Avaya Solution & Interoperability Test Lab

Avaya Aura™ Session Manager Survivable SIP Gateway Solution using Cisco's Integrated Services Router (SRST enabled) in a Distributed Trunking Configuration using Avaya 9600 SIP and Analog Phones at a Remote Branch Office - Issue 1.0

Abstract

These Application Notes present a sample configuration of the Avaya Aura™ Session Manager (SM) interoperating with Cisco Integrated Services Router (ISR) with Survivable Remote Site Telephony (SRST) software in a Distributed Trunking configuration, providing a survivable SIP gateway solution.

This solution addresses the risk of service disruption for SIP endpoints deployed at remote branch locations if connectivity to the centralized Avaya SIP call control platform (Avaya Aura™ Session Manager) located at the Enterprise Headquarters (HQ) is lost. Connectivity loss can be caused by WAN access problems being experienced at the branch or by network problems at the centralized 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 centralized Avaya SIP call control platform. When connectivity loss is detected, Avaya one-X™ Deskphone 9600 Series SIP Telephones as well as the Cisco ISR SRST dynamically switch to survivable mode, restoring telephony services to the branch for intra-branch and PSTN calling.

Testing was conducted at the Avaya Solution and Interoperability Test Lab at the request of the Avaya Solutions and Marketing Team.

<u>**Table of Contents**</u>

1. Introduction

These Application Notes present a sample configuration of the Avaya Aura™ Session Manager Survivable SIP Gateway Solution using the Cisco 2821 Integrated Service Router (ISR) with Survivable Remote Site Telephony (SRST) in a Distributed Trunking scenario using Avaya one-X™ Deskphones, 9600 Series SIP, and analog phones.

The Session Manager Survivable SIP Gateway Solution addresses the risk of service disruption for SIP endpoints deployed at remote branch locations if connectivity to the centralized Avaya SIP call control platform is lost. 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. The Session Manager Survivable SIP Gateway Solution monitors the connectivity health from the remote branch to the centralized Avaya SIP call control platform. When connectivity loss is detected, Avaya one-X™ Deskphone 9600 Series SIP Telephones as well as the Cisco ISR (SRST) dynamically switch to survivable mode, restoring basic telephony services to the branch for intra-branch and PSTN calling.

The survivable SIP gateway solution described in these Application Notes consist of the following components: Avaya Aura™ Session Manager Release 5.2, Avaya Aura™ Communication Manager Release 5.2.1 acting as a Feature Server, Avaya Aura™ Communication Manager Release 5.2.1 acting as an Access Element, Avaya Aura™ Modular Messaging (MM), Cisco 2821 Integrated Services Router (ISR) with Survivable Remote Site Telephony (SRST) enabled and Avaya SIP and Analog phones/faxes at remote branch office locations.

1.1. Interoperability Testing

The interoperability testing focused on the dynamic switch from the Normal Mode (where the network connectivity between the HQ site and the branch site is intact) to the Survivable Mode (where the network connectivity between the HQ site and the branch site is lost) and vice versa.

Testing of multiple phone type interactions for basic calls and basic feature sets in both normal mode and survivable mode:

- Phone Type Interaction Between HQ and Remote Branch:
  - HQ - Avaya 9630 and 9640 SIP
  - HQ - Avaya 9620 and 4621 H.323
  - HQ - Avaya 2420 Digital
  - HQ - Analog/Fax
  - RB - Avaya 9630 and 9640 SIP
  - RB - Avaya 6221 Analog
  - RB - Analog/Fax

- Features:
    - IP-IP Direct Audio (Shuffling) with G.711/G.729
    - Call Abandonment
    - Hold/Resume
    - Conference Add/Drop
    - Unattended Transfer
    - Attended Transfer
    - Message Waiting Indicator (MWI)
    - Fax Over IP/SIP
    - Fax Over PSTN

2. Overview

2.1. Avaya Aura™ Session Manager and Avaya Aura™ Communication Manager (Feature Server)

Session Manger is a routing hub for SIP calls among connected SIP telephony systems. Starting from release 5.2, Session Manager also includes onboard SIP Registrar and Proxy functionality for SIP call control. In the test configuration, all Avaya 9600 Series SIP Phones, either at the HQ site or at the branch sites, register to the Session Manager (the branch phones will failover to register with the Cisco ISR in Survivable Mode) with calling features supported by Communication Manager, which serves as a Feature Server within the Session Manager architecture.[1] The Avaya 9600 Series SIP Phones are configured on Communication Manger as Off-PBX-Stations (OPS) and acquire advanced call features from Communication Manger Feature Server.

2.2. Cisco Integrated Service Router (ISR)

The Cisco 2821 Integrated Services Router, referred to as Cisco ISR throughout the remainder of this document, takes on various roles based on call flows and network conditions. The Cisco ISR includes the "Survivable Remote Site Telephony" or "SRST" feature enabled. The following roles are supported by the ISR:

- SIP PSTN Media Gateway
- NM-HDV with VWIC-2MFT-T1-DI interfaces to PSTN
- VIC-4FXS/DID interfaces to analog endpoints
- SIP Registrar and Proxy (Configured as service applications, used during loss of connectivity between Branch and HQ Session Manager)

[1] See References [6, 7] for application notes on configuring Communication Manager as an Access Element to support H.323 and digital phones.

2.3. Avaya one-X™ Deskphone 9600 Series SIP Telephone

The Avaya one-X™ Deskphone 9600 Series SIP 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 2.5.0 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 Session Manager and dynamically failover to the local Cisco ISR as an alternate or survivable SIP server. See reference [1] for additional information on the Avaya 9600 SIP Phone.

2.4. Analog Phones/Faxes

Analog phones and faxes are connected to FXS ports on the Cisco ISR at the remote branch location. Dial-peers are created on the Cisco ISR with destination patterns matching the analog phone number assigned, directing call flow to the corresponding voice port. Using the SIP User Agent (sip-ua) configuration on the Cisco ISR, the analog phones can register with the Session Manager as SIP endpoints. The station template used on the Session Manger for these analog/fax endpoints was the **DEFAULT_9620SIP**. The analog/fax stations at the remote branch connected to the Cisco ISR FXS ports appear as 9620 SIP phones to the Session Manager.

2.5. Network Modes

Normal Mode: Branch has WAN connectivity to the main Headquarters/Datacenter location and the centralized Avaya SIP call control platform is being used for all branch calls.

Survivable Mode: A Branch has lost WAN connectivity to the Headquarters/Datacenter location. The local branch Cisco ISR with SRST capability is being used for all calls at that branch. Note that if the Session Manager which provides the centralized SIP control loses connectivity to the WAN, all branches will go into survivable mode simultaneously.

2.6. PSTN Trunking Configuration

The 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.

Assuming an enterprise consisting of a main Headquarters/Datacenter location and multiple distributed branch locations all inter-connected over a corporate WAN, the following defines 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 to/from the PSTN media gateway centrally located at the Headquarters/Datacenter location. In Survivable Mode, the PSTN calls to/from the branch phones are through Digital T1 trunk from the Service Provider connected T1 interface ports on the local Cisco ISR branch gateway.

Distributed Trunking: Outgoing PSTN call routing can be determined by the originating sources location using Communication Manager Feature Server Location Based Routing. Local outgoing calls from branch locations can be routed back to the same branch location and go to PSTN through the Digital T1 interface of the local Cisco ISR branch gateway. This 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.

The sample configuration presented in these Application Notes implements a Distributed Trunking configuration. The sample configuration of the Session Manager Survivable SIP Gateway Solution in a Centralized Trunking configuration is described in a separate Application Notes document.

2.7. Call Flows

2.7.1. Distributed Trunking – Normal Mode

Overview:

- **SIP Call Control**: All SIP call control and call routing are provided by the centralized Session Manager.

- **Branch PSTN Outbound Local:** All SIP calls originating at the branch and destined for the local PSTN are routed to the centralized Session Manger via the WAN. The Session Manager uses the originating location to determine routing and routes the call back to the branch Cisco ISR for local branch routing out the T1 interface to the PSTN.

- **Branch PSTN Non-Local (Long Distance – LD)**: PSTN outbound calls from the branch to all Long Distant PSTN numbers are routed to the Session Manager over the WAN. The Session Manager then uses the origination location to route the call back to the branch Cisco ISR for routing out the T1 interface to the PSTN.

- **Branch PSTN Inbound**: Calls from the PSTN to a branch are received on the Cisco ISR's T1 trunk and sent over the WAN to the Session Manager for routing.

- **HQ PSTN Inbound**: Calls from the PSTN to a Headquarters DID number enter the enterprise network at the Headquarters Avaya G650 Media Gateway.

- **HQ PSTN Outbound**: Calls to the PSTN from headquarters users are routed out a centralized Avaya G650 Media Gateway.

Call Flows:

1. **SIP/Analog stations at branch to/from 9600 SIP stations at HQ.**

   SIP/Analog stations ↔ SM ↔ CMFS ↔ HQ 9600 SIP station

2. **SIP/Analog stations at branch to/from H.323 stations at HQ.**

   SIP/Analog stations ↔ SM ↔ CMAE ↔ HQ H.323 station

3. **SIP/Analog stations at branch to/from PSTN endpoint - local calls.**

   SIP/Analog stations ↔ SM ↔ CMFS ↔ SM ↔ Cisco ISR (prefixed for local) (T1) ↔ Local PSTN endpoint

4. **SIP/Analog stations at branch to/from PSTN endpoint - long distance toll calls.**

   SIP/Analog stations ↔ SM ↔ CMFS ↔ SM ↔ Cisco ISR (prefixed for LD) ↔ Long Distance PSTN endpoint

5. **SIP/Analog stations at branch to/from SIP/Analog stations at same branch.**

   SIP/Analog stations ↔ SM ↔ CMFS ↔ SM ↔ SIP/Analog stations

6. **SIP/Analog stations at branch to/from Analog/Fax at HQ.**

   SIP/Analog stations ↔ SM ↔ CMAE ↔ Avaya Media Gateway (G650) ↔ HQ Analog/Fax

7. **SIP/Analog stations at branch to/from Digital stations at HQ.**

   SIP/Analog stations ↔ SM ↔ CMAE ↔ Avaya Media Gateway (G650) ↔ HQ Digital Station

2.7.2. Distributed Trunking – Survivable Mode

Overview:

- **SIP Call Control:** All SIP call control and call routing is provided by the local branch Cisco ISR.

- **SIP Registration:** All branch Avaya 9600 SIP Phones are transitioned to have the registration with the Cisco ISR active.

- **All Branch PSTN Outbound:** Local and Non-Local: Routed to the Cisco ISR T1 interface.

- **Branch PSTN Inbound:** Calls from the PSTN to the branch DID enter the network at the local branch's Cisco ISR T1 interface. The Cisco ISR routes the call to a phone dial-peer maintained on the Cisco ISR either dynamically for the 9600 SIP phones or statically for the analog FXS phones or fax machines.

Call Flows:

1. **SIP/Analog stations at branch to PSTN endpoint.**

   SIP/Analog stations ↔ Cisco ISR (T1) ↔ PSTN endpoint

2. **SIP/Analog stations at branch to/from SIP/Analog stations at same branch.**

   SIP/Analog stations ↔ Cisco ISR ↔ SIP/Analog stations

3. **SIP/Analog stations at branch to H.323/Analog/Fax/Digital at HQ.**

   SIP/Analog stations → Cisco ISR (secondary dial-peer with HQ prefix added) → Cisco ISR (T1) → PSTN → Avaya Media Gateway (G650) → CMAE → HQ H.323/Analog/Fax/Digital endpoint

4. **SIP/Analog stations at branch to SIP Phone at HQ**.

   SIP/Analog stations → Cisco ISR (secondary dial-peer with HQ prefix added) → Cisco ISR (T1) → PSTN → Avaya Media Gateway (G650) → CMAE → SM → CMFS → HQ SIP endpoint

5. **PSTN endpoint to SIP/Analog stations at branch**.

   PSTN endpoint → Cisco ISR (T1) → Incoming dial-peer stripping area code → SIP/Analog stations

2.8. Network Topology

2.8.1. Normal Mode - Distributed Trunking

In the sample configuration shown in **Figure 1**, the remote branch offices are configured for distributed trunking with the Cisco ISR and phones in normal mode.

The Headquarters network is mapped to IP Network Region 1 which is assigned to Location 1 within Avaya Communications Manager Feature Server. Branch 1's network is mapped to IP Network Region 12 which is assigned to Location 12 within Avaya Communication Manager Feature Server. The Distributed Trunking capabilities of the solution utilize the source based call routing feature of Avaya Communication Manager which requires the information presented in **Table 1**. The branch configurations presented throughout these Application Notes focus on Branch 1.

Site	IP Network	IP Network Region	Location	Area Code	Cisco ISR Address
HQ (Avaya Aura™ Servers)	10.80.100.0/24	1	1	303	N/A
HQ (Phones)	10.80.60.224/27	1	1	303	N/A
HQ (DNS, DHCP)	30.1.1.7/24	1	1	303	N/A
Branch 1	10.80.61.32/27	12	12	618	10.80.61.33

Table 1 - Network Information

The Avaya 9600 SIP phones are configured for simultaneous registration to the Session Manager, located in the Enterprise Headquarters, as primary SIP registrar and to the Cisco 2821 ISR at the remote branch location, as secondary SIP registrar. The SIP phones can be configured in either “alternate” or “simultaneous” modes of SIP registration via the 46xxsettings.txt file. In “alternate” mode the 9600 SIP phones maintain a primary and secondary SIP registrar list, but only register with one at a time with the primary being used in normal mode and the secondary being used in failover/survivable mode. “Simultaneous” registration with both the Session Manager and ISR allows the ISR to maintain individual SIP phone registration and upfront creation of dial-peers for failover routing purposes, reducing the processing queue of registration and dial-peer creation experienced in “alternate” SIP phone configurations during failover.

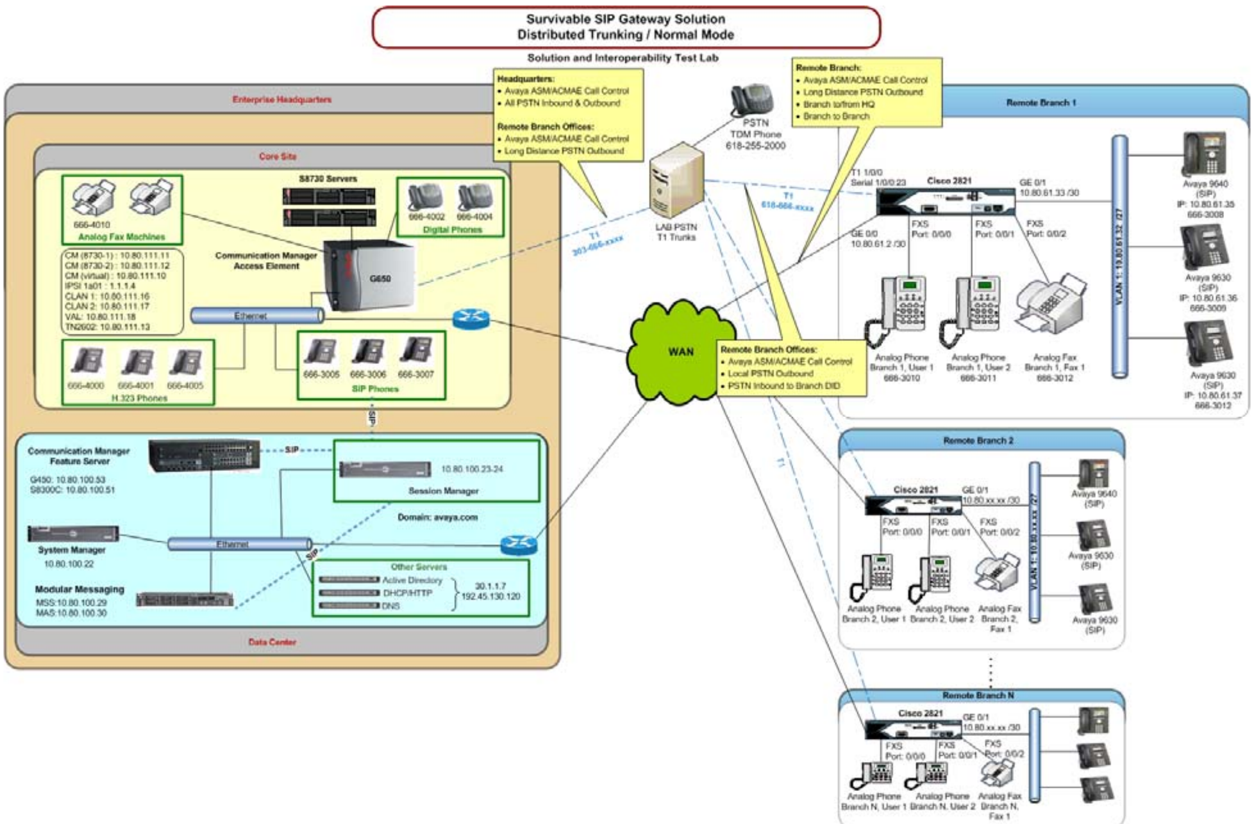


Figure 1: SRST - Distributed Trunking / Normal Mode

2.8.2. Survivable Mode - Distributed Trunking

The survivable SIP Gateway solution devices are configured to allow remote branch office SIP devices to switch over to survivable mode when WAN connectivity is lost or disrupted, see **Figure 2**. During survivable mode, the remote branch office SIP devices registered with the local ISR supporting SRST follow precedence base routing rules to provide call functionality between devices at the branch location and route off-location calls via a local T1 to the PSTN. This allows the branch to maintain normal outgoing HQ dialing rules while the SRST prefixes and routes the calls via the T1/PSTN. Limited functionality of some calling features may exist during survivable mode.

Once WAN connectivity has been restored the remote branch SIP phones return to normal mode and switch SIP call control back to the HQ Session Manager providing full feature functionality.

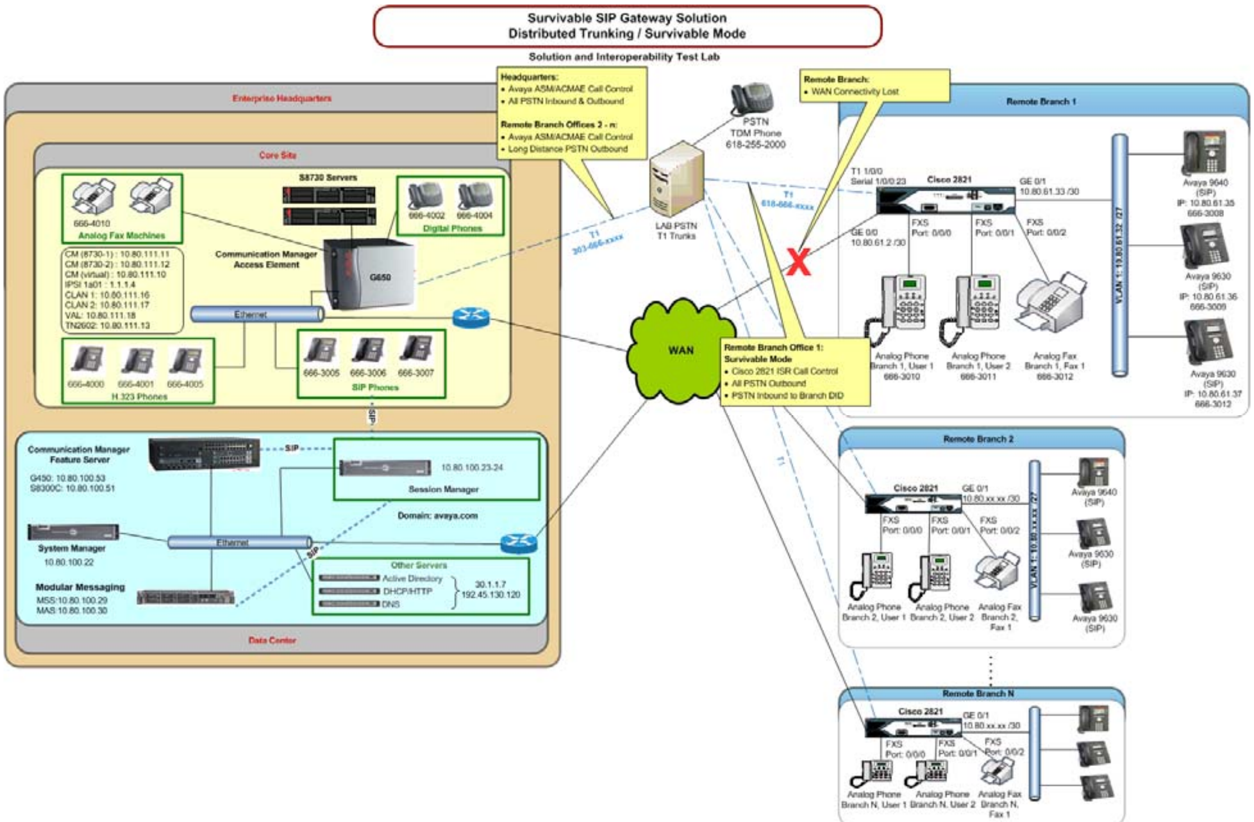


Figure 2: SRST - Distributed Trunking / Survivable Mode

3. Equipment and Software Validated

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

Hardware Component	Software/Firmware Version
S8510 Media Server	Session Manager 5.2.1.1.521012-01-14-2010
	System Manager 5.2 Load: 5.2.8.0
S8300C Server with G450 Media Gateway	Communication Manager 5.2.1 load 16.4 (Feature Server) (Patch 17959)
S8730 Server with G650 Media Gateway	Communication Manager 5.2.1 load 16.4 (Access Element) (Patch 17959)
Avaya Modular Messaging (MAS)	5.2, Build 9.2.150.0 (Patch 8 - 9.2.150.13)
Avaya Modular Messaging (MSS)	5.2, Build 5.2-11.0
Avaya one-X™ Deskphone 9640 IP Telephones (SIP)	2.5.0
Avaya one-X™ Deskphone 9630 IP Telephones (SIP)	2.5.0
Avaya 9620L IP Telephones (H.323)	S3.002
Avaya 4621SW IP Telephones (H.323)	S2.9.1
Avaya 6221 Analog Telephones	--
Analog Fax Machine (Remote Branch)	--
Analog Fax Machine (HQ)	--
Avaya 2420 Digital Phones	--
Cisco 2821 ISR	IOS Version: 124-24.T2 IOS Image: c2800nm-ipvoicek9-mz.124-24.T2.bin
Dell Servers: DHCP/HTTP DNS Active Directory	Windows Server 2008 R2 Standard

4. Configuration

The sample configuration used in these Application Notes assume the items within the Enterprise Headquarters for the Core Site and Datacenter have already been configured to operate together in an Avaya Aura™ Architecture solution allowing calling between SIP phones, H.323 phones, Analog phones, Digital phones and Fax devices. The references section of these Application Notes contain additional information on configuring Communication Manager as an Access Element supporting H.323, Digital and Analog phones, Communication Manager as an Feature Server and Session Manager supporting Avaya 9600 SIP phones.

