**Avaya Solution & Interoperability Test Lab**

---

# Avaya Aura® Session Manager Survivable SIP Gateway Solution using the HP Multi-Service Router 20 Series in a Centralized Trunking Configuration – Issue 1.0

## Abstract

These Application Notes present a sample configuration of the Avaya Aura® Session Manager 6.1 Survivable SIP Gateway Solution using the HP Multi-Service Router 20-40 (MSR20-40) in a Centralized Trunking configuration. HP has stated that the configuration and compliance testing results should be representative of all the HP MSR20 series and MSR20-1x series models when using the HP firmware version specified in Section 4.

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

The Avaya Aura® Session Manager Survivable SIP Gateway Solution monitors the connectivity health from the remote branch to the Avaya SIP call control platform at the main site. When connectivity loss is detected, the Avaya one-X® Deskphone SIP 9600 Series IP Telephones at the branch, as well as the HP MSR20 series, dynamically switch to Survivability Mode, restoring telephony services to the branch for intra-branch and PSTN calling.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

These Application Notes present a sample configuration of the Avaya Aura® Session Manager 6.1 Survivable SIP Gateway Solution using the HP MSR20-40 router in a Centralized Trunking configuration utilizing the SIP Gateway functionality contained in the router.

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

The primary components of this solution are the Avaya one-X® Deskphone SIP 9600 Series IP Telephones, the HP MSR20 series router, as well as Avaya Aura® Session Manager, which provides the centralized SIP control platform with SIP registrar and proxy functions in Normal Mode. The sample configuration shown in these Application Notes utilizes the HP MSR20-40; however, HP has stated that the configuration and compliance testing results should be representative of all the HP MSR20 series and MSR20-1x series models when using the HP firmware version specified in **Section 4**.

# 2. General Test Approach and Test Results

This section details the general approach to the testing, what was covered, and results of the testing.

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

## 2.1. Interoperability Testing

The interoperability testing focused on the dynamic switch from Normal Mode (where the network connectivity between the main site and the branch site is intact) to Survivable Mode (where the network connectivity between the main site and the branch site is broken) and vice versa. The testing also verified interoperability between the Avaya 9600 Series SIP Phones and the HP MSR20-40 in Survivable Mode.

The following features and functionality were verified:

- In Normal Mode, the Session Manager located at the central site serves as the SIP registrar and proxy for phones at both the central and branch sites; in Survivable Mode, the HP MSR20-40 located at the branch location serves as the SIP registrar and proxy for the branch phones.
- Branch phones register to the Session Manager in Normal Mode and the branch HP MSR20-40 in Survivable Mode. Switching between the Normal and the Survivable Modes is automatic and within a reasonable time span.
- In Normal Mode, calls can be placed between phones at the main site and the branch site, and among phones within the site.
- In Normal Mode, all calls to the PSTN from the branch, including both local and long distance toll calls, are routed to the PSTN through the T1 connection on the Avaya Media Gateway at the central location.
- In Survivable Mode, calls can be placed among phones within the branch. In addition, branch phones can still place calls to the PSTN (and to the phones at Headquarters via PSTN) using the FXO interface on the branch HP MSR20-40.
- PBX features including Hold, Transfer, Call Waiting, Call Forwarding and Conference on Avaya 9600 SIP Phones in both Normal and Survivable Modes.
- Messaging system access by branch phones (through internal access number in Normal Mode and PSTN call in Survivable Mode) and proper function of MWI (Messaging Waiting Indicator) on the Avaya 9600 IP Phones in the Normal Mode.
- Proper system recovery after HP MSR20-40 restart and loss/restoration of IP connection.

### 2.1.1. Avaya Aura® Session Manager and Avaya Aura® Communication Manager

Session Manger is a routing hub for SIP calls among connected SIP telephony system components. The Avaya Aura® System Manager provides management functions for Session Manager. In the test configuration, all Avaya 9600 Series SIP Phones at the central location register to the Session Manager. All Avaya 9600 Series SIP Phones at the branch site also register to the Session Manage at the main location (in Normal mode) and to the HP MSR20-40 at the branch (in Survivable mode). Session Manager provides centralized SIP call control in Normal Mode; the HP MSR20-40 provides local SIP control in Survivable Mode. In Normal Mode, the phone calling features are supported by Communication Manager. The Avaya 9600 Series SIP Phones are configured on Communication Manger as Off-PBX-Stations (OPS) and acquire advanced call features from Communication Manger.

### 2.1.2. HP Multi Service Router Line

This section describes the high level features of the MSR product line. Further details can be found on the HP website. The HP Multiple Services Router (MSR) Series is a family of modular devices with a full range of models for requirements from small and remote offices. The MSR product line delivers high performance, secure, integrated services on a single platform. The MSR product line enhances network functionality, reduces complexity and simplifies management. The product line includes a variety of chassis that run Comware – the management software. Comware supports the centralized management suite IMC (Intelligent Management

Center) and a comprehensive integrated security service. Additional benefits of the MSR Series include:

- Convergence of routing, switching, security and voice
- Modular, multi-bus architecture with high reliability and high performance
- Embedded encryption, quality of service, firewall, security features
- Redundant power supply and hot swapping available on select models
- Unified management platform
- Common modules across many platforms
- Open application architecture enabled
- No extra license cost for features

### 2.1.2.1. HP MSR20 Series Overview

The MSR20 Series features a modular design that delivers flexible WAN/LAN connectivity options, while reducing complexity, simplifying management, and increasing control. The HP MSR20 Series routers are targeted at enterprise small branch office and small to medium business branch office router applications. The HP MSR20 Series supports SIC interface modules and has many different models for various density and scalability requirements.

The HP MSR20 Series supports many flexible options:

- WAN-data including MPLS, DSL, Cellular-3G, and others
- Voice (T1, E1, , BRI on MSR20-40)
- VPN
- Wi-Fi Access Point (802.11 b/g/n)
- Additional Ethernet ports
- Analog modems
- Modules with Analog line pass-through when local power fails
    - Available on all FXS modules that include FXO
    - MSR relays FXS to FXO connection to PSTN physically when power fails

Finally, the HP MSR20 product line includes features such as:

- Standards based routing, switching and wireless access
- Support for IPv4/IPv6, RIP, MPLS, IS-IS, BGP, OSPF, L2TP, GRE, PPP
- Support for IPSec, SSL, VPN, status based ASPF Firewall
- ADSL/ISDN WAN Support on certain MSR20 series to support alternate WAN backup to the data center using Dynamic VPN (DVPN).
- Support for QoS, security and VLANs

The HP MSR20 can take on various roles based on call flows and network conditions, including:

The HP MSR20-40 Series routers provide these features:

- 2 FE Ethernet (WAN) ports
- 4 SIC slots and 2 ESM slots
- One VPM slot and one VCPM slot provide support for E1/T1 voice SIC modules (see **Section 2.2** for more details/exceptions)

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

### 2.1.3. Avaya one-X® Deskphone SIP 9600 Series IP Telephone

The Avaya one-X ® Deskphone SIP 9600 Series IP Telephone, referred to as Avaya 9600 SIP Phone throughout the remainder of this document, is a key component of the survivable SIP gateway solution. The firmware 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 HP MSR20-40 as a survivable SIP server.

### 2.1.4. Network Modes

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

**Survivable Mode:** In Survivable Mode, the branch has lost WAN connectivity to the main site. The local branch HP MSR20-40 is used for all calls at that branch. Note that if Session Manager, which provides the centralized SIP call control, loses connectivity to the WAN, all branches will go into Survivable Mode simultaneously.

### 2.1.5. PSTN Trunking Configurations

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

**Centralized Trunking:** In Normal Mode, all PSTN calls, inbound to the enterprise and outbound from the enterprise, are routed from/to the PSTN connection configured on the Avaya Media Gateway (located at the main site). In Survivable Mode, PSTN calls to/from the branch phones are routed through the analog trunks from the Service Provider connected to the FXO interface ports on the branch HP MSR20-40.

**Distributed Trunking:** Outgoing PSTN calls are routed based on the originating source location via Session Manager. Local calls from branch locations are routed back to the same branch location and terminate on the FXO interface of the local HP MSR20-40. This solution has the potential benefits of saving bandwidth on the branch access network, off-loading the WAN and centralized media gateway resources, avoiding Toll Charges, and reducing latency.

Note that with the sample configuration:

1. In both Normal and Survivable Mode, 911 emergency calls from the branch should always be routed through the FXO interfaces on the branch MSR20-40 to the local Emergency Response Center (regardless of whether Centralized or Distributed Trunking is being used).

2. In both Centralized Trunking and Distributed Trunking configurations, routing of DID (Direct Inward Dialing) calls from the PSTN to the FXO interfaces on the branch MSR20-40 is determined by the network mode that the branch is currently operating in:
   - If the branch is in Normal Mode, the DID call will be routed to the Headquarters for further routing decisions. The DID call can terminate either to a Headquarters phone or to a branch phone depending on further digits collected from the calling party.
   - If the branch is in Survivable Mode, the DID call will be terminated to the Auto-Attendant on the MSR20-40 for onward routing to branch phones on user-provided branch extension numbers.

The two trunking configurations share mostly the same configuration procedures on Communication Manager, Session Manager, and the HP MSR20-40. The configuration procedures in this document implement the Centralized Trunking configuration.

## 2.2. Test Results

All test cases passed with the following exceptions/observations:

- During survivability mode, Call Transfer functionality is not supported by the HP MSR for branch phones at the time of compliance testing. This functionality is under investigation by HP.
- Starting in Normal mode, the SIP phones at the branch are registered with Session Manager. When connectivity to Session Manager is lost, and Survivable mode is entered, the SIP phones at the branch register with the HP MSR. When connectivity is restored, the SIP phones should register back to the Session Manager. However, instead of registering with Session Manger automatically, the SIP users are being logged out of their phones. The users must manually log in again in order to be registered with Session Manager again. This issue is currently under investigation by Avaya. HP will be modifying the behavior of the MSR firmware to address this issue with a firmware version to be released in Q4 2012.
- When an Avaya 96x1 phone (firmware version 6.1) attempted to register with the HP MSR, the phone did not respond to a 401 SIP message from HP, causing the registration to fail. This is has been fixed with Avaya phone firmware version 6.2.
- In Survivable mode, the caller-ID for internal calls from all SIP stations was displayed as "Sip-server". This issue is under investigation by HP.
- The HP MSR analog phones at the branch that have a voice mail account (not common) will not provide a stutter tone indication when there is a new voicemail message. This is expected behavior using the HP MSR survivability solution as the voicemail messages are stored in the data center.
- Calls to HP MSR analog phones at the branch which require voice mail (not common) will not have inbound calls automatically forwarded to their voicemail mailbox, instead the call will automatically be forwarded to the voicemail auto-attendant in the data center and caller will have to re-enter the dialed number.
- In Survivable Mode at the branch, the entire conference call terminates when the phone that initiated the conference call drops from the call. This is not an issue, but different from the default Avaya behavior that has the capability to allow the remaining parties to stay on the call when the conferencing party drops.

The following statements have been provided by HP:

"All HP Multi Service Router (MSR) series, including MSR 20-1x, MSR20, MSR30 and MSR50 share the same Comware (CW) platform software. From a software feature perspective, they are the same, however the performance can be different and some voice configuration differences may exist, these are outlined below.

The MSR20 Series consists of the MSR20-20, MSR20-21, MSR20-40 and the MSR20-1x Series consists of the MSR20-10, MSR20-11, MSR20-12, MSR20-13 and MSR20-15s. There is one difference in hardware with MSR 20-1x series, only MSR 20-12's and MSR 20-15' support a VPM slot on the motherboard. That means only MSR 20-12's and MS 20-15's can support E1, T1 and BRI voice interfaces. Additionally, MSR20-10, MSR20-11 and MSR20-13s do not support Voice E1, T1, BRI interfaces and have a different Comware version than the MSR20 Series. However, both MSR20 Series and MSR20-1x Series share a common set of PSTN Gateway Modules and the voice functionality provided by the SIP stack and the Voice Gateways is the same. Further details can be obtained from the release notes posted on the HP Networking router product resources page.

In Avaya's DevConnect survivability solution, the MSR Router was used only as a backup PSTN connection when SIP server failed or if WAN connectivity was lost. This configuration could have only required FXS or FXO interfaces but no E1 and T1 voice interfaces. Thus, in summary, if MSR 20-40 passed the testing, we can say MSR 20-1x, MSR 30 and MSR 50, will all work as part of this survivability solution."

## 2.3. Support

For technical support on the HP MSR20-40, contact HP Networking via the support web site http://www.hp.com/networking/supportnav.

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

## 3. Reference Configuration

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

The Headquarters location hosts a Session Manager (with its companion System Manager) providing enterprise-wide SIP call control, a Communication Manager (with an Avaya G450 Media Gateway) providing advanced feature capabilities to Avaya 9600 SIP Phones and trunks to the PSTN. In addition, the Headquarters location hosts an Avaya IP Phone Configuration File Server for Avaya 9600 SIP Phones to download configuration information.

