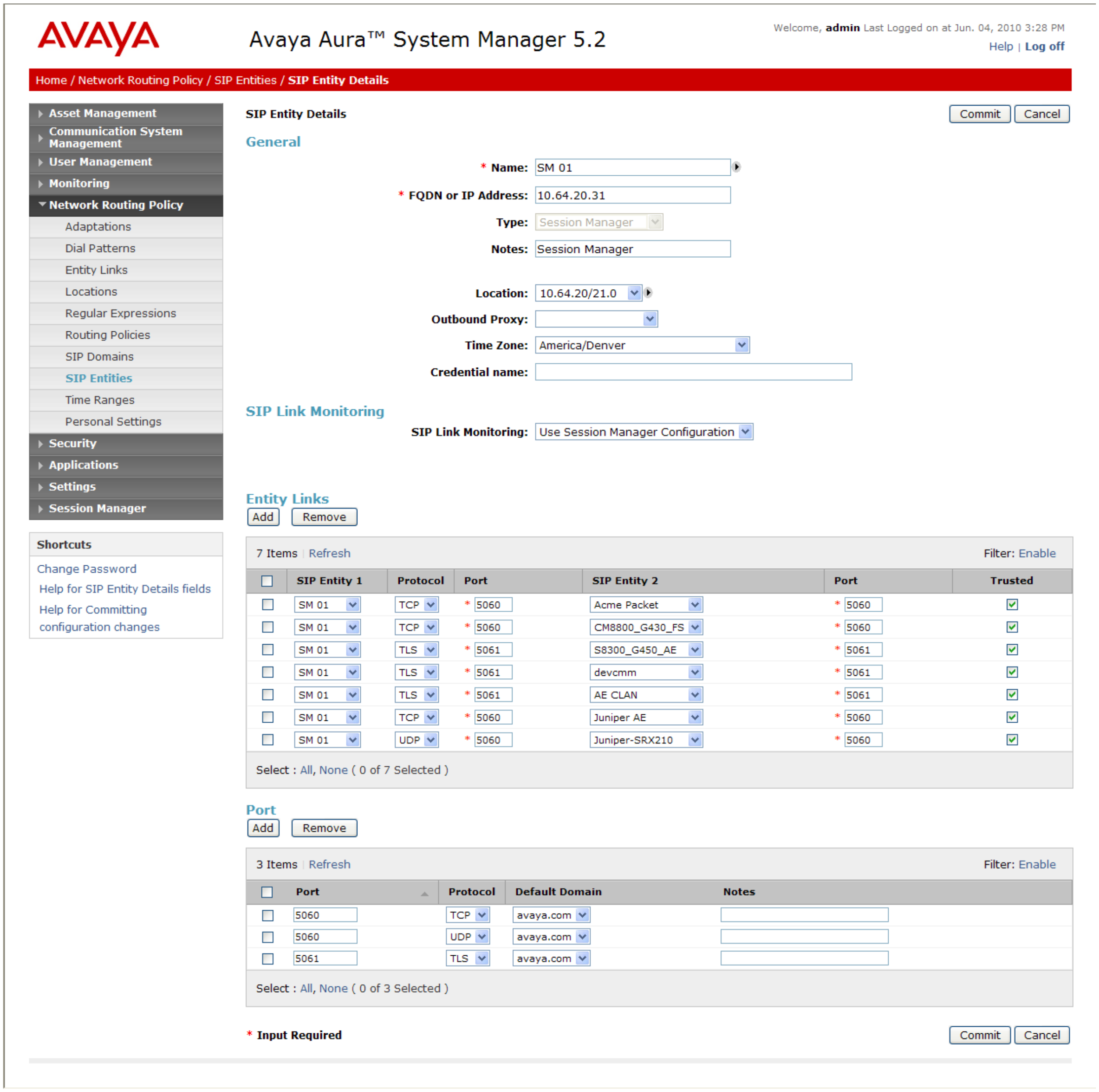
Under *Port* (for adding Session Manager Entity only), click **Add**, then edit the fields in the resulting new row as shown below:

- **Port**: Port number on which the system listens for SIP requests

- **Protocol**: Transport protocol to be used to send SIP requests
- **Default Domain**: Select the SIP Domain configured in **Section 5.1**

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

The following screen shows the addition of the Session Manager. The IP address of the SM-100 Security Module is entered for **FQDN or IP Address**. TCP with port 5060 is used for communication with Communication Manager; UDP with port 5060 is used for communication with the branch SRX210. Other entries are not used for the sample configuration. The *Entity Links* section is automatically populated after Entity Links have been defined.



SIP Entity Details

General

* Name:	SM 01
* FQDN or IP Address:	10.64.20.31
Type:	Session Manager
Notes:	Session Manager
Location:	10.64.20/21.0
Outbound Proxy:	
Time Zone:	America/Denver
Credential name:	

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

Add Remove

7 Items | Refresh Filter: Enable

□	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
□	SM 01	TCP	* 5060	Acme Packet	* 5060	☑
□	SM 01	TCP	* 5060	CM8800_G430_FS	* 5060	☑
□	SM 01	TLS	* 5061	S8300_G450_AE	* 5061	☑
□	SM 01	TLS	* 5061	devcmm	* 5061	☑
□	SM 01	TLS	* 5061	AE CLAN	* 5061	☑
□	SM 01	TCP	* 5060	Juniper AE	* 5060	☑
□	SM 01	UDP	* 5060	Juniper-SRX210	* 5060	☑

Select : All, None (0 of 7 Selected)

Port

Add Remove

3 Items | Refresh Filter: Enable

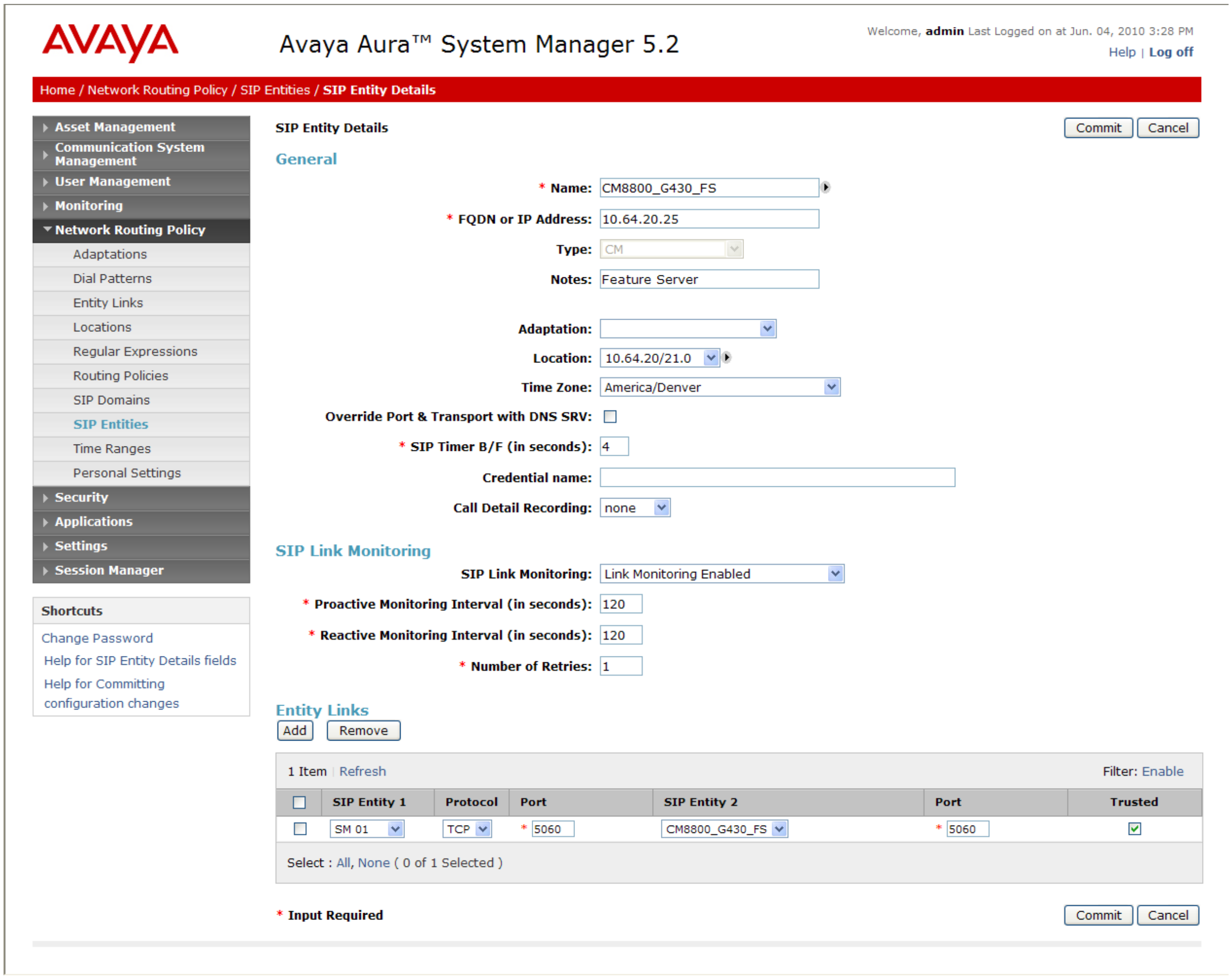
□	Port	Protocol	Default Domain	Notes
□	5060	TCP	avaya.com	
□	5060	UDP	avaya.com	
□	5061	TLS	avaya.com	

Select : All, None (0 of 3 Selected)

* Input Required

The following screen shows the results of adding Communication Manager (Feature Server). The addition of Communication Manager (Access Element) is not shown. In this case, **FQDN or IP Address** is the IP address for the Communication Manager since the G430 Media Gateway used in the sample configuration has its signaling interface integrated into the Communication Manager processor. For other Avaya Media Gateways with C-LAN board installed, the IP address of the C-LAN board in the Media Gateway should be specified. Note the "CM" selection for **Type**.

The *Entity Links* section is automatically populated after Entity Links have been defined.



SIP Entity Details

General

* Name: CM8800_G430_FS

* FQDN or IP Address: 10.64.20.25

Type: CM

Notes: Feature Server

Adaptation:

Location: 10.64.20/21.0

Time Zone: America/Denver

Override Port & Transport with DNS SRV: □

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds): 120

* Reactive Monitoring Interval (in seconds): 120

* Number of Retries: 1

Entity Links

1 Item

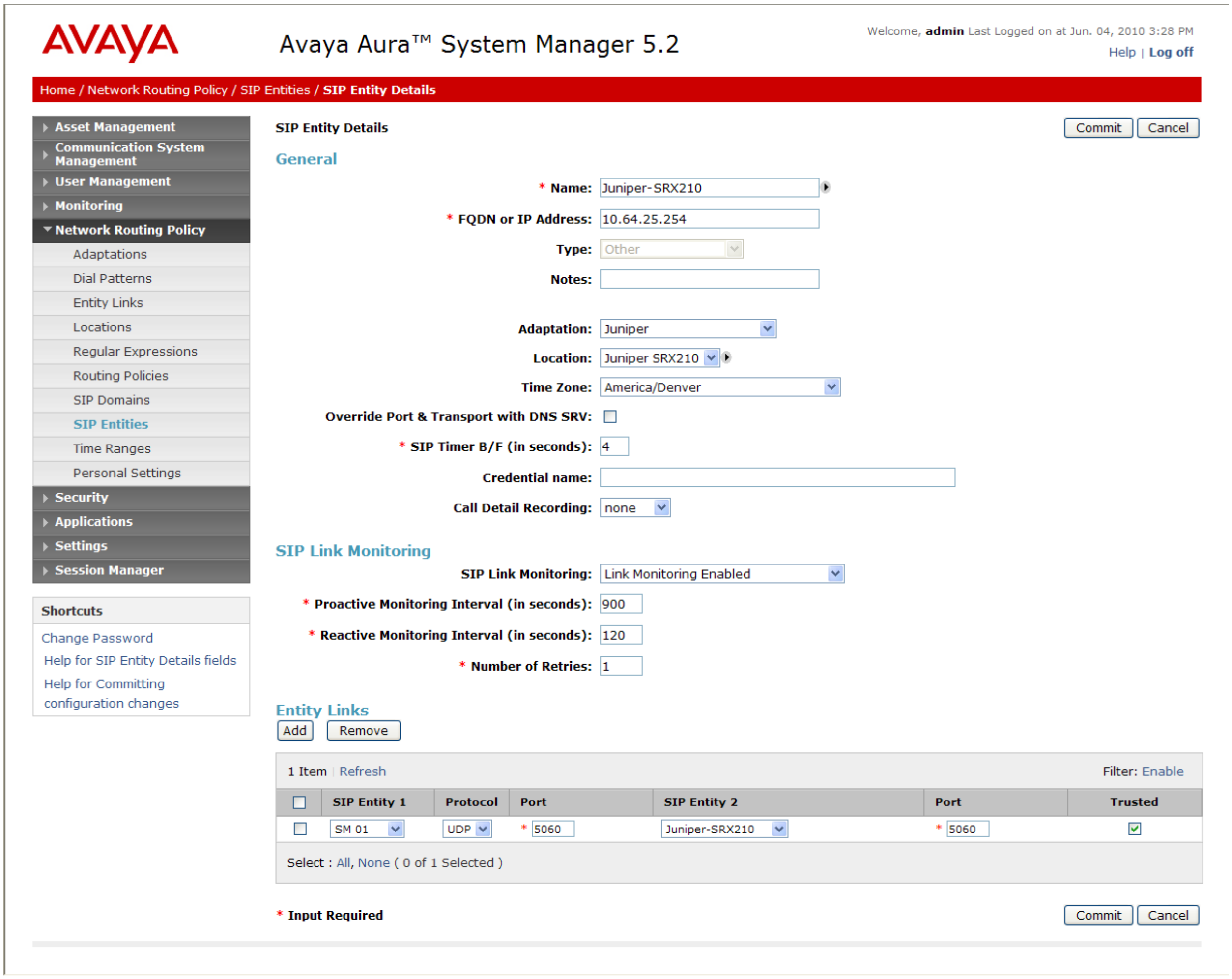
□	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
□	SM 01	TCP	* 5060	CM8800_G430_FS	* 5060	☑

Select : All, None (0 of 1 Selected)

* Input Required

The following screen shows the results of adding the branch Juniper SRX210. In this case, **FQDN or IP Address** is the IP address assigned to port 7 of the branch Juniper SRX210 (which provides connectivity to the WAN). Note the "Other" selection for **Type** as well as the selection of the branch Location as created in **Section 5.2**. Select "Juniper" for **Adaptation** (administered in **Section 5.3**).

The *Entity Links* section is automatically populated after Entity Links have been defined.



SIP Entity Details

General

* Name: Juniper-SRX210

* FQDN or IP Address: 10.64.25.254

Type: Other

Notes:

Adaptation: Juniper

Location: Juniper SRX210

Time Zone: America/Denver

Override Port & Transport with DNS SRV: □

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds): 900

* Reactive Monitoring Interval (in seconds): 120

* Number of Retries: 1

Entity Links

Add Remove

1 Item Refresh Filter: Enable

□	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
□	SM 01	UDP	* 5060	Juniper-SRX210	* 5060	☑

Select : All, None (0 of 1 Selected)

* Input Required

5.5. Add Entity Links

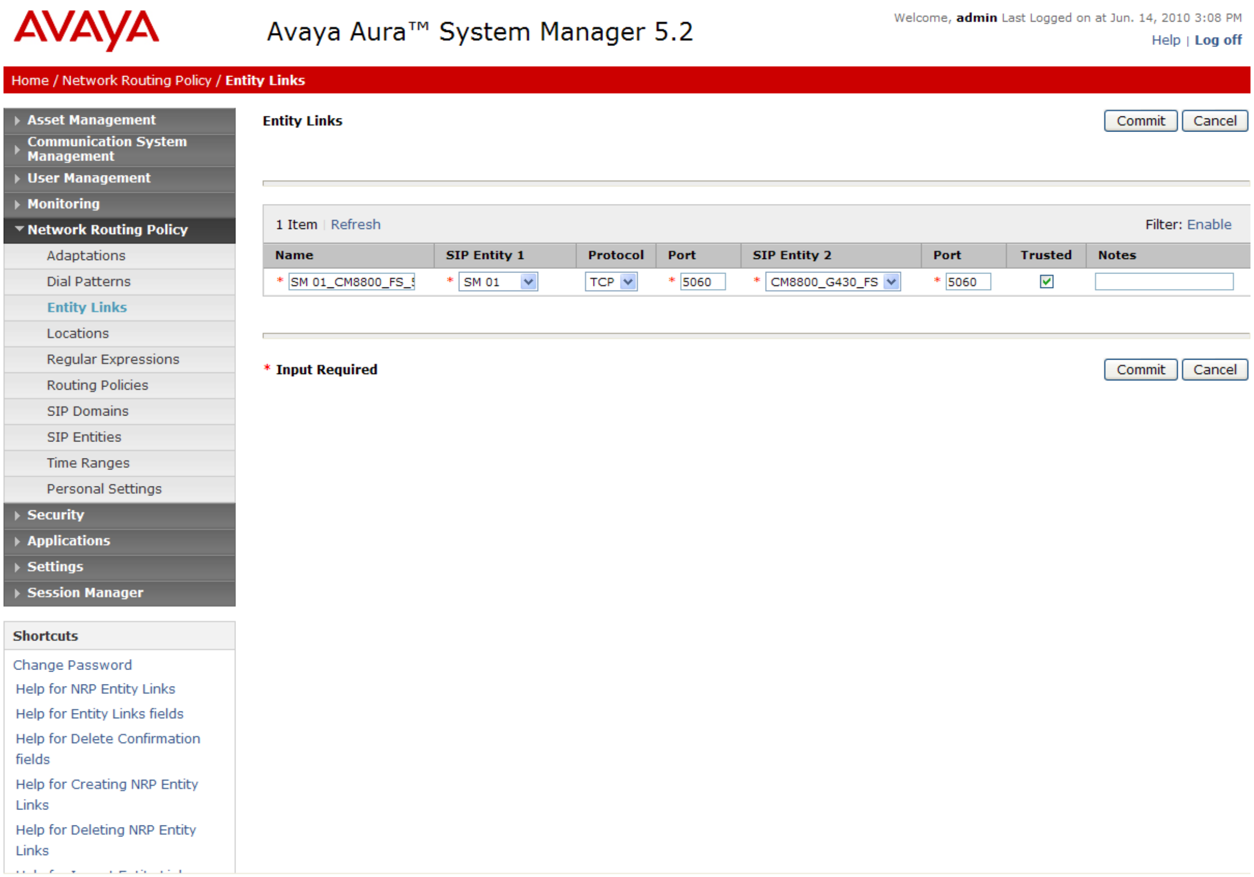
A SIP trunk between Session Manager and a telephony system is described by an Entity link. In the sample configuration, separate Entity Links were configured between Session Manager and the two Communication Mangers. Another Entity Link was created between Session Manager and the branch Juniper SRX210.