4.1. Configure Communication Manager Feature Server

This section shows the necessary steps to configure Communication Manager Feature Server to support the survivable SIP gateway solution in a Distributed Trunking scenario. It is assumed that the basic configuration on Communication Manager Feature Server, the required licensing, the configuration for accessing Modular Messaging (if it is used for voice messaging), has already been administered. See listed documents in the **References** section for additional information.

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

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

- Communication Manager license
- System parameters features
- IP node names
- Locations
- IP codec set
- IP network regions
- IP network map
- Stations
- SIP signaling group and trunk group
- Route pattern
- Private numbering
- Automatic Alternate Routing (AAR)
- Automatic Route Selection (ARS)

4.1.1. Verify Communication Manager Feature Server License

Log into the System Access Terminal (SAT) to verify that the Communication Manager Feature Server 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: 100   8
           Maximum Concurrently Registered IP Stations: 450   0
             Maximum Administered Remote Office Trunks: 450   0
Maximum Concurrently Registered Remote Office Stations: 450   0
              Maximum Concurrently Registered IP eCons: 4     0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 1     0
                   Maximum Video Capable IP Softphones: 10    0
                       Maximum Administered SIP Trunks: 100   20
  Maximum Administered Ad-hoc Video Conferencing Ports: 10    0
   Maximum Number of DS1 Boards with Echo Cancellation: 2     0
                             Maximum TN2501 VAL Boards: 0     0
                     Maximum Media Gateway VAL Sources: 1     1
           Maximum TN2602 Boards with 80 VoIP Channels: 0     0
          Maximum TN2602 Boards with 320 VoIP Channels: 0     0
   Maximum Number of Expanded Meet-me Conference Ports: 10    0
```

4.1.2. 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 that this feature poses significant security risk, and must be used with caution. As alternatives, the trunk-to-trunk feature can be implemented using Class of Restriction (COR) or Class of Service (COS) levels. Refer to the appropriate documentation in the **References** section 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: none
              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
```

4.1.3. Configure IP Node Names

Use the "change node-names ip" command to add an entry for the Session Manager that the Communication Manager Feature Server will connect to. The **Name** "ASM1" and **IP Address** "10.80.100.24" are entered for the Session Manager Security Module (SM-100) interface. The configured node-name "ASM1" will be used later on in the SIP Signaling Group administration (**Section 5.1.9.1**).

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
ASM1                    10.80.100.24
CUCM5                   192.45.130.105
IPO                     33.1.1.51
Nortel-CS1000e          10.80.50.50
default                 0.0.0.0
procr                   10.80.100.51
```

4.1.4. Locations

The locations of the branch as well as Headquarters must be defined within Avaya Communication Manager using the **change locations** command. The values used in the sample configuration are shown below. The location number, name and local area code (NPA) are entered as defined in **Table 1**. All remaining fields have been left at default values. The Timezone Offset can be used if locations reside within different time zones. All locations are within the same time zone in the sample configuration so the default value of 00:00 is used.

```
change locations                                Page   1 of  16
                                 LOCATIONS

         ARS Prefix 1 Required For 10-Digit NANP Calls? y

Loc Name  Timezone Rule NPA ARS  Atd Loc  Disp Prefix Proxy Sel
No          Offset          FAC  FAC Parm Parm          Rte Pat
1:  Main   + 00:00  0   303           1    1
2:             :
3:             :
4:             :
5:             :
6:             :
7:             :
8:             :
9:             :
10:            :
11:            :
12:Branch1 + 00:00 0    618           1    1
13:            :
14:            :
```

4.1.5. 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. The G.711MU codec was used in the test configuration.

Note: During lab testing of interoperability using G.729 codec, this configuration was changed to support the G.729 codec. The codec on the Cisco ISR is configured to use G.711MU as primary and G.729 as secondary.

```
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:
 3:
 4:
 5:
 6:
 7:


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

4.1.6. Configure IP Network Regions

IP Network Regions are defined for the branch location as well as the Headquarters location as defined in **Table 1** using the **change ip-network-region** command. The IP Network Regions are mapped to the Locations previously created. The values used in the sample configuration for Headquarters IP Network Region 1 are shown below. The Location, Name, Codec Set and Authoritative Domain field values shown are specific to the sample configuration. All remaining fields have been left at default values. The Authoritative Domain is the SIP domain name defined within the Session Manager and used throughout the enterprise for SIP communications.

```
change ip-network-region 1                                Page   1 of  19
                               IP NETWORK REGION
  Region:  1
Location:  1      Authoritative Domain: avaya.com
    Name: Headquarters
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? y
   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
```

The values used in the sample configuration for Branch 1 IP Network Region 12 are shown below. The Location, Name, Codec Set and Authoritative Domain field values shown are specific to the sample configuration. All remaining fields have been left at default values. Follow the same steps to create the IP Network Regions for the remaining branch locations.

```
change ip-network-region 12                                   Page   1 of  19
                               IP NETWORK REGION
  Region: 12
Location: 12        Authoritative Domain: avaya.com
    Name: Remote Branch 1
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? y
   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
```

The following screen illustrates a portion of **Page 3** for network region 12. The connectivity between network regions is specified under the **Inter Network Region Connection Management** heading, beginning on **Page 3.** Codec set 1 is specified for connections between network region 12 and network region 1.

```
change ip-network-region 12                         Page   3 of  19

 Source Region: 12  Inter Network Region Connection Management      I        M
                                                                    G  A     e
 dst codec direct WAN-BW-limits   Video      Intervening       Dyn  A  G     a
 rgn  set   WAN  Units   Total Norm  Prio Shr Regions           CAC  R  L     s
 1    1     y    NoLimit                                            n  all
 2
 3
 4
 5
 6
 7
 8
 9
 10
 11
 12  1                                                                 all
 13
```

4.1.7. Configure IP Network Map

IP addresses are used to associate a device with a specific IP Network Region. The IP Network Region can be associated with a specific Location as previously described. The **change ip-network-map** command is used to perform the IP address to IP Network Region mapping. The IP Address Mapping used in the sample configuration is shown below based on the information from **Table 1**. In this case, the subnet for each location is entered with the corresponding IP Network Region number.

```
change ip-network-map                                        Page   1 of  63
                               IP ADDRESS MAPPING

                                             Subnet Network      Emergency
 IP Address                                  Bits   Region VLAN Location Ext
 ------------------------------------------- ------ ------ ---- -------------
 FROM: 10.80.60.224                          /27    1      n
   TO: 10.80.60.254
 FROM: 30.1.1.0                              /24    1      n
   TO: 30.1.1.255
 FROM: 10.80.100.0                           /24    1      n
   TO: 10.80.100.255
 FROM: 10.80.61.32                           /27    12     n
   TO: 10.80.61.62
```

4.1.8. Add Stations

A station must be created on Communication Manager Feature Server for each SIP User account to be created in Session Manager which includes a provisioned Communication Manager Feature Server Extension. The extension assigned to the Communication Manager station must match the Extension assignment in Session Manager (see **Section 4.2.10**).

Use the "add station" command to add a station to Communication Manager. The "add station" command for an Avaya 9640 SIP Phone located at Remote Branch 1 with extension 6663008 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. Of course, feature programming will vary.

```
add station 6663008                                             Page   1 of   6
                                  STATION

Extension: 666-3008                    Lock Messages? n                 BCC: 0
     Type: 9640SIP                     Security Code:                    TN: 1
     Port: S00024                    Coverage Path 1: 1                 COR: 1
     Name: Branch 1 User 1           Coverage Path 2:                   COS: 1
                                     Hunt-to Station:
STATION OPTIONS
                                        Time of Day Lock Table:
           Loss Group: 19
                                              Message Lamp Ext: 666-3008
     Display Language: english                  Button Modules: 0

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

                                                        IP Video? n
```

On **Page 6** of the station form, specify "aar" for **SIP Trunk**.

```
add station 6663008                                          Page   6 of   6
                                  STATION
SIP FEATURE OPTIONS
      Type of 3PCC Enabled: None
                 SIP Trunk: aar
```

Repeat the above procedures for adding each and every 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. The following table lists the SIP phones added for this Application Notes configuration.

Station Number	Phone Type	Location	Note
6663006	9630SIP	HQ	
6663007	9630SIP	HQ	
6663008	9640SIP	Remote Branch 1	
6663009	9630SIP	Remote Branch 1	
6663010	9620SIP	Remote Branch 1	Analog/FXS Phone 1
6663011	9620SIP	Remote Branch 1	Analog/FXS Phone 2
6663012	9620SIP	Remote Branch 1	Analog/Fax 1

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.

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

                    STATION TO OFF-PBX TELEPHONE MAPPING

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

666-3000       OPS        6663000          1  /   10      both         all
666-3001       OPS        6663001          1  /   10      both         all
666-3002       OPS        6663002          1  /   10      both         all
666-3003       OPS        6663003          1  /   10      both         all
666-3005       OPS        6663005          1  /   11      both         all
666-3006       OPS        6663006          1  /   aar     both         all
666-3007       OPS        6663007          1  /   aar     both         all
666-3008       OPS        6663008          1  /   aar     both         all
666-3009       OPS        6663009          1  /   aar     both         all
666-3010       OPS        6663010          1  /   aar     both         all
666-3011       OPS        6663011          1  /   aar     both         all
666-3012       OPS        6663012          1  /   aar     both         all
666-3013       OPS        6663013          1  /   aar     both         all
666-3020       OPS        6663020          1  /   aar     both         all
```

4.1.9. Configure SIP Signaling Group and Trunk Group

4.1.9.1 SIP Signaling Group

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
- Far-end Node Name: "ASM1" Session Manager node name
- Near-end Listen Port: "5060"
- Far-end Listen Port: "5060"
- Far-end Network Region: Network region number "1"
- Far-end Domain: SIP domain name
- DTMF over IP: "rtp-payload"

```
add signaling-group 10                                         Page   1 of   1
                             SIGNALING GROUP

 Group Number: 10          Group Type: sip
                     Transport Method: tcp
  IMS Enabled? y
     IP Video? n


  Near-end Node Name: procr                  Far-end Node Name: ASM1
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): 10
```

The screen below shows signaling group 61 which is used in the sample configuration as the "Secondary" signaling group to be associated with trunk group 61 for routing local PSTN calls from branch phones to Session Manager (for onward routing to local branch Cisco ISR) in

Normal Mode. Note that all the settings for this signaling group are identical to those for signaling group 10 except the **IMS Enabled** which is set to "n" for signaling-group 61.

```
add signaling-group 61                                          Page   1 of   1
                             SIGNALING GROUP

 Group Number: 61          Group Type: sip
                     Transport Method: tcp
  IMS Enabled? n
     IP Video? n



  Near-end Node Name: procr                 Far-end Node Name: ASM1
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? n                   Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n        Alternate Route Timer(sec): 6
```

4.1.9.2 SIP Trunk Group

Use the "add trunk-group n" command, where "n" is an available trunk group number. 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
- Service Type: "tie"
- Signaling Group: The signaling group number
- Number of Members: Equal to the maximum number of concurrent calls supported

```
add trunk-group 10                                         Page   1 of  21
                             TRUNK GROUP

Group Number: 10                Group Type: sip          CDR Reports: y
  Group Name: SIP trunk to ASM1        COR: 1        TN: 1        TAC: #10
   Direction: two-way     Outgoing Display? y
 Dial Access? n                                 Night Service:
Queue Length: 0
Service Type: tie                Auth Code? n

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

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

```
change trunk-group 10                                         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
```

Navigate to **Page 4**, and enter "120" for the **Telephone Event Payload Type** field. Use default values for all other fields.

```
change trunk-group 10                                           Page   4 of  21
                                    PROTOCOL VARIATIONS

                           Mark Users as Phone? y
                  Prepend '+' to Calling Number? n
            Send Transferring Party Information? n
                       Network Call Redirection? n
                          Send Diversion Header? n
                        Support Request History? y
                   Telephone Event Payload Type: 120
```

The trunk group 61 used for routing local PSTN calls from branch phones is similarly configured (not shown).

4.1.10. Configure Route Pattern

Configure a route pattern to correspond to the newly 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.
- **RP No**: The trunk group number from **Section 4.1.9.2**
- **FRL**: Facility Restriction Level that allows access to this trunk, "0" being least restrictive

```
change route-pattern 10                                         Page   1 of   3
                    Pattern Number: 10   Pattern Name: To Sess Mgr
                             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: 10   0                                                                n   user
2: 11   0                                                                n   user
3:                                                                       n   user
4:                                                                       n   user
5:                                                                       n   user
6:                                                                       n   user

  BCC VALUE    TSC CA-TSC ITC BCIE Service/Feature PARM  No. Numbering LAR
 0 1 2 M 4 W      Request                                Dgts Format
                                                       Subaddress
1: y y y y y n  n          rest                                            none
2: y y y y y n  n          rest                                            none
```

```
 change route-pattern 61                                        Page   1 of   3
                Pattern Number: 61  Pattern Name: Branch Lcl PSTN
                           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: 61   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
```

4.1.11. 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 4.1.9.2**. In the example shown below, all calls originating from a 7-digit extension beginning with 666 and routed to trunk group 10 will result in a 7-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
 7  666              10-11                       7        Total Administered: 1
                                                          Maximum Entries: 540
```

4.1.12. Configure AAR

Use the "change aar analysis n" command to add an entry for the extension range where "n" is the first digit of the assigned phone numbers for the SIP phones in the remote branch office configured in **Section 4.1.8** (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 4.1.10**
- Call Type: "aar"

```
change aar analysis 6                                           Page   1 of   2
                          AAR DIGIT ANALYSIS TABLE
                                Location:  all          Percent Full:    2

       Dialed            Total     Route     Call    Node   ANI
       String          Min  Max   Pattern    Type    Num    Reqd
 618                   10   10     10        aar            n
 666                   7    7      10        aar            n
 7                     7    7      10        aar            n
```

4.1.13. Configure Automatic Route Selection (ARS)

4.1.13.1 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   8
                             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:
                       Answer Back Access Code:
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: *8
    Auto Route Selection (ARS) - Access Code 1: *9    Access Code 2:
                 Automatic Callback Activation:        Deactivation:
Call Forwarding Activation Busy/DA: 4006   All: 4007   Deactivation: 4008
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code: 4000
                       Call Pickup Access Code: 4001
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:
```

4.1.13.2 Location Specific ARS Digit Analysis

The "change ars analysis location x y" command is used to make location specific routing entries where the x is the location number and the y is the dialed digit string to match on. Each branch location has an ARS entry for the local area code of the branch. These ARS location tables are used by Communication Manager for source based routing. The location specific ARS entries for the branch are shown below. Route Pattern 61 as defined in **Section 4.1.10** is used when a match is made on any of these ARS entries.

```
change ars analysis location 12 1618                         Page   1 of   2
                           ARS DIGIT ANALYSIS TABLE
                                 Location:  12            Percent Full:    2

          Dialed          Total      Route     Call   Node   ANI
          String          Min  Max  Pattern    Type   Num    Reqd
    1618                  11   11     61       natl           n
    618                   10   10     61       natl           n
```

4.2. Configure Avaya Aura™ Session Manager

This section provides the procedures for configuring Session Manager as provisioned in the reference 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.

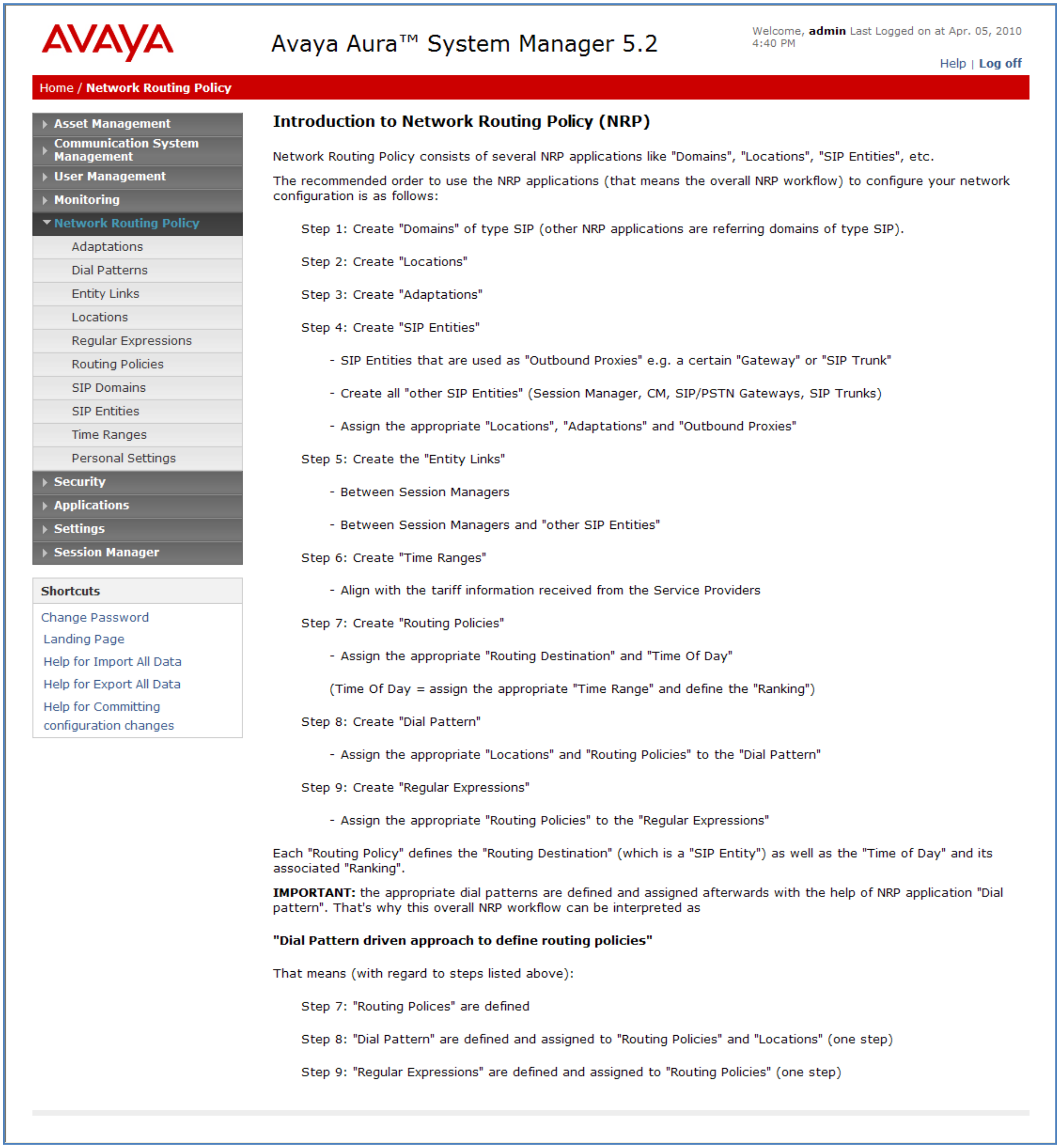
The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

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 for the reference configuration, the IP address assigned to the SM-100 interface is 10.80.100.23 as specified 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 reference configuration, the IP address assigned to the Session Manager management interface is 10.80.100.24. In the reference 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
- **SIP Entities** corresponding to the SIP telephony systems including Communication Manager and Session Manager itself
- **Entity Links** which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- **Session Manager** corresponding to the Session Manager Servers managed by System Manager
- **Local Host Name Resolution** provides host name to IP address resolution
- Communication Manger as a Feature Server
- **User Management** for SIP telephone users

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL "https://<ip-address>/SMGR", where "<ip-address>" is the IP address of System Manager. Log in with the appropriate credentials and 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 four of the above items (**Sections 4.2.1** through 4**.2.4**).