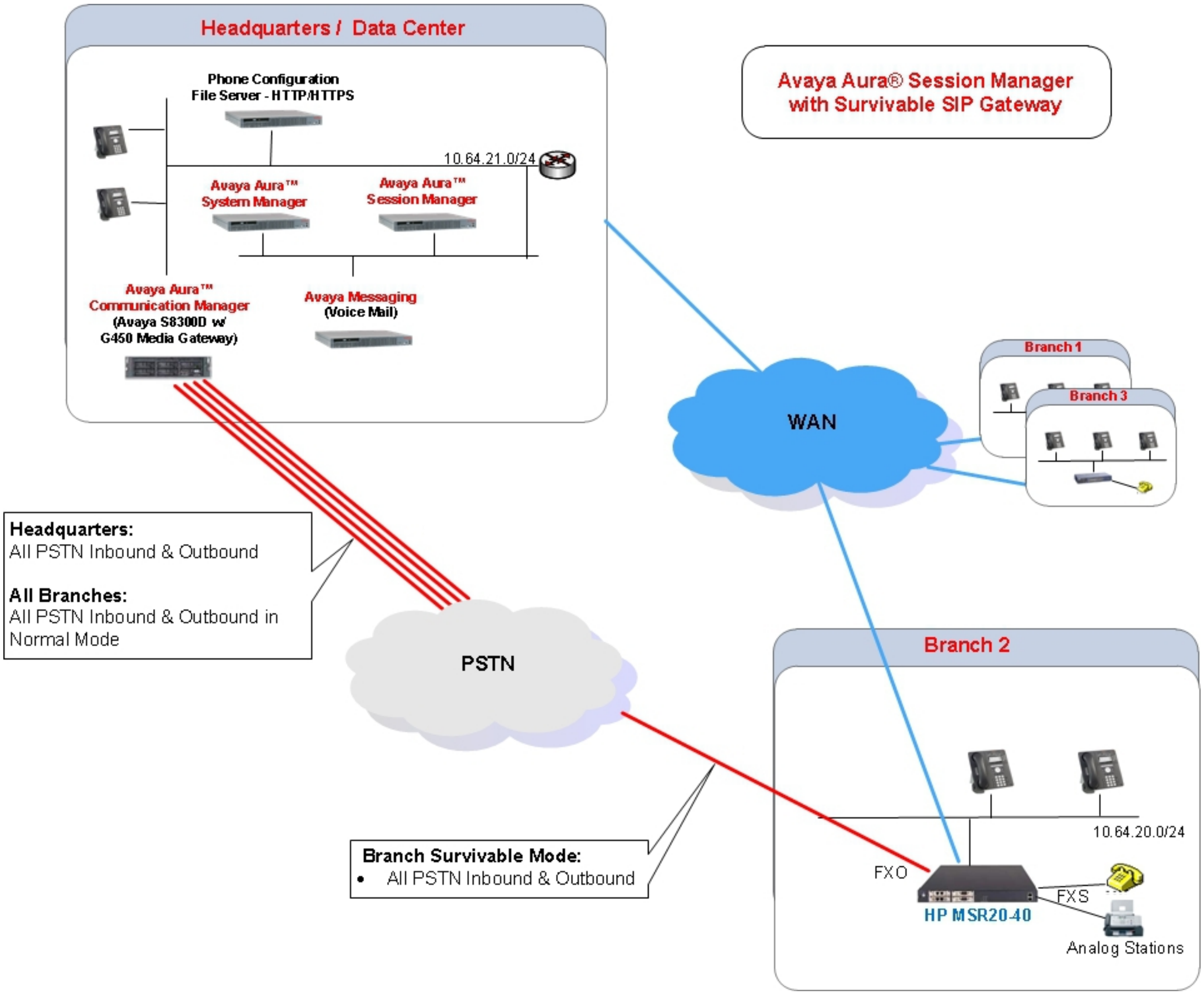

Headquarters / Data Center
Phone Configuration File Server - HTTP/HTTPS
10.64.21.0/24
Avaya Aura™ System Manager
Avaya Aura™ Session Manager
Avaya Aura™ Communication Manager (Avaya S8300D w/ G450 Media Gateway)
Avaya Messaging (Voice Mail)
Avaya Aura® Session Manager with Survivable SIP Gateway
WAN
Branch 1
Branch 3
Headquarters:
All PSTN Inbound & Outbound
All Branches:
All PSTN Inbound & Outbound in Normal Mode
PSTN
Branch 2
10.64.20.0/24
FXO
FXS
HP MSR20-40
Analog Stations
Branch Survivable Mode:
All PSTN Inbound & Outbound

**Figure 1 – Network Diagram**

The Avaya IP Phone Configuration File Server contains a 46xxsettings.txt file used by Avaya IP phones to set values of the phone configuration parameters. **Section 7** includes the parameters of the 46xxsettings.txt file used by the Avaya 9600 SIP Phones for survivability.  The embedded Communication Manager Messaging (used for voicemail) can be reached by dialing the internal extension configured as the voice mail access number, or by dialing a PSTN number that also terminates to the voice messaging application.

The branch locations consist of two Avaya 9600 SIP Phones, a HP MSR20-40 with PSTN analog trunks connected to the FXO interface ports, and two analog phones on the FXS interfaces.

In the sample configuration, all phones at both the main and branch sites are SIP phones.

## 4. Equipment and Software Validated

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

| Equipment/Software | Release/Version |
|---|---|
| HP ProLiant DL360 G7 Server | Avaya Aura® Session Manager 6.1 SP7 |
| Dell™ PowerEdge™ R610 Server | Avaya Aura® System Manager 6.1, |
| Avaya S8300D Server with an Avaya G450 Media Gateway | Avaya Aura® Communication Manager 6.0.1 (R015x.02.1.016.4-17959) |
| Avaya 9600 Series IP Telephones<br>96x0 (SIP)<br>96x1 (SIP) | Avaya one-X® Deskphone Edition SIP 2.6.7<br>Avaya one-X® Deskphone Edition SIP 6.1 |
| Avaya 6210 Analog Telephone | - |
| Hewlett Packard MSR20-40 | MSR20.SI_5.20.R2209 |

# 5. Configure Avaya Aura® Communication Manager

This section shows the necessary steps to configure Communication Manager to support the survivable SIP gateway solution. It is assumed that the basic configuration on Communication Manager and the required licensing has already been administered. See the reference documents in **Section 11** for additional information.

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

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

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

## 5.1. Verify Communication Manger License

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

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

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

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 12000 77
           Maximum Concurrently Registered IP Stations: 18000 5
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 18000 8
                   Maximum Video Capable IP Softphones: 18000 3
                       Maximum Administered SIP Trunks: 24000 180
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   1
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0

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

## 5.2. Configure System Parameters Features

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

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

```
change system-parameters features                               Page   1 of  19
                            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 (or Silence) on Transferred Trunk Calls? no
                       DID/Tie/ISDN/SIP Intercept Treatment: attd
    Internal Auto-Answer of Attd-Extended/Transferred Calls: transferred
                  Automatic Circuit Assurance (ACA) Enabled? n



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

## 5.3. Configure IP Node Names

Use the “change node-names ip” command to add an entry for the Session Manager that the Communication Manager will connect to. The **Name** “SM_21_31” and **IP Address** “10.64.21.31” are entered for the Session Manager signaling interface. The node-name “procr” and “SM_21_31” will be used later in the SIP Signaling Group administration (**Section 5.6.1**).

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
SM_21_31            10.64.21.31
default             0.0.0.0
msgserver           10.64.21.41
procr               10.64.21.41
procr6              ::


( 14 of 14   administered node-names were displayed )
```

## 5.4. Configure IP Codec Set

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

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

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

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n         2        20
 2:
```

## 5.5. Configure IP Network Regions

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

The **Authoritative Domain** “avaya.com” matches the SIP domain configured in the Session Manager (**Section 6.1**). The **Codec Set** for intra-region calls is set to the codec set “1” as configured in **Section 5.4**. The **IP-IP Direct Audio** parameters retain the default “yes” allowing direct IP media paths both within the region and between regions to minimize the use of media resources in the Avaya Media Gateway.

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

## 5.6. Configure SIP Signaling Group and Trunk Group

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

### 5.6.1. SIP Signaling Groups

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**: "tls"
- **IMS Enabled?**: "n"
- **Peer Detection Enabled?** "yes"
- **Peer Server** "SM" (this field will automatically be populated)
- **Near-end Node Name**: "procr" node name from **Section 5.3**
- **Far-end Node Name**: "SM_21_31" Session Manager node name from **Section 5.3**
- **Near-end Listen Port**: "5061"
- **Far-end Listen Port**: "5061"
- **Far-end Network Region**: Network region number "1" from **Section 5.5**
- **DTMF over IP**: "rtp-payload"
- **Direct IP-IP Audio Connections:** "y"

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

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



   Near-end Node Name: procr                 Far-end Node Name: SM_21_31
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1

Far-end Domain:
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? y                    Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n             Alternate Route Timer(sec): 20
```

### 5.6.2. SIP Trunk Groups

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

- **Group Type**: "sip"
- **Group Name**: Descriptive text
- **TAC**: An available trunk access code as per dial plan
- **Service Type**: "tie"
- **Member Assignment Method**: "auto"
- **Signaling Group**: The signaling group number as configured in **Section 5.6.1**
- **Number of Members**: Equal to the maximum number of concurrent calls supported

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

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: to SM_21_31                 COR: 1        TN: 1        TAC: 101
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 1
                                                     Number of Members: 50
```

Navigate to **Page 3**, and enter "unk-pvt" for the **Numbering Format** field as shown below (note, other configurations are possible). Use the default values for all other fields.

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



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

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n


                                Modify Tandem Calling Number: no




 Show ANSWERED BY on Display? y
```

## 5.7. Configure Route Patterns

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

| | |
|---|---|
| **Pattern Name**: | A descriptive name |
| **Grp No**: | The trunk group number configured in **Section 5.6.2** |
| **FRL**: | Facility Restriction Level that allows access to this trunk, “0” being the least restrictive |
| **Numbering Format** | “lev0-pvt” was entered to indicate the Type of Numbering was local, but other configurations are possible. |

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: to SM_21_31
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                                 DCS/ IXC
    No          Mrk Lmt List Del  Digits                                   QSIG
                             Dgts                                          Intw
 1: 1    0                    0                                             n   user
 2:                                                                         n   user
 3:                                                                         n   user
 4:                                                                         n   user
 5:                                                                         n   user
 6:                                                                         n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                               lev0-pvt  none
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

## 5.8. 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 5.6.2**. In the example shown below, all calls originating from a 5-digit extension beginning with “5” that are routed across any trunk group (since **Trk Grp(s)** field is blank) will result in a 5-digit calling number. The calling party number will be in the SIP “From” header.

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

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

## 5.9. Configure Automatic Alternate Routing (AAR)

Use the “change aar analysis” command to add an entry for the extension range corresponding to the SIP telephones (i.e. **531**xx) and the HP FXS stations (i.e. **5**xxxx). 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 5.7** |
| **Call Type**: | Enter the appropriate call type |

```
change aar analysis 5                                           Page   1 of   2
                            AAR DIGIT ANALYSIS TABLE
                                  Location: all          Percent Full: 1

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    5                     5    5     1        aar          n
    531                   5    5     1        unku         n
```

## 5.10. Configure Automatic Route Selection (ARS)

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

### 5.10.1. 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  10
                              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: *50
                       Answer Back Access Code: *37
                         Attendant Access Code:
      Auto Alternate Routing (AAR) Access Code: 8
    Auto Route Selection (ARS) - Access Code 1: 9     Access Code 2:
                 Automatic Callback Activation: *31    Deactivation: *32
Call Forwarding Activation Busy/DA: *33    All: *34    Deactivation: *35
   Call Forwarding Enhanced Status:        Act:        Deactivation:
                         Call Park Access Code: *36
                       Call Pickup Access Code: *38
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:
```

### 5.10.2. ARS Digit Analysis

The “change ars analysis *x*” command is used to make routing entries where the “*x*” is the dialed digit string to match. The ARS Digit Analysis Table used in the sample configuration is shown below. Calls to the PSTN with area code 303 (1 + 10 digits) will match the **Dialed String** of “130” with “11” digits and select **Route Pattern** “2”. Calls to the PSTN with area code “732” will match the **Dialed String** of “173” with “11” digits and select **Route Pattern** “2” too. **Route Pattern** “2” (not shown) routes the call out a local PSTN trunk. Note that in a real deployment environment, calls with other area codes or with no area code restrictions (i.e., **Dialed String** “1xxxxxxxxxx”) can be specified to fit specific business policies.

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

          Dialed           Total      Route     Call   Node   ANI
          String         Min  Max   Pattern    Type   Num    Reqd
    130                  11   11     2         fnpa          n
```