To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

- **Name**: A descriptive name
- **SIP Entity 1**: Select the Session Manager SIP Entity configured in **Section 5.4**
- **Protocol**: Select “TCP” or “UDP”
- **Port**: Port number to which the other system sends SIP requests.
- **SIP Entity 2**: Select the Communication Manager or SRX210 SIP Entity configured in **Section 5.4**
- **Port**: Port number on which the other system receives SIP requests
- **Trusted**: Check this box

Click **Commit** to save the configuration.

The screen below shows the Entity Link configured between Session Manager and Communication Manager (Feature Server).

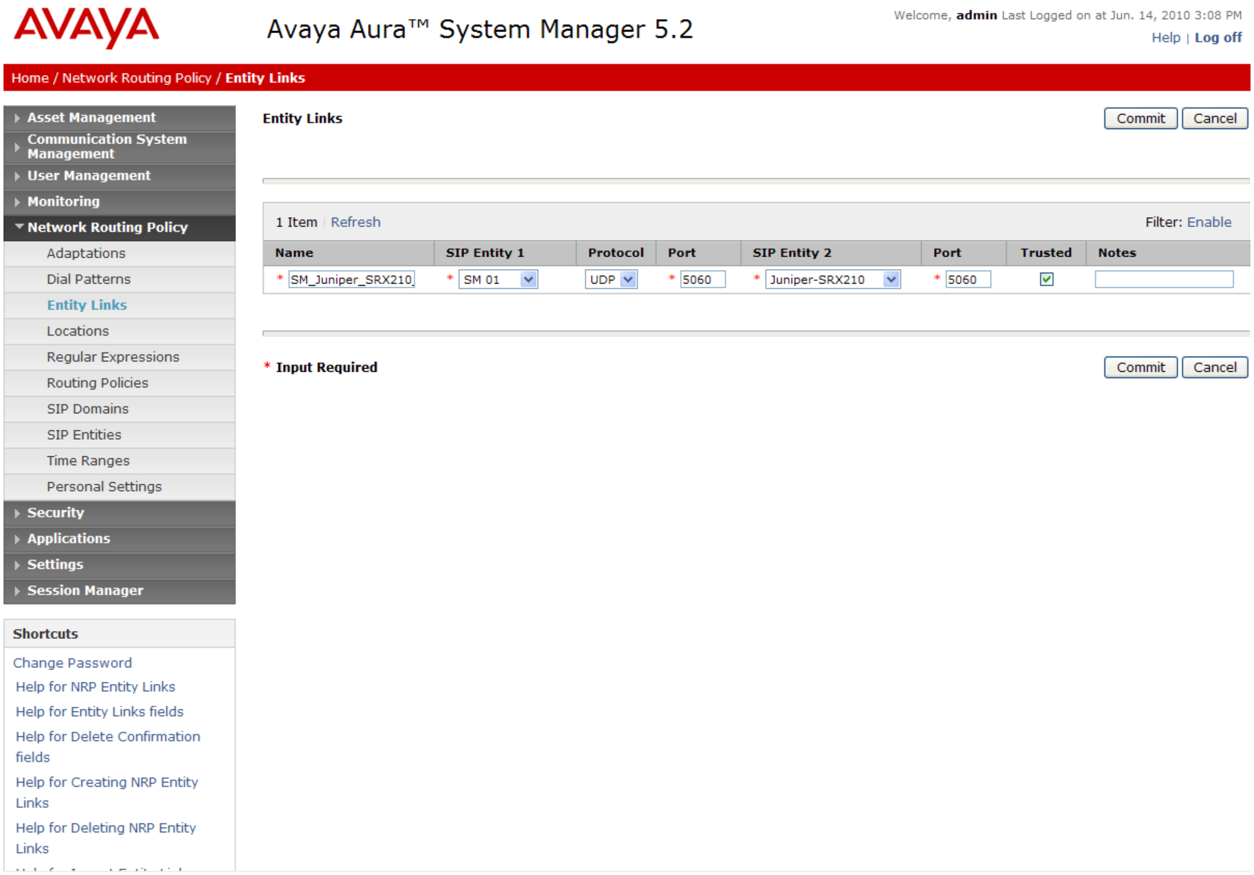


Entity Links

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* SM 01_CM8800_FS_	* SM 01	TCP	* 5060	* CM8800_G430_FS	* 5060	☑	

* Input Required

The screen below shows the Entity Link between Session Manager and the sample branch Juniper SRX210. Note the “UDP” selection for **Protocol** and the **Port** setting 5060 specified for the branch Juniper media gateway.



Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* SM_Juniper_SRX210	* SM 01	UDP	* 5060	* Juniper-SRX210	* 5060	☑	

5.6. Add Routing Policy

Routing policies describe the conditions under which calls will be routed to the SIP Entities. The Routing Policies can be thought of as routing destinations with routing conditions.

The inter-branch and intra-branch calling between phones using extension numbers do not need Routing Policies since all the phones, both at the Headquarters and in the branches, are administered on the Communication Manager and register to the Session Manager. However, calls to the PSTN need Routing Policies to determine where they are going to be routed for eventual termination to the PSTN. These calls could go out to the PSTN through the T1/E1 facilities at the Headquarters, or they could go out through the analog trunks (a.k.a Service Provider CO lines) connected to the FXO ports on the branch SRX210.

Separate Routing Policies need to be created for sending PSTN-bound calls. In the case of Centralized Trunking arrangement, all PSTN-bound calls, regardless of the call originations (either from the Headquarters or from the branches), should be sent to the Headquarters for onward routing to the PSTN. In the case of Distributed Trunking arrangement, all PSTN-bound calls from the Headquarters plus the Long Distance toll calls from the branch locations should be routed to the Headquarters for PSTN termination, but local calls from the branch should be routed back to the local branch SRX210 for going out to the PSTN through the FXO interfaces on the branch SRX210.

To add a routing policy, select **Routing Policies** on the left and click on the **New** button (not shown) on the right. Fill in the following:

Under *General*:
Enter a descriptive name in **Name** and optional text in **Notes**.

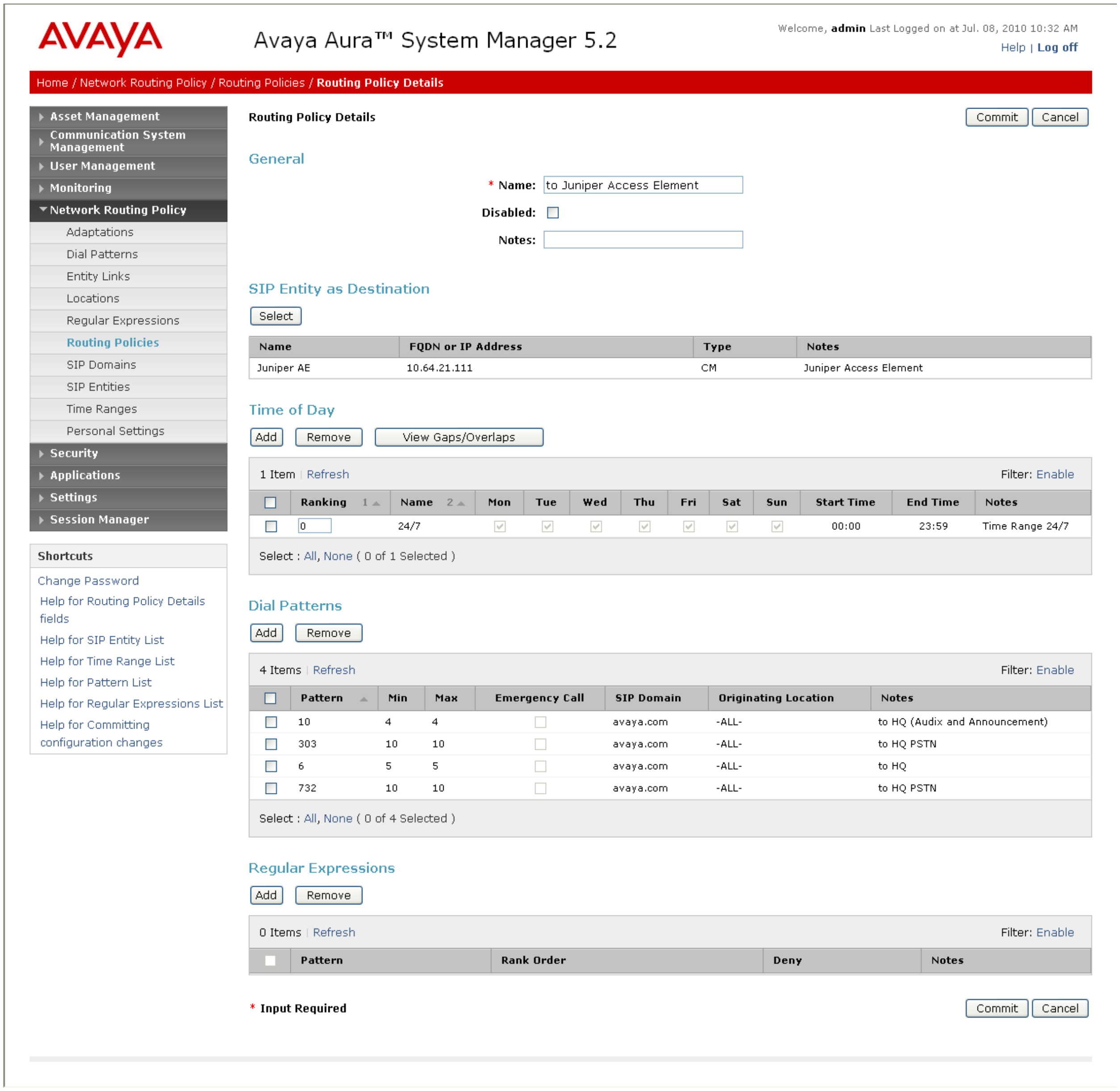
Under *SIP Entity as Destination*:
Click **Select**, and then select the appropriate SIP entity to which this routing policy applies.

Under *Time of Day*:
Click **Add**, and select the default "24/7" time range.

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

The following screen shows the Routing Policy for routing calls to the Headquarters where a Communication Manager (Access Element) would send these calls through a PSTN trunk to the PSTN[3]. Note that the *Dial Patterns* section is automatically populated after Dial Patterns have been defined.

[3] The configuration on this Communication Manager and the Avaya Media Gateway for routing calls to the PSTN (Route Pattern, PSTN Trunk/Signaling Groups, T1/E1 interfaces, etc.) are outside the scope of these Application Notes, and are therefore not included.



Routing Policy Details

General

* Name: to Juniper Access Element

Disabled: □

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Juniper AE	10.64.21.111	CM	Juniper Access Element

Time of Day

1 Item | Refresh Filter: Enable

□	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None (0 of 1 Selected)

Dial Patterns

4 Items | Refresh Filter: Enable

□	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
□	10	4	4	□	avaya.com	-ALL-	to HQ (Audix and Announcement)
□	303	10	10	□	avaya.com	-ALL-	to HQ PSTN
□	6	5	5	□	avaya.com	-ALL-	to HQ
□	732	10	10	□	avaya.com	-ALL-	to HQ PSTN

Select : All, None (0 of 4 Selected)

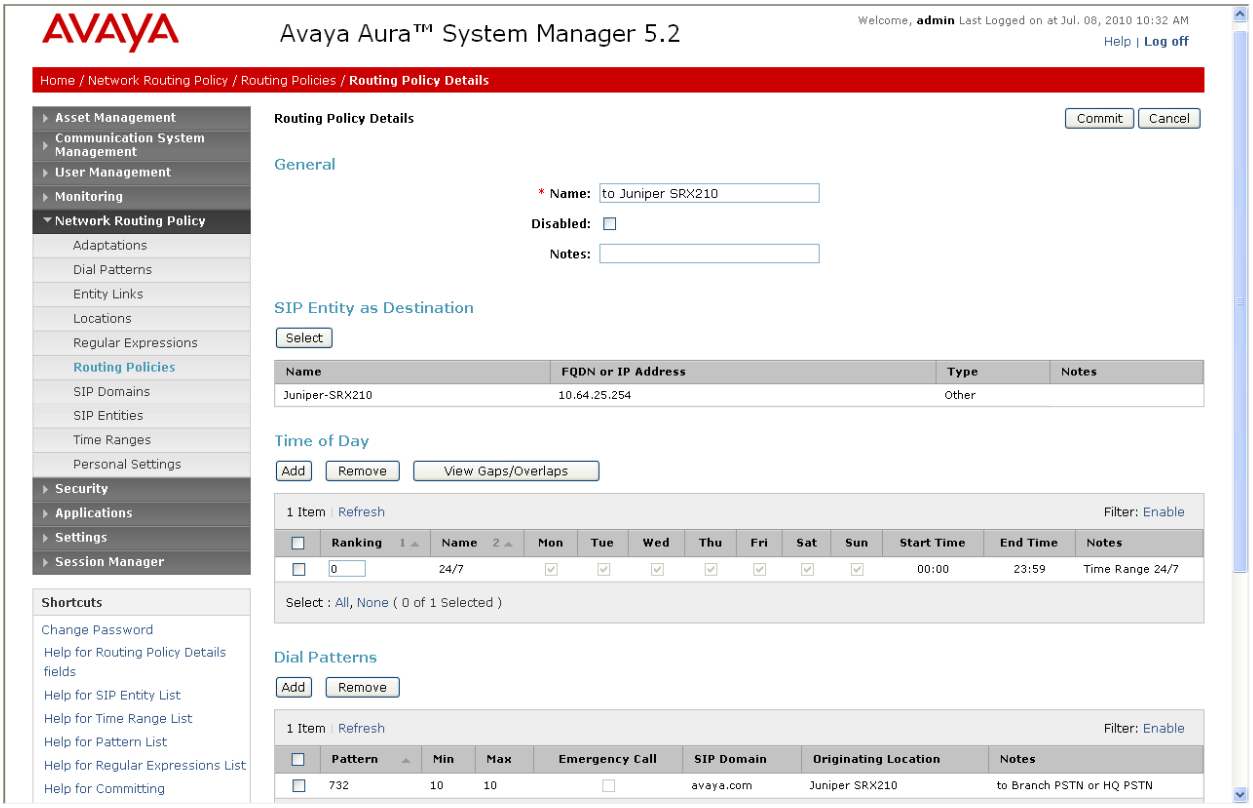
Regular Expressions

0 Items | Refresh Filter: Enable

□	Pattern	Rank Order	Deny	Notes

* Input Required

The following screen shows the Routing Policy for routing PSTN calls to the local branch Juniper SRX210. Note that the *Dial Patterns* section is automatically populated after Dial Patterns have been defined.



Routing Policy Details

General

* Name: to Juniper SRX210

Disabled: □

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Juniper-SRX210	10.64.25.254	Other	

Time of Day

1 Item | Refresh

□	Ranking 1	Name 2	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None (0 of 1 Selected)

Dial Patterns

1 Item | Refresh

□	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
□	732	10	10	□	avaya.com	Juniper SRX210	to Branch PSTN or HQ PSTN

5.7. Add Dial Patterns

Define a Dial Pattern for matching calls based on Area Codes. A Dial Patterns is then associated with a Routing Policy to direct calls with the matched dialed digit strings to the destinations (SIP Entities as specified in Routing Policies).