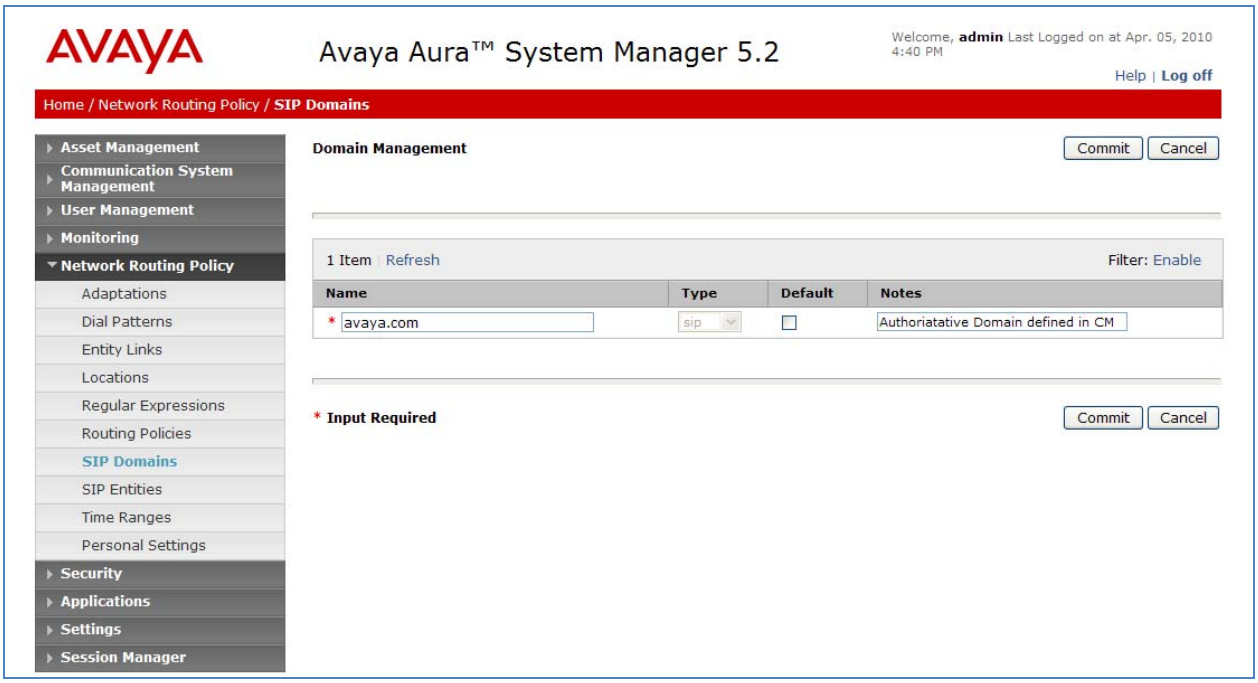

AVAYA
Avaya Aura™ System Manager 5.2
Welcome, admin Last Logged on at Apr. 05, 2010 4:40 PM
Help | Log off
Home / Network Routing Policy
Asset Management
Communication System Management
User Management
Monitoring
Network Routing Policy
Adaptations
Dial Patterns
Entity Links
Locations
Regular Expressions
Routing Policies
SIP Domains
SIP Entities
Time Ranges
Personal Settings
Security
Applications
Settings
Session Manager
Shortcuts
Change Password
Landing Page
Help for Import All Data
Help for Export All Data
Help for Committing configuration changes
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"
- Assign the appropriate "Routing Policies" to the "Regular Expressions"
Each "Routing Policy" defines the "Routing Destination" (which is a "SIP Entity") as well as the "Time of Day" and its associated "Ranking".
IMPORTANT: the appropriate dial patterns are defined and assigned afterwards with the help of NRP application "Dial pattern". That's why this overall NRP workflow can be interpreted as
"Dial Pattern driven approach to define routing policies"
That means (with regard to steps listed above):
Step 7: "Routing Polices" are defined
Step 8: "Dial Pattern" are defined and assigned to "Routing Policies" and "Locations" (one step)
Step 9: "Regular Expressions" are defined and assigned to "Routing Policies" (one step)

4.2.1. 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 consistent with the domain configuration on Communication Manager (see **Section 4.1.6**)
- **Notes:** Descriptive text (optional)

Click **Commit**.



4.2.2. Add Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of 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:

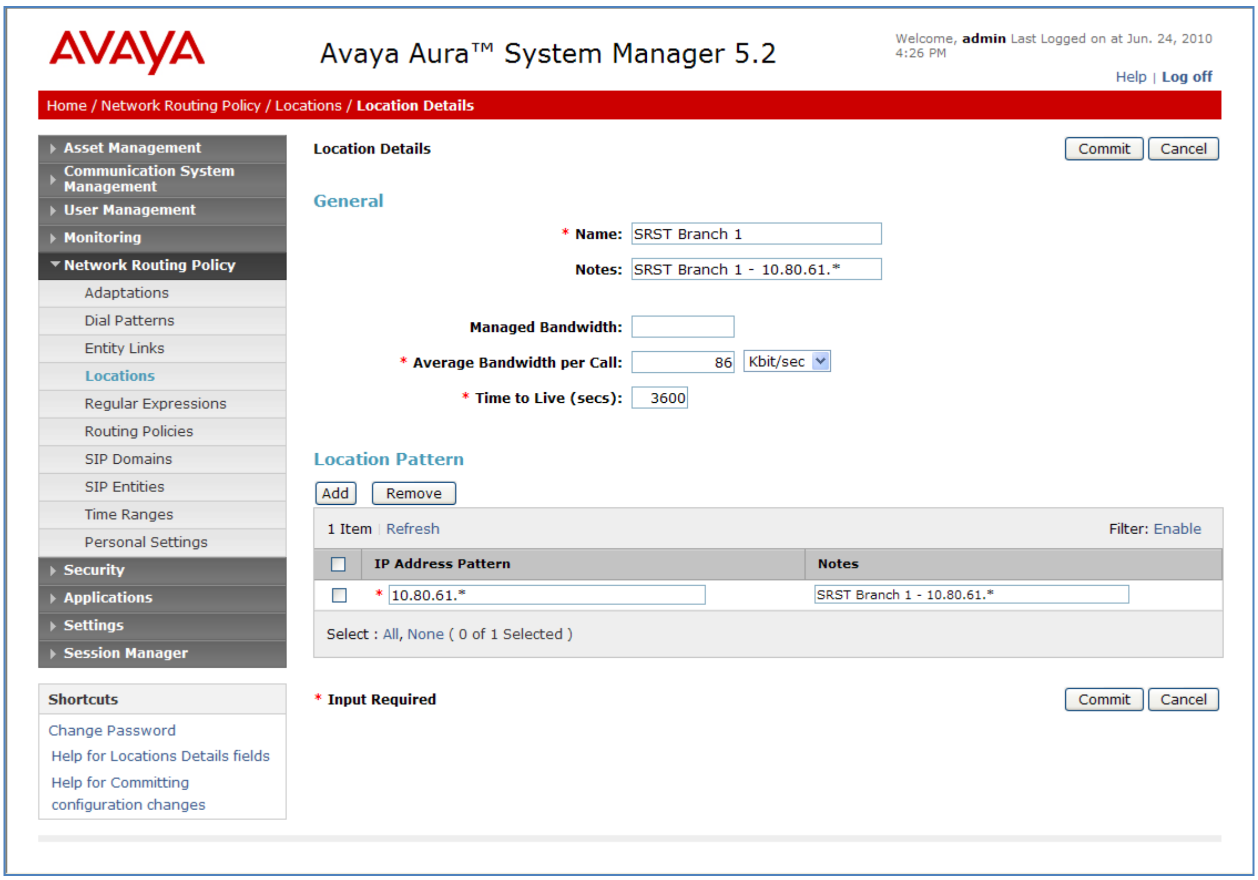
- **Name**: A descriptive name
- **Notes**: Descriptive text (optional)

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 although not implemented in the sample configuration, routing policies can be defined based on location.

Under *Location Pattern*:

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

The screen below shows the addition of the "SRST Branch 1" location, which includes the IP address range of the SIP telephones located at remote branch 1 (10.80.61.* subnet). Click **Commit** to save the Location definition.



Repeat steps to add a location for the HQ Server location with **Name** as "10_80_100", **Notes** as "10.80.100 Subnet", **IP Address Pattern** as "10.80.100.*" and **Location Pattern Notes** for this entry as "10.80.100 Subnet."

4.2.3. 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, Communication Manager acting as a Feature Server, Communication Manager acting as an Access Element, and Cisco ISR.

The steps to create a SIP Entity are as follows:

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

Under *General*:

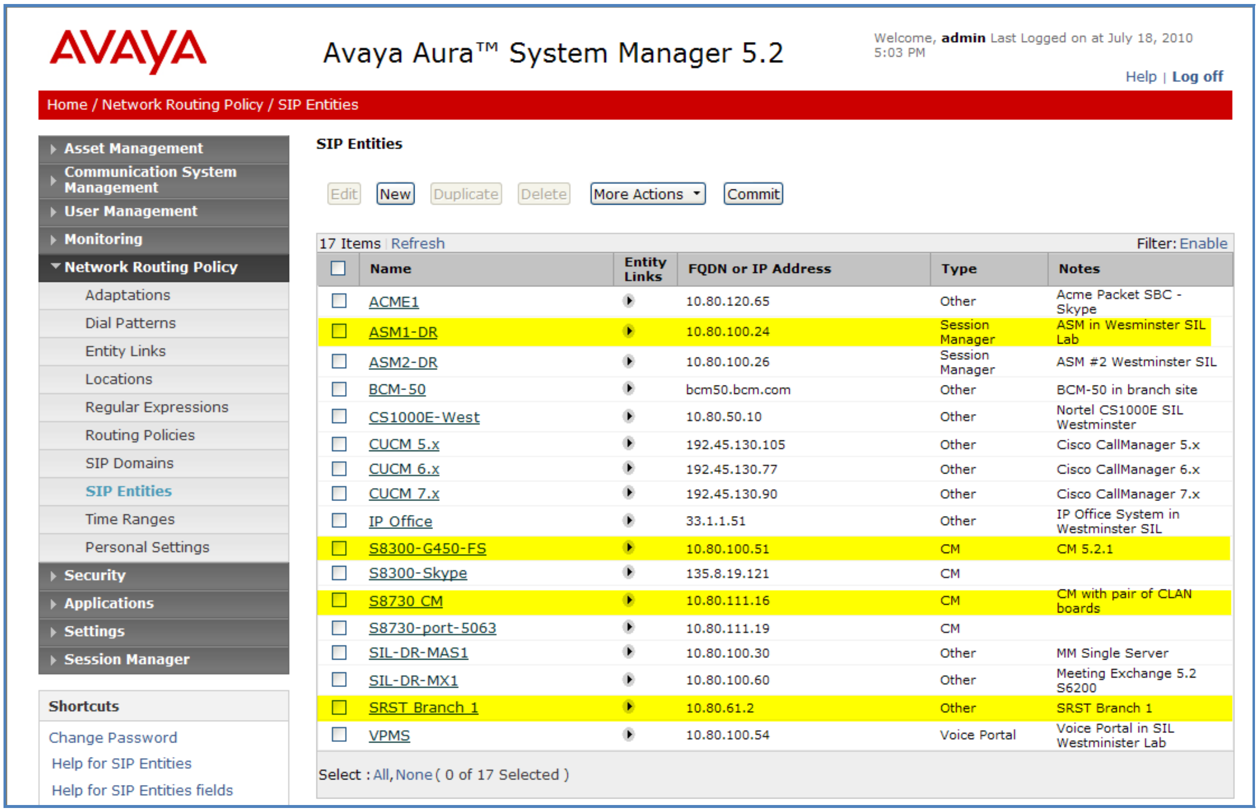
- **Name** A descriptive name
- **FQDN or IP Address**: FQDN or IP address of the signaling interface on the Session Manager or other telephony systems
- **Type**: "Session Manager" for Session Manager, "CM" for Communication Manager and "Other" for Cisco ISR
- **Adaptation**: Leave blank
- **Location:** Select the Location the SIP Entity will use
- **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:

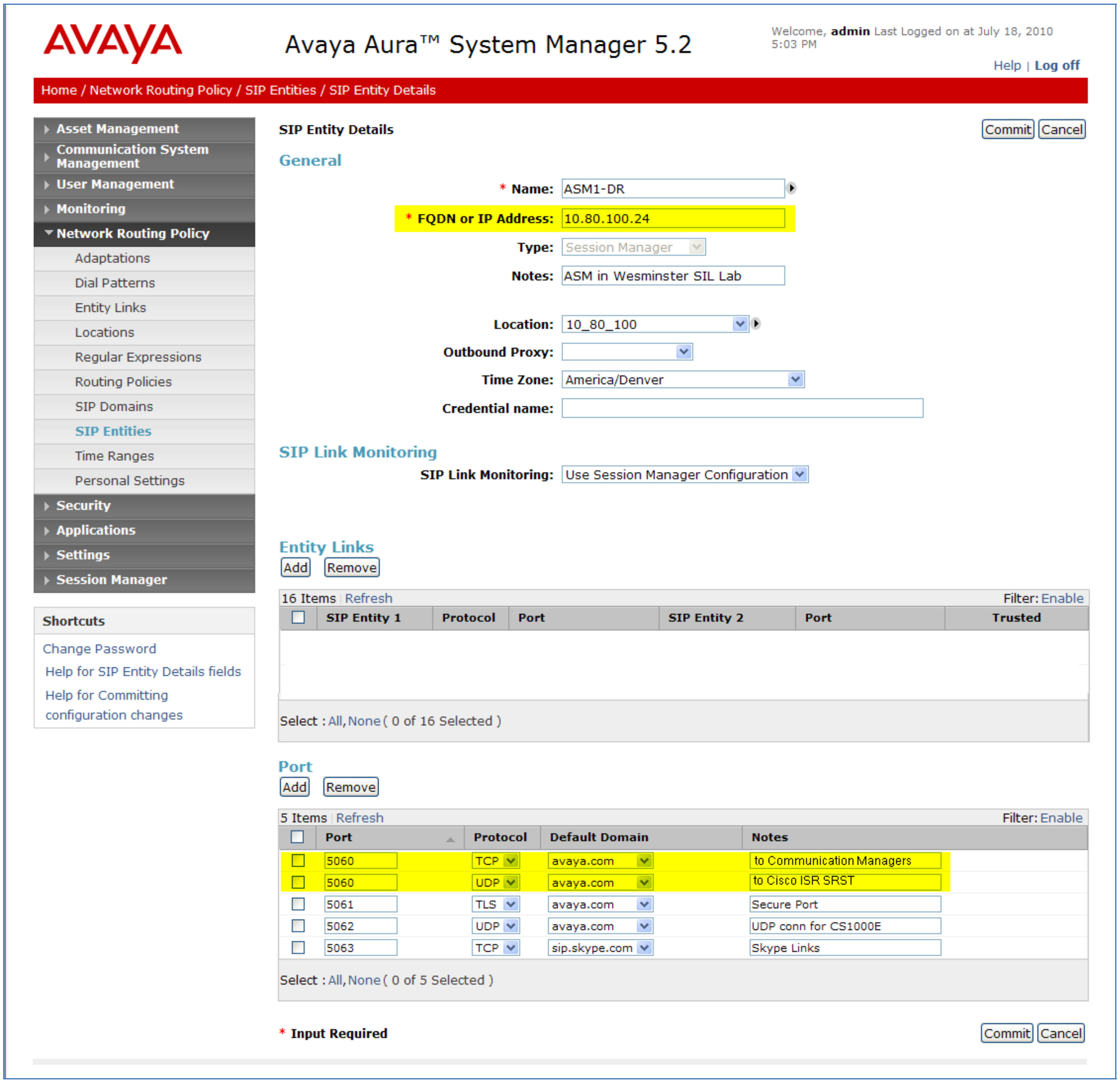
- **Port**: Port number on which the system listens for SIP requests.
- **Protocol**: Transport protocol to be used to send SIP requests.
- **Default Domain**: Select the SIP Domain created previously.

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

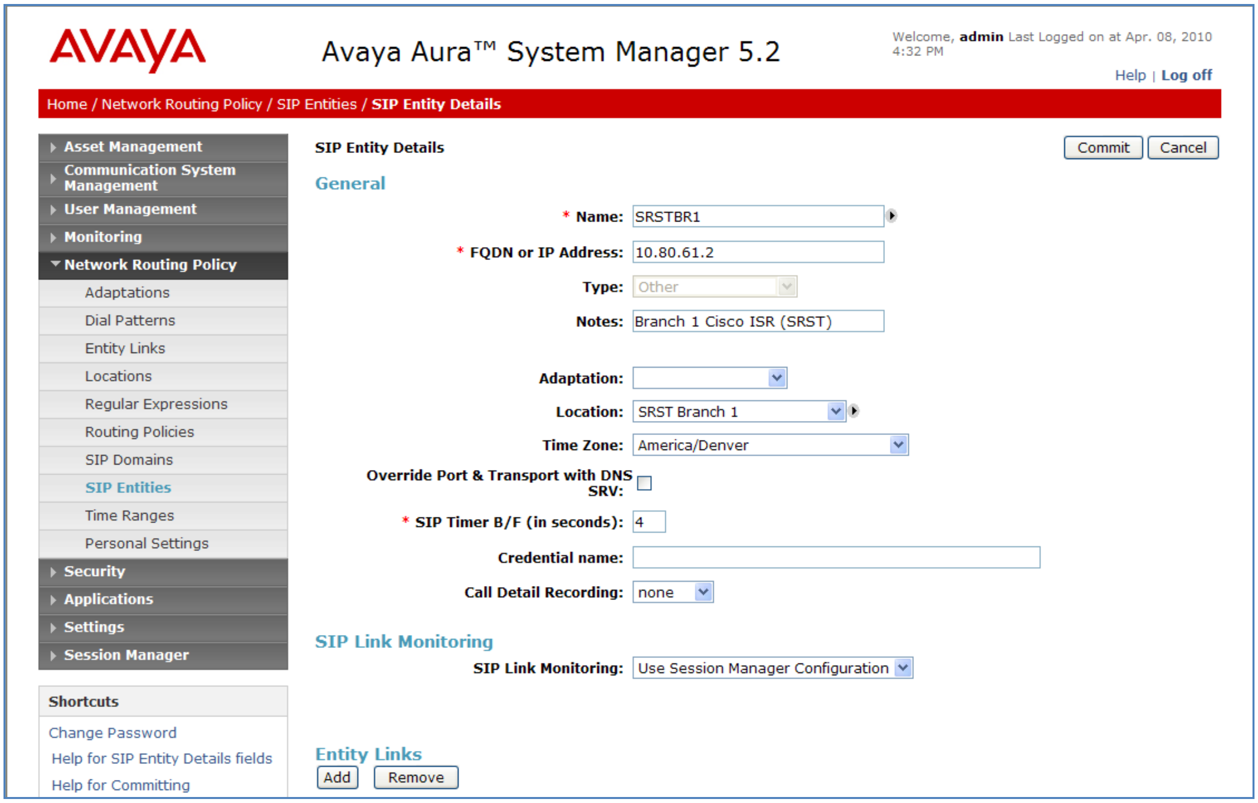
Using the steps above, create SIP Entities for the following items highlighted below:



The following screen shows the addition of Session Manager SIP Entity. The IP address of the SM-100 Security Module is entered for **FQDN or IP Address**. TCP port 5060 is used for communications with Communication Manager acting as an Access Element and Communication Manager acting as a Feature Server. UDP port 5060 is used for communications with the Cisco ISR.



The following screen shows the results of adding the branch Cisco ISR for Branch 1. In this case, **FQDN or IP Address** is the IP address assigned to the branch Cisco ISR. Note the "Other" selection for **Type** as well as the selection of the branch Location as created in **Section 4.2.2**.



SIP Entities for the two Communication Managers should be created (not shown).

4.2.4. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity link. In the sample configuration, three entity links are created:

1. Session Manager to Communication Manger acting as an Feature Server
2. Session Manager to Communication Manager acting as an Access Element
3. Session Manager to Cisco ISR.

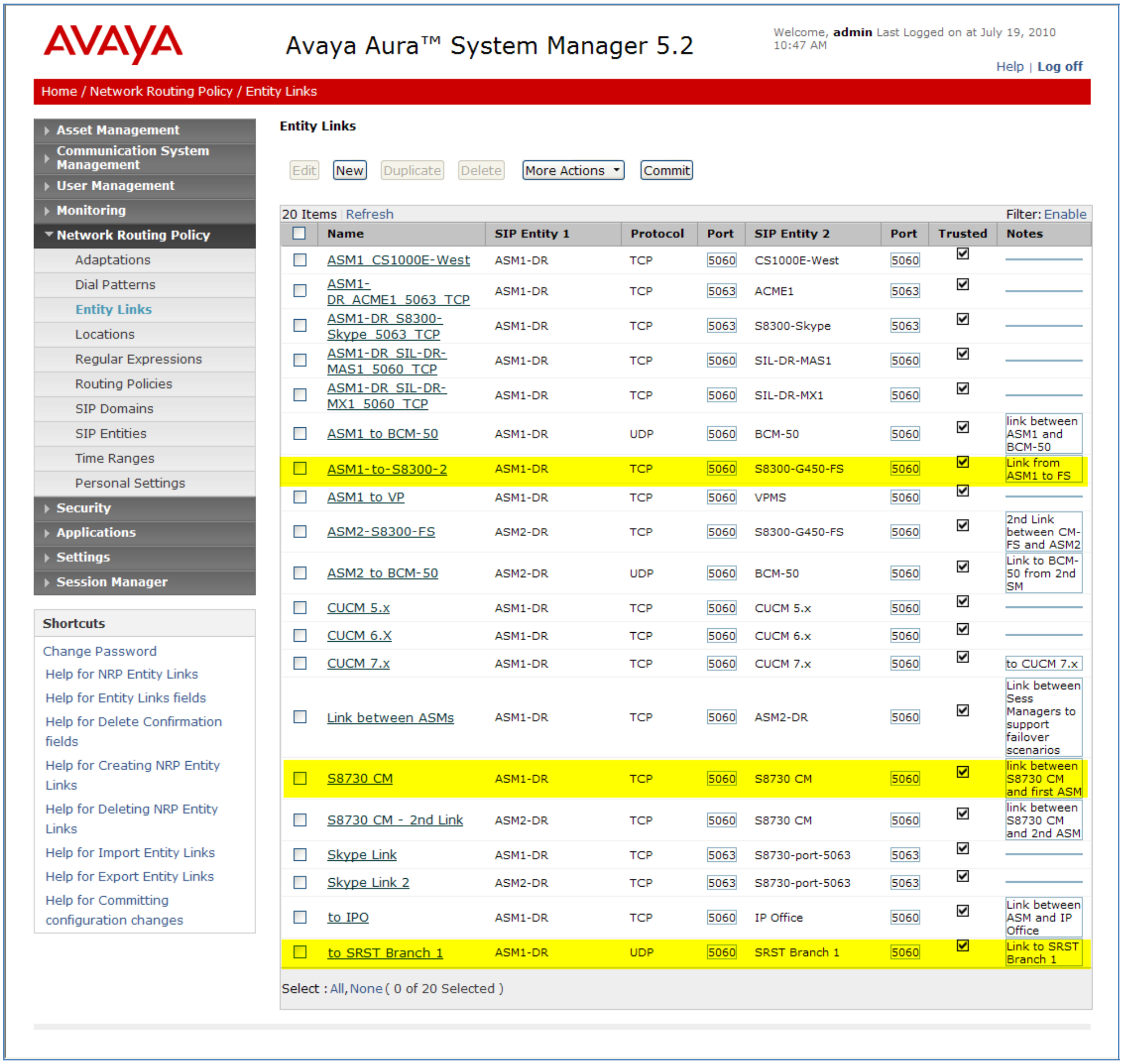
Steps to create an Entity Link are as follows:

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
- **Protocol**: Select "TCP"
- **Port**: Port number to which the other system sends SIP requests.
- **SIP Entity 2**: Select the Communication Manager SIP Entity
- **Port**: Port number on which the other system receives SIP requests.
- **Trusted**: Check this box

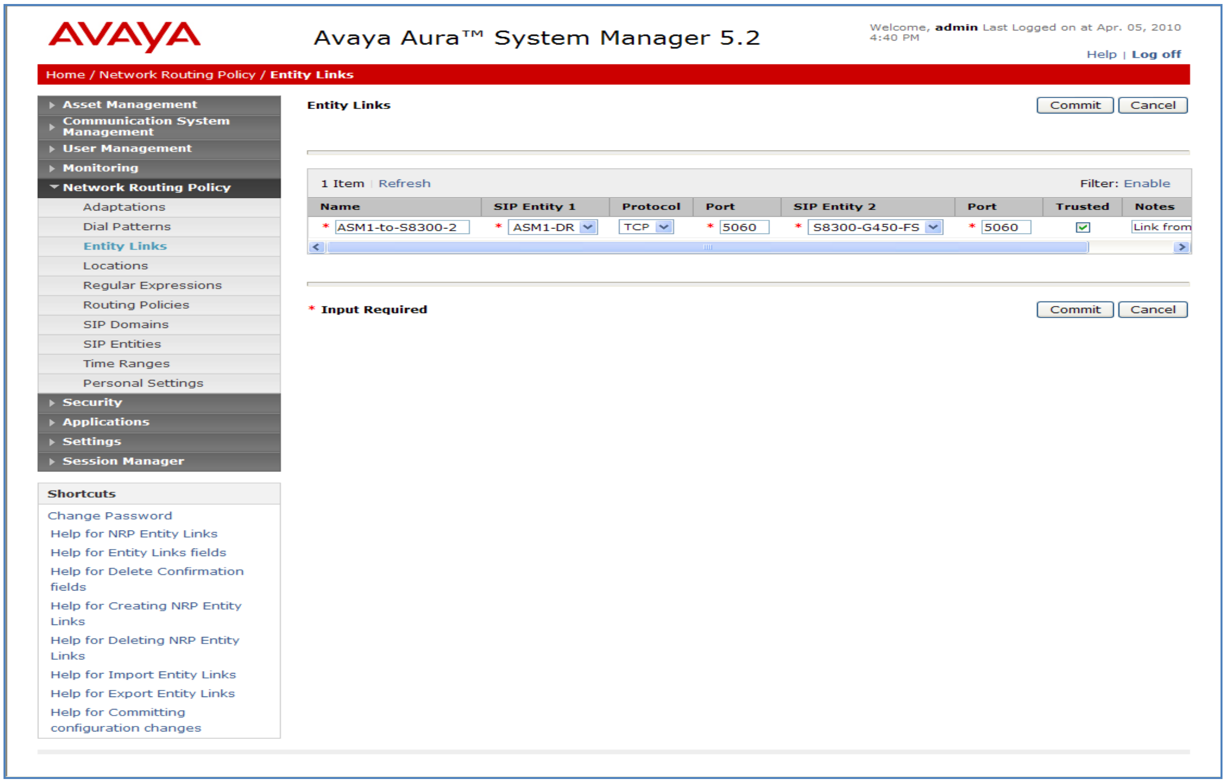
Click **Commit** to save the configuration.