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

          Dialed           Total      Route     Call   Node   ANI
          String         Min  Max   Pattern    Type   Num    Reqd
    173                  11   11     2         fnpa          n
```

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

- Route E-911 calls originated from the branch in the Normal Mode to go out to the PSTN through the FXO interfaces on the branch HP MSR20-40
- Route E-911 calls originated from the Headquarters to go out to the PSTN through the E1/T1 facilities at the central site

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

# 6. Configure Avaya Aura® Session Manager

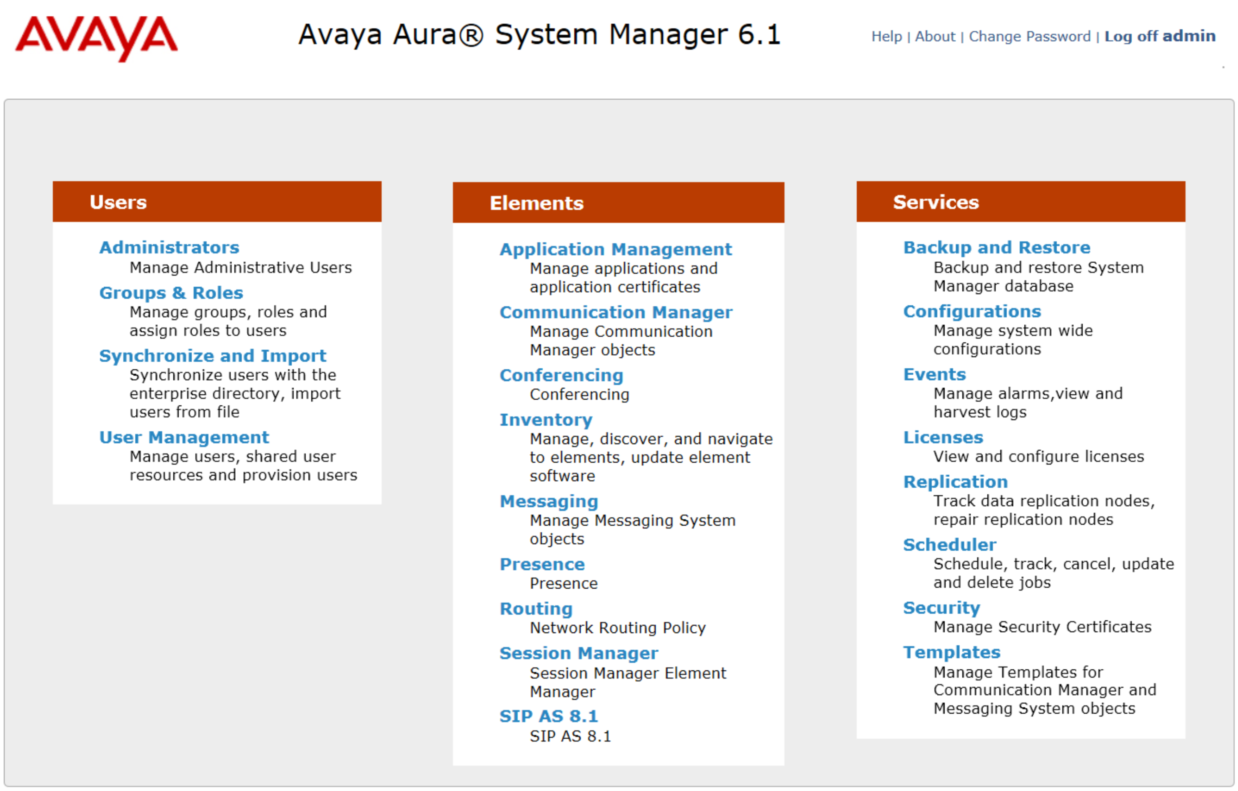
This section provides the procedures for configuring Session Manager as provisioned in the sample configuration. Session Manager is comprised of two functional components: the Session Manager server and the System Manager management server. All SIP call provisioning for Session Manager is performed via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

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

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, branch HP MSR20-40 and Session Manager itself
- **Entity Links** which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- **Routing Policies** which control call routing between the SIP Entities
- **Dial Patterns** which govern to which SIP Entity a call is routed
- **User Management**

Configuration of Session Manager is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. Log in with the appropriate credentials and click on **OK** in the subsequent confirmation screen. The menu shown below is then displayed. Navigate to **Elements → Routing**.

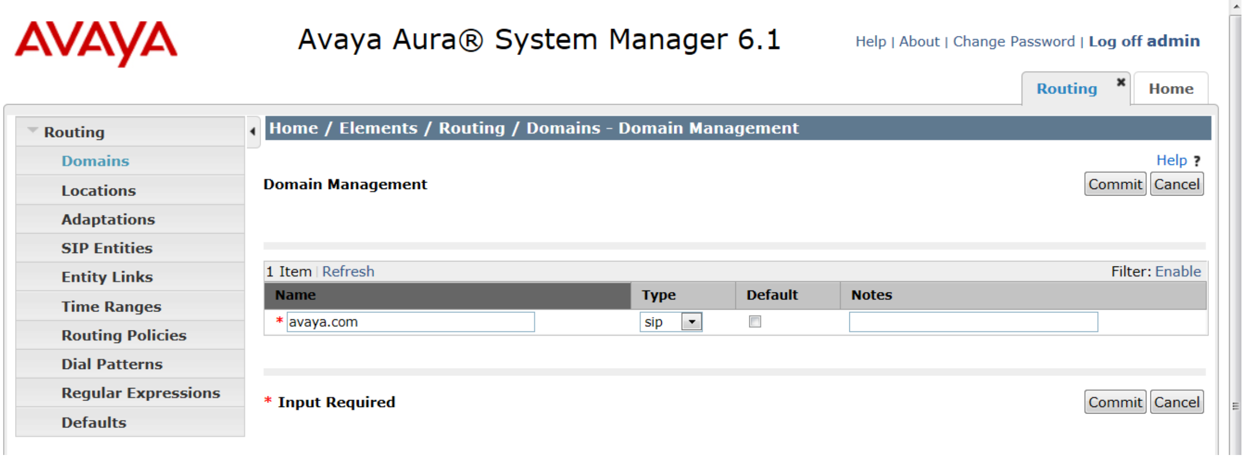

AVAYA
Avaya Aura® System Manager 6.1
Help | About | Change Password | Log off admin
Users
Administrators
Manage Administrative Users
Groups & Roles
Manage groups, roles and assign roles to users
Synchronize and Import
Synchronize users with the enterprise directory, import users from file
User Management
Manage users, shared user resources and provision users
Elements
Application Management
Manage applications and application certificates
Communication Manager
Manage Communication Manager objects
Conferencing
Conferencing
Inventory
Manage, discover, and navigate to elements, update element software
Messaging
Manage Messaging System objects
Presence
Presence
Routing
Network Routing Policy
Session Manager
Session Manager Element Manager
SIP AS 8.1
SIP AS 8.1
Services
Backup and Restore
Backup and restore System Manager database
Configurations
Manage system wide configurations
Events
Manage alarms,view and harvest logs
Licenses
View and configure licenses
Replication
Track data replication nodes, repair replication nodes
Scheduler
Schedule, track, cancel, update and delete jobs
Security
Manage Security Certificates
Templates
Manage Templates for Communication Manager and Messaging System objects

## 6.1. Specify SIP Domain

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

- **Name**: The authoritative domain name matching the domain configuration on Communication Manager (see **Section 5.5**)
- **Type**: “sip”
- **Notes**: Descriptive text (optional)

Click **Commit**.



| Name | Type | Default | Notes |
|---|---|---|---|
| * avaya.com | sip | ☐ | |

## 6.2. Add Locations

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

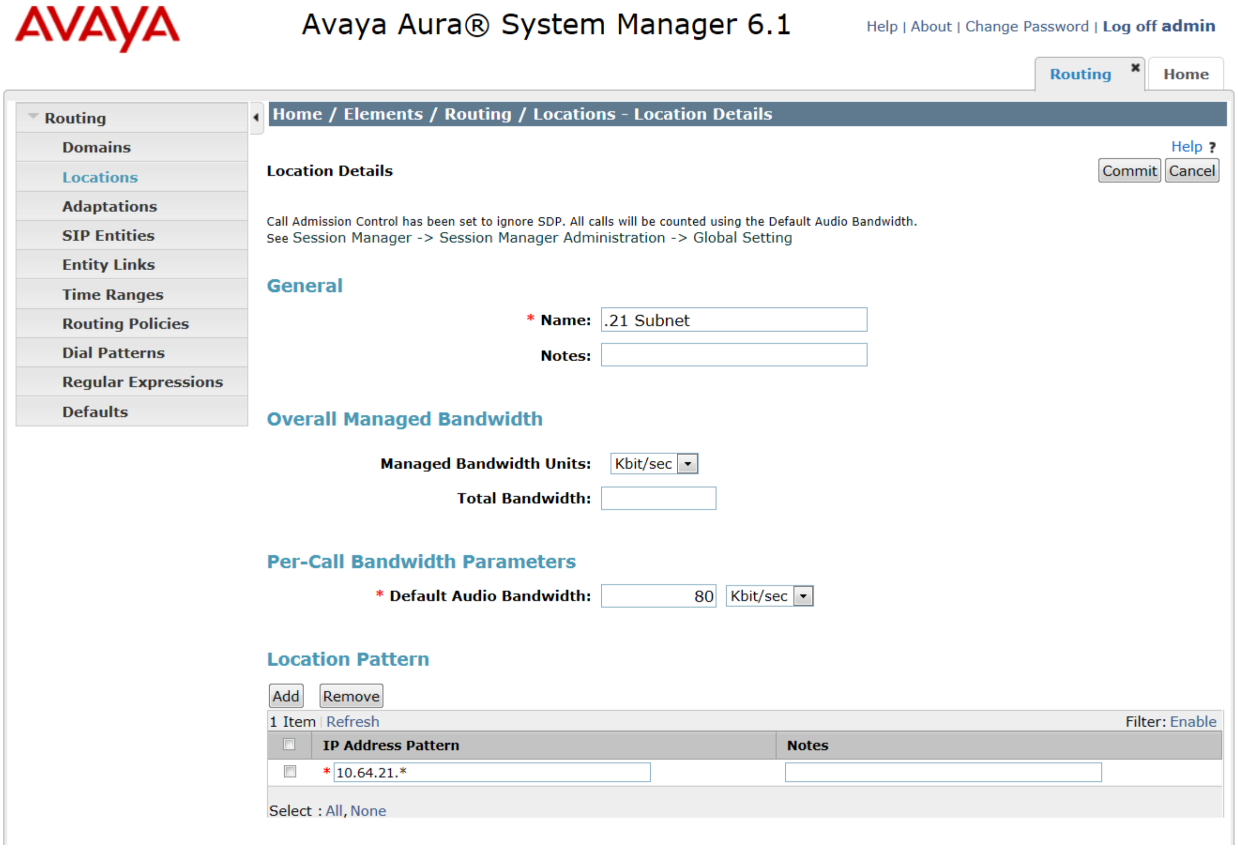
- **Name**: A descriptive name
- **Notes**: Descriptive text (optional)

The remaining bandwidth fields can be filled in to specify bandwidth management parameters between Session Manager and this location. These were not used in the sample configuration, and reflect default values. Note also that routing policies can be defined based on Locations.

Under *Location Pattern*, to add a new row, click the **Add** button and enter the following :

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

The screen below shows addition of the ".21 Subnet" Location for the Headquarters site, which includes the 10.64.21.0/24 network. Click **Commit** to save the **Location Details** definition.



Location Details

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.
See Session Manager -> Session Manager Administration -> Global Setting

General

* Name: .21 Subnet
Notes:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec
Total Bandwidth:

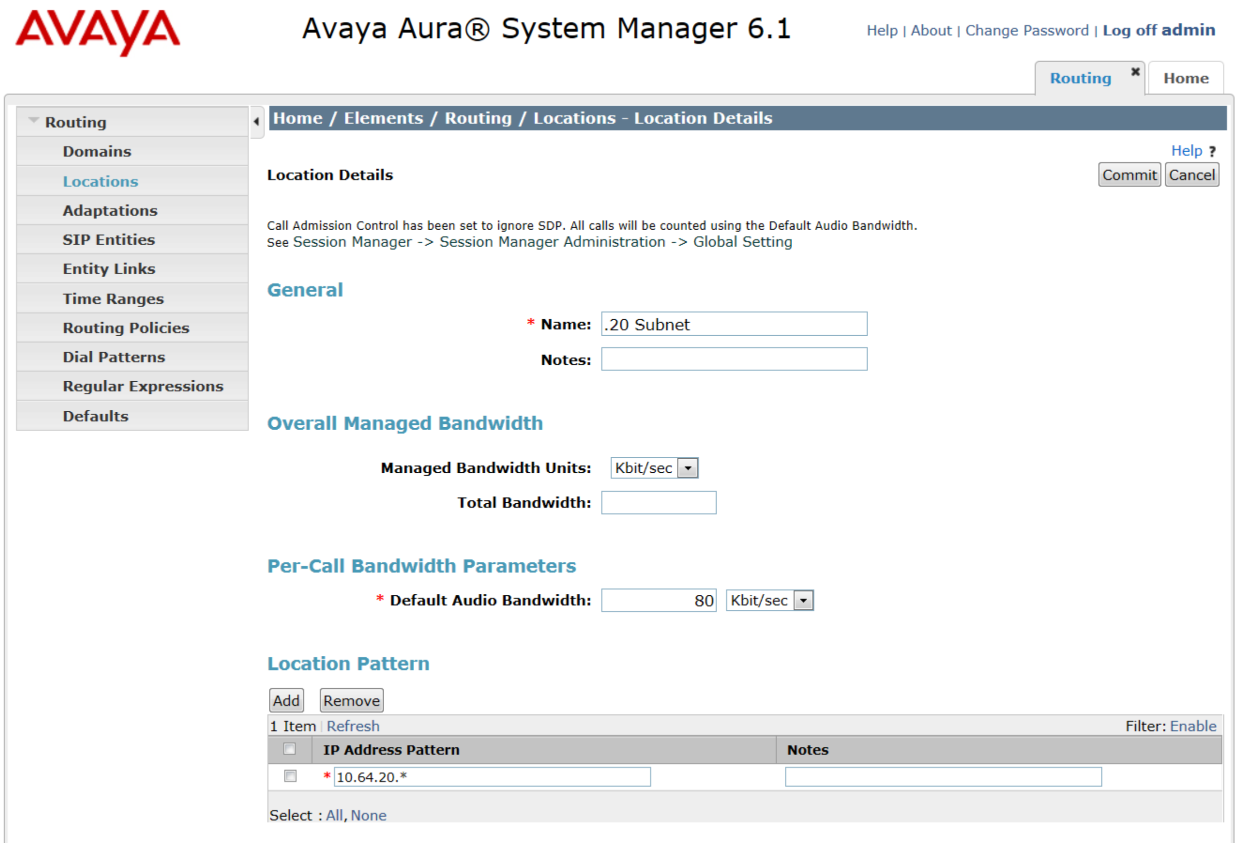
Per-Call Bandwidth Parameters

* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

| ☐ | IP Address Pattern | Notes |
|---|---|---|
| ☐ | * 10.64.21.* | |

In addition to the Location created for the Headquarters site, each branch needs to have its own Location defined. Each branch Location is similarly configured as shown below with its own **Name** and **IP Address Patterns**. The IP address pattern 10.64.20.* was specified for the sample branch.



Location Details

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth.
See Session Manager -> Session Manager Administration -> Global Setting

General

* Name: .20 Subnet

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Per-Call Bandwidth Parameters

* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

| ☐ | IP Address Pattern | Notes |
|---|---|---|
| ☐ | * 10.64.20.* | |

## 6.3. 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 itself, Communication Manager at the Headquarters, and the HP MSR20-40 at the branch.

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

Under *General*:

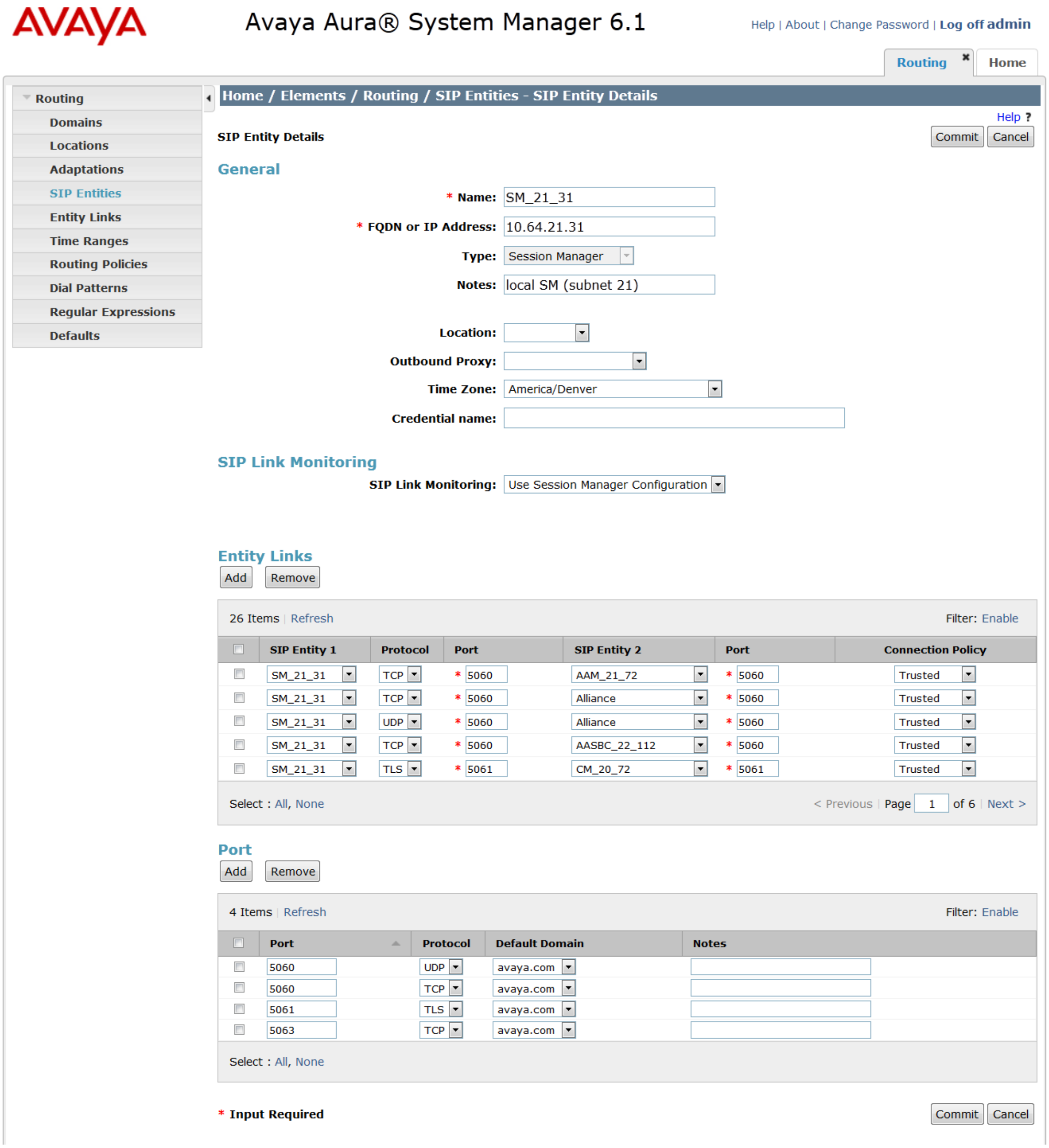
- **Name** A descriptive name
- **FQDN or IP Address**: FQDN or IP address of the signaling interface on the telephony system
- **Type**: "Session Manager" for Session Manager; "CM" for Communication Manager; "Survivability Server" for the HP MSR20-40
- **Location:** Select the appropriate Location configured in **Section 6.2**
- **Time Zone:** Select the proper time zone for this installation

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

- **Port**: Port number on which the system listens for SIP requests
- **Protocol**: Transport protocol to be used to send SIP requests
- **Default Domain**: Select the SIP Domain configured in **Section 6.1**

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