To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following, as shown in the screens below:
Under *General*:

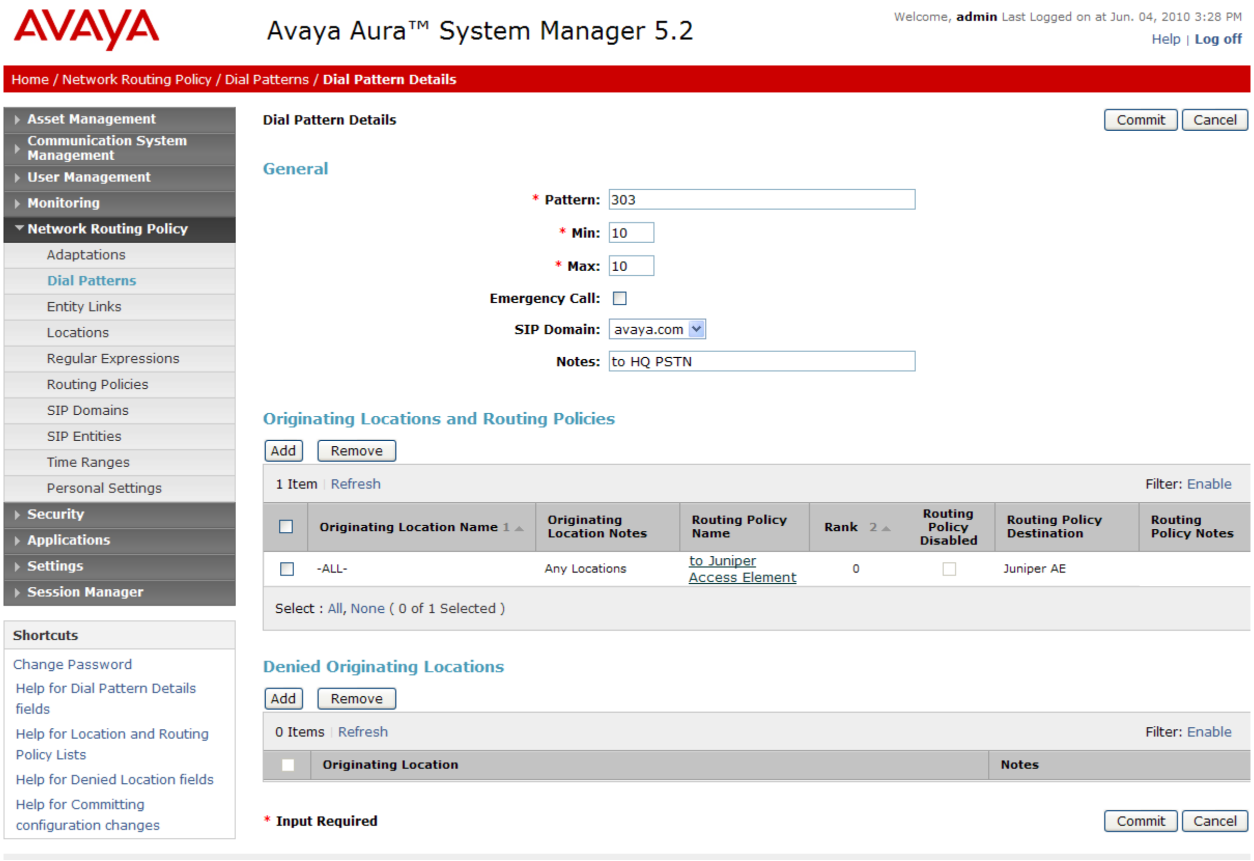
- **Pattern**: Dialed number or prefix
- **Min**: Minimum length of dialed number
- **Max**: Maximum length of dialed number
- **SIP Domain**: SIP domain specified in **Section 5.1**
- **Notes**: Comment on purpose of dial pattern.

Under *Originating Locations and Routing Policies*:
Click **Add**, and then select the appropriate Location (or "-ALL-") for **Originating Location Name** field and routing policy from the list.

Defaults can be used for the remaining fields. Click **Commit** to save the Dial Pattern.

The following screen shows the Dial Pattern defined for routing calls to the PSTN with the “303” area code. Since the calls to the “303” area code are Long-Distance toll calls for the branch location in the sample configuration, “-ALL-“ was selected for **Originating Location Name** so that calls from both the Headquarters and the branches would be routed to the Headquarters telephony infrastructure for termination to the PSTN through the T1/E1 facilities.

In Normal Mode, this Dial Pattern is also used to route incoming PSTN calls that the branch SRX210 receives over its FXO interfaces. The SRX210 was configured to route incoming PSTN calls to "3035383509". Session Manager then routes the call to Communication Manager for further call processing (such as delivering the call to an Auto-Attendant).


AVAYA
Avaya Aura™ System Manager 5.2
Welcome, admin Last Logged on at Jun. 04, 2010 3:28 PM
Help | Log off
Home / Network Routing Policy / Dial Patterns / Dial Pattern Details
Asset Management
Communication System Management
User Management
Monitoring
Network Routing Policy
Adaptations
Dial Patterns
Entity Links
Locations
Regular Expressions
Routing Policies
SIP Domains
SIP Entities
Time Ranges
Personal Settings
Security
Applications
Settings
Session Manager
Shortcuts
Change Password
Help for Dial Pattern Details fields
Help for Location and Routing Policy Lists
Help for Denied Location fields
Help for Committing configuration changes
Commit
Cancel
Add
Remove
Refresh
Filter: Enable

Dial Pattern Details

General

* Pattern: 303

* Min: 10

* Max: 10

Emergency Call: □

SIP Domain: avaya.com

Notes: to HQ PSTN

Originating Locations and Routing Policies

1 Item

□	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-	Any Locations	to Juniper Access Element	0	□	Juniper AE	

Select : All, None (0 of 1 Selected)

Denied Originating Locations

0 Items

□	Originating Location	Notes

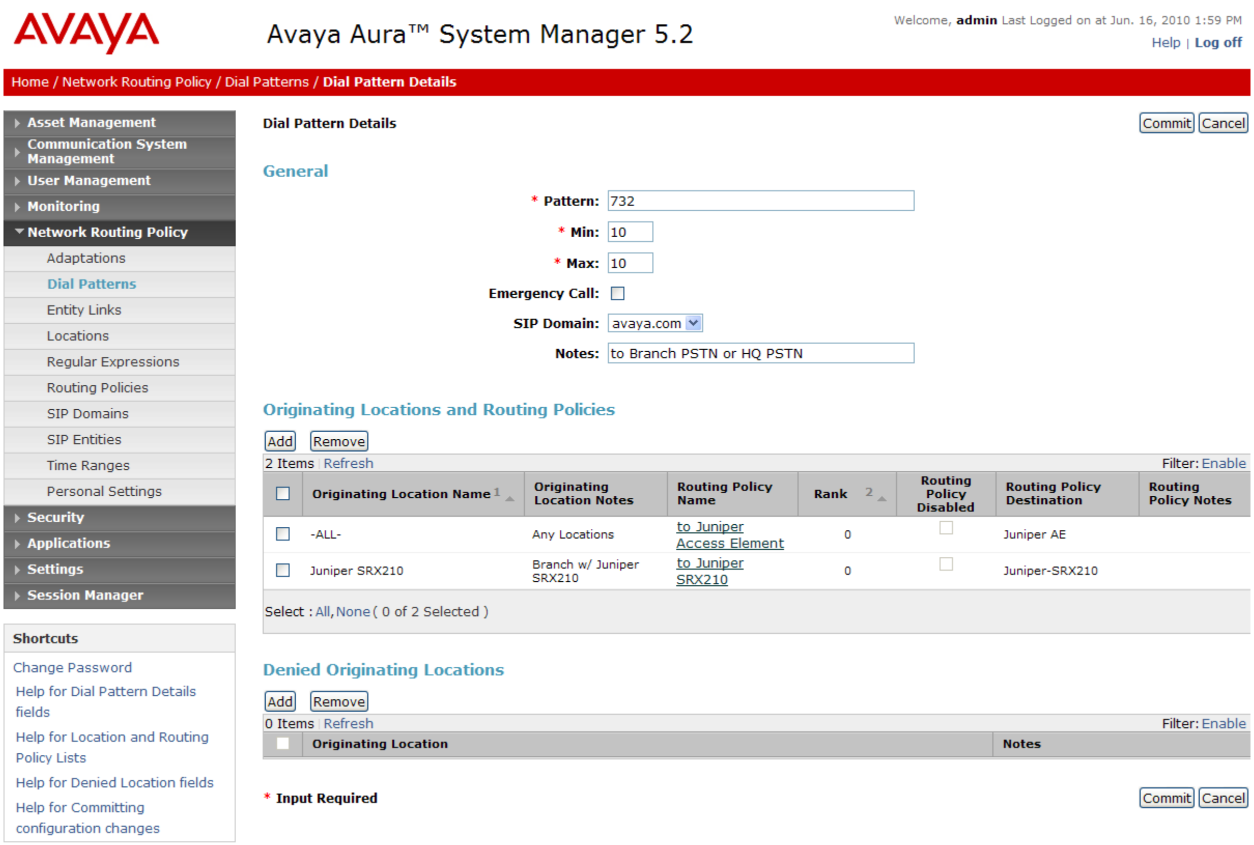
* Input Required

The following screen shows the Dial Pattern defined for routing calls to the PSTN with the "732" area code.

Since the calls to the "732" area code are local calls for the branch location, the Location "Juniper SRX210" (as defined in **Section 5.2**) was selected for **Originating Location Name** so that calls to the "732" area code from the sample branch would be routed to the SIP Entity "Juniper-SRX210" as specified in the Routing Policy "to Juniper SRX210". The branch SRX210 would route these calls out to the PSTN through its FXO interface ports.

A second entry was specified for the "732" Dial Pattern that would route calls to the "732" area code from all Locations, except the sample branch, to the Headquarters telephony infrastructure for termination to the PSTN through the T1/E1 facilities.

Note: In the case of Centralized Trunking arrangement, the branch specific entry is not needed since all PSTN calls, regardless of their origination locations, should be routed to the central location for termination to the PSTN.


AVAYA
Avaya Aura™ System Manager 5.2
Welcome, admin Last Logged on at Jun. 16, 2010 1:59 PM
Help | Log off
Home / Network Routing Policy / Dial Patterns / Dial Pattern Details
Asset Management
Communication System Management
User Management
Monitoring
Network Routing Policy
Adaptations
Dial Patterns
Entity Links
Locations
Regular Expressions
Routing Policies
SIP Domains
SIP Entities
Time Ranges
Personal Settings
Security
Applications
Settings
Session Manager
Shortcuts
Change Password
Help for Dial Pattern Details fields
Help for Location and Routing Policy Lists
Help for Denied Location fields
Help for Committing configuration changes
Commit
Cancel

Dial Pattern Details

General

* Pattern:	732
* Min:	10
* Max:	10
Emergency Call:	□
SIP Domain:	avaya.com
Notes:	to Branch PSTN or HQ PSTN

Originating Locations and Routing Policies

Add
Remove
Refresh
Filter: Enable

2 Items

□	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-	Any Locations	to Juniper Access Element	0	□	Juniper AE	
□	Juniper SRX210	Branch w/ Juniper SRX210	to Juniper SRX210	0	□	Juniper-SRX210	

Select : All, None (0 of 2 Selected)

Denied Originating Locations

0 Items

□	Originating Location	Notes

* Input Required

The routing of E-911 calls is outside the scope of these Application notes. However, 911 calls from the branch location in the Normal Mode should be routed back to the branch SRX210 to go out through the FXO interfaces to the local Emergency Response Center.

In the Survivable Mode, the routing policy on the branch SRX210 will route 911 calls from the branch to the PSTN through its FXO interfaces too.

Note that in real deployments, each branch should have its own entry under *Originating Location and Routing Policies* so that 911 calls from each branch would be routed to the local Emergency Response Center.

5.8. Add Avaya Aura™ Session Manager

Adding the Session Manager provides the linkage between System Manager and Session Manager. This configuration procedure should have already been properly executed if the Session Manager used has been set up for other purposes. This configuration step is included here for reference and completeness. To add Session Manager, expand the **Session Manager** menu on the left and select **Session Manager Administration**. Then click **Add** (not shown), and fill in the fields as described below and shown in the following screen (note that the screen below is for **Edit Session Manager** since it was already administered):

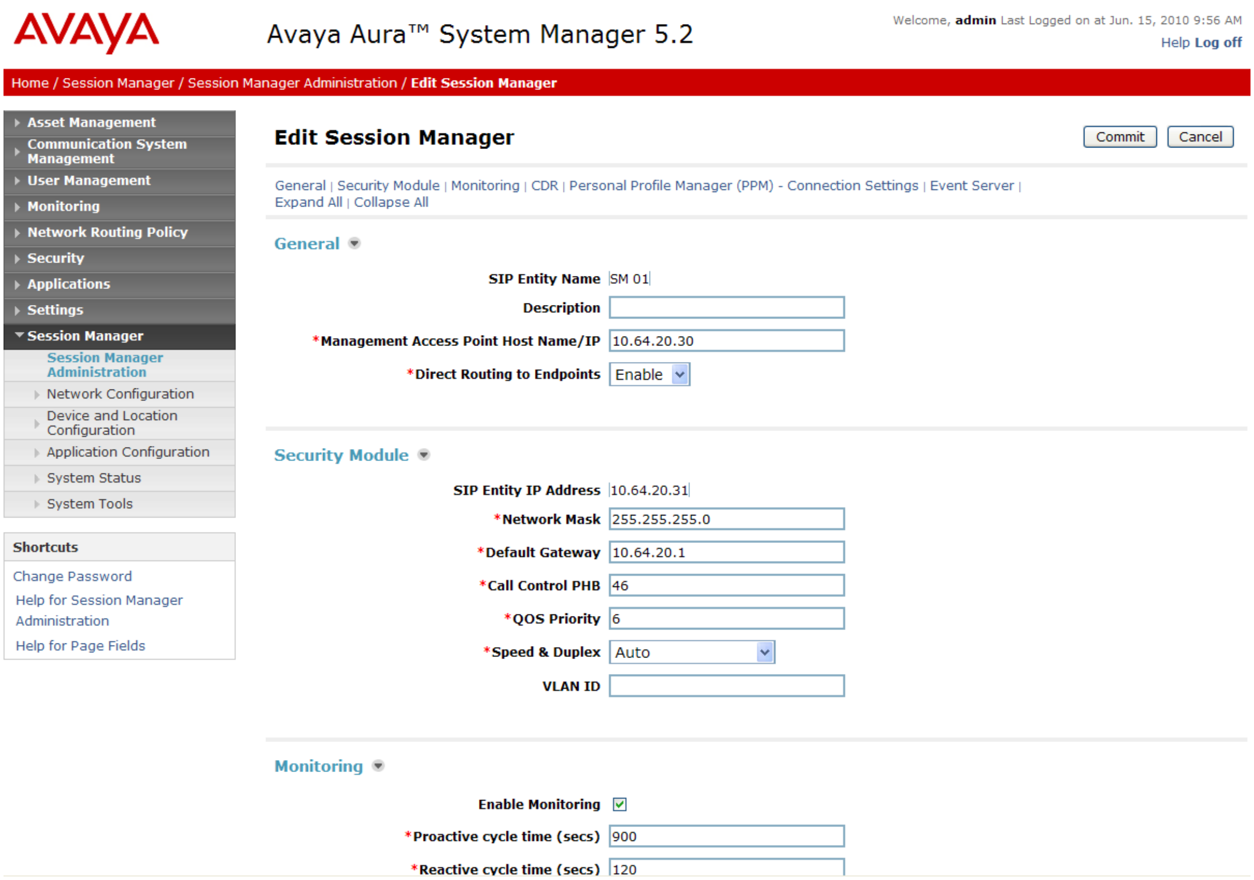
Under *General*:

- **SIP Entity Name**: Select the name of the SIP Entity created for Session Manager
- **Description**: Any descriptive text
- **Management Access Point Host Name/IP**: IP address of the Session Manager management interface

Under *Security Module*:

- **Network Mask**: Enter the proper network mask for Session Manager
- **Default Gateway**: Enter the default gateway IP address for Session Manager

Accept default settings for the remaining fields.