Create Entity Links for the following highlighted items:



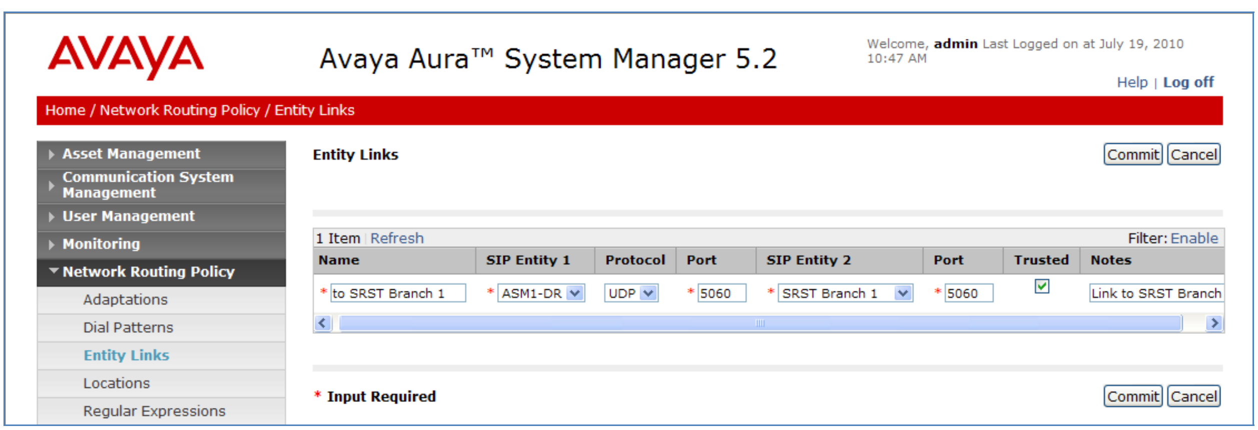
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
ASM1_CS1000E-West	ASM1-DR	TCP	5060	CS1000E-West	5060	☑	
ASM1-DR_ACME1_5063_TCP	ASM1-DR	TCP	5063	ACME1	5063	☑	
ASM1-DR_S8300-Skype_5063_TCP	ASM1-DR	TCP	5063	S8300-Skype	5063	☑	
ASM1-DR_SIL-DR-MAS1_5060_TCP	ASM1-DR	TCP	5060	SIL-DR-MAS1	5060	☑	
ASM1-DR_SIL-DR-MX1_5060_TCP	ASM1-DR	TCP	5060	SIL-DR-MX1	5060	☑	
ASM1 to BCM-50	ASM1-DR	UDP	5060	BCM-50	5060	☑	link between ASM1 and BCM-50
ASM1-to-S8300-2	ASM1-DR	TCP	5060	S8300-G450-FS	5060	☑	Link from ASM1 to FS
ASM1 to VP	ASM1-DR	TCP	5060	VPMS	5060	☑	
ASM2-S8300-FS	ASM2-DR	TCP	5060	S8300-G450-FS	5060	☑	2nd Link between CM-FS and ASM2
ASM2 to BCM-50	ASM2-DR	UDP	5060	BCM-50	5060	☑	Link to BCM-50 from 2nd SM
CUCM 5.x	ASM1-DR	TCP	5060	CUCM 5.x	5060	☑	
CUCM 6.X	ASM1-DR	TCP	5060	CUCM 6.x	5060	☑	
CUCM 7.x	ASM1-DR	TCP	5060	CUCM 7.x	5060	☑	to CUCM 7.x
Link between ASMs	ASM1-DR	TCP	5060	ASM2-DR	5060	☑	Link between Sess Managers to support failover scenarios
S8730 CM	ASM1-DR	TCP	5060	S8730 CM	5060	☑	link between S8730 CM and first ASM
S8730 CM - 2nd Link	ASM2-DR	TCP	5060	S8730 CM	5060	☑	link between S8730 CM and 2nd ASM
Skype Link	ASM1-DR	TCP	5063	S8730-port-5063	5063	☑	
Skype Link 2	ASM2-DR	TCP	5063	S8730-port-5063	5063	☑	
to IPO	ASM1-DR	TCP	5060	IP Office	5060	☑	Link between ASM and IP Office
to SRST Branch 1	ASM1-DR	UDP	5060	SRST Branch 1	5060	☑	Link to SRST Branch 1

Below is the screen for the first entity link, between Session Manager and Communication Manager acting as a Feature Server.



The second entity link between Session Manager and Communication Manager (for routing branch local calls to PSTN in Normal Mode) is similarly configured (not shown). In the sample configuration, this third Entity Link was configured to use **Protocol** UDP and **Port** 5060.

The screen below shows the Entity Link between Session Manager and the Branch Cisco ISR.



4.2.5. Add Routing Policy

Routing policies describe the conditions under which calls will be routed to the SIP Entities. A routing policy must be added for routing the branch local PSTN call (sent over to Session Manager from Communication Manager after its location-based routing decision) to the branch Cisco ISR. Each branch should have its own Routing Policy defined.

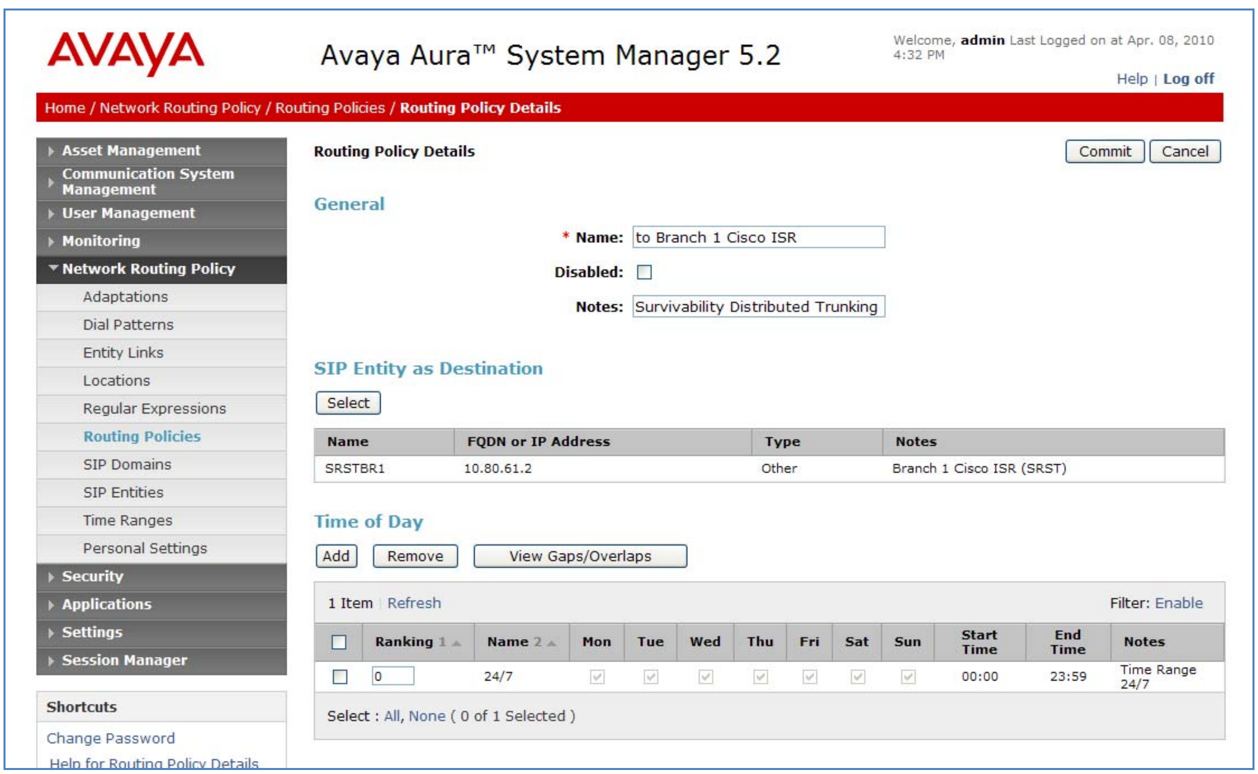
To add a routing policy, select **Routing Policies** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

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 branch 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 local PSTN calls to Branch 1.



4.2.6. Add Dial Patterns

4.2.6.1 Branch PSTN Outbound Local Calls

Define a Dial Pattern for matching local PSTN calls based on Area Code. A Dial Patterns is then associated with a Routing Policy to direct calls with the matched Area Code to the branch where the call to the PSTN will be a non-toll local call.

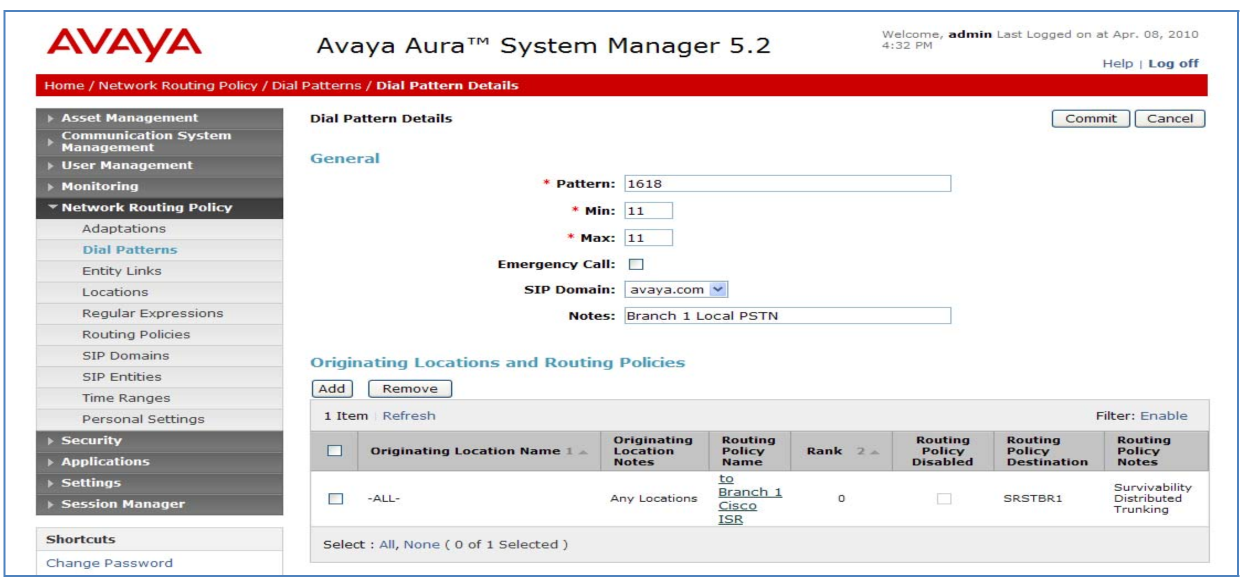
To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following, as shown in the screens below:

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 4.2.1**
- **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 local PSTN calls to Branch 1.



4.2.6.2 Branch PSTN Outbound Long Distant Calls

Define a Dial Pattern for matching branch Long Distant PSTN calls. The Dial Patterns is then associated with a Routing Policy which uses the Origination Location to route the long distant call back to the Cisco ISR at the branch location. The Cisco ISR will then use dial peers to route the call out the Cisco ISR T1 interface to the PSTN.

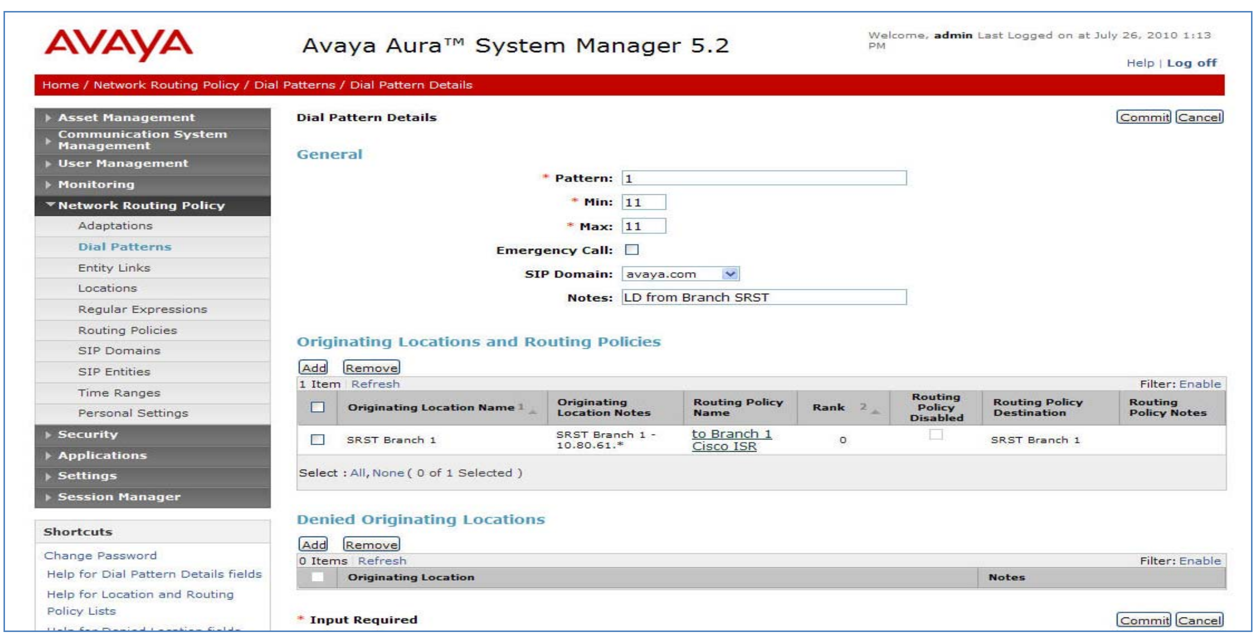
To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following, as shown in the screens below:

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 4.2.1**
- **Notes**: Comment on purpose of dial pattern.

Under *Originating Locations and Routing Policies*:
Click **Add**, and then select the **"SRST Branch 1"** location for **Originating Location Name** field and **"to Branch 1 Cisco ISR"** 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 long distant PSTN calls from Branch 1.



4.2.7. Add 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 a 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):

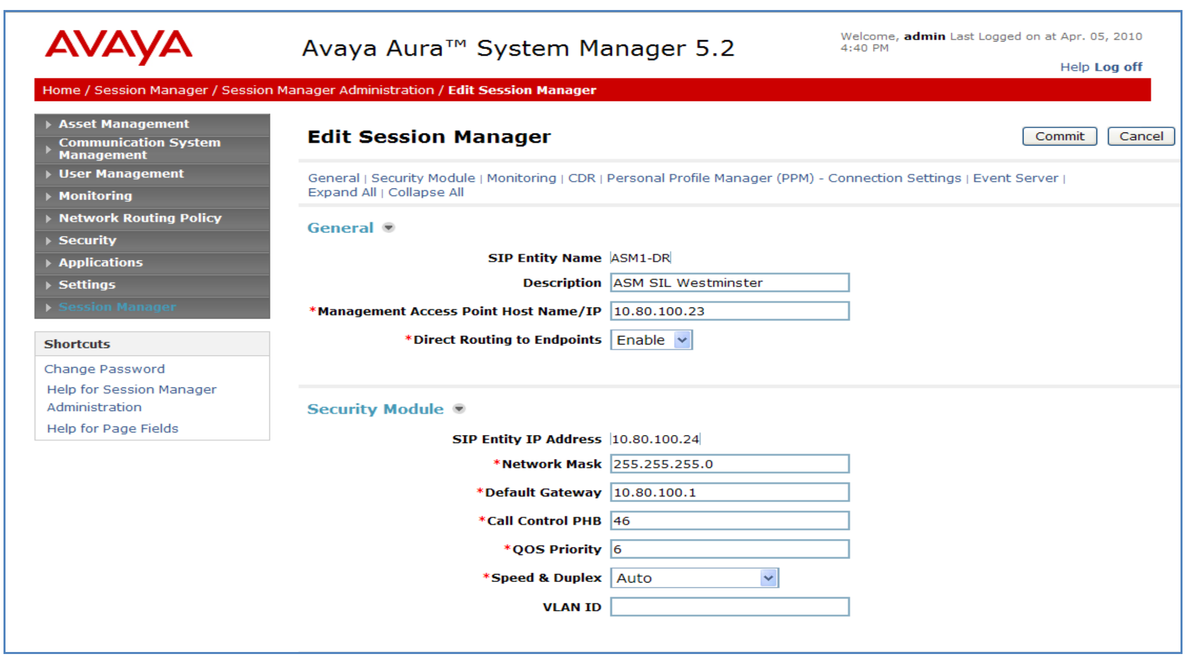
Under *General*:

- **SIP Entity Name**: Select the name of the SIP Entity created for Session Manager
- **Description**: 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.

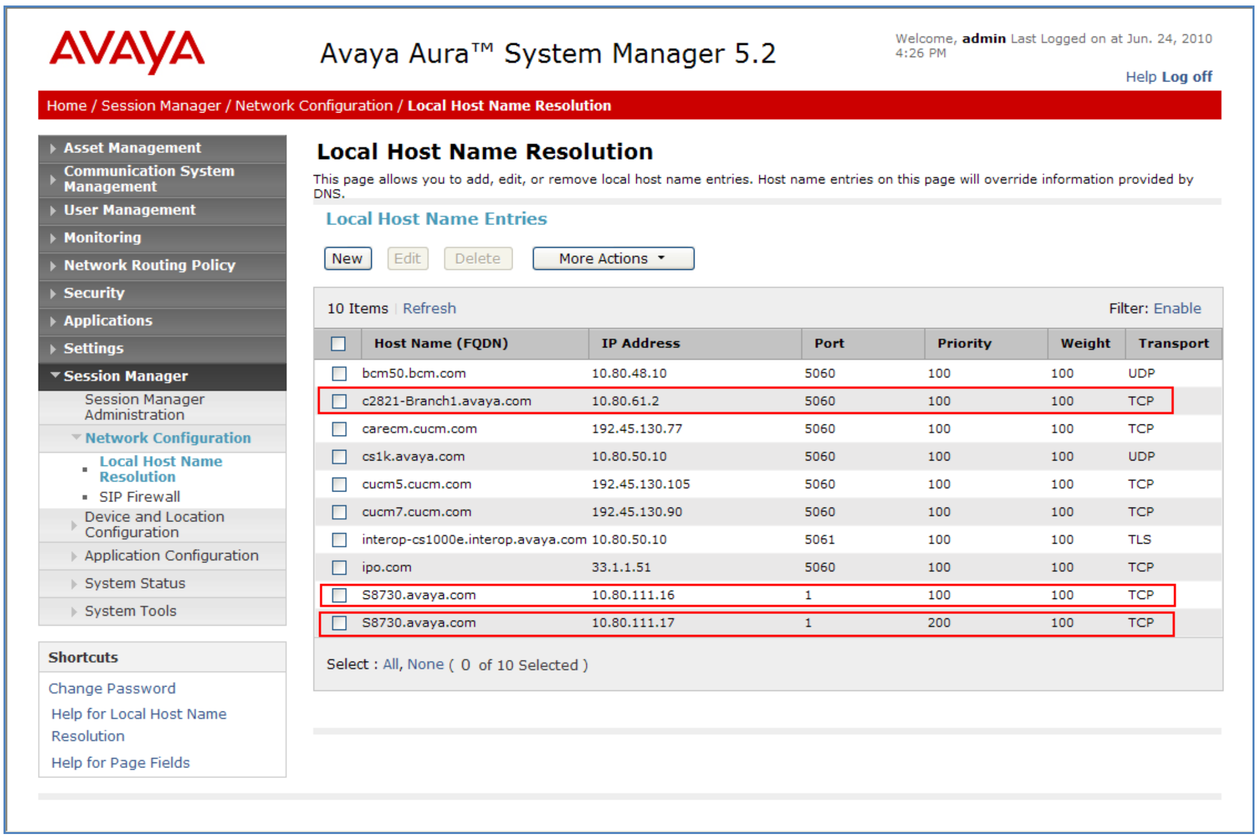


4.2.8. Define Local Host Name Resolution

The host names referenced in the definitions of the previous sections must be defined. To do so, Select **Session Manager → Network Configuration → Local Host Name Resolution** on the left. For each host name, click **New** and enter the following:

- **Host Name**: Name used for the host
- **IP Address:** IP address of the host's network interface
- **Port:** Port number to which SIP requests are sent by the host
- **Transport:** Transport Layer protocol to be used for SIP requests

Defaults can be used for the remaining fields. The **Priority** and **Weight** fields are used when multiple IP addresses are defined for the same host. The following screen shows the host name resolution entries used in the sample configuration.