The following screen shows the addition of the Session Manager. The *Entity Links* section is automatically populated after Entity Links have been defined.



**SIP Entity Details**

**General**

|  |  |
|---|---|
| * Name: | SM_21_31 |
| * FQDN or IP Address: | 10.64.21.31 |
| Type: | Session Manager |
| Notes: | local SM (subnet 21) |
| Location: |  |
| Outbound Proxy: |  |
| Time Zone: | America/Denver |
| Credential name: |  |

**SIP Link Monitoring**

|  |  |
|---|---|
| SIP Link Monitoring: | Use Session Manager Configuration |

**Entity Links**

26 Items | Refresh Filter: Enable

| ☐ | SIP Entity 1 | Protocol | Port | SIP Entity 2 | Port | Connection Policy |
|---|---|---|---|---|---|---|
| ☐ | SM_21_31 | TCP | * 5060 | AAM_21_72 | * 5060 | Trusted |
| ☐ | SM_21_31 | TCP | * 5060 | Alliance | * 5060 | Trusted |
| ☐ | SM_21_31 | UDP | * 5060 | Alliance | * 5060 | Trusted |
| ☐ | SM_21_31 | TCP | * 5060 | AASBC_22_112 | * 5060 | Trusted |
| ☐ | SM_21_31 | TLS | * 5061 | CM_20_72 | * 5061 | Trusted |

Select : All, None < Previous | Page 1 of 6 | Next >

**Port**

4 Items | Refresh Filter: Enable

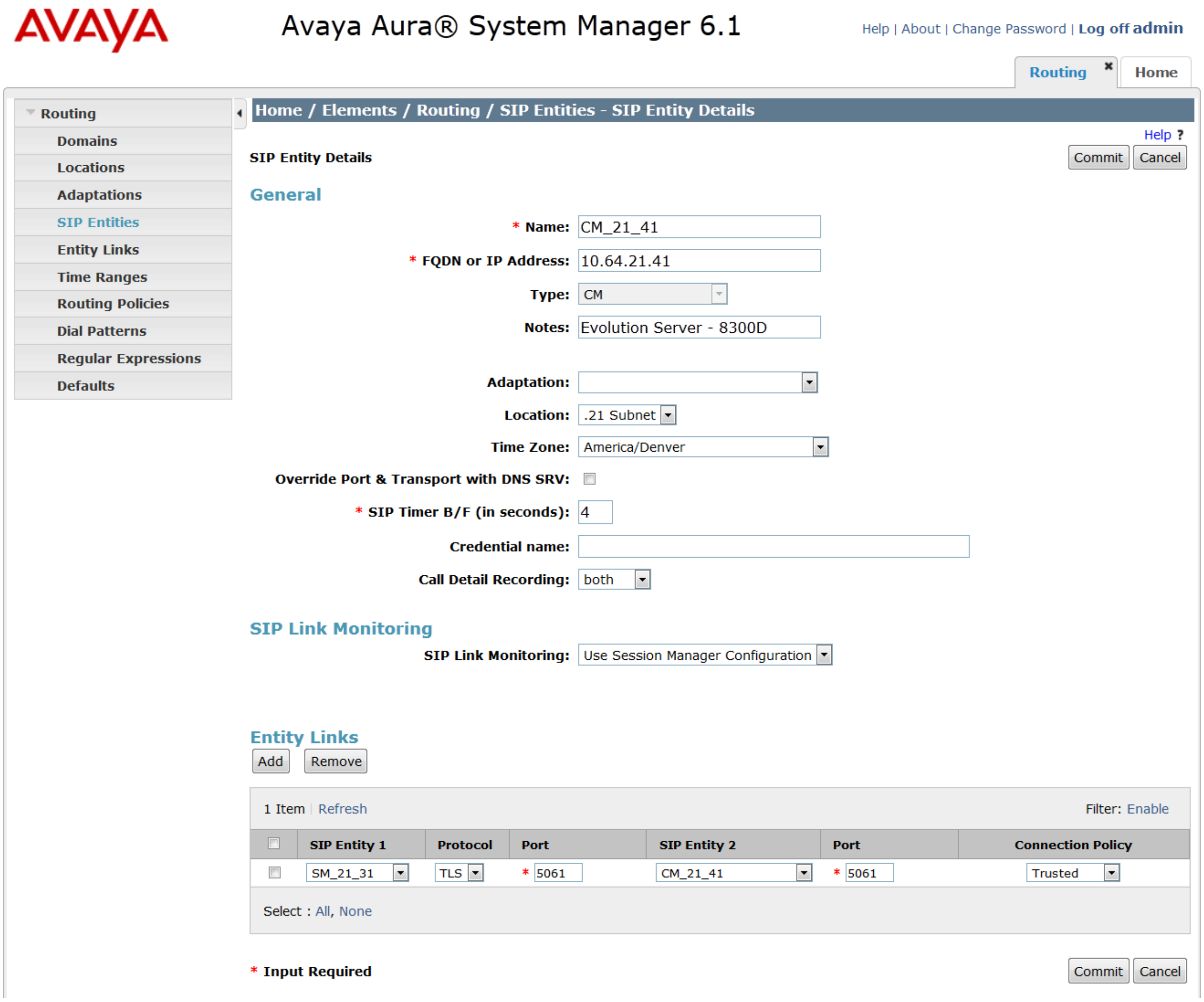
| ☐ | Port | Protocol | Default Domain | Notes |
|---|---|---|---|---|
| ☐ | 5060 | UDP | avaya.com |  |
| ☐ | 5060 | TCP | avaya.com |  |
| ☐ | 5061 | TLS | avaya.com |  |
| ☐ | 5063 | TCP | avaya.com |  |

Select : All, None

* Input Required

The following screen shows the results of adding Communication Manager. In this case, **FQDN or IP Address** is the IP address for the Communication Manager since the G450 Media Gateway used in the sample configuration has its signaling interface integrated into the Communication Manager processor. For other Avaya Media Gateways with a C-LAN board installed, the IP address of the C-LAN board in the Media Gateway should be specified. Note the "CM" selection for **Type**.

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



SIP Entity Details

General

* Name: CM_21_41

* FQDN or IP Address: 10.64.21.41

Type: CM

Notes: Evolution Server - 8300D

Adaptation:

Location: .21 Subnet

Time Zone: America/Denver

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: both

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

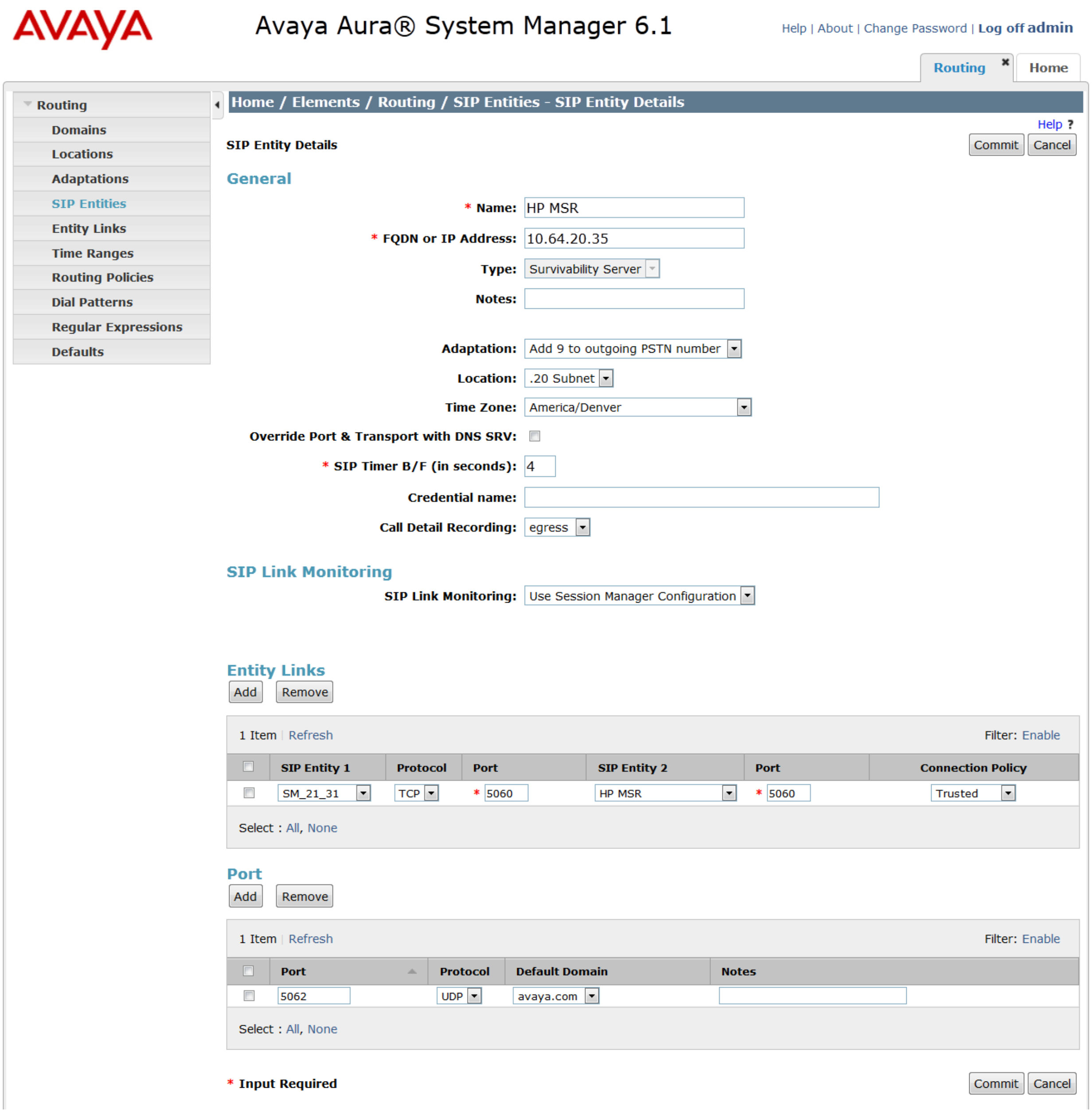
1 Item

| ☐ | SIP Entity 1 | Protocol | Port | SIP Entity 2 | Port | Connection Policy |
|---|---|---|---|---|---|---|
| ☐ | SM_21_31 | TLS | * 5061 | CM_21_41 | * 5061 | Trusted |

* Input Required

The following screen shows the results of adding the HP MSR20-40. Note the "Survivability Server" selection for **Type**. Note, the *Port* section where port **5062** and **UDP** were selected to match the preferred port and default protocol configuration of the HP MSR20-40.

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



Home / Elements / Routing / SIP Entities - SIP Entity Details

**SIP Entity Details**

**General**

* Name: HP MSR
* FQDN or IP Address: 10.64.20.35
Type: Survivability Server
Notes:
Adaptation: Add 9 to outgoing PSTN number
Location: .20 Subnet
Time Zone: America/Denver
Override Port & Transport with DNS SRV: ☐
* SIP Timer B/F (in seconds): 4
Credential name:
Call Detail Recording: egress

**SIP Link Monitoring**

SIP Link Monitoring: Use Session Manager Configuration

**Entity Links**

1 Item | Refresh — Filter: Enable

| ☐ | SIP Entity 1 | Protocol | Port | SIP Entity 2 | Port | Connection Policy |
|---|---|---|---|---|---|---|
| ☐ | SM_21_31 | TCP | * 5060 | HP MSR | * 5060 | Trusted |

Select : All, None

**Port**

1 Item | Refresh — Filter: Enable

| ☐ | Port | Protocol | Default Domain | Notes |
|---|---|---|---|---|
| ☐ | 5062 | UDP | avaya.com | |

Select : All, None

* Input Required

## 6.4. Add Entity Links

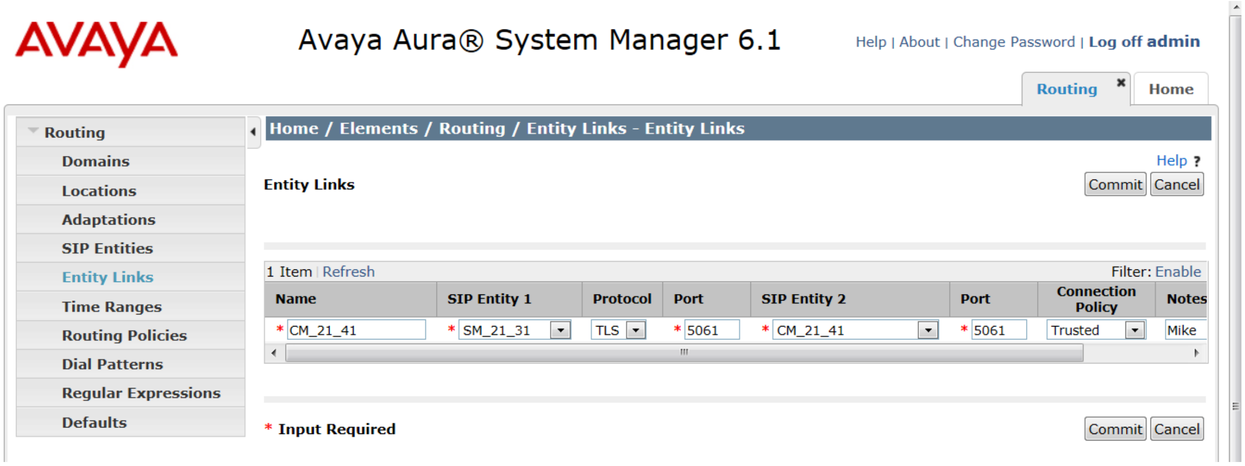
A SIP trunk between Session Manager and a telephony system is described by an Entity link. In the sample configuration, an Entity Link was configured between Session Manager and Communication Manger. Another Entity Link was configured between Session Manager and the branch HP MSR20-40.

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

- **Name**: A descriptive name
- **SIP Entity 1**: Select the Session Manager SIP Entity configured in **Section 6.3**
- **Protocol**: “TLS” was used for the link to Communication Manager, select “TCP” for the HP MSR20-40 link
- **Port**: Port number to which the other system sends SIP requests.
- **SIP Entity 2**: Select the appropriate SIP Entity configured in **Section 6.3**
- **Port**: Port number on which the other system receives SIP requests
- **Trusted**: Check this box

Click **Commit** to save the configuration.

The screen below shows the Entity Link configured between Session Manager and Communication Manager.

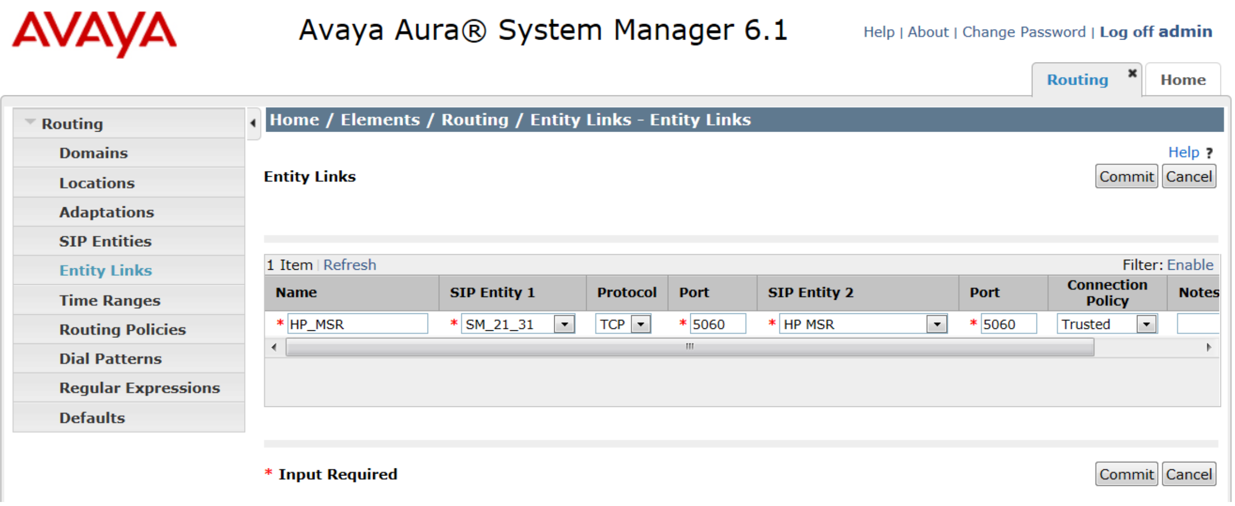


**Entity Links**

| Name | SIP Entity 1 | Protocol | Port | SIP Entity 2 | Port | Connection Policy | Notes |
|---|---|---|---|---|---|---|---|
| * CM_21_41 | * SM_21_31 | TLS | * 5061 | * CM_21_41 | * 5061 | Trusted | Mike |

* **Input Required**

The screen below shows the Entity Link between Session Manager and the HP MSR20-40.



Entity Links

| Name | SIP Entity 1 | Protocol | Port | SIP Entity 2 | Port | Connection Policy | Notes |
|---|---|---|---|---|---|---|---|
| * HP_MSR | * SM_21_31 | TCP | * 5060 | * HP MSR | * 5060 | Trusted | |

## 6.5. Add Routing Policy

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

The inter-branch and intra-branch calling between SIP phones using extension numbers do not need Routing Policies since all the phones, both at the Headquarters and in the branches, are administered on the Communication Manager and register to the Session Manager. However, calls to the PSTN need Routing Policies to determine where they are going to be routed for eventual termination to the PSTN. These calls could go out to the PSTN through the T1 facilities at the Headquarters, or they could go out through the analog trunks (a.k.a Service Provider CO lines) connected to the FXO ports on the branch MSR20-40.

In the case of Centralized Trunking arrangement, all PSTN-bound calls, regardless of the call originations (either from the Headquarters or from the branches), should be sent to the Headquarters for onward routing to the PSTN. In the case of Distributed Trunking arrangement, all PSTN-bound calls from the Headquarters plus the Long Distance toll calls from the branch locations should be routed to the Headquarters for PSTN termination, but local calls from the branch should be routed to the branch HP MSR20-40 for going out to the PSTN through the FXO interfaces on the HP MSR20-40.