AVAYA
Avaya Aura™ System Manager 5.2
Welcome, admin Last Logged on at Jun. 15, 2010 9:56 AM
Help Log off
Home / Session Manager / Session Manager Administration / Edit Session Manager
Asset Management
Communication System Management
User Management
Monitoring
Network Routing Policy
Security
Applications
Settings
Session Manager
Session Manager Administration
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
Shortcuts
Change Password
Help for Session Manager Administration
Help for Page Fields
Commit
Cancel
General | Security Module | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |
Expand All | Collapse All

Edit Session Manager

General

SIP Entity Name	SM 01
Description	
*Management Access Point Host Name/IP	10.64.20.30
*Direct Routing to Endpoints	Enable

Security Module

SIP Entity IP Address	10.64.20.31
*Network Mask	255.255.255.0
*Default Gateway	10.64.20.1
*Call Control PHB	46
*QOS Priority	6
*Speed & Duplex	Auto
VLAN ID	

Monitoring

Enable Monitoring	☑
*Proactive cycle time (secs)	900
*Reactive cycle time (secs)	120

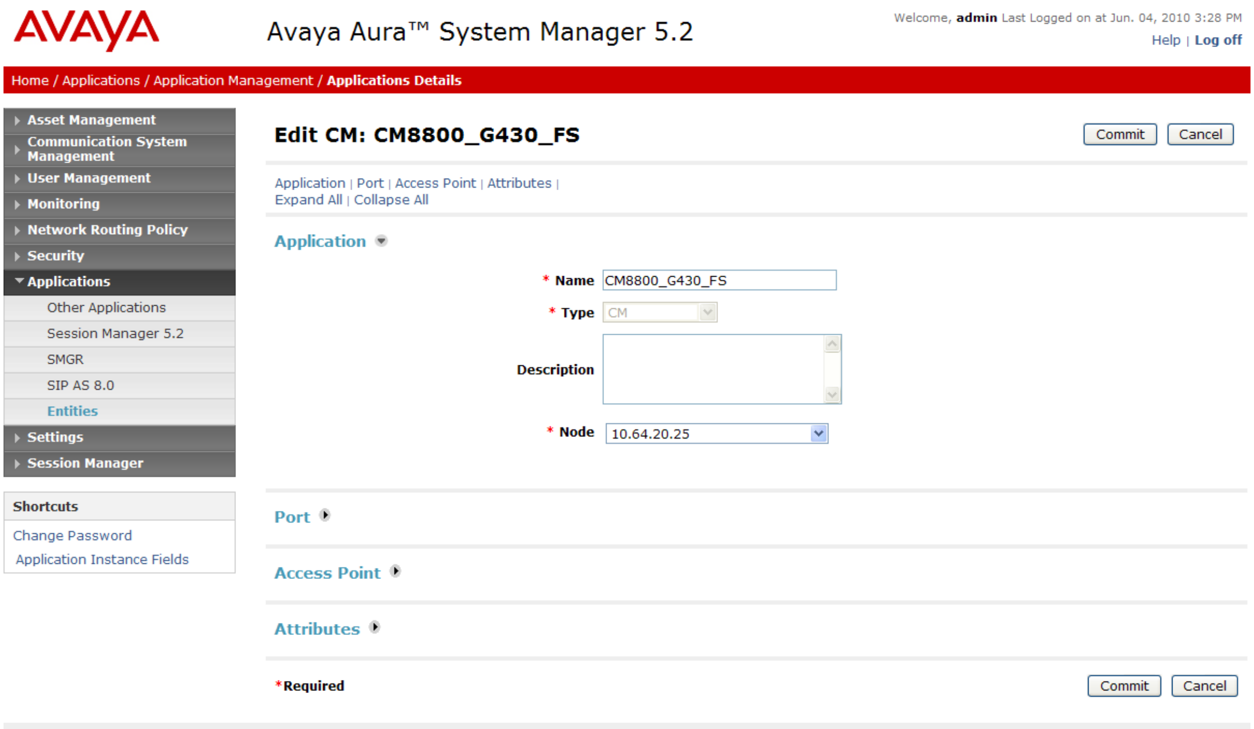
5.9. Add Avaya Aura^{TM} Communication Manger as a Feature Server

In order for Communication Manager to provide configuration and Feature Server support to SIP telephones when they register to Session Manager, Communication Manager must be added as an application for Session Manager. This is a four step process.

Step 1

Select **Applications → Entities** on the left. Click on **New** (not shown). Select "CM" for **Type**, and in the displayed "New CM Instance" page, enter the following fields. Use defaults for the remaining fields:

- **Name**: A descriptive name
- **Type**: "CM"
- **Node**: Select IP address for Communication Manager SAT access


AVAYA
Avaya Aura™ System Manager 5.2
Welcome, admin Last Logged on at Jun. 04, 2010 3:28 PM
Help | Log off
Home / Applications / Application Management / Applications Details
Asset Management
Communication System Management
User Management
Monitoring
Network Routing Policy
Security
Applications
Other Applications
Session Manager 5.2
SMGR
SIP AS 8.0
Entities
Settings
Session Manager
Shortcuts
Change Password
Application Instance Fields
Commit
Cancel
Application | Port | Access Point | Attributes |
Expand All | Collapse All
Application
Port
Access Point
Attributes
*Required
Commit
Cancel

Edit CM: CM8800_G430_FS

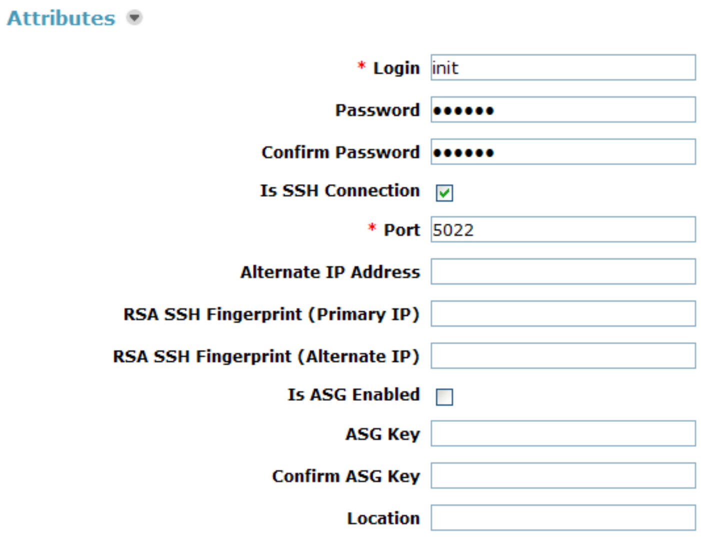
* Name	CM8800_G430_FS
* Type	CM
Description	
* Node	10.64.20.25

Under the *Attributes* section, enter the following fields, and use defaults for the remaining fields:

- **Login**: Login used for SAT access
- **Password**: Password used for SAT access
- **Confirm Password**: Password used for SAT access

Click on **Commit**. This will set up data synchronization with Communication Manager to occur periodically in the background.

The screen shown below is the Edit screen since the Application Entity has already been added.



Attributes

* Login	init
Password	••••••
Confirm Password	••••••
Is SSH Connection	☑
* Port	5022
Alternate IP Address	
RSA SSH Fingerprint (Primary IP)	
RSA SSH Fingerprint (Alternate IP)	
Is ASG Enabled	□
ASG Key	
Confirm ASG Key	
Location	

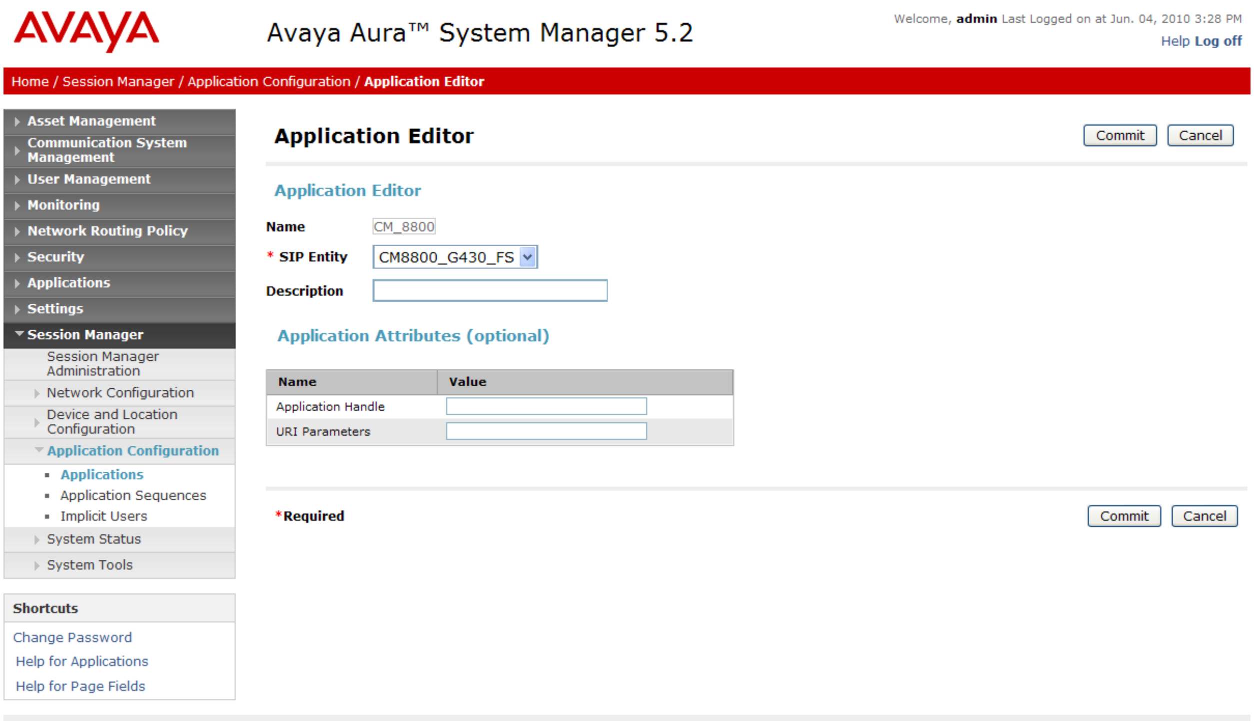
Step 2

Select **Session Manager → Application Configuration → Applications** on the left. Click on **New** (not shown). Enter the following fields, and use defaults for the remaining fields:

- **Name**: A descriptive name
- **SIP Entity**: Select the Communication Manager SIP Entity (see **Section 5.3**)

Click on **Commit**.

The screen shown below is the Edit screen since the Application has already been configured.



Application Editor

Application Editor

Name: CM_8800

* SIP Entity: CM8800_G430_FS

Description:

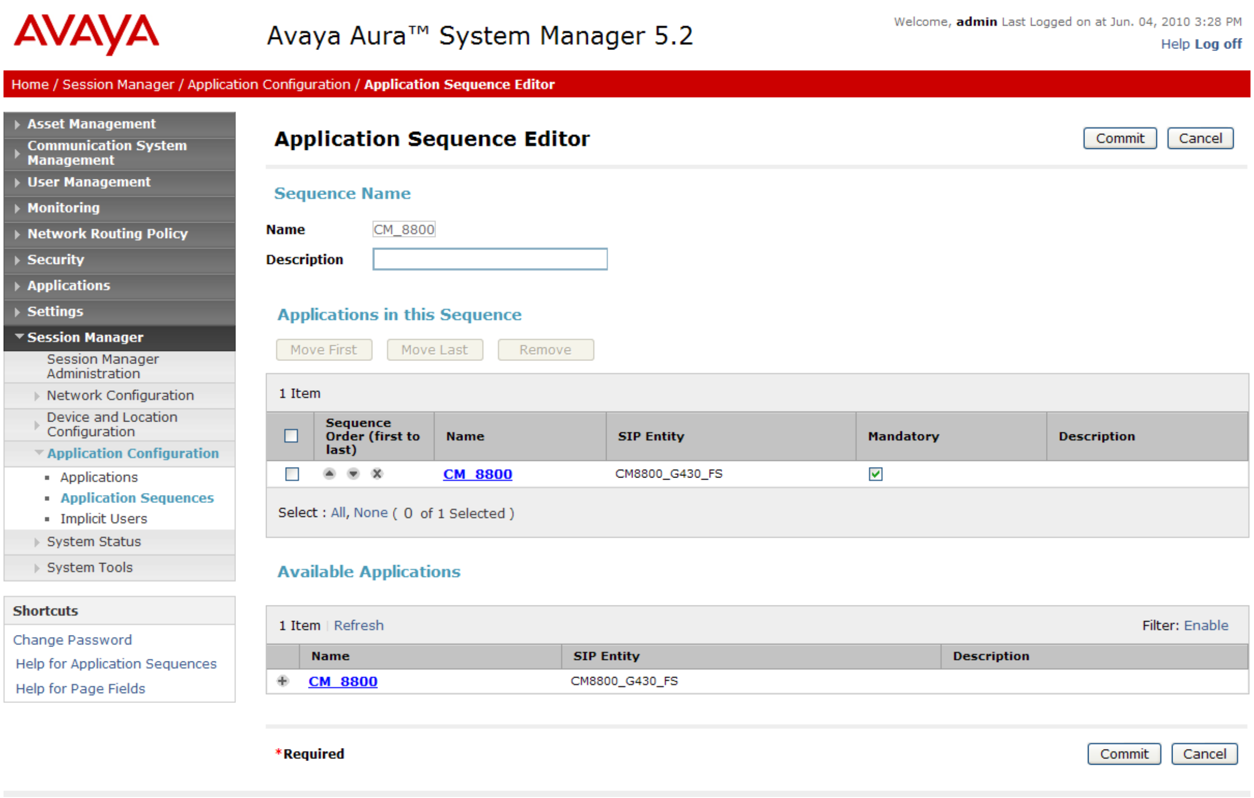
Application Attributes (optional)

Name	Value
Application Handle	
URI Parameters	

Step 3

Select **Session Manager → Application Configuration → Application Sequences** on the left. Click on **New** (not shown). Enter a descriptive Name. Click on the "+" sign next to the appropriate *Available Applications*, and the selected available application will be moved up to the *Applications in this Sequence* section. In the sample configuration, "CM_8800" was selected, as shown in the screen below (which is the Edit screen since the Application Sequence has already been configured).

Click on **Commit**.


AVAYA
Avaya Aura™ System Manager 5.2
Welcome, admin Last Logged on at Jun. 04, 2010 3:28 PM
Help Log off
Home / Session Manager / Application Configuration / Application Sequence Editor
Asset Management
Communication System Management
User Management
Monitoring
Network Routing Policy
Security
Applications
Settings
Session Manager
Session Manager Administration
Network Configuration
Device and Location Configuration
Application Configuration
Applications
Application Sequences
Implicit Users
System Status
System Tools
Shortcuts
Change Password
Help for Application Sequences
Help for Page Fields
Commit
Cancel
Move First
Move Last
Remove

Application Sequence Editor

Sequence Name

Name	CM_8800
Description	

Applications in this Sequence

1 Item

☐	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
☐	▲ ▼ ✕	CM_8800	CM8800_G430_FS	☑	

Select : All, None (0 of 1 Selected)

Available Applications

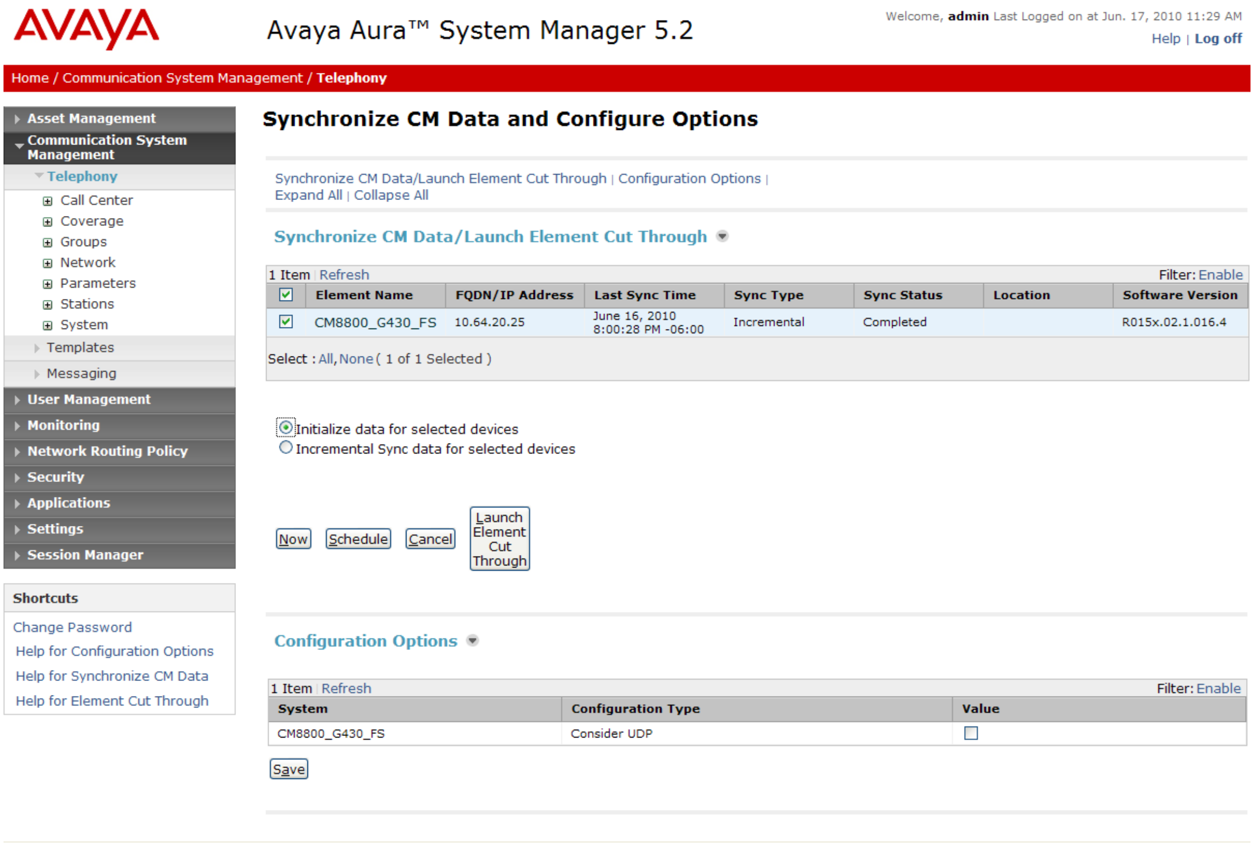
1 Item | Refresh　　Filter: Enable

	Name	SIP Entity	Description
+	CM_8800	CM8800_G430_FS	

*Required

Step 4

Select **Communication System Management → Telephony** on the left. Select the appropriate Element Name ("CM8800_G430_FS" in this case). Select **Initialize data for selected devices**. Then click on **Now**. This will cause a data synchronization task to start. This may take some time to complete.