4.2.9. Add Communication Manager 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). Enter the following fields, and use defaults for the remaining fields:

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

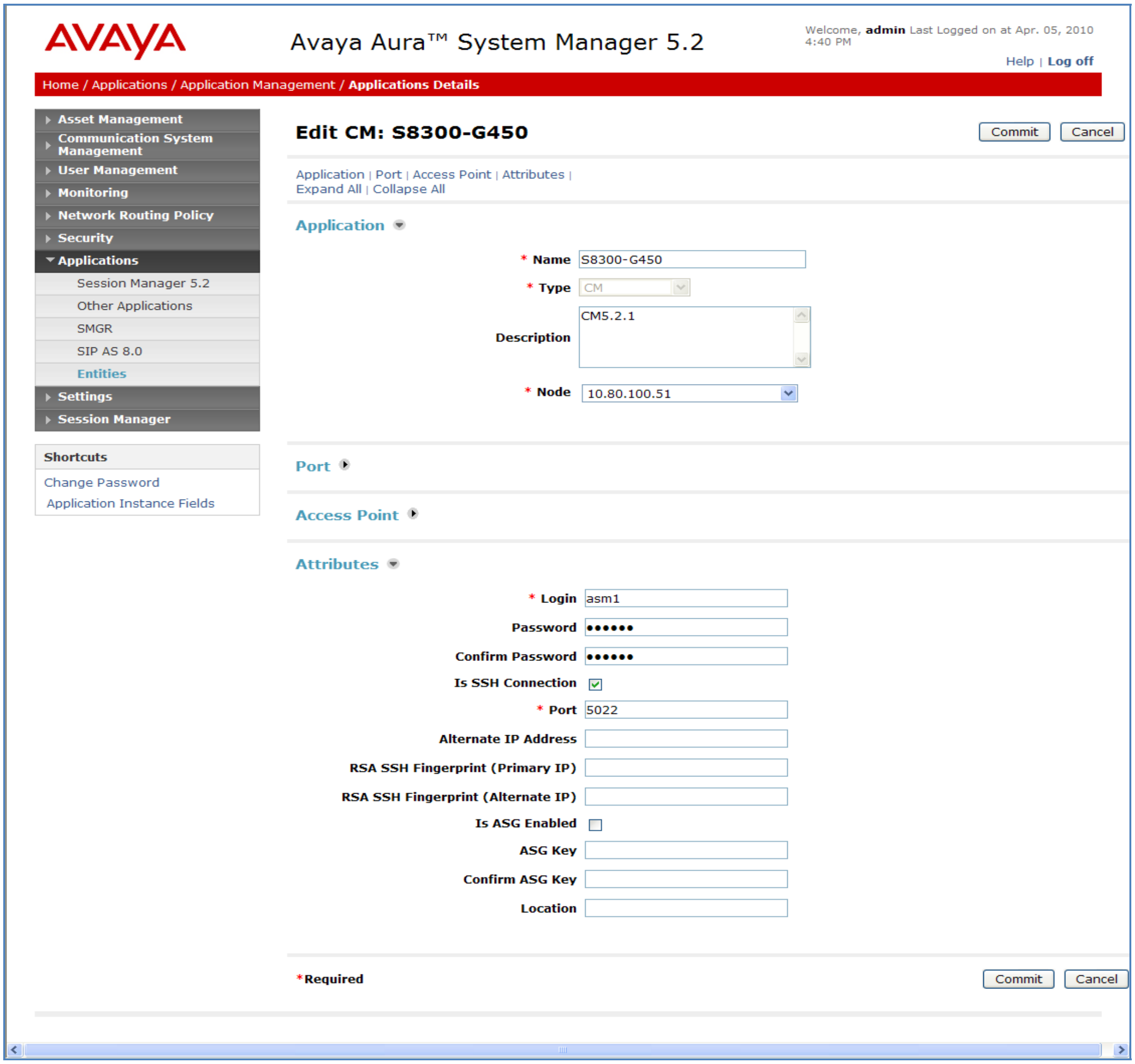
Under the *Attributes* section, enter the following fields, and use defaults for the remaining fields:

- **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.


AVAYA
Avaya Aura™ System Manager 5.2
Welcome, admin Last Logged on at Apr. 05, 2010 4:40 PM
Help | Log off
Home / Applications / Application Management / Applications Details
Asset Management
Communication System Management
User Management
Monitoring
Network Routing Policy
Security
Applications
Session Manager 5.2
Other Applications
SMGR
SIP AS 8.0
Entities
Settings
Session Manager
Shortcuts
Change Password
Application Instance Fields
Edit CM: S8300-G450
Commit
Cancel
Application | Port | Access Point | Attributes |
Expand All | Collapse All
Application
* Name S8300-G450
* Type CM
Description CM5.2.1
* Node 10.80.100.51
Port
Access Point
Attributes
* Login asm1
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
*Required
Commit
Cancel

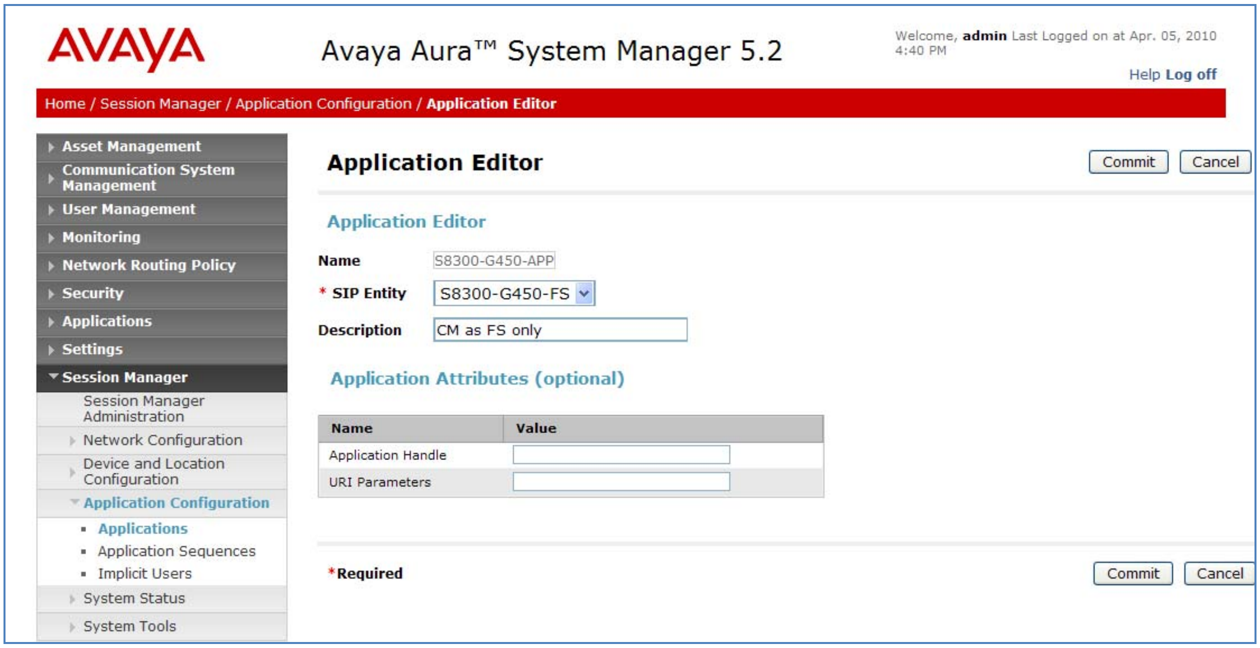
Step 2

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

Click on **Commit**.

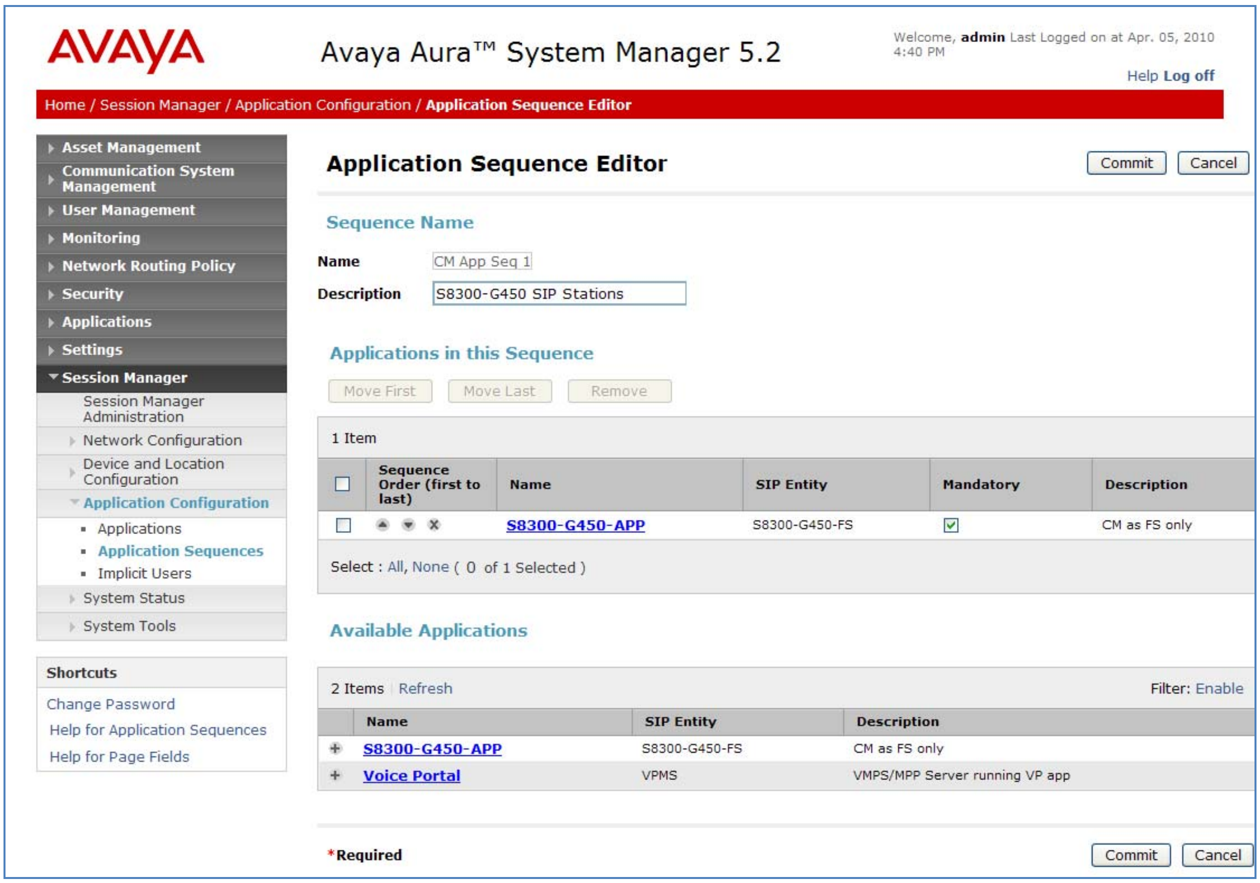
The screen shown below is the Edit screen since the Application has already been configured.



Step 3

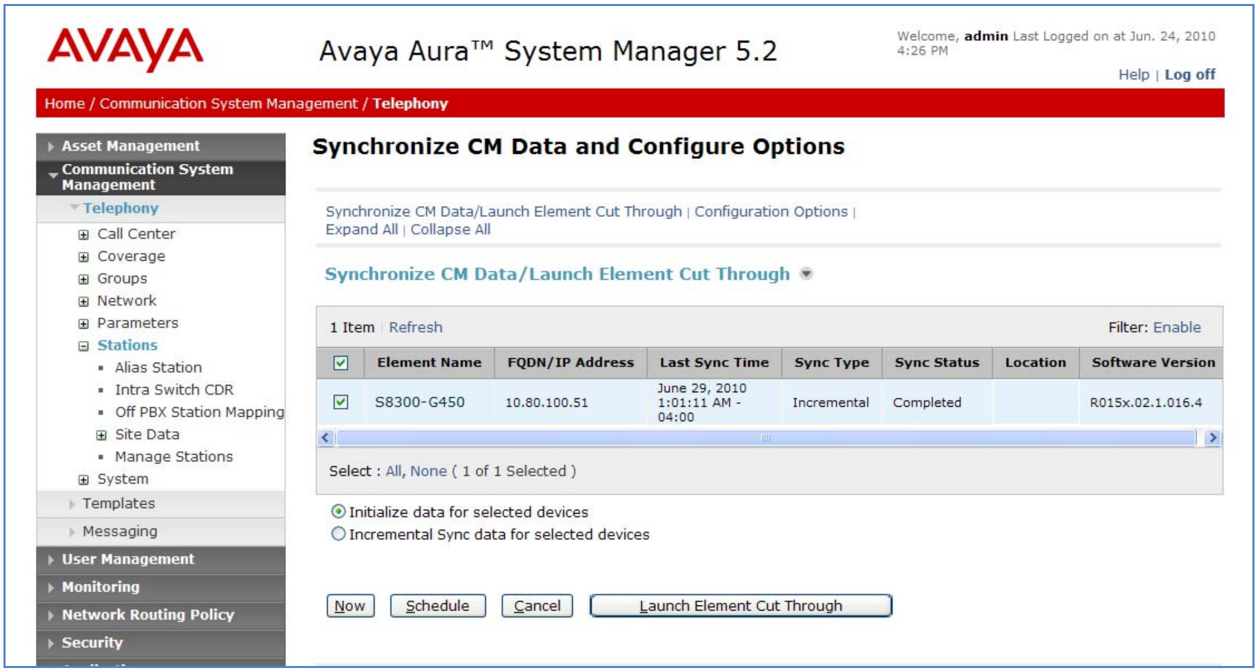
Select **Session Manager → Application Configuration → Application Sequences** on the left. Click on **New** (not shown). Enter a descriptive name in the **Name** field. Click on the "+" sign next to the appropriate *Available Applications*, and the selected available application will be moved up to the *Applications in this Sequence* section. In this sample configuration, "CM App Seq 1" was shown in the screen below (which is the Edit screen since the Application Sequence has already been configured).

Click on **Commit**.

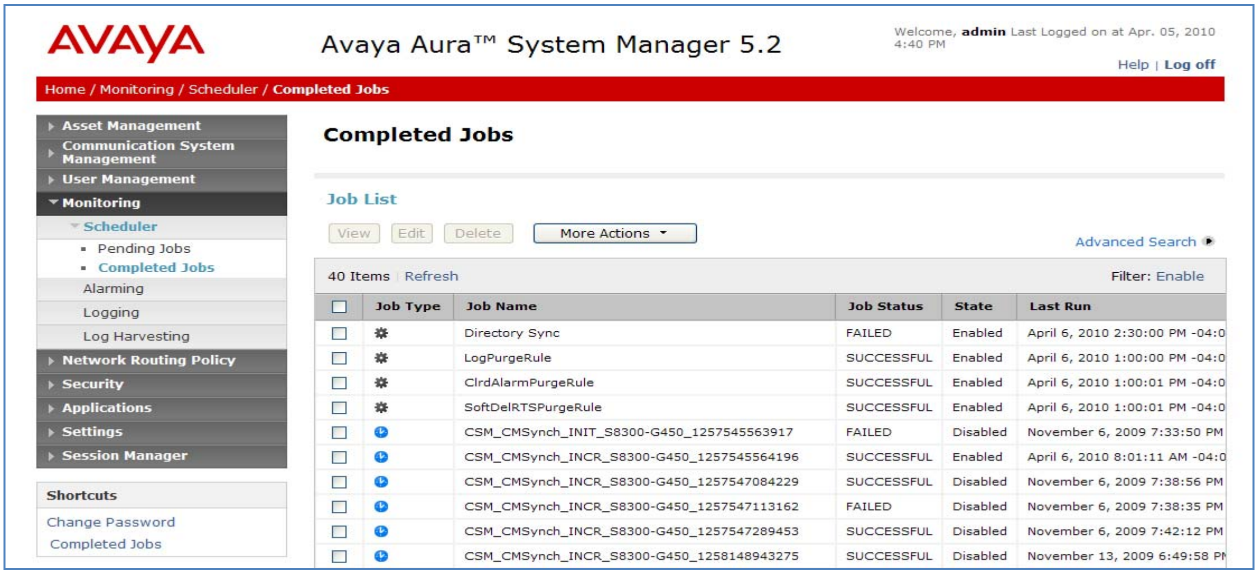


Step 4

Select **Communication System Management → Telephony** on the left. Select the appropriate Element Name ("S8300-G450" in this case). Check the **Initialize data for selected devices** checkbox. Then click on **Now**. This will cause a data synchronization task to start. This may take some time to complete.

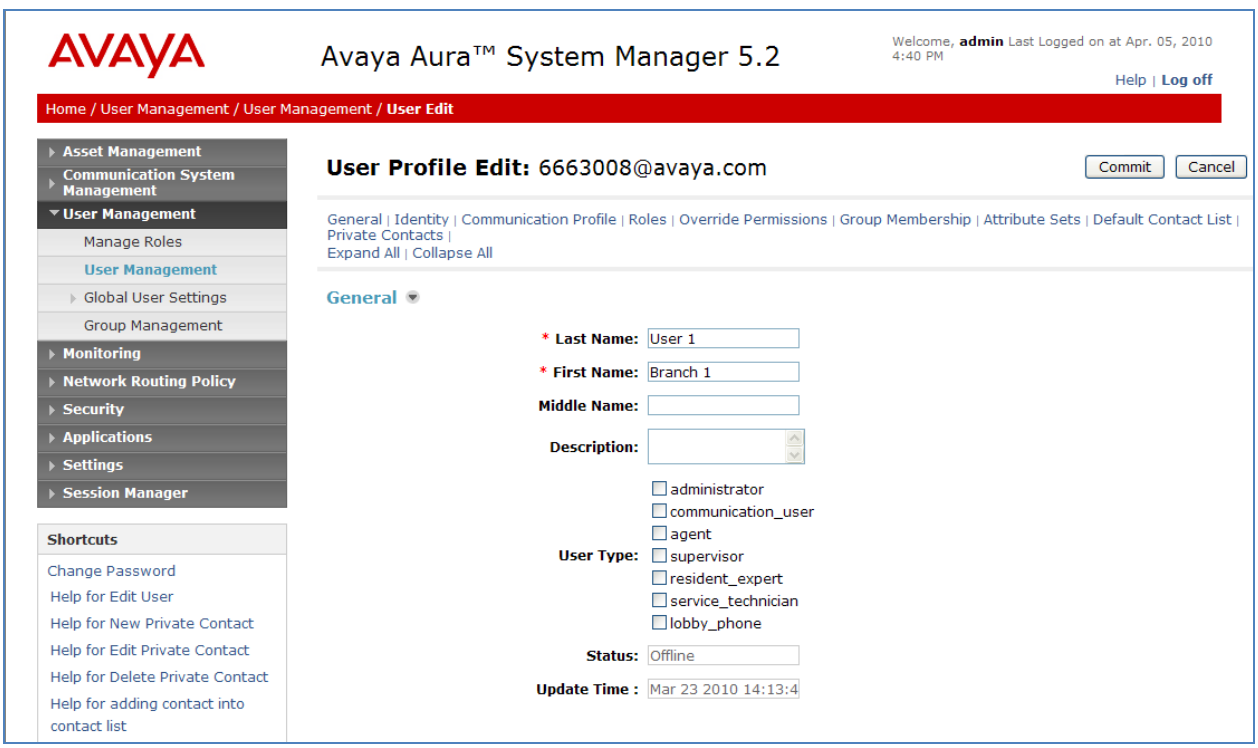


Use the menus on the left under **Monitoring → Scheduler → Completed Jobs** to determine when the task has completed, as shown below (see entry with embedded Communication Manager name "S8300-G450" for the sample configuration).



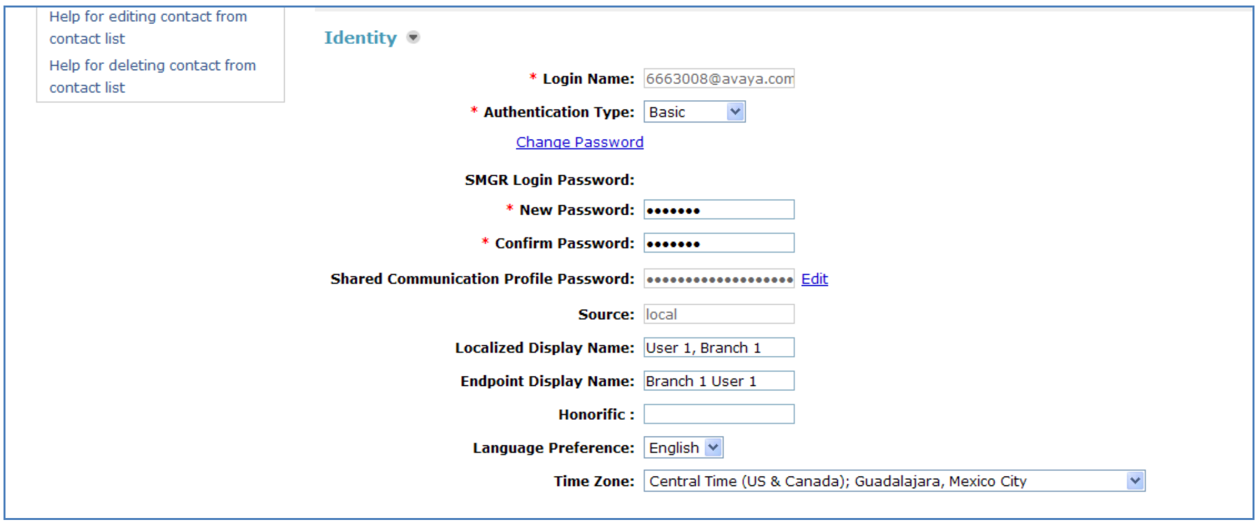
4.2.10. User Management for Adding SIP Telephone Users

Users must be added to Session Manager corresponding to the SIP stations added in Communication Manager (see **Section 4.1.8**). 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 to add.