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

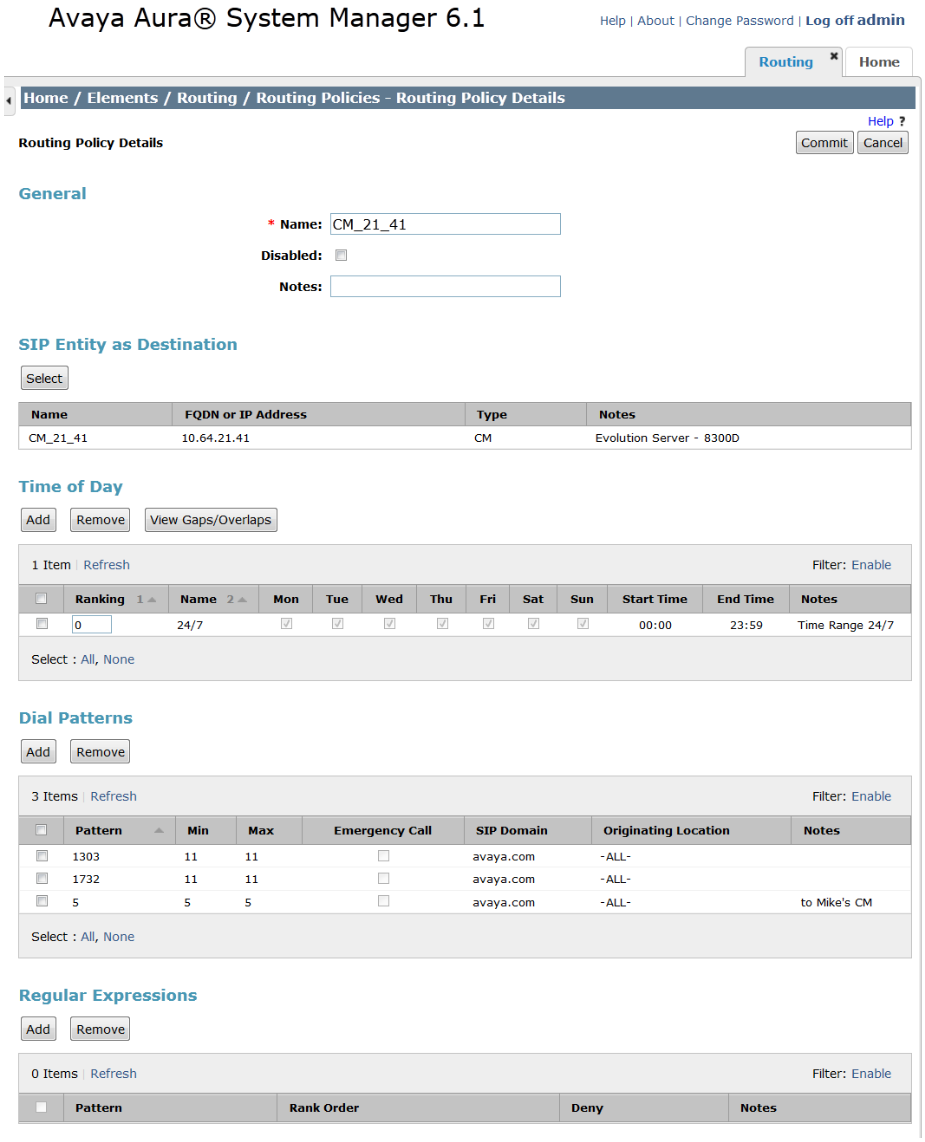
Under *General*:
Enter a descriptive name in **Name** and optional text in **Notes**.

Under *SIP Entity as Destination*:

Click **Select**, and then select the appropriate SIP entity to which this routing policy applies.
Under *Time of Day*:
Keep the default "24/7" time range.

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

The following screen shows the Routing Policy for routing calls to the Headquarters. For PSTN calls, Communication Manager was configured to route the calls over a T1 trunk to the PSTN[1]. Note that the *Dial Patterns* section is automatically populated after Dial Patterns have been defined.


Avaya Aura® System Manager 6.1
Help | About | Change Password | Log off admin
Routing
Home
Home / Elements / Routing / Routing Policies - Routing Policy Details
Help ?
Commit
Cancel

Routing Policy Details

General

* Name: CM_21_41

Disabled: ☐

Notes:

SIP Entity as Destination

| Name | FQDN or IP Address | Type | Notes |
|---|---|---|---|
| CM_21_41 | 10.64.21.41 | CM | Evolution Server - 8300D |

Time of Day

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

Dial Patterns

| ☐ | Pattern | Min | Max | Emergency Call | SIP Domain | Originating Location | Notes |
|---|---|---|---|---|---|---|---|
| ☐ | 1303 | 11 | 11 | ☐ | avaya.com | -ALL- | |
| ☐ | 1732 | 11 | 11 | ☐ | avaya.com | -ALL- | |
| ☐ | 5 | 5 | 5 | ☐ | avaya.com | -ALL- | to Mike's CM |

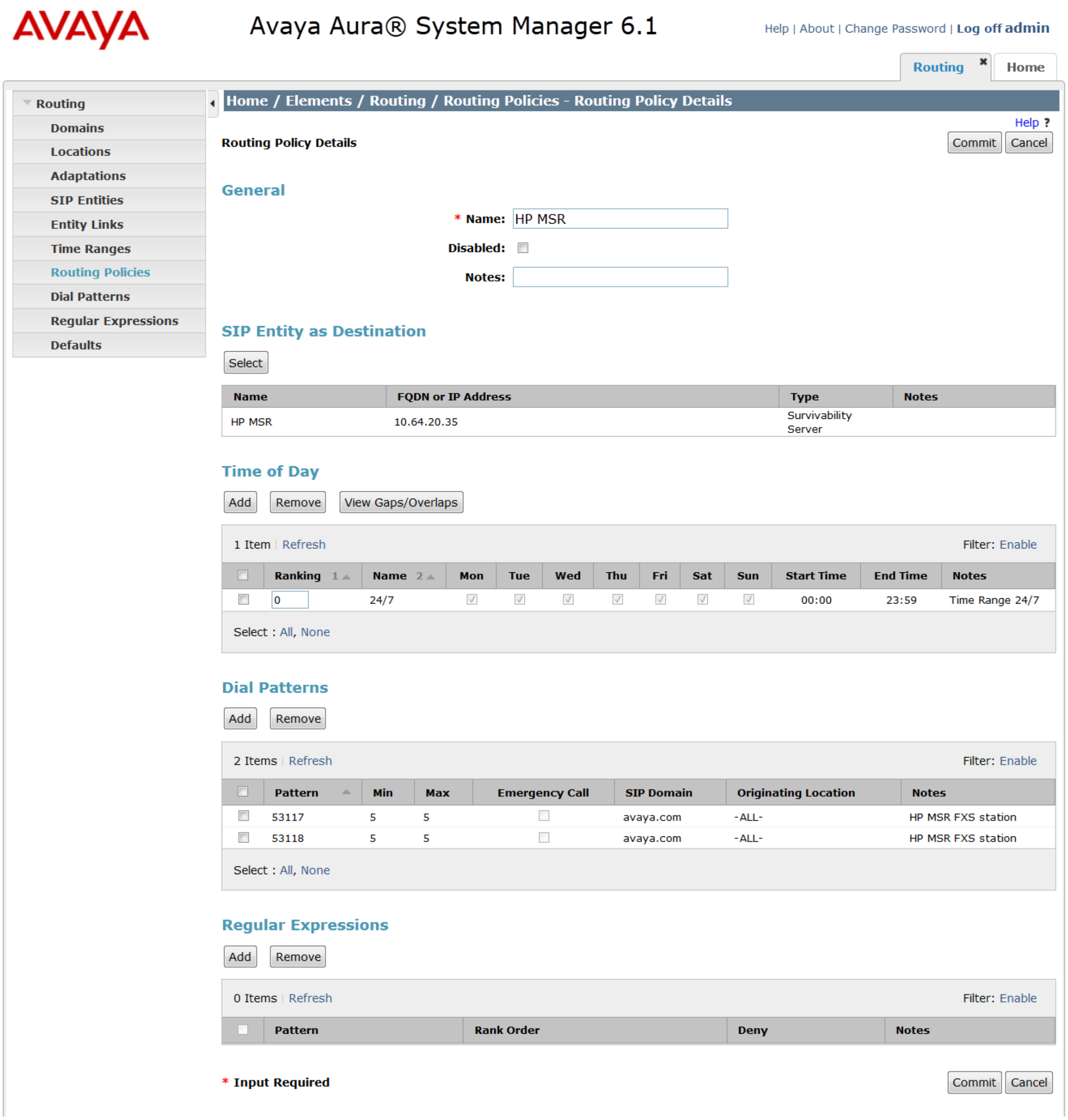
Regular Expressions

| ☐ | Pattern | Rank Order | Deny | Notes |
|---|---|---|---|---|

---

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

The following screen shows the Routing Policy for routing calls to the branch HP MSR20-40.



**Routing Policy Details**

**General**

* **Name:** HP MSR

**Disabled:** ☐

**Notes:**

**SIP Entity as Destination**

| Name | FQDN or IP Address | Type | Notes |
|---|---|---|---|
| HP MSR | 10.64.20.35 | Survivability Server | |

**Time of Day**

1 Item | Refresh Filter: Enable

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

Select : All, None

**Dial Patterns**

2 Items | Refresh Filter: Enable

| ☐ | Pattern | Min | Max | Emergency Call | SIP Domain | Originating Location | Notes |
|---|---|---|---|---|---|---|---|
| ☐ | 53117 | 5 | 5 | ☐ | avaya.com | -ALL- | HP MSR FXS station |
| ☐ | 53118 | 5 | 5 | ☐ | avaya.com | -ALL- | HP MSR FXS station |

Select : All, None

**Regular Expressions**

0 Items | Refresh Filter: Enable

| ☐ | Pattern | Rank Order | Deny | Notes |
|---|---|---|---|---|

* **Input Required**

## 6.6. Add Dial Patterns

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

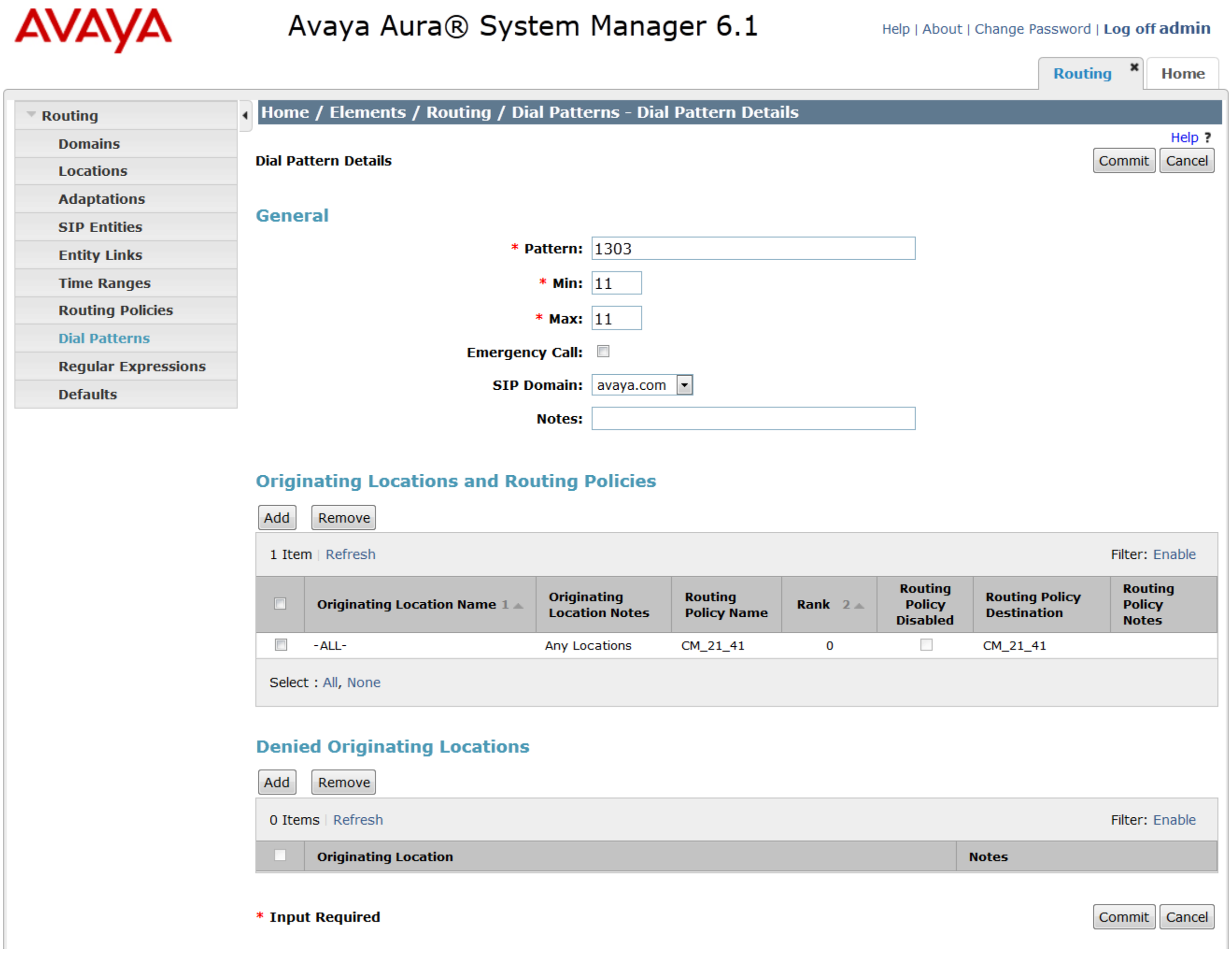
To add a dial pattern, navigate to **Routing → Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following, as shown in the screens below:
Under *General*:

- **Pattern**: Dialed number or prefix
- **Min**: Minimum length of dialed number
- **Max**: Maximum length of dialed number
- **SIP Domain**: SIP domain specified in **Section 6.1**
- **Notes**: Comment on purpose of dial pattern.

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

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

The following screen shows the Dial Pattern defined for routing calls to the PSTN starting with “1303”.  “-ALL-" was selected for **Originating Location Name** so that calls from both the Headquarters and the branches would be routed to the Headquarters telephony infrastructure for termination to the PSTN through the T1 facilities.



Dial Pattern Details

General

* Pattern: 1303

* Min: 11

* Max: 11

Emergency Call: ☐

SIP Domain: avaya.com

Notes:

Originating Locations and Routing Policies

1 Item

| ☐ | Originating Location Name | Originating Location Notes | Routing Policy Name | Rank | Routing Policy Disabled | Routing Policy Destination | Routing Policy Notes |
|---|---|---|---|---|---|---|---|
| ☐ | -ALL- | Any Locations | CM_21_41 | 0 | ☐ | CM_21_41 | |

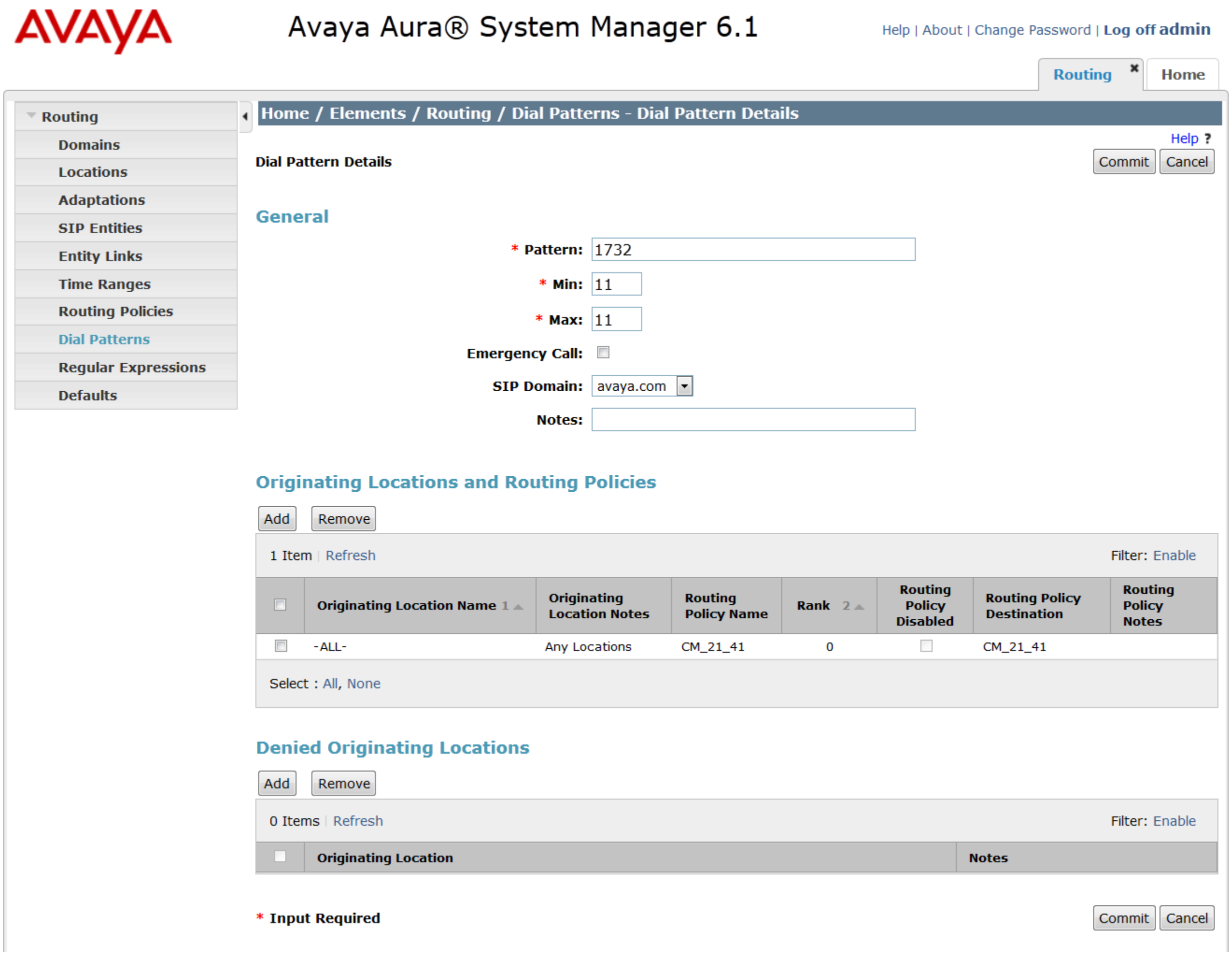
Denied Originating Locations

0 Items

| ☐ | Originating Location | Notes |
|---|---|---|

* Input Required

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



Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details

General

* Pattern: 1732

* Min: 11

* Max: 11

Emergency Call: ☐

SIP Domain: avaya.com

Notes:

Originating Locations and Routing Policies

1 Item | Refresh

| ☐ | Originating Location Name | Originating Location Notes | Routing Policy Name | Rank | Routing Policy Disabled | Routing Policy Destination | Routing Policy Notes |
|---|---|---|---|---|---|---|---|
| ☐ | -ALL- | Any Locations | CM_21_41 | 0 | ☐ | CM_21_41 | |

Select : All, None

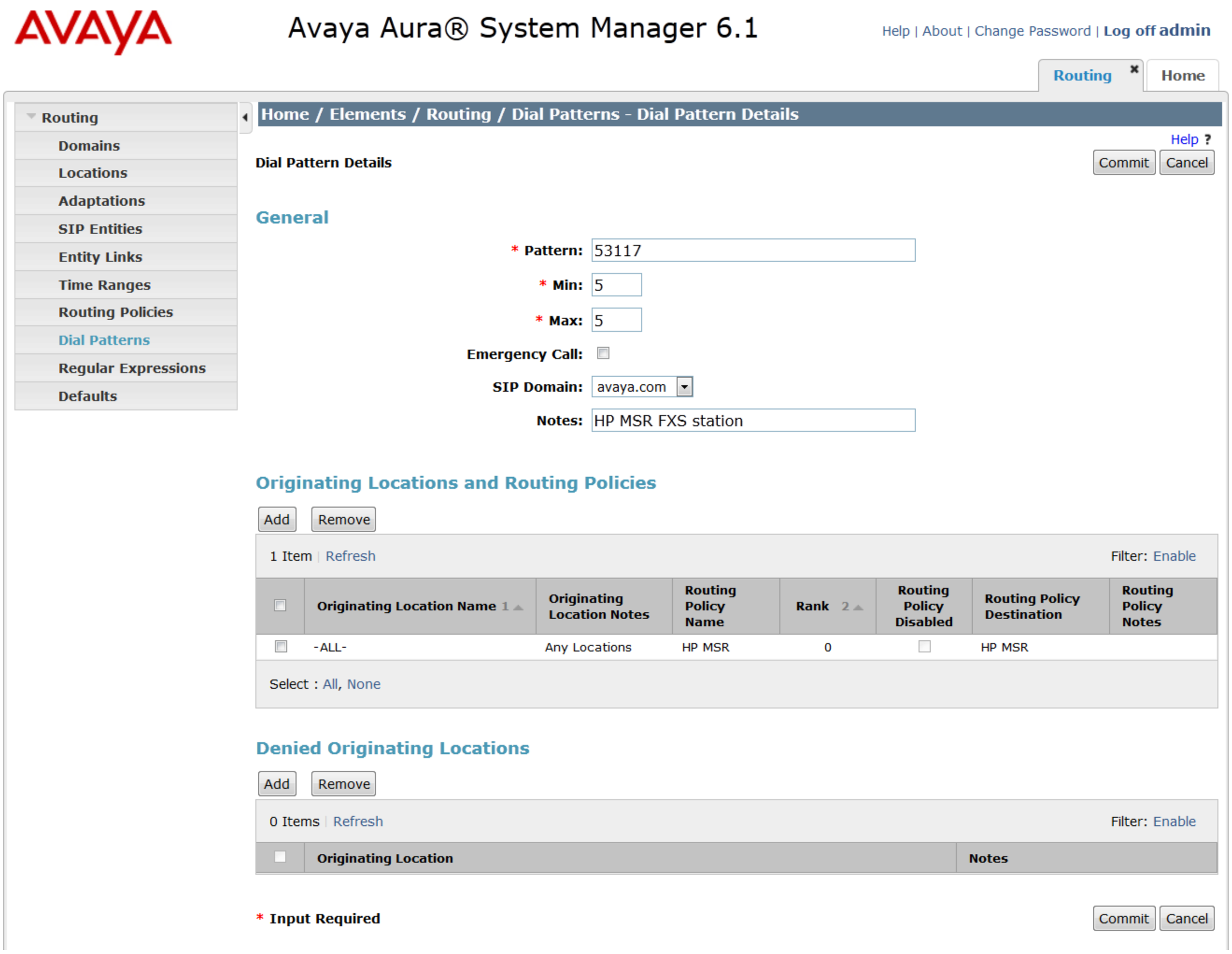
Denied Originating Locations

0 Items | Refresh

| ☐ | Originating Location | Notes |
|---|---|---|

* Input Required

The following screen shows the Dial Pattern defined for routing calls to the FXS station (extension 53117) to the HP MSR. A similar dial pattern (not shown) was created for the other FXS station (extension 53118).



Dial Pattern Details

General

* Pattern: 53117

* Min: 5

* Max: 5

Emergency Call: ☐

SIP Domain: avaya.com

Notes: HP MSR FXS station

Originating Locations and Routing Policies

1 Item | Refresh

| ☐ | Originating Location Name | Originating Location Notes | Routing Policy Name | Rank | Routing Policy Disabled | Routing Policy Destination | Routing Policy Notes |
|---|---|---|---|---|---|---|---|
| ☐ | -ALL- | Any Locations | HP MSR | 0 | ☐ | HP MSR | |

Denied Originating Locations

0 Items | Refresh

| ☐ | Originating Location | Notes |
|---|---|---|

* Input Required

The routing of E-911 calls is outside the scope of these Application notes. However, 911 calls from the branch location in the Normal Mode should be routed back to the branch MSR20-40 to go out through the FXO interfaces to the local Emergency Response Center.

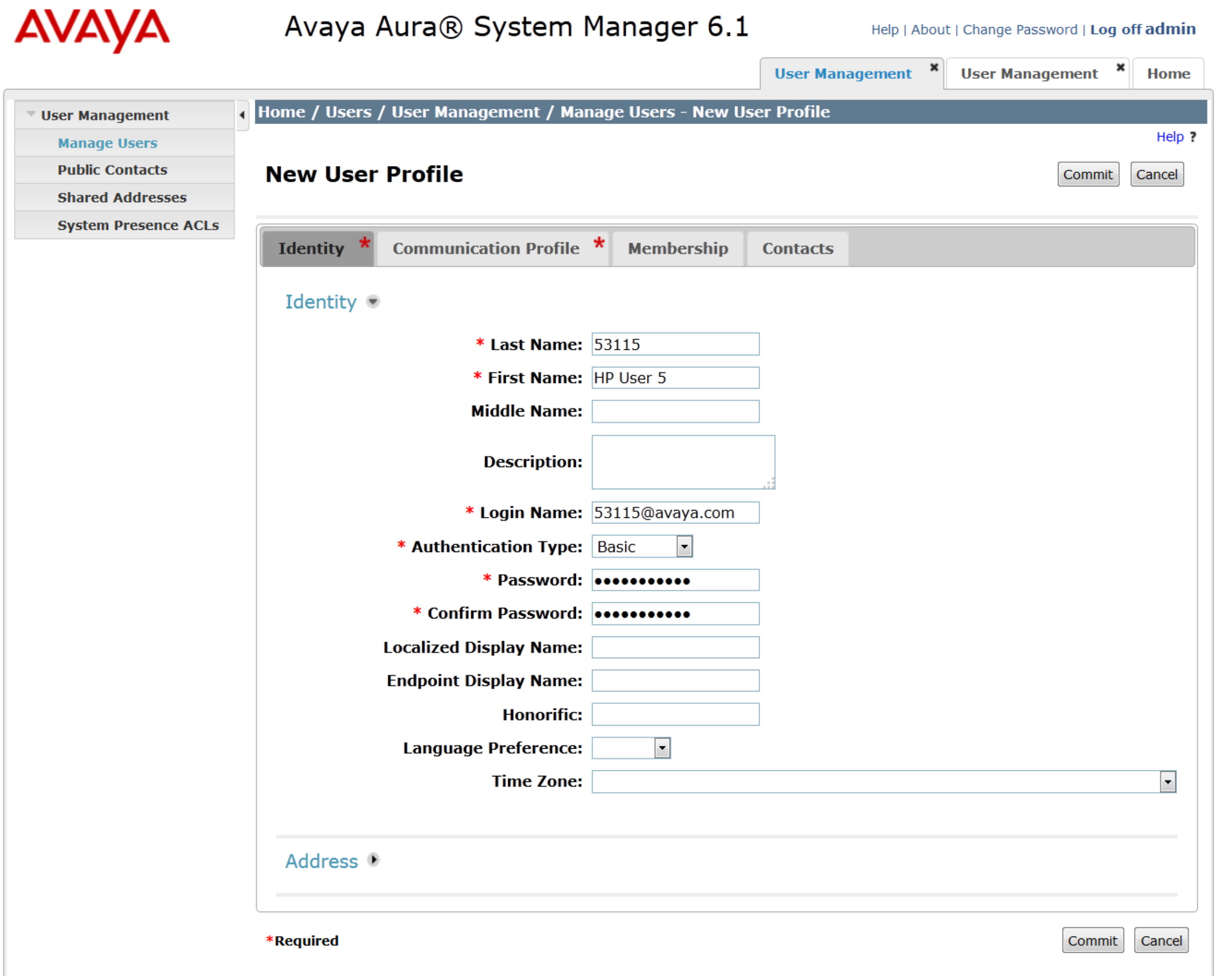
In the Survivable Mode, the routing policy on the branch MSR20-40 will route 911 calls from the branch to the PSTN through its FXO interfaces too.