AVAYA
Avaya Aura™ System Manager 5.2
Welcome, admin Last Logged on at Jun. 17, 2010 11:29 AM
Help | Log off
Home / Communication System Management / Telephony
Asset Management
Communication System Management
Telephony
Call Center
Coverage
Groups
Network
Parameters
Stations
System
Templates
Messaging
User Management
Monitoring
Network Routing Policy
Security
Applications
Settings
Session Manager
Shortcuts
Change Password
Help for Configuration Options
Help for Synchronize CM Data
Help for Element Cut Through
Synchronize CM Data/Launch Element Cut Through | Configuration Options |
Expand All | Collapse All
Now
Schedule
Cancel
Launch Element Cut Through
Save

Synchronize CM Data and Configure Options

Synchronize CM Data/Launch Element Cut Through

1 Item Refresh Filter: Enable

☑	Element Name	FQDN/IP Address	Last Sync Time	Sync Type	Sync Status	Location	Software Version
☑	CM8800_G430_FS	10.64.20.25	June 16, 2010 8:00:28 PM -06:00	Incremental	Completed		R015x.02.1.016.4

Select : All, None (1 of 1 Selected)

● Initialize data for selected devices
○ Incremental Sync data for selected devices

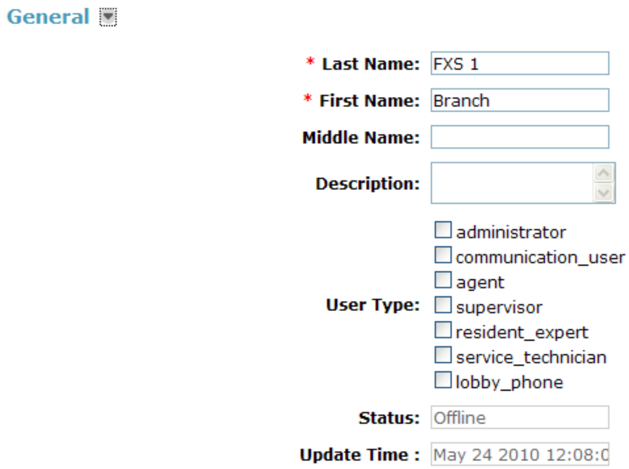
Configuration Options

1 Item Refresh Filter: Enable

System	Configuration Type	Value
CM8800_G430_FS	Consider UDP	□

5.10. User Management for Adding SIP Telephone Users

Users must be added to Session Manager corresponding to the SIP stations added in Communication Manager (see **Section 4.6**). Select **User Management → User Management** on the left. Then click on **New** (not shown) to open the New User Profile page. Enter a **First Name** and **Last Name** for the user being added.

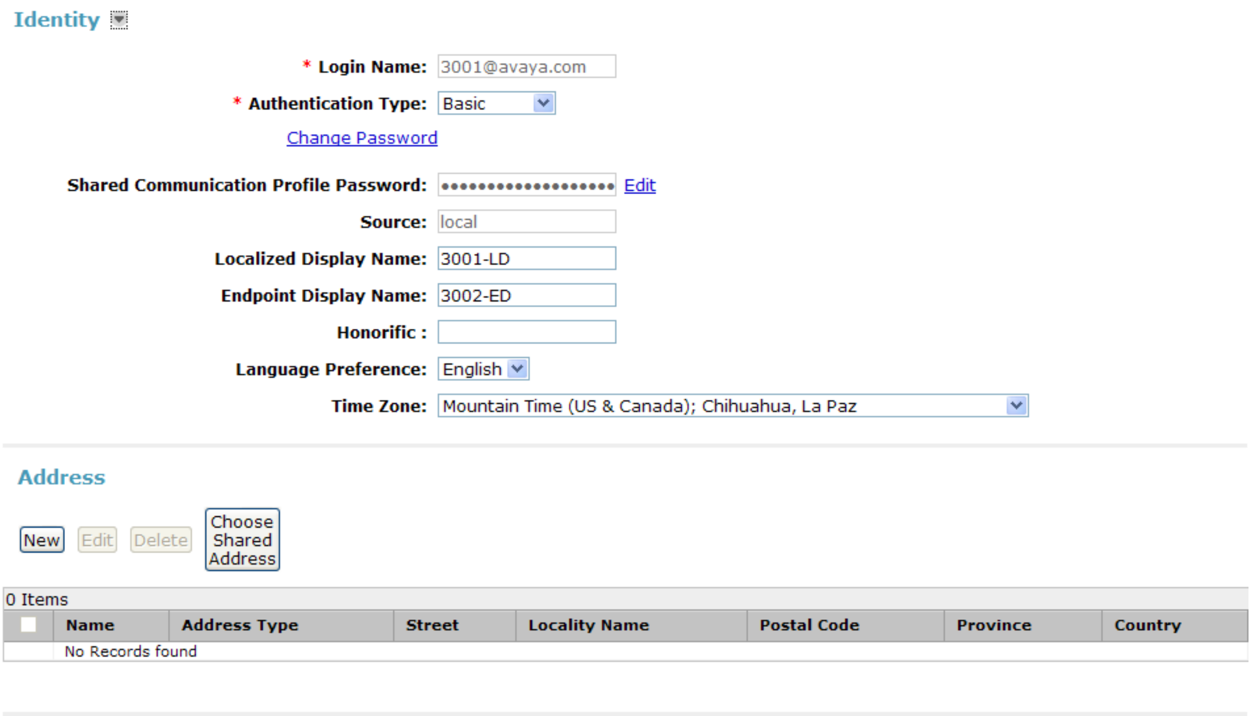


General

* Last Name:	FXS 1
* First Name:	Branch
Middle Name:	
Description:	
User Type:	□ administrator □ communication_user □ agent □ supervisor □ resident_expert □ service_technician □ lobby_phone
Status:	Offline
Update Time :	May 24 2010 12:08:0

Click on *Identity* to expand that section. Enter the following fields, and use defaults for the remaining fields:

- **Login Name**: Telephone extension with domain suffix (see **Section 5.1**)
- **Authentication Type** Basic
- **SMGR Login Password**:
  - **Password**: Password used to log into System Manger
  - **Shared Communication Profile Password**: Password used to log onto the telephone
- **Localized Display Name**: Name to be used as calling party
- **Endpoint Display Name**: Full name of user
- **Language Preference**: Select the appropriate language preference
- **Time Zone:** Select the appropriate time zone



Identity

* Login Name:	3001@avaya.com
* Authentication Type:	Basic
Change Password	
Shared Communication Profile Password:	●●●●●●●●●●●●●●●●●● Edit
Source:	local
Localized Display Name:	3001-LD
Endpoint Display Name:	3002-ED
Honorific :	
Language Preference:	English
Time Zone:	Mountain Time (US & Canada); Chihuahua, La Paz

Address

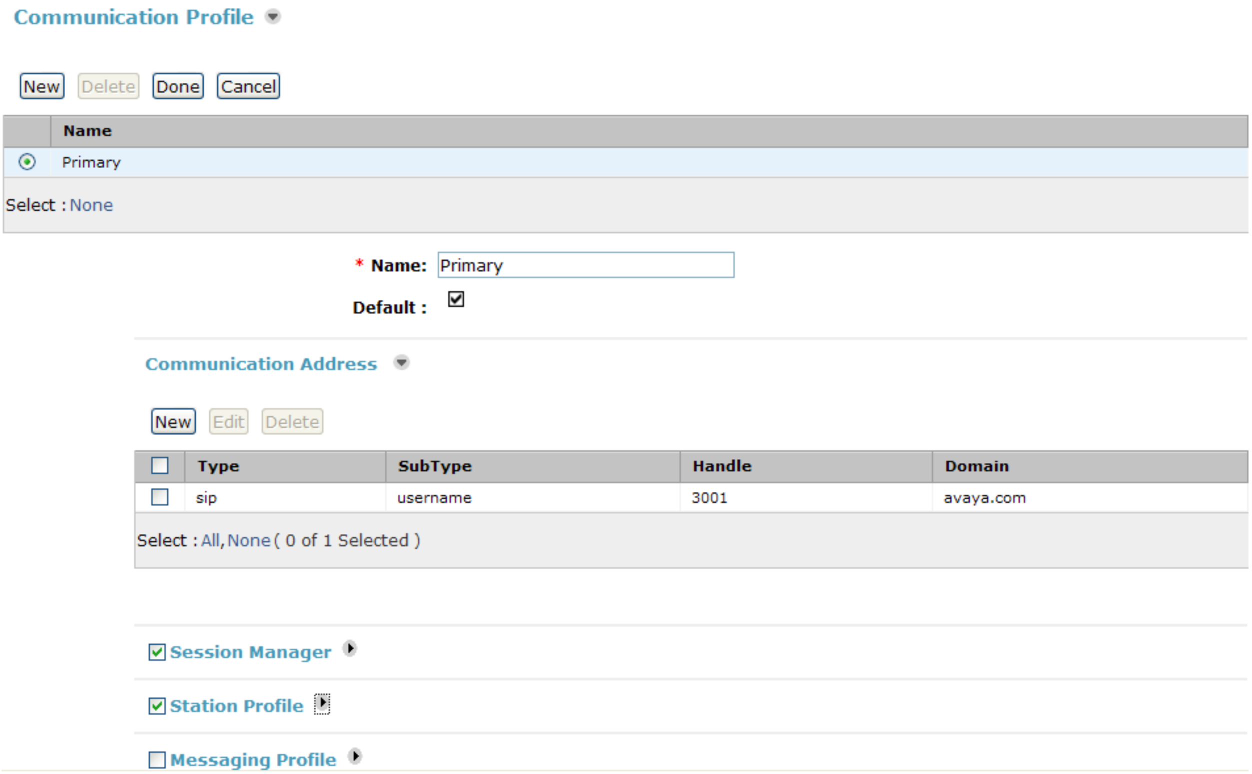
0 Items

□	Name	Address Type	Street	Locality Name	Postal Code	Province	Country
	No Records found						

Click on *Communication Profile* to expand that section. Then click on *Communication Address* to expand that section. Enter appropriate values in the following fields and use defaults for the remaining fields:

- **Type**: Select “sip”
- **SubType**: Select “username”
- **Fully Qualified Address**: Enter the extension and select the domain as specified in **Section 5.1**

Click on **Add** to add the record with the above information (the table entry for the added record is shown in the screen below).



Communication Profile

	Name
●	Primary

Select : None

* Name: Primary

Default : ☑

Communication Address

□	Type	SubType	Handle	Domain
□	sip	username	3001	avaya.com

Select : All, None (0 of 1 Selected)

☑ Session Manager

☑ Station Profile

□ Messaging Profile

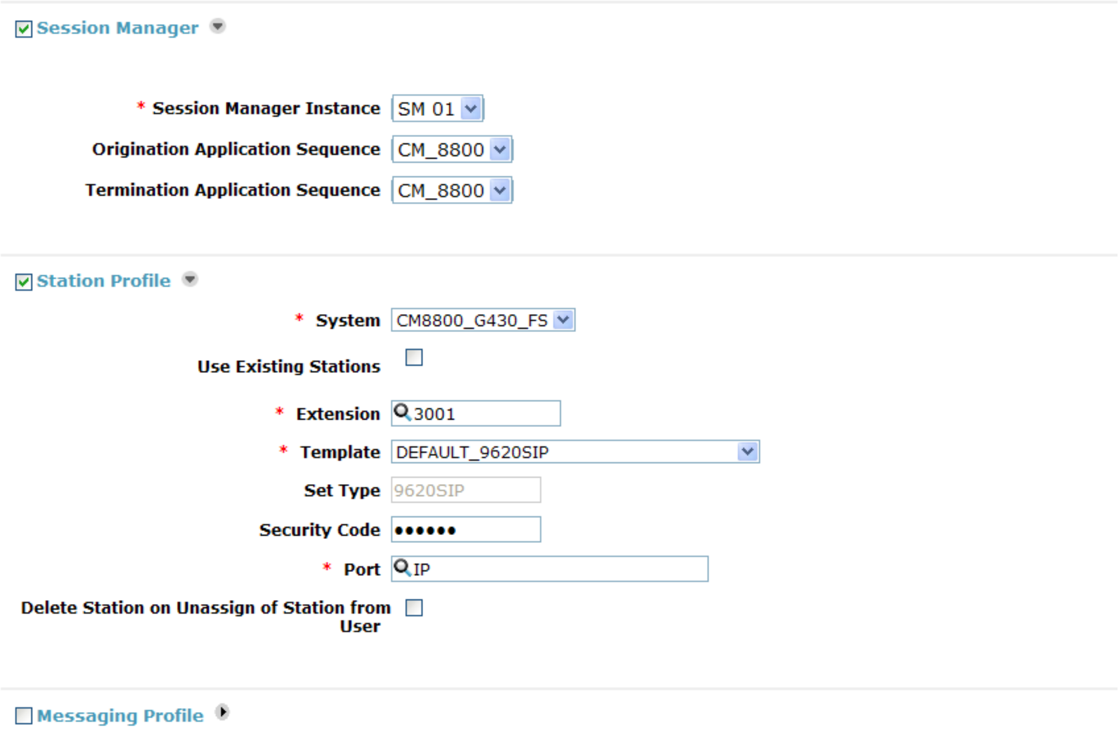
Click on *Session Manager* to expand that section. Select the appropriate Session Manager server for **Session Manager Instance**. For **Origination Application Sequence** and **Termination Application Sequence**, select the Application Sequence configured in **Section 5.9 Step 3**.

Click on *Station Profile* in the above screen to expand that section. Enter the following fields and use defaults for the remaining fields:

- **System**: Select the Communication Manager (Feature Server) entity
- **Extension**: Enter the extension
- **Template**: Select an appropriate template matching the telephone type as configured on Communication Manger (see **Section 4.6**)

- **Security Code**: Password to be entered by the user when logging onto the telephone
- **Port**: Click on the Search icon to select "IP" (a specific port number is then automatically populated in this field)

Click on **Commit** (not shown).