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

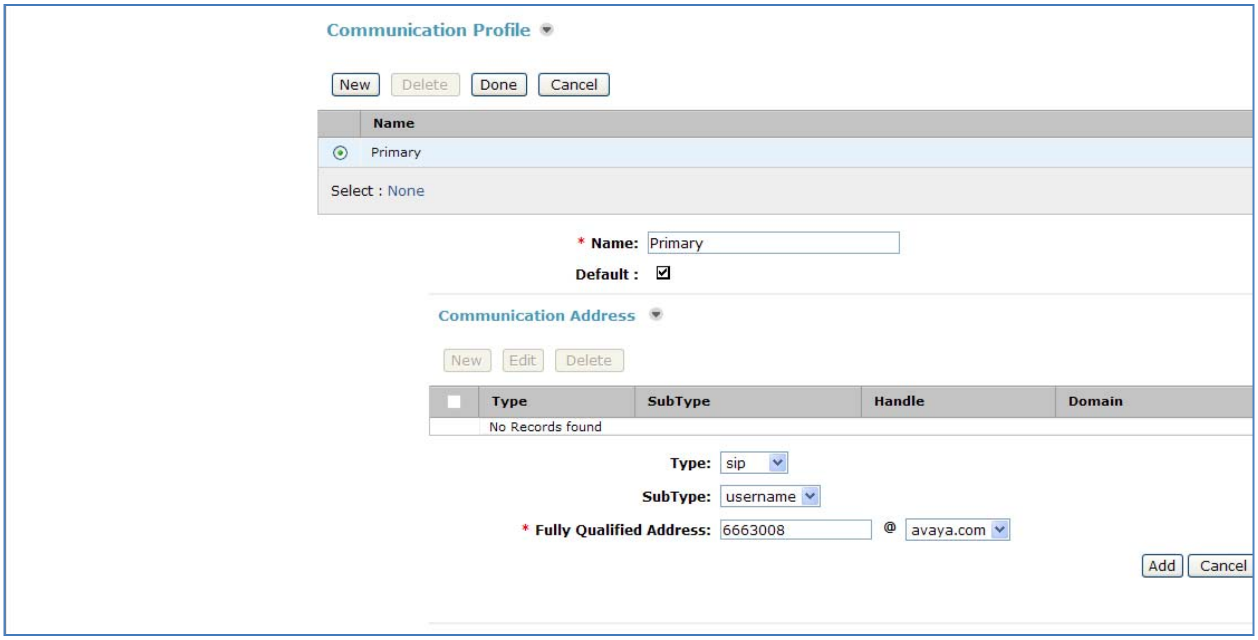
- **Login Name**: Telephone extension (see **Section 4.1.8**)
- **SMGR Login Password**: Password to log into System Manger
- **Shared Communication Profile Password**: Password to be entered by the user when logging into the telephone
- **Localized Display Name**: Name to be used as calling party
- **Endpoint Display Name**: Full name of user
- **Language Preference**: Select the appropriate language preference
- **Time Zone:** Select the appropriate time zone



Click on *Communication Profile* to expand that section. Then click on *Communication Address* to expand that section. Enter 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 defined in **Section 4.1.8** and **4.1.6**

Click on **Add** to add the record with the above information.

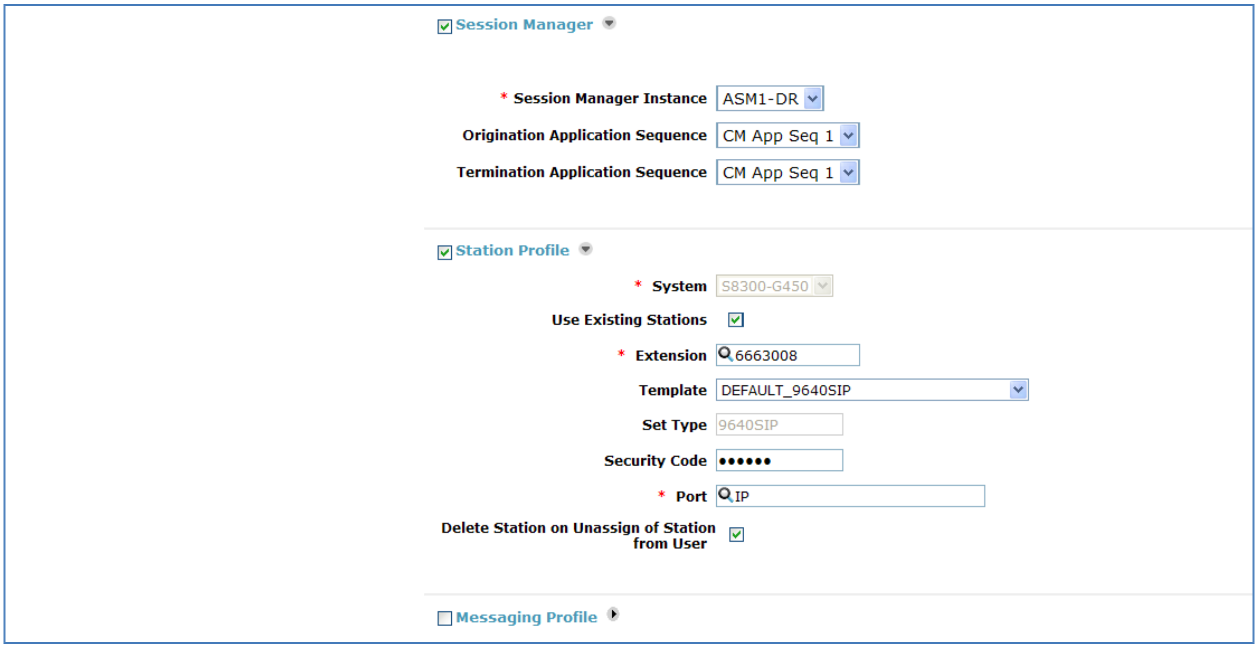


Click on *Session Manager* to expand that section. Select the appropriate Session Manager server for **Session Manager Instance**. For **Origination Application Sequence** and **Termination Application Sequence**, select the Application Sequence configured in **Section 4.2.9 Step 3**.

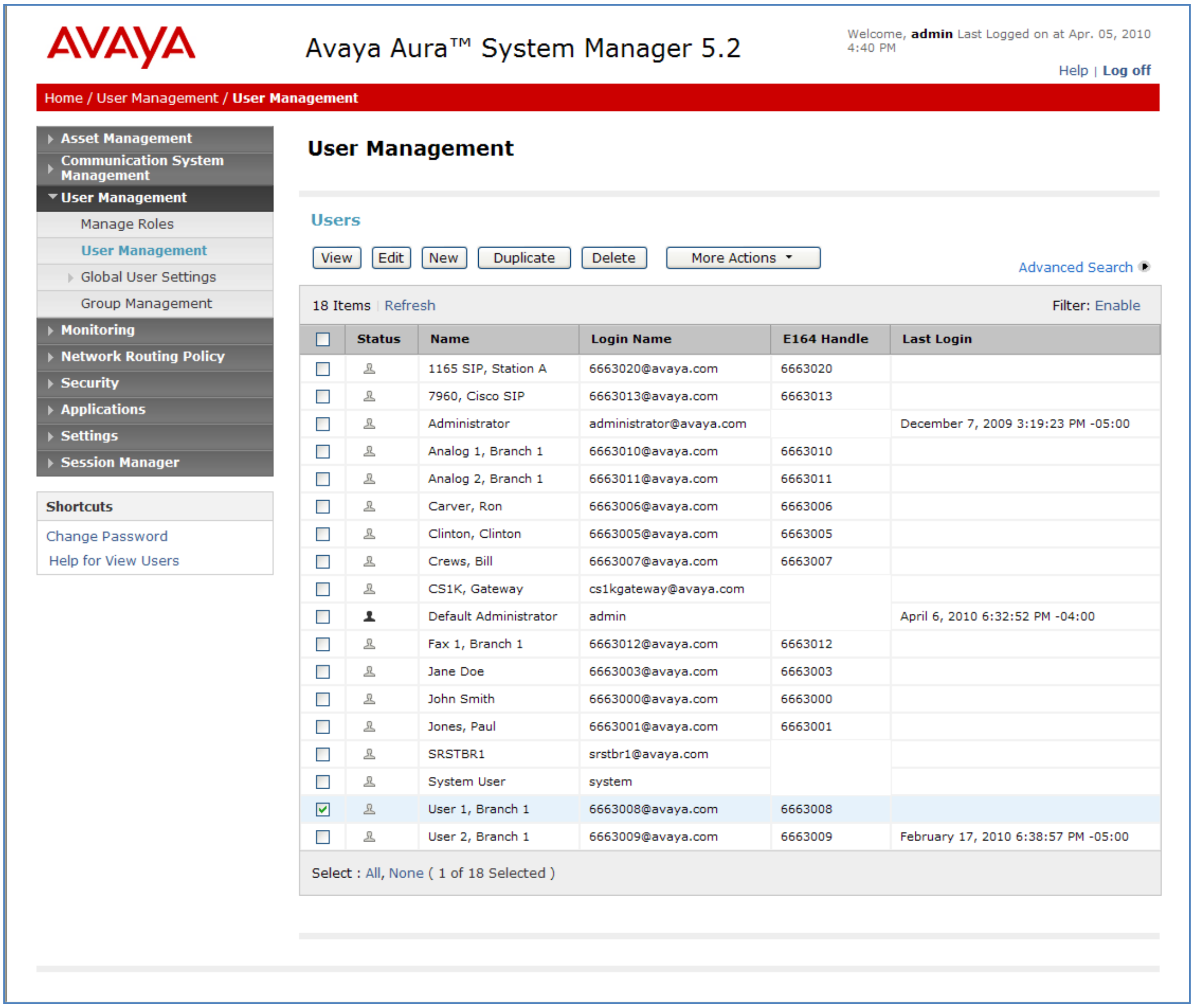
Click on *Station Profile* to expand that section. Enter the following fields and use defaults for the remaining fields:

- **System**: Select the Communication Manager entity
- **Use Existing Stations**: Check this box
- **Extension**: Enter the extension
- **Template**: Select an appropriate template matching the telephone type.
- **Port**: Click on the Search icon to pick a port (in this case "IP")

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



Repeat the above procedures to add each SIP telephone user for the Headquarters site as well as the Remote Branch site (including the analog phones connected to the FXS interface ports on the Cisco ISR). The follow User Management screen shows the SIP telephone users configured in the sample configuration for the Headquarters site and Remote Branch 1 (6663006 and 6663007 are Headquarters Avaya 9600 SIP Phone users; 6663008 and 6663009 are Avaya 9600 SIP Phone users at Remote Branch 1; 6663010 and 6663011 are analog phones connected to the Cisco ISR FXS ports; 6663012 is an analog fax connected to the Cisco ISR FXS port).

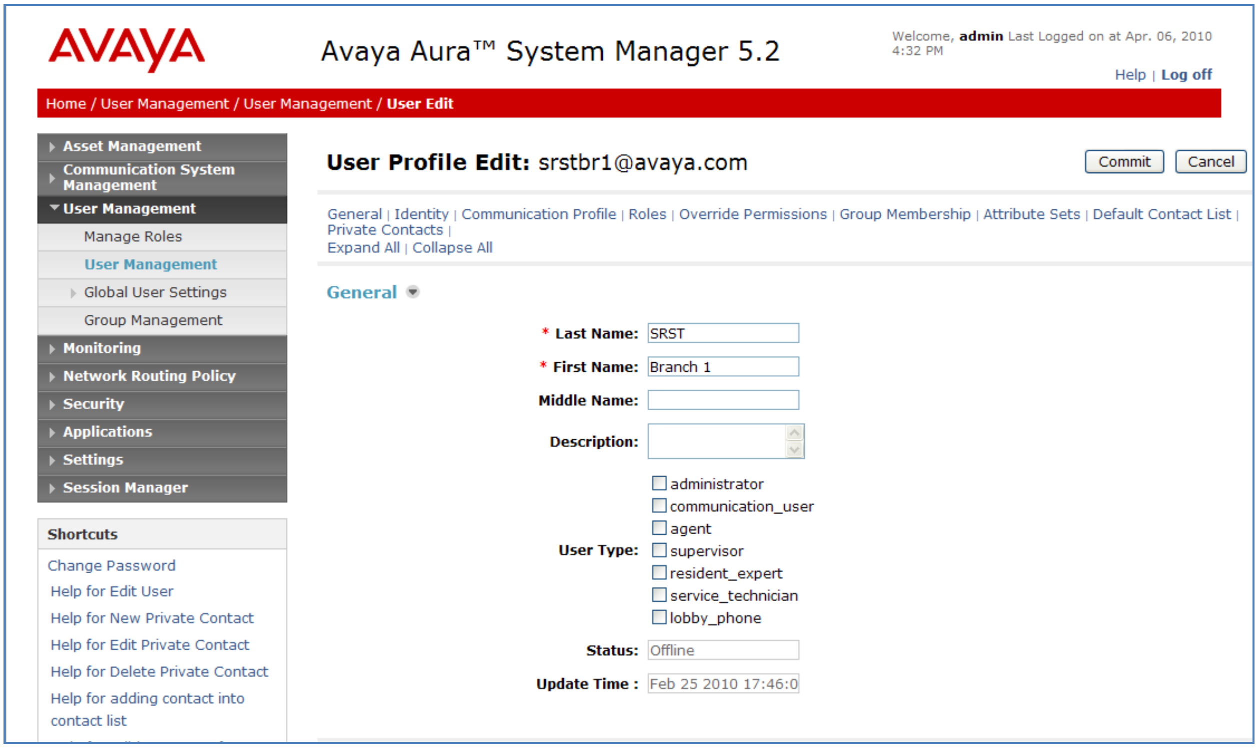


4.2.11. Add User for Cisco ISR SIP User Agent

Communication from the Cisco ISR to the Session Manager occurs through the SIP-UA configuration level on the Cisco ISR using SIP. In order for the Session Manager to allow SIP message exchange with the Cisco ISR SIP-UA, authentication must be established using user name and password. Since this user will only be used for authentication of the SIP-UA with Session Manager, there is no need to assign a station to the user.

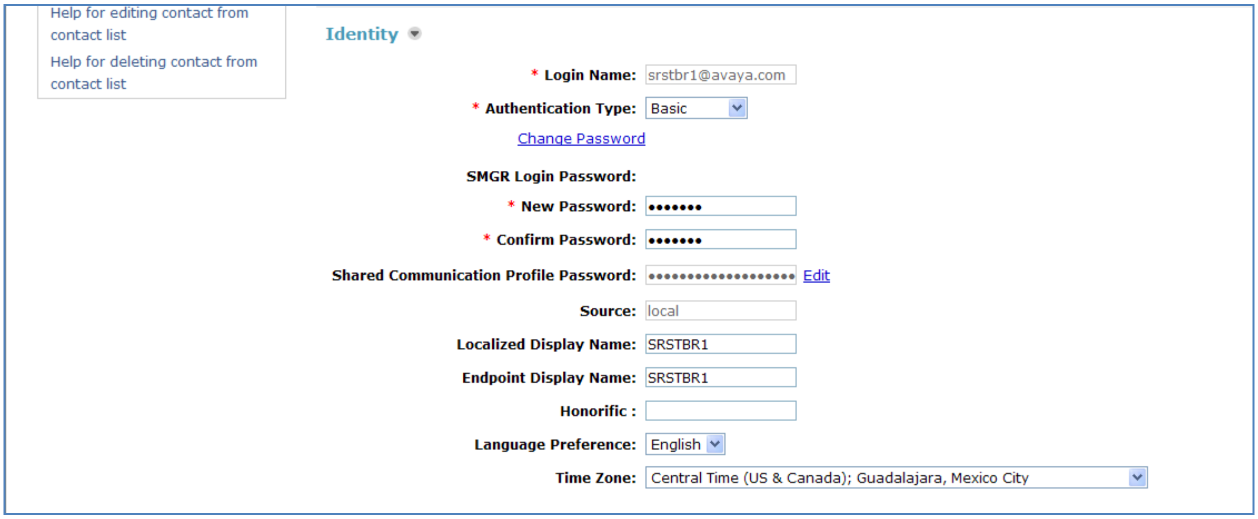
In the sample configuration used in these Application Notes a user was created representing the Cisco ISR at the remote branch location, i.e. srstbr1@avaya.com

Select **User Management** → **User Management** on the left. Then click on **New** to open the New User Profile page. Enter a **First Name** and **Last Name** for the user to add.



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

- **Login Name**: Name to use for authentication from SIP-UA
- **SMGR Login Password**: Password to log into System Manger
- **Shared Communication Profile Password**: Password to be used
- **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



4.3. Remote Branch Configuration

4.3.1. SIP 9600 Stations

4.3.1.1 46xxsettings.txt file

The configuration parameters of the Avaya 9600 SIP Phone specific to SIP Survivability and the sample configuration are described in this section. See reference [1] before setting or changing the parameters shown below.

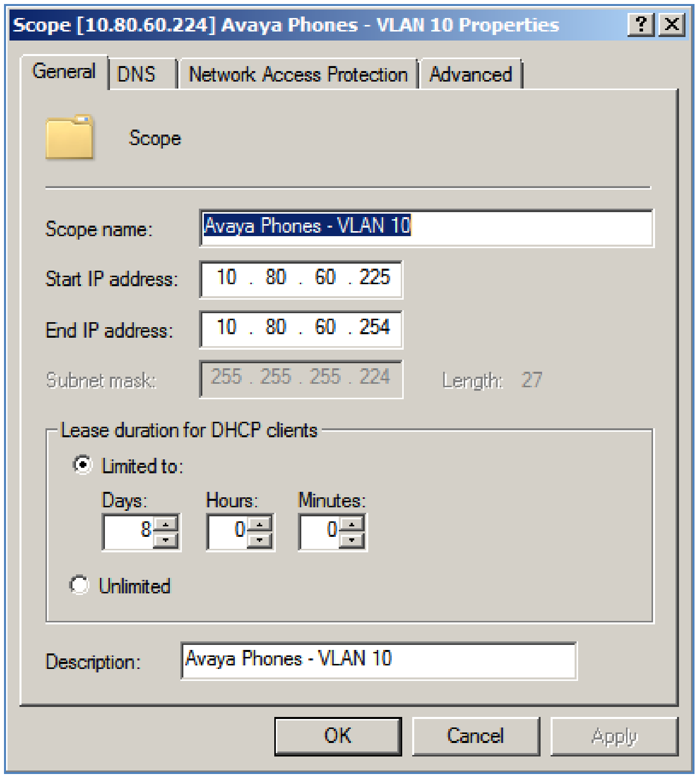
46xxsettings.txt Parameter Name	Values Used in Sample Configuration	Description
SIPDOMAIN	avaya.com	Sets the SIP domain name to be used during registration.
SIP_CONTROLLER_LIST	10.80.100.24:5060; transport=tcp, 10.80.61.33:5060; transport=tcp	A priority list of SIP Servers for the phone to use for SIP services. The port and transport use the default values of 5061 and TLS when not specified. The current settings have the Session Manager as the primary SIP registration server and the local branch Cisco ISR as the secondary SIP registration server.
FAILBACK_POLICY	auto	While in Survivable Mode, this parameter 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.

46xxsettings.txt Parameter Name	Values Used in Sample Configuration	Description
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 is 4 seconds. After the SIP INVITE is terminated, the phone immediately transitions to Survivable Mode.
MSGNUM	6665000	The number dialed when the Message button is pressed and the phone is in Normal Mode.
PSTN_VM_NUM	6665000	The number dialed when the Message button is pressed and the phone is in Survivable Mode.
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.
GMTOFFSET	"-7:00"	Sets the time zone the phone should use.
DSTOFFSET	"1"	Sets the daylight savings time adjustment value.
DIALPLAN	"[666]xxxx|91xxxxxxxxxx|9[2-9]xxxxxxxxxx|[618]xxxxxx"	Enables the acceleration of dialing when the WAN is down and the Cisco ISR is active, by defining the dial plan used in the phone. In normal mode, the Avaya telephone does not require these settings to expedite dialing.

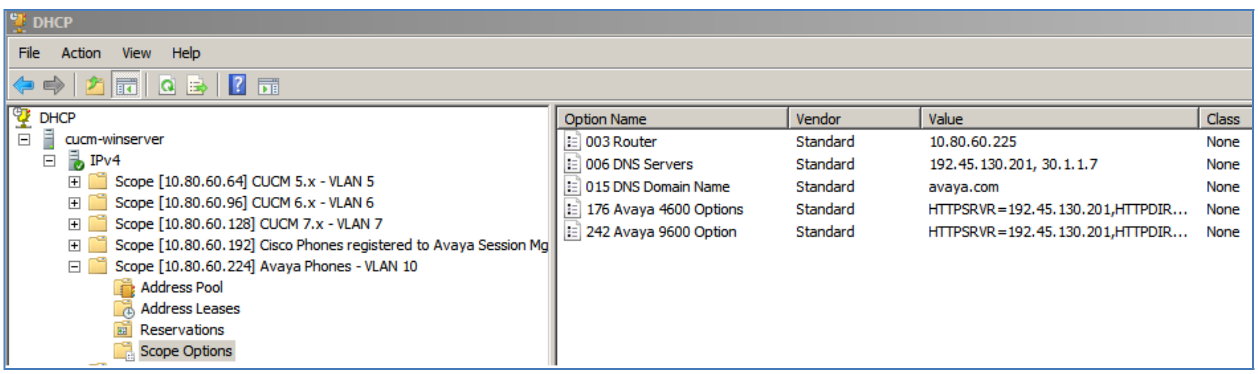
4.3.1.2 DHCP Configuration

Both HQ and Remote Branch 9600 SIP phones were configured to DHCP their IP address, Network Mask, Gateway Address, DNS and Option 242 settings. Microsoft DHCP Server on Windows Server 2008 R2 was used to administrator the DHCP scopes for the HQ and Remote Branch phones.