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

## 6.7. User Management for Adding SIP Telephone Users

To add a SIP user, navigate to **Users → User Management → Manager Users**. Click on the **New** link (not shown) on the right. On the *Identity* tab, enter the following fields, and use defaults for the remaining fields:

| | |
|---|---|
| **First Name:** | First name of user |
| **Last Name:** | Last name of user |
| **Login Name**: | Telephone extension with domain suffix (see **Section 6.1**) |
| **Authentication Type** | Basic |
| **Password**: | Enter password |
| **Confirm Password**: | Re-enter passwerd |



* Last Name: 53115

* First Name: HP User 5

Middle Name:

Description:

* Login Name: 53115@avaya.com

* Authentication Type: Basic

* Password: ●●●●●●●●●●●

* Confirm Password: ●●●●●●●●●●●

Localized Display Name:

Endpoint Display Name:

Honorific:

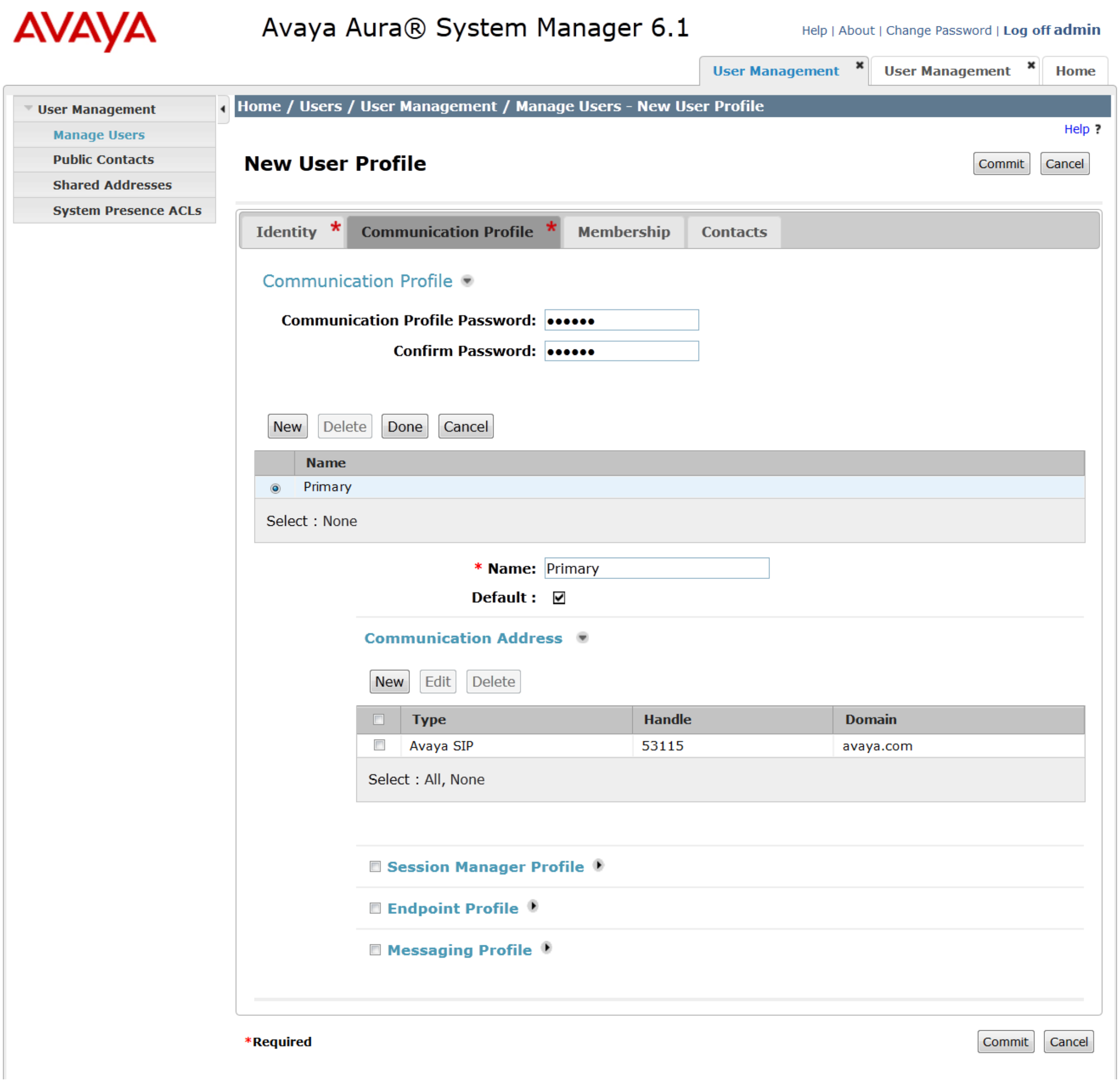
Language Preference:

Time Zone:

Click the *Communication Profile* tab. Under *Communication Profile*, enter and confirm the **Communication Profile Password**. Under *Communication Address*, click the **New** button. Enter appropriate values in the following fields and use defaults for the remaining fields:

| | |
|---|---|
| **Type**: | Select "Avaya SIP" |
| **Fully Qualified Address**: | Enter the extension and select the domain as specified in **Section 6.1** |

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



**New User Profile**

Communication Profile

Communication Profile Password: ••••••

Confirm Password: ••••••

| | Name |
|---|---|
| ● | Primary |

Select : None

* Name: Primary

Default : ☑

Communication Address

| ☐ | Type | Handle | Domain |
|---|---|---|---|
| ☐ | Avaya SIP | 53115 | avaya.com |

Select : All, None

Check the *Session Manager Profile* box. Enter the following fields and use defaults for the remaining fields (note, the configuration of Application Sequences is outside the scope of this document:

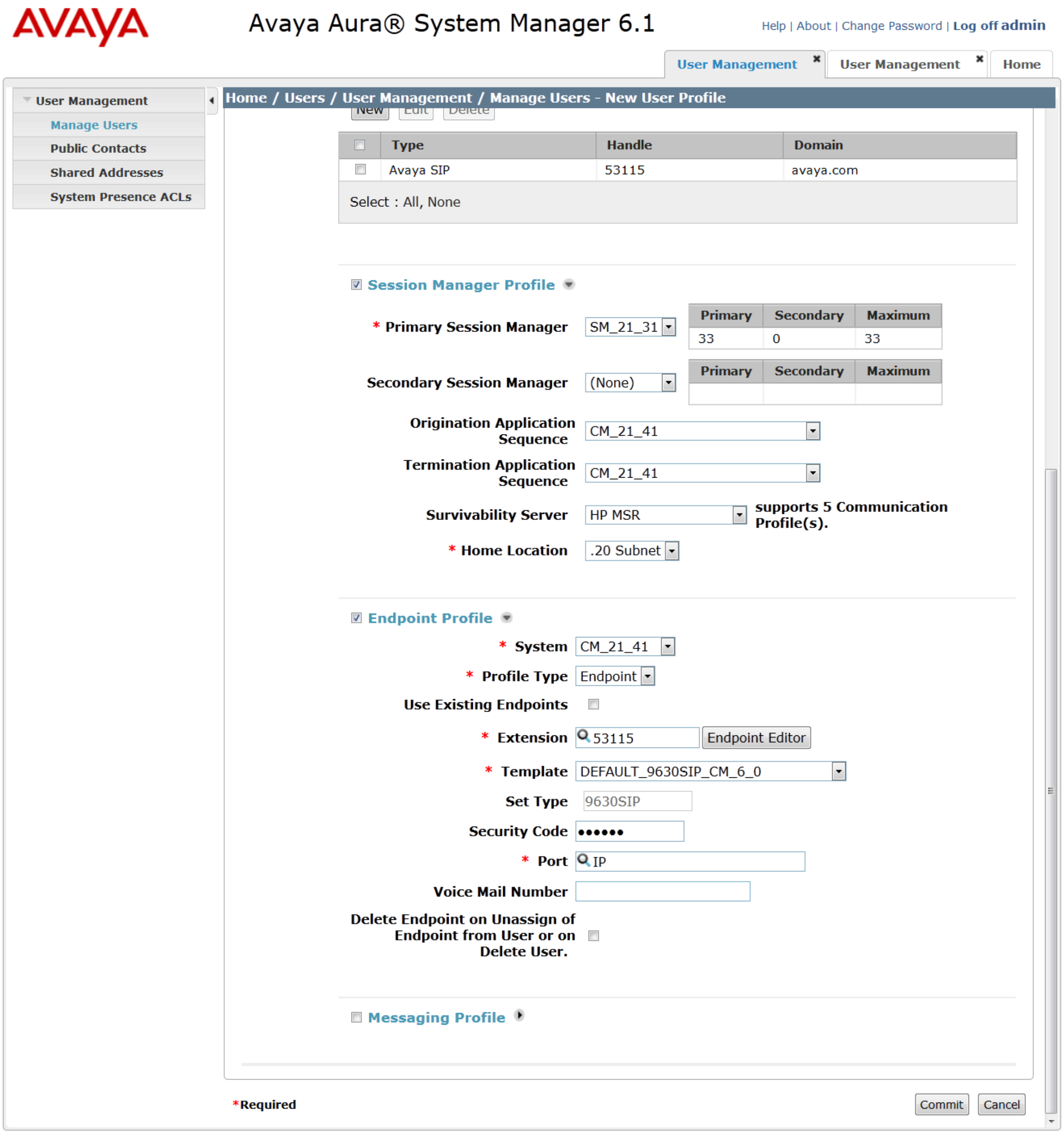
- **Primary Session Manager:** Select the Session Manager SIP entity
- **Origination Application Sequence:** Select the Communication Manager application sequence
- **Termination Application Sequence**:Select the Communication Manager application sequence
- **Survivability Server:**For the branch phones located at the HP MSR location, select the HP MSR SIP entity. For phones at the Headquarters location, leave the default value of “None”.
- **Home Location:** Select the appropriate location configured in **Section 6.2**

Check the *Endpoint Profile* box. Enter the following fields and use defaults for the remaining fields:

- **System**: Select the Communication Manager entity
- **Profile Type**: Select “Endpoint”
- **Extension**: Enter the extension of the user
- **Template**: Select an appropriate template matching the telephone type
- **Security Code**: Password to be entered by the user when logging onto the telephone
- **Port**: Click on the Search icon to select “IP” (a specific port number is then automatically populated in this field)

Click the **Commit** button.

Repeat the above procedure to add each SIP telephone user for the Headquarters site as well as the branch site.



Avaya Aura® System Manager 6.1

Home / Users / User Management / Manage Users - New User Profile

| ☐ | Type | Handle | Domain |
|---|---|---|---|
| ☐ | Avaya SIP | 53115 | avaya.com |

Select : All, None

☑ **Session Manager Profile**

* **Primary Session Manager** SM_21_31

| Primary | Secondary | Maximum |
|---|---|---|
| 33 | 0 | 33 |

**Secondary Session Manager** (None)

| Primary | Secondary | Maximum |
|---|---|---|
| | | |

**Origination Application Sequence** CM_21_41

**Termination Application Sequence** CM_21_41

**Survivability Server** HP MSR **supports 5 Communication Profile(s).**

* **Home Location** .20 Subnet

☑ **Endpoint Profile**

* **System** CM_21_41

* **Profile Type** Endpoint

**Use Existing Endpoints** ☐

* **Extension** 53115

* **Template** DEFAULT_9630SIP_CM_6_0

**Set Type** 9630SIP

**Security Code** ••••••

* **Port** IP

**Voice Mail Number**

**Delete Endpoint on Unassign of Endpoint from User or on Delete User.** ☐

☐ **Messaging Profile**

***Required**

# 7. Configure Avaya 9600 Series SIP Phones

The Avaya 9600 SIP Phones at all sites were configured to use Session Manager (IP address 10.64.21.31) as the SIP Proxy Server. The configuration parameters of the Avaya 9600 SIP Phone specific to SIP Survivability in the 46xxsettings file are listed in the table below.

| 46xxsettings.txt Parameter Name | Value Used in Sample Configuration | Description |
|---|---|---|
| **SIP_CONTROLLER_LIST** | 10.64.21.31:5061;transport=tls | Specifies a list of SIP controller designators, separated by commas without any intervening spaces. |
| **SIMULTANEOUS_REGISTRATIONS** | 1 | Specifies the number of Session Managers with which the telephone will simultaneously register. |
| **FAILBACK_POLICY** | auto | When the FAILBACK_POLICY parameter is set to "auto", the phone's active controller will always be the highest priority available controller. |
| **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. |
| **MSGNUM** | 59990 | The number dialed when the Message button is pressed and the phone is in Normal Mode. |
| **PSTN_VM_NUM** | 913035383501 | The number dialed when the Message button is pressed and the phone is in Survivable Mode. |
| **RECOVERYREGISTERWAIT** | 10 | When RECOVERYREGISTERWAIT is set with a value, then phone will retry the monitoring attempt after a randomly selected delay of 50% - 90% of the reactive monitoring interval specified in the RECOVERYREGISTERWAIT |

| 46xxsettings.txt Parameter Name | Value Used in Sample Configuration | Description |
|---|---|---|
| | | parameter. |
| **DISCOVER_AVAYA_ENVIRONMENT** | 1 | Automatically determines if the active SIP Server is an Avaya server or not. |
| **SIPDOMAIN** | avaya.com | The enterprise SIP domain. Must be the same for all SIP controllers in the configuration. SIPDOMAIN is set to "avaya.com" in the sample configuration. |

# 8. Configure Hewlett Packard MSR20-40

This section shows the configuration of the HP MSR20-40 used during compliance testing. Contact Hewlett Packard to customize the configuration per user requirements.