☑ Session Manager

* Session Manager Instance	SM 01
Origination Application Sequence	CM_8800
Termination Application Sequence	CM_8800

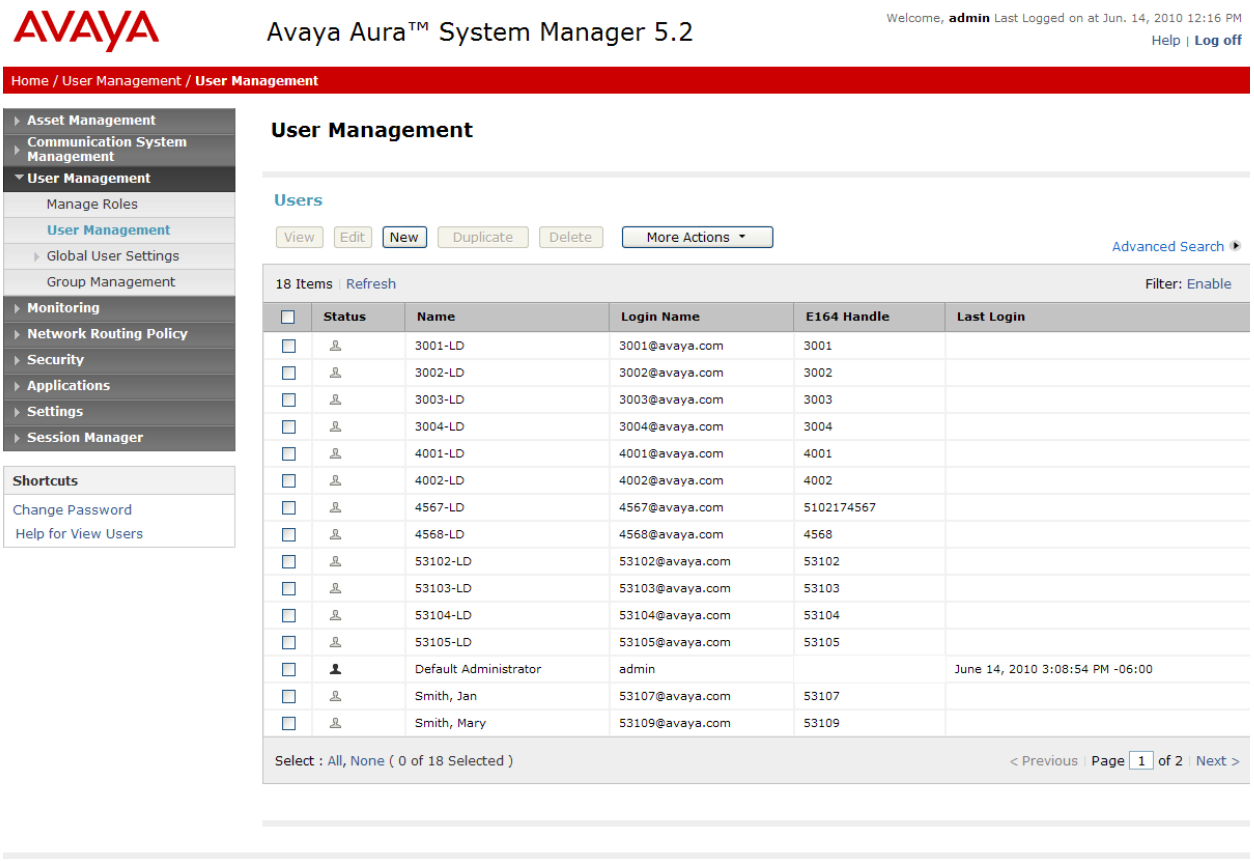
☑ Station Profile

* System	CM8800_G430_FS
Use Existing Stations	□
* Extension	3001
* Template	DEFAULT_9620SIP
Set Type	9620SIP
Security Code	••••••
* Port	IP
Delete Station on Unassign of Station from User	□

□ Messaging Profile

Repeat the above procedures to add each SIP telephone user for the Headquarters site as well as the branch site (including the analog phones connected to the FXS interface ports on the SRX210). The following User Management screen shows the SIP telephone users configured for the Headquarters site and the branch:

- 4001 and 4002 are Headquarters Avaya 9630 SIP Phone users
- 3003 and 3004 are branch Avaya 9620 SIP Phone users
- 3001 and 3002 are branch analog phones connected to the SRX210 FXS ports



□	Status	Name	Login Name	E164 Handle	Last Login
□	👤	3001-LD	3001@avaya.com	3001	
□	👤	3002-LD	3002@avaya.com	3002	
□	👤	3003-LD	3003@avaya.com	3003	
□	👤	3004-LD	3004@avaya.com	3004	
□	👤	4001-LD	4001@avaya.com	4001	
□	👤	4002-LD	4002@avaya.com	4002	
□	👤	4567-LD	4567@avaya.com	5102174567	
□	👤	4568-LD	4568@avaya.com	4568	
□	👤	53102-LD	53102@avaya.com	53102	
□	👤	53103-LD	53103@avaya.com	53103	
□	👤	53104-LD	53104@avaya.com	53104	
□	👤	53105-LD	53105@avaya.com	53105	
□	👤	Default Administrator	admin		June 14, 2010 3:08:54 PM -06:00
□	👤	Smith, Jan	53107@avaya.com	53107	
□	👤	Smith, Mary	53109@avaya.com	53109	

Select : All, None (0 of 18 Selected)
< Previous | Page 1 of 2 | Next >

6. Configure Avaya 9600 SIP Phones

The Avaya 9600 SIP Phones at all sites will use the Session Manager (10.64.20.31) as the SIP Proxy Server. The Avaya 9620 SIP Phones at the branch sites will also configure the on-site SRX210 (10.64.27.1) as an additional call server for survivability. The table below shows an example of the SIP telephone configuration settings for the Headquarters and the branch.

	Headquarters	**Sample Branch**
Extension	4001	3003
IP Address (DHCP)	10.64.21.116	10.64.27.102
Subnet Mask	255.255.255.0	255.255.255.0
Router	10.64.21.1	10.64.27.1
File Server	10.64.21.200	10.64.21.200
SIP Domain	avaya.com	avaya.com
SIP Proxy Server	10.64.20.31	10.64.20.31
Alternate SIP Proxy Server		10.64.27.1

Note: The alternate SIP Proxy Server can be configured manually on the Avaya 9600 SIP Phones or through the 46xxsetttings configuration file.

The configuration parameters of the Avaya 9600 SIP Phone specific to SIP Survivability in the 46xxsettings file are listed in the table below. See **[7]** for more details.

46xxsettings.txt Parameter Name	**Value Used in Sample Configuration**	**Description**
SIP_CONTROLLER_LIST	10.64.20.31:5060;transport=tcp, 10.64.27.1;transport=udp	A priority list of SIP Servers for the phone to use for SIP services. The port and transport use the default values of 5061 and TLS when not specified. The setting used in the sample configuration shows the values used for this parameter for a phone in the sample branch. The Session Manager is the first priority SIP Server listed using port 5060 and TCP transport. Separated by a comma, the sample branch Juniper SRX210 is the next priority SIP Server using port 5060 and UDP transport. The SIP Server list for each branch would require different values for

46xxsettings.txt Parameter Name	Value Used in Sample Configuration	Description
		the SIP_CONTROLLER_LIST, e.g. the list for Branch 1 phones will include the Session Manager and the Branch 1 Juniper SRX210 while the list for Branch 2 phones will include the Session Manager and the Branch 2 Juniper SRX210. To accomplish this, the GROUP system value mechanism can be implemented as described in **[7]**.
FAILBACK_POLICY	Auto	While in Survivable Mode, determines the mechanism to use to fail back to the centralized SIP Server. **Auto** = the phone periodically checks the availability of the primary controller and dynamically fails back.
FAST_RESPONSE_TIMEOUT	2	The timer terminates SIP INVITE transactions if no SIP response is received within the specified number of seconds after sending the request. Useful when a phone goes off-hook after connectivity to the centralized SIP Server is lost, but before the phone has detected the connectivity loss. The default value of 4 seconds may be retained if desired. After the SIP INVITE is terminated, the phone immediately transitions to Survivable Mode.
MSGNUM	4999	The number dialed when the Message button is pressed and the phone is in Normal Mode.
PSTN_VM_NUM	913035383501	The number dialed when the Message button is pressed and the phone is in Survivable Mode.
RECOVERYREGISTERWAIT	60	A Reactive Monitoring Interval. If no response to a "maintenance

46xxsettings.txt Parameter Name	Value Used in Sample Configuration	Description
		check" REGISTER request is received within the timeout period, the phone will retry the monitoring attempt after a randomly selected delay of 50% - 90% of this parameter.
DISCOVER_AVAYA_ENVIRONMENT	1	Automatically determines if the active SIP Server is an Avaya server or not.
SIPREGPROXYPOLICY	simultaneous	A policy to control how the phone treats a list of proxies in the SIP_CONTROLLER_LIST parameter **alternate** = remain registered with only the active controller **simultaneous** = remain registered with all available controllers
SIPDOMAIN	avaya.com	The enterprise SIP domain. Must be the same for all SIP controllers in the configuration. SIPDOMAIN is set to “avaya.com” in the sample configuration.

7. Configure Juniper SRX210

This section shows the configuration of the Juniper SRX210 Services Gateway to provide connectivity to a remote centralized SIP Peer-Call-Server (in this case a Session Manager) which is providing call routing and handling for the branch during normal operations. It also shows the Branch SRX Survivable-Call-Server configuration providing local call handling and call routing when the Session Manager at the central site is no longer reachable.

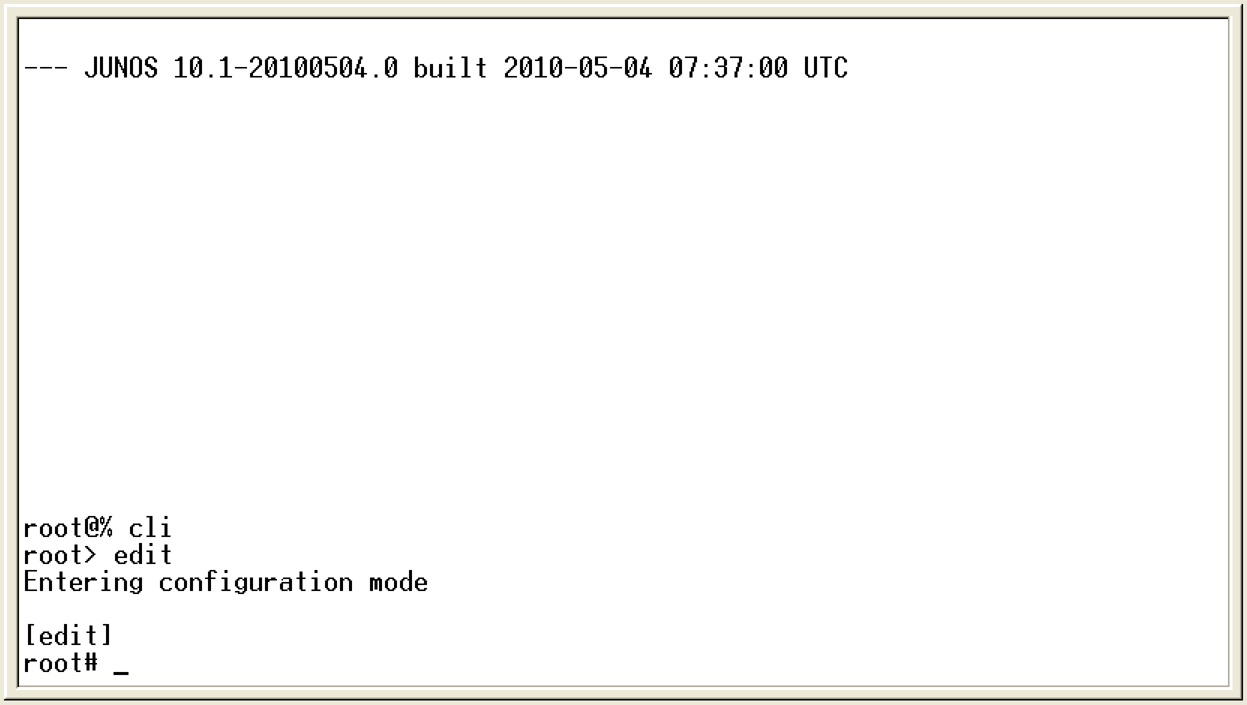
The procedures described in this section include configurations in the following areas. It is assumed that the basic configuration of the Juniper SRX210 has already been administered. See **[11]** and **[12]** for additional information.

- Verify POE and DHCP configuration
- Configuring Class of Restriction and Station Templates
- Configuring Analog and SIP Stations
- Configuring SRX Peer-call-Server
- Configuring Trunks and Trunk Groups
- Configuring Dial Plan for Normal Mode
- Configuring Media Gateway
- Configuring Dial Plan for Survivable Mode
- Configuring ICS Survivable Call Server
- Configuring Voice Mail Forwarding and Remote Access

The Juniper SRX210 configurations are performed through configuration CLI (Command Line Interface) commands in a terminal session using either of the following 2 access methods:

- Connect a PC to the branch SRX210 console port using a serial connection, then start a terminal session using Windows HyperTerminal
- Establish an SSH session to the SRX210 using either its trusted or untrusted IP address as listed in **Table 1** in **Section 2**.

Once a communications session is properly established, log in with administrative credentials, then enter the configuration mode as shown below. The configuration commands shown in the ensuing sections are all issued from the CLI configuration mode.



```
--- JUNOS 10.1-20100504.0 built 2010-05-04 07:37:00 UTC









root@% cli
root> edit
Entering configuration mode

[edit]
root# _
```

7.1. Verifying POE and DHCP Configuration

DHCP is used to provide IP Addresses and configuration for the branch IP Phones. If POE and DHCP are already configured, this step may be skipped.

Use the following commands to enable POE and verify DHCP Services on a Branch SRX210. Note that the DHCP IP address ranges were previously administered for the sample configuration. Note that the sample configuration used the IP address space 10.64.27.0/24 only for voice communications; the IP address space 10.64.26.0/24 was set up for data communications and was not used in the sample configuration.

Optional: Configure DHCP Options for BOOTP Server and Filename:

If the DHCP Provisioning method is used, you may need to specify option 242 for Avaya 9600-Series IP Phones. Setting `option 242 string HTTPSRVR=10.64.21.200,L2QVLAN=0` tells the phones within the specified DHCP pool to connect to the HTTP Server at 10.64.21.200 to download configuration information and firmware:

```
   [edit]
   root# set poe interface all

   root# edit system services dhcp

   Under [edit system services dhcp], issue following commands:

   set option 242 string “HTTPSRVR=10.64.21.200,L2QVLAN=0”
```

7.2. Configuring Class of Restriction and Station Templates

A Class of Restriction policy is required before making any calls. The COR statements specify types of calls and whether or not they’re allowed. If a policy allows a certain type of call and the Class of Restriction (COR) configuration that it belongs to is assigned to a station (or to a template that is assigned to a station), a user of the station’s telephone is allowed to place the call. If a policy denies the call type, the user cannot make the call. By default, emergency and intra-branch calls do not require a Class of Restriction. In the sample configuration, any call type is configured to be allowed.

```
[edit]
root# edit services converged-services

Under [edit services converged-services], issue following commands:

set class-of-restriction cor1 policy 1 call-type any-call
set class-of-restriction cor1 policy 1 permission allow
```

A station template is a set of values configured to apply to stations of the same kind. Station templates for SIP and analog phones contain different parameters. Values configured for a station template are inherited by all stations it is applied to.

```
[edit]
root# edit services converged-services

Under [edit services converged-services], issue following commands:

set station-template sip-template SIPT dtmf-method rfc-2833
set station-template sip-template SIPT class-of-restriction cor1
set station-template sip-template SIPT codec G711-MU

set station-template analog-template Analog class-of-restriction cor1
```

7.3. Configuring Analog and SIP Stations

Analog stations connect to FXS interfaces on the branch SRX210. The branch SRX210 will register these stations to the Session Manager using the auth-id and auth-passwords specified. The station extension used here should have also been configured on the Communication Manager and the Session Manager as described in **Section 4.6** and **Section 5.10**. Configure the analog stations and apply the station-template "Analog" (created in **Section 7.2**) as follows:

```
[edit]
root# edit services converged-services

Under [edit services converged-services], issue following commands:

set station 3001 extension 3001
set station 3001 caller-id 3001
set station 3001 auth-id 3001 auth-password 123456
set station 3001 station-type analog template Analog
set station 3001 station-type analog tdm-interface fxs-0/0/10

set station 3002 extension 3002
set station 3002 caller-id 3002
set station 3002 auth-id 3002 auth-password 123456
set station 3002 station-type analog template Analog
set station 3002 station-type analog tdm-interface fxs-0/0/11
```

When the branch SRX210 is in Survivable Mode, local SIP phones will register to it. If authentication is desired, configure the branch SIP stations with an auth-id and auth-password. Configure the SIP stations and apply the station-template "SIPT" (created in **Section 7.2**) as follows:

```
[edit]
root# edit services converged-services

Under [edit services converged-services], issue following commands:

set station 3003 extension 3003
set station 3003 caller-id 3003
set station 3003 station-type sip template SIPT
set station 3003 auth-password 123456
   set station 3004 extension 3004
   set station 3004 caller-id 3004
   set station 3004 station-type sip template SIPT
   set station 3004 auth-password 123456
```

7.4. Configuring the SRX Peer-Call-Server

The branch SRX210 uses the Session Manager at the Headquarters to provide call handling and call routing services for all directly attached analog (FXS) and SIP endpoints in Normal Mode. This is accomplished by configuring the Peer-Call-Server on the branch SRX210. Below is the configuration of the Peer-Call-Server named “AvayaSM” as used during compliance testing.

```
[edit]
root# edit services converged-services
```

Under **[edit system services converged-services]**, issue following commands:

```
set peer-call-server AvayaSM address ipv4-addr 10.64.20.31
set peer-call-server AvayaSM codec G711-MU
set peer-call-server AvayaSM dtmf-method rfc-2833
set peer-call-server AvayaSM auth-id 3035383509
```

The 4th command above (“`set peer-call-server AvayaSM auth-id 3035383509`”) configures the number that the branch SRX210, in the Normal Mode, will send to the Peer-Call-Server for further routing when the branch SRX210 receives PSTN calls on its FXO interfaces. In the Survivable Mode, the auto-attendant on the FXO interfaces will be enabled to handle these inbound FXO calls.