The scope range used for the HQ SIP phones was configured as follows:



The HQ Scope Options used are shown below:

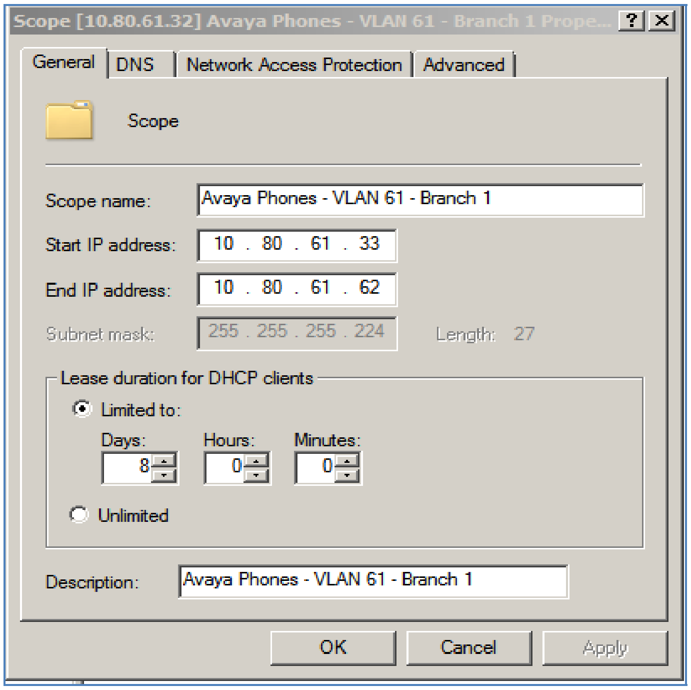


Option 242 has a configured string value of:

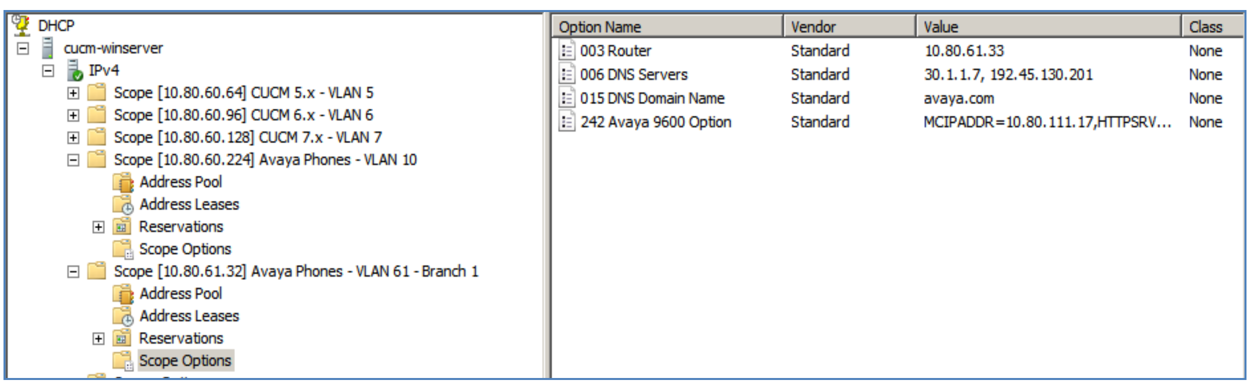
"MCIPADDR=10.80.111.17,HTTPSRVR=192.45.130.201,SNMPSTRING=public,SIPPROXYSRVR=10.80.100.24"

The "MCIPADD" setting is used for H.323 phones for registering to the Communication Manager Access Element. The "SIPPROXYSRVR" setting is used by the 96xx SIP phones for SIP registration to the Session Manager. The "HTTPSRVR" setting is used by the phones to locate the HTTP server from which to download firmware updates and load its 46xxsetting.txt file shown in **Section 5.3.1.1**.

The scope range used for Remote Branch 1 was configured as follows:



The Remote Branch Scope Options used are shown below:



Option 242 has a configured string value of:

"MCIPADDR=10.80.111.17,HTTPSRVR=192.45.130.201,SNMPSTRING=public,SIPPROXYSRVR=10.80.100.24"

4.3.2. Add User and Station to Avaya Aura™ Session Manager

Refer to **Section 5.2.10** to complete this step if not already configured.

4.3.3. Configure Cisco ISR

This section describes the commands necessary to configure the SRST feature Cisco 2821 ISR. SIP registrar functionality on Cisco IOS enables the Cisco router to become a backup SIP proxy and accept SIP registration messages from SIP phones. A registrar accepts SIP register requests and dynamically builds VoIP dial peers, allowing the Cisco IOS Voice Gateway software to route calls to SIP phones.

Under normal operation, the Avaya 9600 SIP phones are registered with the HQ Session Manager as the primary proxy, and with the Cisco ISR router as the backup proxy. If the HQ Session Manager is not available (e.g., a WAN failure), the Cisco ISR will function as an active proxy to route calls for the Avaya 9600 SIP phones. This “fail-over” happens after the router loses connection to the primary proxy. Once the primary proxy server (HQ Session Manager) is reachable again (e.g., WAN is restored), the Avaya 9600 SIP phones will automatically “fall back” to re-register with the primary proxy server.

It is assumed that basic network configuration of the Cisco ISR has already been completed, please see References section, References [8] for more information.

4.3.3.1 Cisco ISR Checks System Hardware

To view the hardware detected by the Cisco ISR, use the command **show diag**
Connect to the Cisco ISR using the standard Cisco console cable, or network terminal if the device is already configured for such.

```
c2821-Branch1#sh diag
Slot 0:
        C2821 Motherboard with 2GE and integrated VPN Port adapter, 2 ports
        Port adapter is analyzed
        Port adapter insertion time 4d10h ago
        Onboard VPN             : v2.3.3
        EEPROM contents at hardware discovery:
        PCB Serial Number        : FOC09284209
        Hardware Revision        : 4.0
        Top Assy. Part Number    : 800-21933-02
        Board Revision           : B0
        Deviation Number         : 0
        Fab Version              : 08
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Processor type           : 87
        Hardware date code       : 20050719
        Chassis Serial Number    : FTX0931A39N
        Chassis MAC Address      : 0014.f2c1.30e8
        MAC Address block size   : 32
        CLEI Code                : CNMJ6N0BRA
```

```
        Product (FRU) Number      : CISCO2821
        Part Number               : 73-8854-12
        Version Identifier        : V01
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF C1 8B 46 4F 43 30 39 32 38 34 32 30 39 40
          0x10: 03 E8 41 04 00 C0 46 03 20 00 55 AD 02 42 42 30
          0x20: 88 00 00 00 00 02 08 03 00 81 00 00 00 00 04 00
          0x30: 09 87 83 01 31 F3 1F C2 8B 46 54 58 30 39 33 31
          0x40: 41 33 39 4E C3 06 00 14 F2 C1 30 E8 43 00 20 C6
          0x50: 8A 43 4E 4D 4A 36 4E 30 42 52 41 CB 8F 43 49 53
          0x60: 43 4F 32 38 32 31 20 20 20 20 20 20 82 49 22 96
          0x70: 0C 89 56 30 31 20 D9 02 40 C1 FF FF FF FF FF FF

        PVDM Slot 0:                     PVDM resource for Analog Ports
        32-channel (G.711) Voice/Fax PVDMII DSP SIMM PVDM daughter card
        Hardware Revision         : 3.2
        Part Number               : 73-8539-04
        Board Revision            : A0
        Deviation Number          : 0
        Fab Version               : 03
        PCB Serial Number         : FOC09251MHW
        RMA Test History          : 00
        RMA Number                : 0-0-0-0
        RMA History               : 00
        Processor type            : 00
        Product (FRU) Number      : PVDM2-32
        Version Identifier        : NA
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF 40 03 EE 41 03 02 82 49 21 5B 04 42 41 30
          0x10: 88 00 00 00 00 02 03 C1 8B 46 4F 43 30 39 32 35
          0x20: 31 4D 48 57 03 00 81 00 00 00 00 04 00 09 00 CB
          0x30: 88 50 56 44 4D 32 2D 33 32 89 4E 41 20 20 D9 02
          0x40: 40 C1 FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

        WIC Slot 0:                                Analog Ports
        FXS Voice daughter card (4 port)
        Hardware Revision         : 3.1
        Part Number               : 73-6918-02
        Board Revision            : F0
        Deviation Number          : 0
        Fab Version               : 02
        PCB Serial Number         : FOC11514K0B
        RMA Test History          : 00
        RMA Number                : 0-0-0-0
        RMA History               : 00
        Top Assy. Part Number     : 800-17016-02
        Connector Type            : 01
        CLEI Code                 : IP9IABYCAA
        Product (FRU) Number      : VIC-4FXS/DID=
        EEPROM format version 4
```

```
        EEPROM contents (hex):
          0x00: 04 FF 40 00 3A 41 03 01 82 49 1B 06 02 42 46 30
          0x10: 88 00 00 00 00 02 02 C1 8B 46 4F 43 31 31 35 31
          0x20: 34 4B 30 42 03 00 81 00 00 00 00 04 00 C0 46 03
          0x30: 20 00 42 78 02 05 01 C6 8A 49 50 39 49 41 42 59
          0x40: 43 41 41 FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

Slot 1:
        High Density Voice Port adapter
        Port adapter is analyzed
        Port adapter insertion time 4d10h ago
        EEPROM contents at hardware discovery:
        Hardware Revision        : 1.1
        Top Assy. Part Number    : 800-03567-01
        Board Revision           : F1
        Deviation Number         : 0-0
        Fab Version              : 02
        PCB Serial Number        : JAB05070QTM
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        Product (FRU) Number     : NM-HDV=
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF 40 00 CC 41 01 01 C0 46 03 20 00 0D EF 01
          0x10: 42 46 31 80 00 00 00 00 02 02 C1 8B 4A 41 42 30
          0x20: 35 30 37 30 51 54 4D 03 00 81 00 00 00 00 04 00
          0x30: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x40: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

        HDV SIMMs: Product (FRU) Number: PVDM-12=
         SIMM slot 0: PVDM-12 SIMM present.
         SIMM slot 1: PVDM-12 SIMM present.
         SIMM slot 2: PVDM-12 SIMM present.
         SIMM slot 3: PVDM-12 SIMM present.
         SIMM slot 4: Empty.

        WIC Slot 0:                                      T1 Ports
        T1 (2 Port) Multi-Flex Trunk (Drop&Insert) WAN Daughter Card
        Hardware revision 1.0           Board revision B0
        Serial number     29788066      Part number    800-04614-03
        FRU Part Number     VWIC-2MFT-T1-DI=
        Test history      0x0           RMA number     00-00-00
        Connector type    PCI
        EEPROM format version 1
        EEPROM contents (hex):
          0x20: 01 24 01 00 01 C6 87 A2 50 12 06 03 00 00 00 00
          0x30: 58 00 00 00 03 02 15 00 FF FF FF FF FF FF FF FF
```

```
        HDV firmware: Compiled Fri 19-Nov-04 14:23 by michen
        HDV memory size 524280 heap free 167869

AIM Module in slot: 0
AIM ATM: 0
        ATM AIM
        Hardware Revision        : 1.0
        Top Assy. Part Number    : 800-06558-05
        Board Revision           : A0
        Deviation Number         : 0-0
        Fab Version              : 03
        PCB Serial Number        : FOC09282AXN
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        FRU Part Number          : AIM-ATM
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF 40 01 B0 41 01 00 C0 46 03 20 00 19 9E 05
          0x10: 42 41 30 80 00 00 00 00 02 03 C1 8B 46 4F 43 30
          0x20: 39 32 38 32 41 58 4E 03 00 81 00 00 00 00 04 00
          0x30: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x40: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

AIM Module in slot: 1
        PCB Serial Number        : FOC092711BZ
        Hardware Revision        : 1.0
        Top Assy. Part Number    : 800-24799-01
        Board Revision           : D0
        Deviation Number         : 0
        Fab Version              : 03
        RMA Test History         : 00
        RMA Number               : 0-0-0-0
        RMA History              : 00
        CLEI Code                : CNP5FFNAAA
        Product (FRU) Number     : AIM-VPN/EPII-PLUS
        Version Identifier       :   NA
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF C1 8B 46 4F 43 30 39 32 37 31 31 42 5A 40
          0x10: 01 4B 41 01 00 C0 46 03 20 00 60 DF 01 42 44 30
          0x20: 88 00 00 00 00 02 03 03 00 81 00 00 00 00 04 00
          0x30: C6 8A 43 4E 50 35 46 46 4E 41 41 41 CB 91 41 49
          0x40: 4D 2D 56 50 4E 2F 45 50 49 49 2D 50 4C 55 53 89
          0x50: 20 20 4E 41 FF FF FF FF FF FF FF FF FF FF FF FF
          0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

4.3.3.2 Running Configuration

To view the contents of the **running** configuration file, use the command **show run.** The configuration changes made to the ISR for this testing are highlighted below with an explanation of what the command does to the ISR, listed opposite in blue highlighting.

Cisco ISR Running Configuration	
Configuration Commands	**Notes/Comments**
c2821-Branch1#show runnning-config	
Building configuration...	
Current configuration : 5015 bytes	
!	
version 12.4	
service timestamps debug datetime msec	
service timestamps log datetime msec	
no service password-encryption	
!	
hostname c2821-Branch1	Set Hostname
!	
boot-start-marker	
boot-end-marker	
!	
logging message-counter syslog	
enable secret 5 $1$3gXA$hQrCTAOpgNOnK2y64cGts/	
enable password interop	
!	
no aaa new-model	
no network-clock-participate slot 1	
no network-clock-participate aim 0	
!	
voice-card 0	
!	
voice-card 1	
dspfarm	
!	
!	
!	
dot11 syslog	
ip source-route	
!	
!	
ip cef	
!	
!	
ip domain name avaya.com	Set the domain name
no ipv6 cef	
!	
multilink bundle-name authenticated	
!	
!	

!	
!	
isdn switch-type primary-ni	Set the global isdn switch-type to
!	primary-ni
!	
!	
voice service voip	Enter voice service configuration
allow-connections h323 to h323	Allow H.323 to H.323 Call Control
allow-connections h323 to sip	Allow H.323 to SIP Call Control
allow-connections sip to h323	Allow SIP to H.323 Call Control
allow-connections sip to sip	Allow SIP to SIP Call Control
redirect ip2ip	Enable IP to IP Calls
fax protocol t38 ls-redundancy 0 hs-redundancy 0 fallback	Use T.38 Fax Protocol
cisco	SIP Configuration level
sip	
registrar server expires max 600 min 60	
redirect contact order best-match	
!	
!	
!	
voice class codec 1	Create voice class codec group
codec preference 1 g711ulaw	Set G.711uLaw as preference 1
codec preference 2 g729br8	Set G.929 as preference 2
!	
!	
!	
!	
!	
!	
!	
!	
voice register global	Set the voice register global
	settings
max-dn 100	Max DNs of 100
max-pool 2	Allow Max Pools of 2
authenticate realm avaya.com	
!	
voice register pool 1	Create SIP registration pool
id network 10.80.61.0 mask 255.255.255.0	Allow SIP registration from IP range
application session	Enable Application SIP
preference 2	Set local branch proxy preference
proxy 10.80.100.24 preference 1 monitor probe icmp-ping	Primary SIP Proxy to monitor
presence call-list	
dtmf-relay rtp-nte	Use RFC 2833 Standard for DTMF
voice-class codec 1	Use codecs defined in voice-class 1
!	
!	
voice translation-rule 1	Voice Translation Rule for incoming
rule 1 /^618/ //	PSTN calls which need the local
!	area code removed.
!	
voice translation-profile 618	Translation profile to use rule 1 to
translate called 1	strip the 618 area code.
!	
!	

!	
!	
vtp version 2	
!	
!	
!	
archive	
log config	
hidekeys	
!	
!	
controller T1 1/0/0	T1 Controller Configuration
pri-group timeslots 1-24	Set timeslots for T1
!	
controller T1 1/0/1	
!	
!	
interface GigabitEthernet0/0	Enter GB Ethernet Configuration 0/0
description SRST WAN Connection	Connection Interface to WAN
ip address 10.80.61.2 255.255.255.252	Set the Controller IP address
ip helper-address 192.45.130.201	Forward those DHCP requests
duplex auto	
speed auto	
no mop enabled	
!	
interface GigabitEthernet0/1	Enter GB Ethernet Configuration 0/1
description to PoE Phone Switch	Connection to PoE Phone Switch
ip address 10.80.61.33 255.255.255.224	
duplex auto	
speed auto	
!	
interface Serial1/0/0:23	Serial Interface from configured T1
no ip address	
encapsulation hdlc	
isdn switch-type primary-ni	Local Switch-Type to use is primary-ni
isdn incoming-voice voice	Treat incoming calls as voice
isdn send-alerting	Send Q.931 alerting message
isdn sending-complete	Send Q.931 complete message
no cdp enable	
!	
ip default-gateway 10.80.61.1	Set default IP gateway
no ip classless	
ip forward-protocol nd	
ip route 0.0.0.0 0.0.0.0 10.80.61.1	Default IP route
no ip http server	
no ip http secure-server	
!	
control-plane	
!	
call fallback active	Enable SIP registration to fallback to primary when WAN connection is restored. Turn on SRST.
!	
!	
!	
voice-port 0/0/0	FXS/Analog Voice Port Config

	6663010
mwi	Enable message waiting indicator
station-id number 6663010	Assign station-id number
caller-id enable	Enable Caller-ID
!	
voice-port 0/0/1	FXS/Analog Voice Port Config 6663011
mwi	Enable mwi
station-id number 6663011	Assign station-id number
caller-id enable	Enable Caller-ID
!	
voice-port 0/0/2	FXS/Analog Fax Port Config 6663012
mwi	Enable mwi
station-id number 6663012	Assign station-id number
caller-id enable	Enable Caller-ID
!	
voice-port 0/0/3	
!	
voice-port 1/0/0:23	Voice Port Config for T1 Connection
no non-linear	
playout-delay maximum 170	Settings for packet jitter
playout-delay nominal 80	Settings for packet jitter
playout-delay minimum low	Settings for packet jitter
no comfort-noise	
bearer-cap 3100Hz	Information transfer capability
!	
!	
dial-peer voice 6663010 pots	Create a POTS dial-peer for Analog Station
description Branch 1 User 1 Analog 6663010	
destination-pattern 6663010	Matching extension 6663010
fax rate voice	Set Fax rate to voice
port 0/0/0	Use FXS port 0/0/0
forward-digits 0	
authentication username 6663010 password 7 08701E1D5D4C53	Needed to authenticate with Session Manager
!	
dial-peer voice 6663011 pots	Create a POTS dial-peer for Analog Station
description Branch 1 User 2 Analog 6663011	
destination-pattern 6663011	Matching extension 6663011
fax rate voice	Set Fax rate to voice
port 0/0/1	Use FXS port 0/0/1
forward-digits 0	
authentication username 6663011 password 7 03550958525A77	Needed to authenticate with Session Manager
!	
dial-peer voice 666 voip	Create a VoIP dial-peer for outgoing HQ calls when in Normal Mode for incoming PSTN calls.
description to allow incoming PSTN call to reach HQ extn’s	
destination-pattern 666....	
session protocol sipv2	Call Control via HQ Session Manager
session target sip-server	
dtmf-relay rtp-nte	Use RFC 2833 Standard for DTMF
!	
dial-peer voice 1618 pots	Create a POTS dial-peer for

description Distributed Trunking for Local PSTN	outgoing HQ calls when in
destination-pattern 1618T	Survivable Mode
fax rate voice	
port 1/0/0:23	
forward-digits 10	
!	
dial-peer voice 303666 pots	
description To HQ via PSTN in Survivable Mode	
preference 1	Secondary route selection for
destination-pattern 666....	666….
port 1/0/0:23	Use T1 interface send calls out
	PSTN
prefix 303	Need to prefix area code for PSTN
	call
!	
dial-peer voice 66630 voip	VoIP dial-peer for handling
description To support incoming Fax via SIP	incoming Analog/Fax calls via SIP
voice-class codec 1	
session protocol sipv2	Use SIP procotol version 2
session target sip-server	Proxy is Session Manager
incoming called-number 666301[0-2]	Match on incoming number
dtmf-relay rtp-nte	Use RFC 2833 Standard for DTMF
no vad	
!	
dial-peer voice 6663012 pots	Create a POTS dial-peer for Analog
description Branch 1 Fax 1 Analog 6663012	Station/Fax
destination-pattern 6663012	Matching extension 6663012
fax rate voice	Set Fax rate to voice
port 0/0/2	Use FXS port 0/0/2
forward-digits 0	
authentication username 6663012 password 7	Needed to authenticate with
075E731F1A5C4F	Session Manager
!	
dial-peer voice 6186663 pots	POTS dial-peer for incoming PSTN
description Incoming PSTN calls with 618 area code	calls having the local area code 618
translation-profile incoming 618	Use Translation profile to strip 618
incoming called-number 618666....	Match incoming called number
fax rate voice	Set Fax rate to voice
direct-inward-dial	route via direct-inward-dial
port 1/0/0:23	Incoming on T1 PSTN interface
forward-digits 0	
!	
sip-ua	Enter ISR SIP User Agent Config
authentication username srstbr1 password 7	Branch Username/PW for Session
040A59555B741A	Manager authentication.
!	
mwi-server ipv4:10.80.100.24 expires 3600 port 5060	MWI server for Analog/FXS ports
transport tcp unsolicited	
registrar ipv4:10.80.100.24 expires 3600	Enable SIP Reg. for Analog/FXS
	ports
sip-server ipv4:10.80.100.24	Set IP of Primary SIP Server
!	
!	