```
******************************************************************************
* Copyright (c) 2010-2012 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<HP>display current configuration
#
 sysname HP
#
 domain default enable system
#
 telnet server enable
#
 dar p2p signature-file cfa0:/p2p_default.mtd
#
 port-security enable
#
vlan 1
#
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
user-group system
 group-attribute allow-guest
#
local-user admin
 password cipher $c$3$Tawg2wM1mDLjSALVzF//AghKX0MZnErM
 authorization-attribute level 3
 service-type telnet
 service-type web
#
cwmp
 undo cwmp enable
#
#
voice-setup
```

```
dtmf time interval 150
dtmf time persist 150
area north-america
cptone country-type US
distinguish-localtalk
#
server-group 1
 hot-swap enable
 address 1 ipv4 10.64.21.31
 address 2 ipv4 10.64.20.35
#
server-group 5
 hot-swap enable
 keepalive options interval 10
 address 1 ipv4 10.64.21.31 port 5060 transport tcp                    (Session Manager)
 address 2 ipv4 10.64.20.35 port 5062                  (HP MSR20-40, defaults to UPD)
#
sip
 source-bind signal ipv4 10.64.20.35
 source-bind media ipv4 10.64.20.35
 sip-domain avaya.com                                                 (sets SIP domain)
 registrar ipv4 10.64.21.31                 (sets Session Manager as primary registrar)
 registrar ipv4 10.64.20.35 port 5062 slave (sets HP MSR20-40 as secondary registrar)
 wildcard-register enable
 privacy asserted
 remote-party-id
 timer session-expires 90
#
sip-server
 mode alive-server
 probe remote-server ipv4 10.64.21.31
 server-bind ipv4 10.64.20.35 port 5062
 server enable
 #
 call-rule-set
  #
   service 0
   rule 0 deny outgoing 1900.......
   rule 1 deny outgoing 91900.......
 #
 srs 0
 #
 trusted-point ipv4 10.64.20.35
 trusted-point ipv4 10.64.21.31
 #
 call-route
```