7.5. Configuring Trunks and Trunk Groups

The SRX210 dial plan includes route patterns that have one or more trunk groups. Each trunk group specifies one or more trunks to be used to route calls that specify a trunk's prefix, referred to as a trunk access code. To route calls to the PSTN from the branch, the branch SRX210 uses PSTN trunks for which interfaces are configured. The following commands illustrate how to configure two FXO trunks named "fxo12" and "fxo13" for PSTN access.

```
[edit]
root# edit services converged-services

Under [edit services converged-services], issue following commands:

set trunk fxo12 trunk-type fxo tdm-interface fxo-0/0/12
set trunk fxo13 trunk-type fxo tdm-interface fxo-0/0/13
```

Trunk groups combine trunks to be used to route calls. Add one or more trunks to a trunk group in the order they will be used. In the sample configuration, one trunk group named "MyTrunkGroup" was configured for PSTN and emergency calls.

```
[edit]
root# edit services converged-services

[edit services converged-services]
set trunk-group MyTrunkGroup trunk fxo12 trunk fxo13
```

Note: The SRX210 also supports a connection to a SIP trunk provided by a Service Provider. A SIP trunk can replace branch PSTN lines with a SIP trunking service from a Service Provider for branch calls to the PSTN. In the sample configuration, no direct SIP trunk to the Service Provider was configured. See **Section 1.1.5** for PSTN trunking configurations used in the sample configuration. The Distributed Trunking arrangement provides cost savings by routing local PSTN calls through the branch SRX210 FXO interfaces and long-distance toll calls via the T1/E1 facilities at the central site through the Avaya G-Series Media Gateway.

7.6. Configuring Dial Plan for Normal Mode

A dial plan for the Normal Mode must be configured to specify where calls will be routed, should the Session Manager route the call back to the branch SRX210. Route patterns of a dial plan include digit patterns against which called numbers are matched. Configure the dial plan for the Normal Mode when the Peer–Call-Server (the Session Manager at the central site) is in control.

```
[edit]
root# edit services converged-services

Under [edit services converged-services],issue following commands:

set dial-plan plan2 route-pattern 911 call-type trunk-call
set dial-plan plan2 route-pattern 911 trunk-group MyTrunkGroup
set dial-plan plan2 route-pattern 91732XXXXXXX call-type trunk-call
set dial-plan plan2 route-pattern 91732XXXXXXX trunk-group MyTrunkGroup
```

911 and PSTN calls to the "732" area code from the branch will be sent back by the Session Manager, based on its Dial Patterns and Routing Policies, to the SRX210 and then be routed out to the PSTN through the "MyTrunkGroup" trunk group as configured in **Section 7.5**.

7.7. Configuring Media Gateway

The Media Gateway must be configured for handling calls routed back from the Session Manager to the Branch SRX210. The Media Gateway "MGW", as configured below, is bound to the peer-call-server "AvayaSM" and requires a dial-plan as configured in **Section 7.6**. The dial-plan associated with the Media Gateway is active whenever the Peer-Call-Server is reachable.

```
[edit]
root# edit services converged-services

Under [edit services converged-services], issue following commands:

set media-gateway MGW peer-call-server AvayaSM
set media-gateway MGW dial-plan plan2
set media-gateway MGW protocol sip port 5060
set media-gateway MGW protocol sip transport udp
```

7.8. Configuring Dial Plan for Survivable Mode

When the SRX210 is in Survivable Mode, a separate call routing dial plan is put into use. In the Normally Mode, the SRX210 relies on the Session Manager at the central site to route calls, but when it is unreachable the SRX210 takes control and the dial plan for the Survivable Mode becomes active. The dial plan for the Survivable Mode may emulate the Peer-Call-Server dial plan ("plan2" in the sample configuration) so users will have a seamless experience (e.g. using the same dialed digits).

```
[edit]
root# edit services converged-services
Under [edit services converged-services], issue following commands:

Set digit-manipulation digit-transform del-9 regular-expression "s/^9//"

set dial-plan plan1 route-pattern 911 call-type emergency-call
set dial-plan plan1 route-pattern 911 trunk-group MyTrunkGroup

set dial-plan plan1 route-pattern 91303XXXXXXX call-type long-distance-
call

set dial-plan plan1 route-pattern 91303XXXXXXX trunk-group MyTrunkGroup
set dial-plan plan1 route-pattern 91732XXXXXXX call-type local-call
set dial-plan plan1 route-pattern 91732XXXXXXX trunk-group MyTrunkGroup

set dial-plan plan1 route-pattern 9911 call-type emergency-call
set dial-plan plan1 route-pattern 9911 trunk-group MyTrunkGroup digit-
transform del-9
```

Note: With the sample configuration above, calls to the PSTN with area codes "732" and "303" from the branch are allowed. In real deployments, the dial-plan may be modified in accordance with appropriate business policies.

Note: For the branch phones to dial out to the PSTN, "9" must be dialed first before the actual dialed digits (as consistent with the Normal Mode dialing). The flexibility to not dial the "9" first may or may not be desirable in real deployments, and therefore should be modified as appropriate.

7.9. Configuring Survivable-Call-Server

When the Peer-Call-Server (Session Manager) is not available, the Survivable-Call-Server (SCS) on the SRX210 activates to provide call routing and handling services within the branch for analog FXS and local SIP phones. The following SCS configuration named "SCS" allows the SRX210 SCS to monitor the health of the Peer-Call-Server and provide call handling and routing when the Peer-Call-Server is unreachable. The dial-plan for the Survivable Mode must be associated with the SCS.

```
[edit]
root# edit services converged-services
```

```
Under [edit services converged-services], issue following commands:

set survivable-call-service SCS peer-call-server AvayaSM
set survivable-call-service SCS dial-plan plan1
set survivable-call-service SCS registration-expiry-timeout 3600
```

7.10. Configuring Voice Mail Remote Access

In the Survivable Mode, the SRX210 covers unanswered calls at branch phones to the following PSTN remote access number of the voice mail messaging system (Modular Messaging was used in the sample configuration) if the call is not answered by the 4th ring.

```
[edit]
root# edit services converged-services
```

```
[edit services converged-services]
root# set features voicemail extension 4999 remote-access-number
913035383501
```

8. General Test Approach and Test Results

This section describes the validation test used to verify the sample configuration for the Session Manager Survivable SIP Gateway Solution using the Juniper SRX210 Services Gateway in the branch. This section covers the general test approach and the test results.

8.1. General Test Approach

The general test approach was to break and restore network connectivity from the branch site to the Headquarters site to verify that

- When network connectivity is broken, the branch Juniper SRX210 gateway automatically assumes the SIP proxy and SIP registrar functions. In this Survivable Mode, the branch phones can still call each other and reach PSTN through the Juniper SRX210 FXO analog trunk interface.
- When network connectivity is restored, the Session Manager at the Headquarters location automatically assumes the SIP proxy and SIP registrar functions for providing centralized SIP call control. In this Normal Mode, PSTN access by phones at both the headquarters and branch sites are through the T1/E1 connection on the Avaya Media Gateway at the central location with the exception that local non-toll calls from the branch phones are routed to the PSTN through the branch Juniper SRX210.

8.2. Test Results

The following features and functionality were verified. Any observations related to these tests are listed at the end of this section:

- In Normal Mode, the Session Manager located at the central site serves as the SIP registrar and proxy for phones at both the central and branch sites; in Survivable Mode, the Juniper SRX210 located at the branch location serves as the SIP registrar and proxy for the branch phones.

- Branch phones register to the Session Manager and the branch Juniper SRX210 simultaneously. Switching between the Normal and the Survivable Modes is automatic and within a reasonable time span (within about 1 minute).
- In Normal Mode, calls can be placed between phones at the main site and the branch site, and among phones within the site.
- In Normal Mode, local non-toll calls from the branch are routed to the PSTN through the FXO interfaces on the Juniper SRX210; long-distance toll calls from the branch phones are routed to the PSTN through the T1/E1 connection on the Avaya Media Gateway at the central location.
- In Survivable Mode, calls can be placed among phones within the branch. In addition, branch phones can still place calls to the PSTN (and to the phones at Headquarters via PSTN) using the FXO interface on the branch Juniper SRX210.
- PBX features including Hold, Transfer, Call Waiting, Call Forwarding and Conference on Avaya 9600 SIP Phones in both Normal and Survivable Modes.
- Analog phones connected to the FXS ports on the Juniper SRX210 are properly adapted as SIP phones in both Normal and Survivable Modes.
- Messaging system access by branch phones (through internal access number in Normal Mode and PSTN call in Survivable Mode) and proper function of MWI (Messaging Waiting Indicator) on the Avaya 9600 IP Phones in the Normal Mode.
- Proper system recovery after Juniper SRX210 restart and loss/restoration of IP connection.

The following problems were observed during compliance testing with disposition notes from Juniper (the JUNOS release in the notes refers to the Juniper SRX Services Gateway firmware):

1. There is no Music-On-Hold for the branch phones in the Survivable Mode.

   Note: Juniper reports this problem has been fixed with JUNOS release 10.2 R2.

2. There is no SRX configuration to control the number of rings before a call goes to coverage through FXO in the Survivable Mode.

   Note: Juniper reports this problem has been fixed with JUNOS release 10.2 R2.

The following functions/capabilities are currently unsupported by the Juniper SRX Services Gateway firmware (with notes made by Juniper):

- Normal Mode: Music-On-Hold (MoH) when the branch FXS phone calls branch and Headquarters endpoints and places the call on hold[4].
  Note: The FXS ports on SRX210 do not support any supplementary services, including Hold; therefore, MoH is not an expected behavior.

- Alpha-numeric Caller-ID in the Survivable Mode.

[4] In the compliance tested configuration, the FXS phone Hold function is a function on the Avaya analog phone itself. It is not a capability on the SRX210.

Note: The SRX currently supports numeric digit Caller-ID, but not alpha-numeric. This can be an enhancement per customer request.

- Call waiting using switch-hook flash to switch between calls on FXS-connected analog phones.
  Note: The FXS ports on SRX210 do not support any supplementary services, including switch-hook flash.

- Message Waiting Indicator (MWI) on branch IP phones and stutter-tone on branch FXS-connected analog phones for message waiting alert in the Survivable Mode.
  Note: MWI received by SIP phones prior to outage will keep blinking during outage. Stutter tone for analog phones can be an enhancement per customer request.

- The SRX210 does not respond properly to the SIP Options messages from the Session Manager. The SRX210 responds with a "404 Not Found" rather than with a "200 OK".
  Note: This can be an enhancement per customer request.

- Survivable Mode: Entire conference terminates when the conference initiating phone drops from the conference first
  Note: SRX implements 3-way calling in the Survivable Mode by having the handset mix the calls. This 3-way call model was tested with a variety of industry phones to work as designed. However, this call model differs from Avaya's call conference model. Juniper is to offer a solution similar to Avaya's call conference model where this caveat becomes critical.

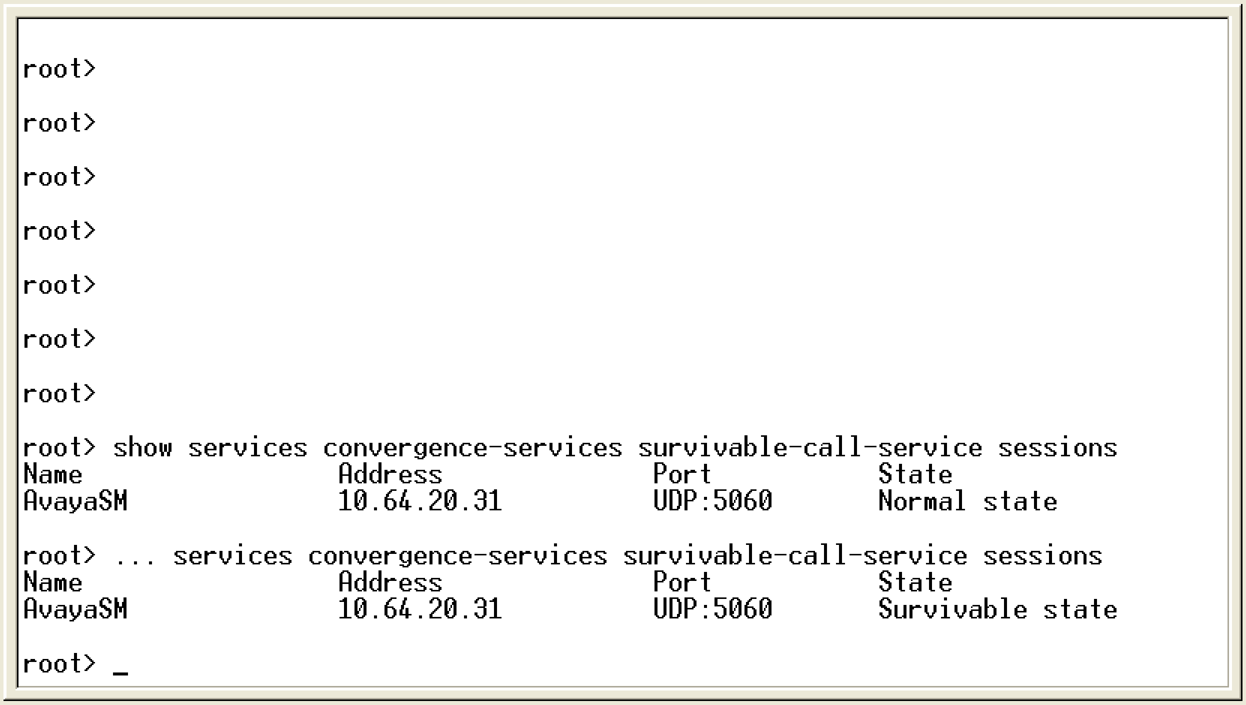
9. Verification Steps

9.1. SRX210 Survivable-Call-Service State

The survivable-call-service state of the Juniper SRX210 can be verified by a CLI (Command Line Interface) command. Connect a PC to the SRX210 console port using a serial connection, then start a terminal session using Windows HyperTerminal. The commands to type and the command output are shown in the screen below.

Normal Mode:
In Normal Mode, the "State" will be "Normal State" as shown in the first output line below.

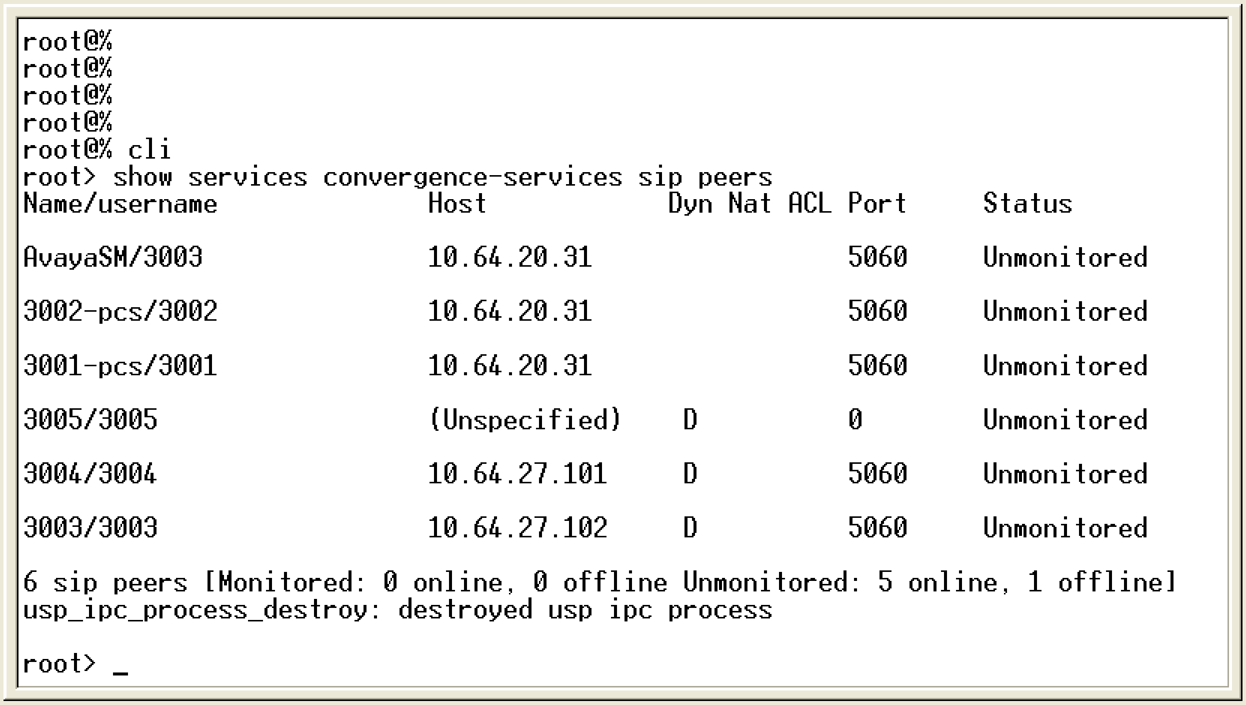
Survivable Mode:
Before entering the same command again, the WAN cable was pulled out. The second output line shows "State" as "Survivable state".



```

root>

root>

root>

root>

root>

root>

root>

root> show services convergence-services survivable-call-service sessions
Name                 Address             Port          State
AvayaSM              10.64.20.31         UDP:5060      Normal state

root> ... services convergence-services survivable-call-service sessions
Name                 Address             Port          State
AvayaSM              10.64.20.31         UDP:5060      Survivable state

root> _
```

9.2. Registered Peers on SRX210

The following screen shows registered peers (including Session Manager, branch FXS-connected analog phones, and SIP Phones) on the SRX210:

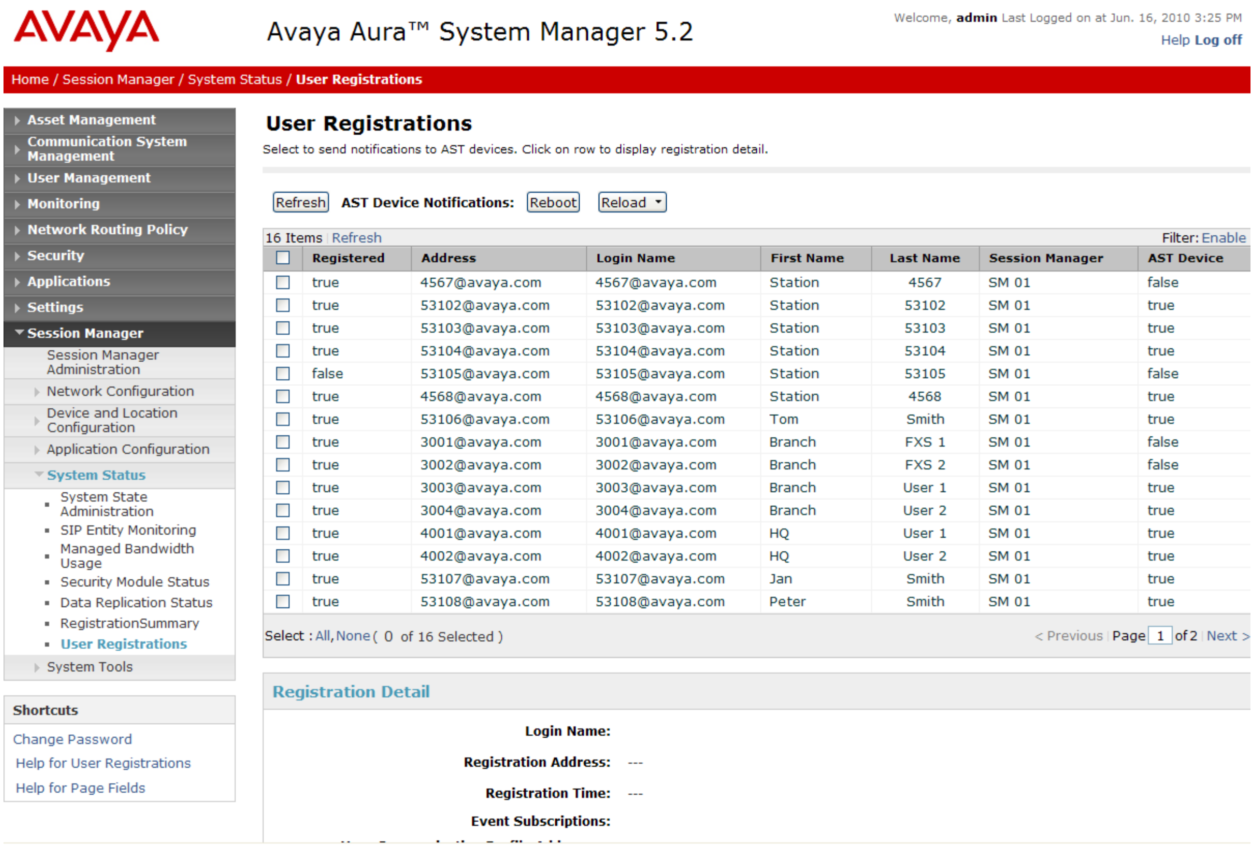


```
root@%
root@%
root@%
root@%
root@% cli
root> show services convergence-services sip peers
Name/username               Host             Dyn Nat ACL Port     Status

AvayaSM/3003                10.64.20.31                  5060     Unmonitored

3002-pcs/3002               10.64.20.31                  5060     Unmonitored

3001-pcs/3001               10.64.20.31                  5060     Unmonitored

3005/3005                   (Unspecified)     D          0        Unmonitored

3004/3004                   10.64.27.101      D          5060     Unmonitored

3003/3003                   10.64.27.102      D          5060     Unmonitored

6 sip peers [Monitored: 0 online, 0 offline Unmonitored: 5 online, 1 offline]
usp_ipc_process_destroy: destroyed usp ipc process

root> _
```

9.3. Avaya Aura^{TM} Session Manager Registered Users

The following screen shows Session Manager registered users in Normal Mode. This screen can be accessed from the left navigation menu **Session Manager → System Status → User Registrations** on System Manger.

Note the user registrations for the 2 Avaya 9600 SIP Phones (3003 and 3004) and the two FXS stations (3001 and 3002) in the branch. Also note the user registrations for the main site Avaya 9600 SIP Phones (4001 and 4002). The **AST Device** field indicates whether the registered phone is an Avaya SIP Telephone set.



User Registrations

Select to send notifications to AST devices. Click on row to display registration detail.

16 Items | Refresh

☐	Registered	Address	Login Name	First Name	Last Name	Session Manager	AST Device
☐	true	4567@avaya.com	4567@avaya.com	Station	4567	SM 01	false
☐	true	53102@avaya.com	53102@avaya.com	Station	53102	SM 01	true
☐	true	53103@avaya.com	53103@avaya.com	Station	53103	SM 01	true
☐	true	53104@avaya.com	53104@avaya.com	Station	53104	SM 01	true
☐	false	53105@avaya.com	53105@avaya.com	Station	53105	SM 01	false
☐	true	4568@avaya.com	4568@avaya.com	Station	4568	SM 01	true
☐	true	53106@avaya.com	53106@avaya.com	Tom	Smith	SM 01	true
☐	true	3001@avaya.com	3001@avaya.com	Branch	FXS 1	SM 01	false
☐	true	3002@avaya.com	3002@avaya.com	Branch	FXS 2	SM 01	false
☐	true	3003@avaya.com	3003@avaya.com	Branch	User 1	SM 01	true
☐	true	3004@avaya.com	3004@avaya.com	Branch	User 2	SM 01	true
☐	true	4001@avaya.com	4001@avaya.com	HQ	User 1	SM 01	true
☐	true	4002@avaya.com	4002@avaya.com	HQ	User 2	SM 01	true
☐	true	53107@avaya.com	53107@avaya.com	Jan	Smith	SM 01	true
☐	true	53108@avaya.com	53108@avaya.com	Peter	Smith	SM 01	true

Select : All, None (0 of 16 Selected)

Registration Detail

Login Name:

Registration Address: ---

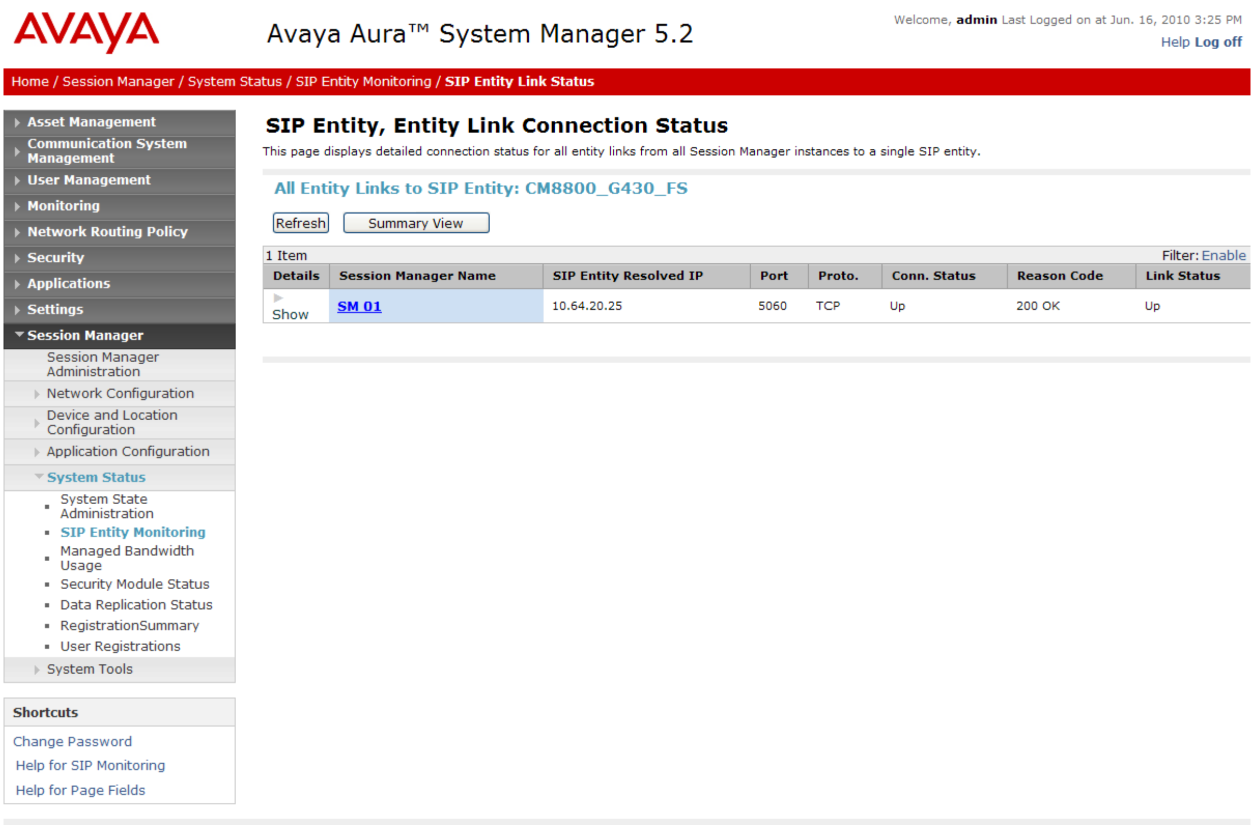
Registration Time: ---

Event Subscriptions:

9.4. Avaya Aura^{TM} Session Manager Entity Link Status

The following 2 screens show Session Manager Entity Link statuses on the Entity Links between Session Manager and Communication Manager (Feature Server) and between Session Manager and the SRX210. The Entity Link status screen can be accessed from the left navigation menu **Session Manager → System Status → SIP Entity Monitoring** on System Manger. At the SIP Entity Link Monitoring Status Summary page, select the relevant SIP Entity from the All Monitored SIP Entity list.

The screen below shows the Entity Link status between Session Manager and Communication Manager (Feature Server):



Welcome, **admin** Last Logged on at Jun. 16, 2010 3:25 PM

Home / Session Manager / System Status / SIP Entity Monitoring / **SIP Entity Link Status**

SIP Entity, Entity Link Connection Status

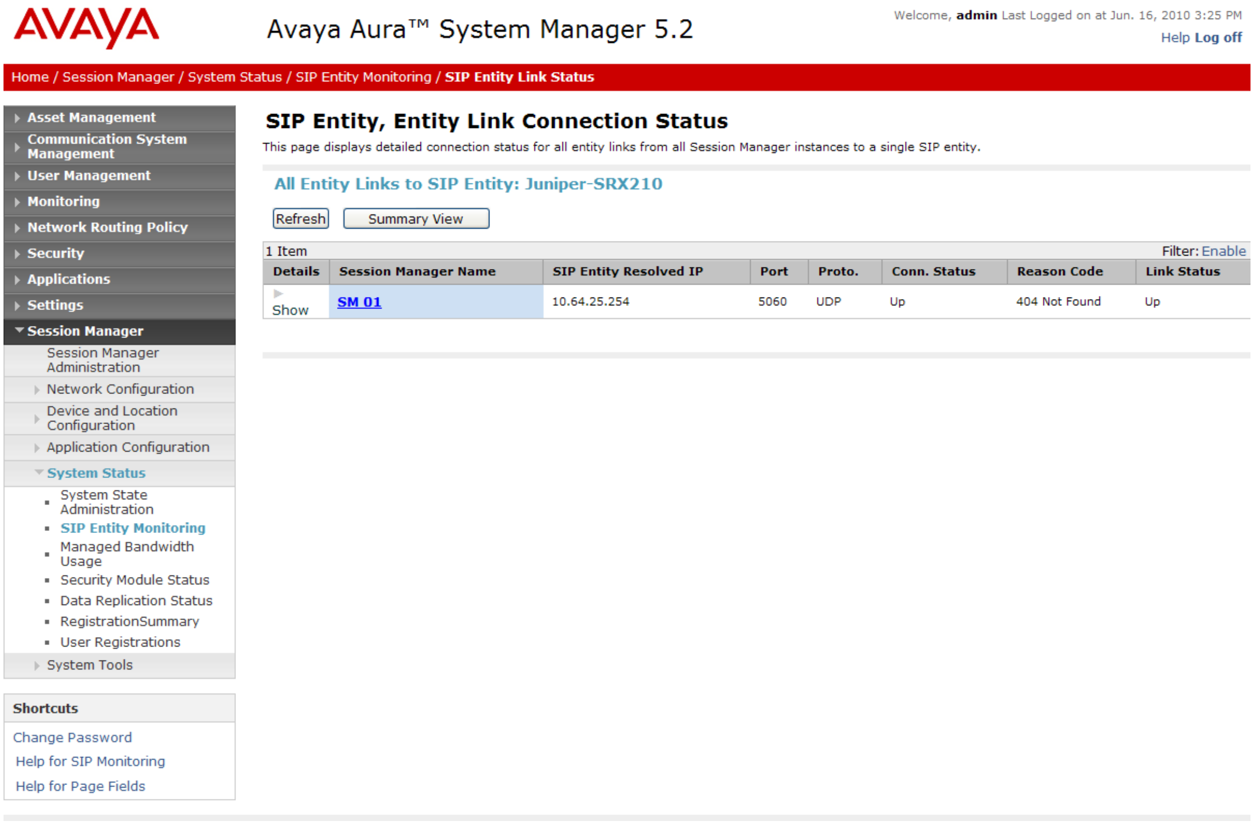
This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: CM8800_G430_FS

1 Item

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Show	SM 01	10.64.20.25	5060	TCP	Up	200 OK	Up

The screen below shows the Entity Link status between Session Manager and the SRX210. Note the **Reason Code** "404 Not Found" shown for the Up link. This is caused by the SRX210 not responding properly to the SIP Options messages from the Session Manager (a capability not yet supported on the SRX210).



SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: Juniper-SRX210

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶ Show	SM 01	10.64.25.254	5060	UDP	Up	404 Not Found	Up

9.5. Verify Basic Calls

In the Normal Mode, make calls between the Headquarters and the branch; verify that the calls are successful with a two-way talk-path. Make calls between the PSTN and the branch through the Headquarters; verify that the calls are successful with a two-way talk-path.

In the Survivable Mode, make calls between the branch phones; verify that the calls are successful with a two-way talk-path. Make calls between the PSTN and the branch through the FXO interfaces on the SRX210; verify that the calls are successful with a two-way talk-path

10. Conclusion

SIP endpoints deployed at remote branch locations risk a loss of service if a break in connectivity to the centralized SIP call control platform occurs. Connectivity loss can be caused by WAN access problems being experienced at the branch or network problems at the centralized site blocking access to the Avaya SIP call control platform. These Application Notes present the configuration steps to implement the Avaya Aura^{TM} Session Manager Survivable SIP Gateway

Solution using the Juniper SRX210 Services Gateway to minimize service disruption impact to the remote branch SIP endpoints.

11. Additional References

The following Avaya documentation is available at: http://support.avaya.com.

Avaya Aura™ Session Manager 5.2.x:

[1] *Avaya Aura™ Session Manager Overview*, Doc ID 03-603323, March 2010.

[2] *Administering Avaya Aura™ Session Manager*, Doc ID 03-603324, March 2010.

[3] *Maintaining and Troubleshooting Avaya Aura™ Session Manager*, Doc ID 03-603325, January 2010.

[4] *Administering Avaya Aura™ Communication Manager as a Feature Server*, Doc ID 03-603479, March 2010.

Avaya Aura™ Communication Manager 5.2.x:

[5] *SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers*, Doc ID 555-245-206, May 2009.

[6] *Administering Avaya Aura™ Communication Manager*, Doc ID 03-300509, May 2009.

Avaya one-X Deskphone Edition 9600 Series SIP IP Telephones (SIP 2.5.x):

[7] *Avaya one-X Deskphone Edition for 9600 SIP IP Telephones Administrator Guide Release 2.5*, Doc ID 16-601944, November 2009.

Avaya Modular Messaging:

[8] *Installing Avaya Modular Messaging on a Single Server Configuration*, December 2009.

[9] *Modular Messaging Admin Guide Release 5.2 with Avaya MSS*, November 2009.

Avaya Application Notes:

[10] *Configuring Avaya Aura^{TM} Session Manager 5.2 with Avaya Aura^{TM} Communication Manager Access Element, Avaya Voice Portal and Avaya AuraTM Communication Manager Feature Server – Issue 1.0*

The following Juniper documentation can be found at: http://www.juniper.net/techpubs/hardware/junos-srx/srx210/index.html.

Juniper SRX210 Services Gateway:

[11] *SRX 210Hardware Guide*, Revision 02, May 2010.

[12] *SRX210 Documentation*, May 2010.

The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.