```
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password interop
 logging synchronous level all
 login
line vty 5 513
 login
line vty 514
 logging synchronous
 login
!
scheduler allocate 20000 1000
end
```

4.3.3.3 SIP-UA Keep-Alive Feature

With regards to a **keep-alive** feature on the Cisco ISR configuration, there are two options, Standard icmp ping or a SIP message **keep-alive**. The SIP message keep-alive mechanism may be more suitable for production environments. This configuration is not listed in the **show configuration** output on the Cisco ISR shown in **Section 5.3.3.2**. The following command shows how to set up the **sip-ua keepalive** feature to contact the Session Manager.

SIP-UA Keep-Alive Config	
c2821-Branch1#**config t** c2821-Branch1(config)#**sip-ua** c2821-Branch1(config-sip-ua)#**keepalive target ipv4:10.80.100.24 tcp** c2821-Branch1(config-sip-ua)#**exit** c2821-Branch1(config)#**exit**	**Enter Config menu** **Enter sip-ua config menu** **Enter the keepalive parameters** **Exit from sip-ua config menu** **Exit from config menu**

The Branch Cisco ISR will send a keepalive request in the form of a SIP options message. HQ Session Manager simply responds with a 200 OK. To save the ISR configuration use the command:

copy running-config startup-config

4.3.3.4 Adding Branch Username/Password for SIP-UA

The SIP User Agent (SIP-UA) communicates with the HQ Session Manager on behalf of the Analog/FXS stations via the SIP protocol. These Analog/FXS stations are configured on the Session Manager to appear as Avaya SIP 9630 SIP phone stations requiring registration authentication from the assigned user to station assignment. If the SIP-UA Keep-Alive Config is adopted, the SIP-UA must authenticate with the Session Manager also, if it expects to get back a reply to the SIP options message.

Two authentication configuration approaches are possible on the Cisco ISR:

1. All Analog/FXS stations with username and password can be configured under their corresponding dial-peer configuration. The SIP-UA will still have to have a username/password created on the System Manager and that username/password combination configured under the SIP-UA configuration level on the Cisco ISR. This is the approach used in the sample configuration contained in these Application Notes.

SIP-UA Username/PW (option 1)	
sip-ua **authentication username srstbr1 password 7 040A595B741A** **!** **dial-peer voice 6663010 pots** **description Branch 1 User 1 Analog 6663010** **destination-pattern 6663010** **fax rate voice** **port 0/0/0** **forward-digits 0** **authentication username 6663010 password 7 040A595B741B** **!** **dial-peer voice 6663011 pots** **description Branch 1 User 2 Analog 6663011** **destination-pattern 6663011** **fax rate voice** **port 0/0/1** **forward-digits 0** **authentication username 6663011 password 7 040A595B741C** **!**	**Enter SIP-UA config level** **Branch Username/PW for Session Manager authentication** **Analog station username/pw for 6663010** **Analog station username/pw for 6663011**

2. All Analog/FXS stations with username and password can be configured under the SIP-UA configuration level along with a Branch username/password that has been created on the Avaya Aura™ System Manager, which is not assigned to any station.

SIP-UA Username/PW (option 2)	
sip-ua	Enter SIP-UA config level
authentication username srstbr1 password 7 040A595B741A	Branch Username/PW for Session Manager authentication
authentication username 6663010 password 7 040A595B741B	Analog station username/pw for 6663010
authentication username 6663011 password 7 040A595B741C	Analog station username/pw for 6663011
authentication username 6663012 password 7 040A595B741D	Analog station username/pw for 6663012
!	
!	
dial-peer voice 6663010 pots description Branch 1 User 1 Analog 6663010 destination-pattern 6663010 fax rate voice port 0/0/0 forward-digits 0 !	Dial-Peer for Analog station 6663010 does not need to have username/pw if it is configured under the sip-ua config level
dial-peer voice 6663011 pots description Branch 1 User 2 Analog 6663011 destination-pattern 6663011 fax rate voice port 0/0/1 forward-digits 0 !	Dial-Peer for Analog station 6663011 does not need to have username/pw if it is configured under the sip-ua config level

5. General Test Approach and Test Results

This section describes the testing used to verify the sample configuration for the Session Manager Survivable SIP Gateway Solution using the Cisco ISR with Survivable Remote Site Telephony support in a Distributed Trunking scenario. This section covers the general test approach and the test results.

5.1. General Test Approach

The general test approach was to break and restore network connectivity from the branch site to the headquarters location to verify the following:

- **Connectivity / Failover**
  Testing focused on transitions of the 96xx series phones and Cisco ISR to/from normal mode and survivable mode.

- **Distributed Trunking – Normal Mode**
  Testing focused on Distributed Trunking endpoint to endpoint call flows and feature invocation when the branch connectivity is in Normal Mode. In this Normal Mode, PSTN access by phones at both the headquarters and the branch site are through the T1 connection on the Avaya Media Gateway at the central location with the exception of local non-toll calls from the branch phones are routed to the PSTN through the branch Cisco ISR.

  Features tested include:

  Hold/Resume, Conference Add/Drop, Call Transfer – Attended/Un-attended, Call Waiting, Voice Mail Dialing and Faxing.

  - SIP call routing is controlled by a centralized Avaya Aura™ Session Manager for both the enterprise headquarters and remote branch sites.
  - Feature services for the SIP phones are supplied by Avaya Aura™ Communication Manager acting as a Feature Server.
  - Call routing for the Enterprise Headquarters (HQ) H.323 phones and analog phones/fax machines are provided by the Avaya Aura™ Communication Manager acting as an Access Element.
  - Both Avaya Aura™ Communication Manager (Access Element) and Avaya Aura™ Communication Manager (Feature Server) are configured with IP-IP Direct Audio enabled.
  - Local non-toll calls from the branch phones are routed to the Session Manager and back to the branch for routing out the Cisco ISR T1 interface to the PSTN.

- Long Distance toll calls from the branch phones are routed to the Session Manager and back to the branch, based on originating location, for routing out the Cisco ISR T1 interface to the PSTN.
- All branch 96xx phones are registered to the centralized Avaya Aura™ Session Manager.
- All branch FXS stations are registered via the Cisco ISR as SIP Avaya 9620 stations to the centralized Avaya Aura™ Session Manager.

- **Distributed Trunking – Survivable Mode**
  Testing focused on Distributed Trunking endpoint to endpoint call flows and feature invocation when the branch loses WAN connectivity and is in Survivable Mode. Features tested include: Hold/Resume, Conference Add/Drop, Call Transfer – Attended/Un-attended, Call Waiting, Voice Mail Dialing and Faxing.

  - All branch 96xx phones are transitioned to have their secondary registrar (Cisco ISR) become active.
  - All call routing is controlled by the local branch Cisco ISR.
  - All branch calls to HQ phones are routed to the Cisco ISR T1 Controller port and over the PSTN to the HQ. Dialing from branch phones to HQ phones will remain transparent to branch users, i.e. the same number used to dial HQ phones will be routed via failover dial-peer and automatically prefixed for routing via T1 to the PSTN and onto HQ.
  - All PSTN outbound calls are routed to the Cisco ISR T1 Controller port.
  - PSTN inbound calls to Branch Cisco ISR are routed for local endpoints only.

5.2. Test Results

The functionality and features described in **Section 5.1** were verified during testing. The following expected behaviors were observed:

- In Normal Mode, branch phones register to all available controllers.
- Switching between Normal and the Survivable Modes was automatic and within a reasonable time span (within one to two minutes).
- In Normal Mode, calls can be placed between phones at the HQ and the branch site, and among phones within the branch site.
- In Survivable Mode, calls can be placed between phones within the branch site. In addition, branch phones can still place calls to the PSTN (and to phones at HQ via PSTN) using the T1 interface on the Cisco ISR located at the branch site. Secondary preference dial-peers are used to route “survivable mode” calls to the

HQ via the PSTN, prefixing the dialed number and routing the call out the T1 interface, allowing users to continue to use the same dial plan they use during normal mode for HQ calls.

- Analog phones connected to the FXS ports on the Cisco ISR are properly adapted as SIP phones in both Normal and Survivable Modes.
- Faxing in both directions between HQ and branch analog fax machines worked correctly in Normal and Survivable Modes. An additional incoming dial-peer was created to be able to accept faxes into the branch Cisco ISR gateway via the WAN connection using SIP and supporting T.38 mode.
- Avaya 96xx SIP phones at the branch were able to reregister with the Session Manager once WAN connectivity was restored within a reasonable time span (within one to two minutes).

The following unexpected behaviors were observed during testing:

- Call features including Hold/Resume, Conference Add/Drop, Call Transfer Attended/Un-attended, Call Waiting, Voice Mail Dialing and Faxing worked in Normal and Survivable Mode with exceptions noted below:
    - Branch to branch 96xx calls which use the conference feature to add a third party experience only the conference party connected when the join button is pressed and the other party is placed on hold and is not participating in the conference.
    - Call waiting tone is not heard on incoming call when in an active call, 2nd calling party hears busy instead of ringing. This was experienced in both Normal and Survivable Modes.
    - In survivable mode, when a branch 96xx phone tries to transfer (attended and unattended), the source and target callers getting dropped.
- Active intra-branch calls remain up during WAN connectivity loss and during Normal to Survivable Mode transition by the Cisco ISR. However, on 96xx SIP to Analog calls only one-way voice path exists after the Normal to Survivable transition of the Cisco ISR. After the calls were ended and they called each other while in survivable mode, two-way voice existed. This behavior was not experienced on 96xx SIP to 96xx SIP phone calls during the survivable transition.
- The 96xx SIP phones would only support one call appearance during survivable mode even though they continued to show three available.
- Analog phones at the branch did not support the flash button for placing call on hold and being able to resume.

6. Verification

6.1. Cisco ISR

6.1.1. Verify Analog Phones Are Registered With Session Manager

Use the command **"show sip-ua register status"** to display the analog phones which are registered with Session Manager.

```
c2821-Branch1#show sip-ua register status
Line                              peer        expires(sec)  registered
================================  ==========  ============  ==========
666....                           303666      146           no
6663010                           6663010     1134          yes
6663011                           6663011     1946          yes
6663012                           6663012     84            yes
9303*                             9303        146           no
9618*                             9618        146           no
```

6.1.2. Verify Registeration Status of 9600 SIP Phones

The 9600 SIP phones at the branch are configured in the 46xxsettings.txt file to use "simultaneous" SIP registeration with the Session Manager as primary and the Cisco ISR as secondary. Use the command **"show sip-ua status registrar"** to display the SIP phones which have registered with the Cisco ISR.

The example below shows that both 96xx SIP phones with station numbers 6663008 and 6663009 have completed their secondary registeration with the Cisco ISR. Note the last number of each listing i.e. (40001 and 40003) are the dynamically created dial-peers that have been created for each of these phones to provide call routing if network connectivity to the Session Manager is lost, triggering the Cisco ISR and 9600 SIP phones to switch over to Survivable Mode.

```
c2821-Branch1#show sip-ua status registrar
Line           destination      expires(sec)  contact
               call-id
               peer
============================================================
6663008        10.80.61.36      154           10.80.61.36
               1_181c-2ac4cc3b386d5be0_R@10.80.61.36
               40001

6663009        10.80.61.35      524           10.80.61.35
               1_634-c79dfea386d49e0_R@10.80.61.35
               40003
```

6.1.3. Verify Dial-Peers

To verify dial-peers, use the command **"show dial-peer voice summary"**. The analog phones should show their station tag, type (pots), their operation status (up/down) and the matching destination pattern being used to match for the dial-peer. The 9600 SIP phones should show their dial-peer as listed in **Section 7.1.2** to the Cisco ISR with type (voip), operation status (up/down), the destination pattern the dial-peer is matching on, the preference (2 for the dial-peers with phones registered to the Cisco ISR) and the ip:port of the session-target. There will be second dial-peer for the 9600 SIP phones also which represent the dial-peer with registration to the Session Manager. These Session Manager registered dial-peers should show preference of 1 (primary registration) and ip:port values equal to that on the Session Manager.

```
c2821-Branch1#show dial-peer voice summary
dial-peer hunt 0
             AD                                    PRE PASS                OUT
TAG    TYPE  MIN  OPER PREFIX    DEST-PATTERN      FER THRU SESS-TARGET    STAT PORT
66630- pots  up   up             6663010            0                      up   0/0/0
10
66630- pots  up   up             6663011            0                      up   0/0/1
11
30366- pots  up   up   303       666....            1                      up
1/0/0:23
6
66630  voip  up   up                                0  syst sip-server
66630- pots  up   up             6663012            0                      up   0/0/2
12
61866- pots  up   up                                0                      down
1/0/0:23
63
9618   pots  up   up             9618T              1                      up
1/0/0:23
9303   pots  up   up             9303T              0                      up
1/0/0:23
555    voip  up   up             555T               0  syst sip-server
777    voip  up   up             777T               0  syst sip-server
666    voip  up   up             666....            0  syst sip-server
40003  voip  up   up             6663009            2  syst ipv4:10.80.61.35:506
40004  voip  up   up             6663009            1  syst ipv4:10.80.100.24:50
40001  voip  up   up             6663008            2  syst ipv4:10.80.61.36:506
40002  voip  up   up             6663008            1  syst ipv4:10.80.100.24:50
1618   pots  up   up             1618T              0                      up
1/0/0:23
```

6.1.4. Verify T1 Status

To verify the T1 trunk has established connection with the proper framing, line-code, timing (network/user) and switch-type has come into service, use the command **"show isdn status"**. Check Layer 1 Status shows "**ACTIVE**" and the Layer 2 State has "**MULTIPLE__FRAME__ESTABLISHED**"

```
c2821-Branch1#show isdn status
Global ISDN Switchtype = primary-ni
ISDN Serial1/0/0:23 interface
        dsl 0, interface ISDN Switchtype = primary-ni
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Active dsl 0 CCBs = 0
    The Free Channel Mask:  0x807FFFFF
    Number of L2 Discards = 0, L2 Session ID = 0
    Total Allocated ISDN CCBs = 0
```

Also check the see if the channels are **"Idle"** and the signaling channel is set to **"Reserved"** by using the command **"show isdn service"**.

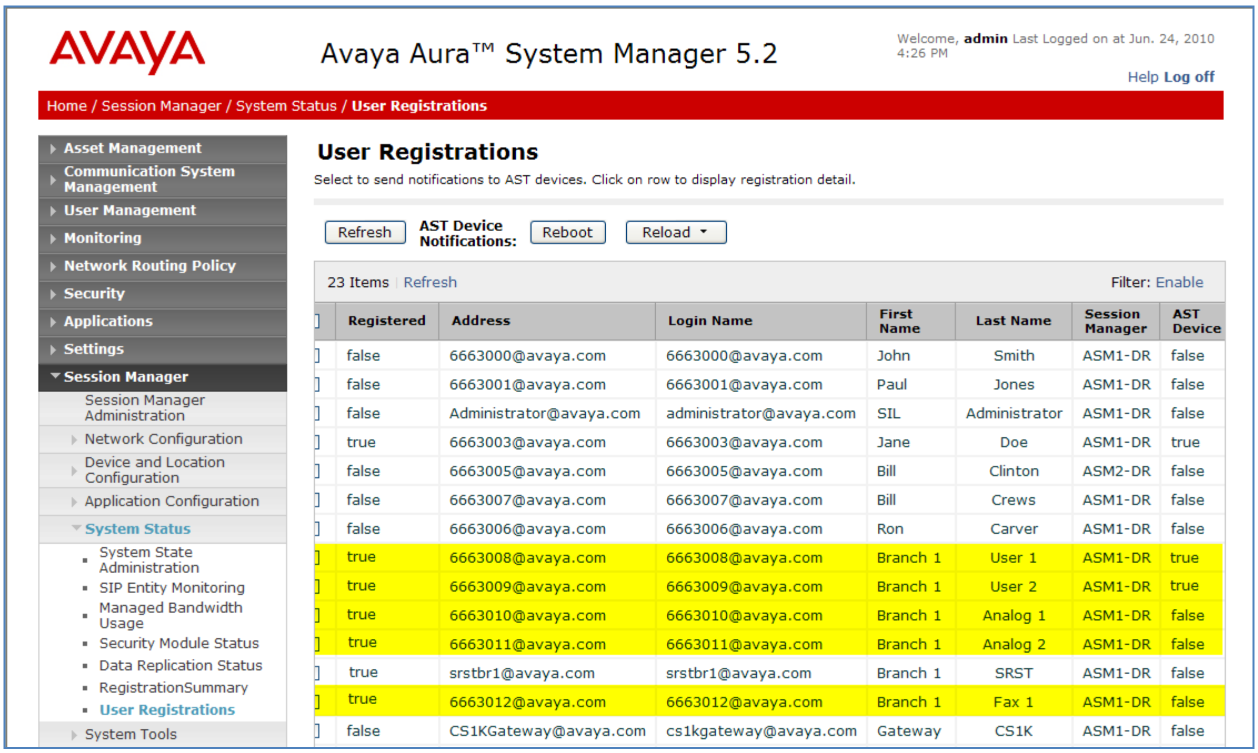
```
c2821-Branch1#show isdn service
PRI Channel Statistics:
ISDN Se1/0/0:23, Channel [1-24]
  Configured Isdn Interface (dsl) 0
   Channel State (0=Idle 1=Proposed 2=Busy 3=Reserved 4=Restart 5=Maint_Pend)
    Channel :  1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4
    State   :  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 3
   Service State (0=Inservice 1=Maint 2=Outofservice 8=MaintPend 9=OOSPend)
    Channel :  1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4
    State   :  0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 2
```

6.2. 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 Branch 96xx SIP phones (6663008, 6663009), the two analog FXS stations (6663010, 6663011), and the analog FXS Fax (6663012) at the Branch location.

Also note the user registrations for the main site Avaya 96xx SIP Phones (6663006 and 6663007). The **AST Device** field indicates whether the registered phone is an Avaya SIP Telephone set.



Registered	Address	Login Name	First Name	Last Name	Session Manager	AST Device
false	6663000@avaya.com	6663000@avaya.com	John	Smith	ASM1-DR	false
false	6663001@avaya.com	6663001@avaya.com	Paul	Jones	ASM1-DR	false
false	Administrator@avaya.com	administrator@avaya.com	SIL	Administrator	ASM1-DR	false
true	6663003@avaya.com	6663003@avaya.com	Jane	Doe	ASM1-DR	true
false	6663005@avaya.com	6663005@avaya.com	Bill	Clinton	ASM2-DR	false
false	6663007@avaya.com	6663007@avaya.com	Bill	Crews	ASM1-DR	false
false	6663006@avaya.com	6663006@avaya.com	Ron	Carver	ASM1-DR	false
true	6663008@avaya.com	6663008@avaya.com	Branch 1	User 1	ASM1-DR	true
true	6663009@avaya.com	6663009@avaya.com	Branch 1	User 2	ASM1-DR	true
true	6663010@avaya.com	6663010@avaya.com	Branch 1	Analog 1	ASM1-DR	false
true	6663011@avaya.com	6663011@avaya.com	Branch 1	Analog 2	ASM1-DR	false
true	srstbr1@avaya.com	srstbr1@avaya.com	Branch 1	SRST	ASM1-DR	false
true	6663012@avaya.com	6663012@avaya.com	Branch 1	Fax 1	ASM1-DR	false
false	CS1KGateway@avaya.com	cs1kgateway@avaya.com	Gateway	CS1K	ASM1-DR	false

6.3. Timing Expectations for Fail-over to Cisco ISR

This section is intended to set expectations for the *approximate* length of time before Avaya 9600 SIP Telephones in the branch will acquire service from the Cisco ISR, when a failure occurs such that the branch is unable to communicate with the central Session Manager. In practice, failover timing will depend on a variety of factors. Using the configuration described in these Application Notes, when the IP WAN is disconnected, idle Avaya SIP Telephones in the branch will typically display the "Acquiring Service…" screen in approximately 45 seconds.

With multiple identical idle phones in the same branch, it would not be unusual for some phones to switch their "active" registration from the Session Manager to the Cisco ISR before others, with the earliest switching in approximately one minute and the latest registering in approximately two minutes. In other words, the Avaya SIP Telephones in the branch can typically place and receive calls processed by the Cisco ISR approximately two minutes after the branch is isolated by a WAN failure.

6.4. Timing Expectations for Fail-back to Normal Mode

This section is intended to set expectations for the *approximate* length of time before Avaya 9600 SIP Telephones registered to the Cisco ISR in survivable mode will re-acquire service from the Session Manager for normal service, once the branch communications with the central Session Manager is restored. In practice, failover timing will depend on a variety of factors. Using the configuration described in these Application Notes, when the IP WAN is restored such that the branch telephones can again reach the Session Manager, idle Avaya SIP Telephones in the branch will typically be registered with the Session within one minute or less. With multiple identical idle phones in the same branch, it would not be unusual for some phones to register back with the Session Manager before others. For example, some may register within 30 seconds, others within 45 seconds, with others registering in approximately one minute.

7. 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 Session Manager Survivable SIP Gateway Solution to avoid service disruptions to these remote branch SIP endpoints.

8. References

The following references are relevant to these Application Notes:

Avaya one-X™ Deskphone Edition 9600 Series SIP Telephones

[1] ***Avaya one-X™ Deskphone Edition for 9600 Series SIP Telephones Administrator Guide Release 2.5***, Doc ID: 16-601944, Issue 5, November 2009, available at http://support.avaya.com.

Avaya Aura™ Session Manager

[2] ***Avaya Aura™ Session Manager Overview***, Doc ID 03-603473, available at http://support.avaya.com.

[3] ***Installing and Upgrading Avaya Aura™ Session Manager***, Doc ID 03-603324, available at http://support.avaya.com.

[4] ***Maintaining and Troubleshooting Avaya Aura™ Session Manager***, Doc ID 03-603325, available at http://support.avaya.com.

[5] ***Administering Avaya Aura™ Communication Manager as a Feature Server***, Doc ID 03-603479, available at http://support.avaya.com.

Avaya Aura™ Communication Manager 5.2

[6] ***SIP Support in Avaya Aura™ Communication Manager Running on Avaya S8xxx Servers***, Doc ID 555-245-206, May, 2009, available at http://support.avaya.com.

[7] ***Administering Avaya Aura™ Communication Manager***, Doc ID 03-300509, May, 2009, available at http://support.avaya.com.

Cisco Integrated Services Router

[8] ***Cisco 2800 Series Integrated Services Routers Quick Start Guide***, Revised: October 11, 2005, 78-16015-07, available at http://www.cisco.com

[9] ***Dial Peer Configuration on Voice Gateway Routers, Release 12.4T***, Revised: March 5, 2009, available at http://www.cisco.com

[10] ***Cisco Unified SRST and Cisco Unified SIP SRST Command Reference (All Versions)***, March 19, 2010, available at http://www.cisco.com

[11] ***Cisco Unified SIP SRST System Administrator Guide (All Versions)*****,** July 11, 2008, available at http://www.cisco.com

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com