```
   trunk 0 called-number 5.... ipv4 10.64.20.35
   trunk 1 called-number 1.......... ipv4 10.64.20.35
   trunk 2 called-number 91.......... ipv4 10.64.20.35
  #
  register-user 53113                    (example of SIP user without local authentication)
   number 53113
  #
  register-user 53114
   number 53114
  #
  register-user 53115                    (example of SIP user with local authentication)
   number 53115
   authentication username 53115 password cipher
$c$3$PwfsSd1eBsbCMOKsxroZcZgdinQ+8/Mn1g==
  #
  register-user 53116
   number 53116
   authentication username 53116 password cipher
$c$3$nMF7zBCyKiJ9/Ix/szEDM4+gLyrbkaoPtg==
 #
 dial-program
  default entity fax protocol standard-t38
  default entity fax protocol standard-t38 hb-redundancy 0
  default entity fax protocol standard-t38 lb-redundancy 0
  #
  number-substitute 2000
   rule 0 91.......... 1..........
  #
  number-substitute 3000
   dot-match right-left
   rule 0 ^1732.......$ 91732.......
   rule 1 ^59990$ 913035383509
   rule 2 ^5....$ 913035383501
  #
  entity 1 pots
   line 2/0
   undo register-number
   match-template 53117
  #
  entity 2 pots
   line 2/1
   undo register-number
   match-template 53118
  #
  entity 10000 voip
   address sip server-group 5
 fax baudrate 9600
 description Avaya MSR Survivable
 match-template 5311.
 outband nte
 undo vad-on
 payload-size g729 20
 compression 1st-level  g711ulaw
 compression 3rd-level  g729r8
#
entity 10001 voip
 address sip ip 10.64.21.31 port 5060
 transport tcp
 url sip
 fax baudrate 9600
 description To Avaya
 match-template 5....
 outband nte
 priority 1
 undo vad-on
 payload-size g729 20
 compression 1st-level  g711ulaw
 compression 3rd-level  g729r8
#
entity 16001 voip
 address sip ip 10.64.21.31 port 5060
 transport tcp
 url sip
 description toAvaya303
 match-template 91303.......
 substitute called 2000
#
entity 19000 pots
 line 1/0
 undo register-number
 send-number all
 match-template .T
 priority 5
 substitute called 3000
 undo vad-on
 compression 1st-level  g711ulaw
 compression 2nd-level  g711alaw
 compression 3rd-level  g729r8
#
entity 19001 pots
 line 1/1
 undo register-number
```

```
   send-number all
   match-template .T
   priority 5
   substitute called 3000
   undo vad-on
   compression 1st-level  g711ulaw
   compression 2nd-level  g711alaw
   compression 3rd-level  g729r8
  #
  gw-access-number 53110
   redialtimes 3
   selectlanguage english
 #
 aaa-client
#
subscriber-line1/0
 private-line 53113
 impedance us-non-loaded
#
subscriber-line1/1
 private-line 53110
 impedance us-non-loaded
#
subscriber-line2/0                                              (FXS1 configuration details)
 calling-name MSR FXS1
 timer hookflash-detect 50-1200
 impedance us-non-loaded
 call-forwarding no-reply enable forward-number 59990
 call-forwarding unavailable enable forward-number 59990
 call-hold enable
 call-waiting enable
 call-transfer enable
#
subscriber-line2/1
 calling-name MSR FXS2                                          (FXS2 configuration details)
 timer hookflash-detect 50-1200
 impedance us-non-loaded
 call-forwarding no-reply enable forward-number 59990
 call-forwarding unavailable enable forward-number 59990
 call-hold enable
 call-waiting enable
 call-transfer enable
#
subscriber-line3/0
#
subscriber-line3/1
```

```
#
 ip route-static 0.0.0.0 0.0.0.0 10.64.20.1                    (default gateway for HP MSR20-40)
#
 ssh server enable
#
 load xml-configuration
#
 load tr069-configuration
#
user-interface con 0
user-interface tty 13
user-interface aux 0
user-interface vty 0 4
 authentication-mode scheme
#
return
<HP>
```

# 9. Verification Steps

## 9.1. Verify Registered Users on HP MSR

In Normal Mode, enter the “display voice SIP sip-server register-user all” command on the HP MSR command line to verify no SIP phones at the branch are registered with the HP MSR (note, only stations 53115 and 53116 are configured for the example screens shown below):

```
<HP>display voice sip-server register-user all
user       number                           status    address
-------------------------------------------------------------------------------
53113      53113                            offline
53114      53114                            offline
53115      53115                            offline
53116      53116                            offline
```

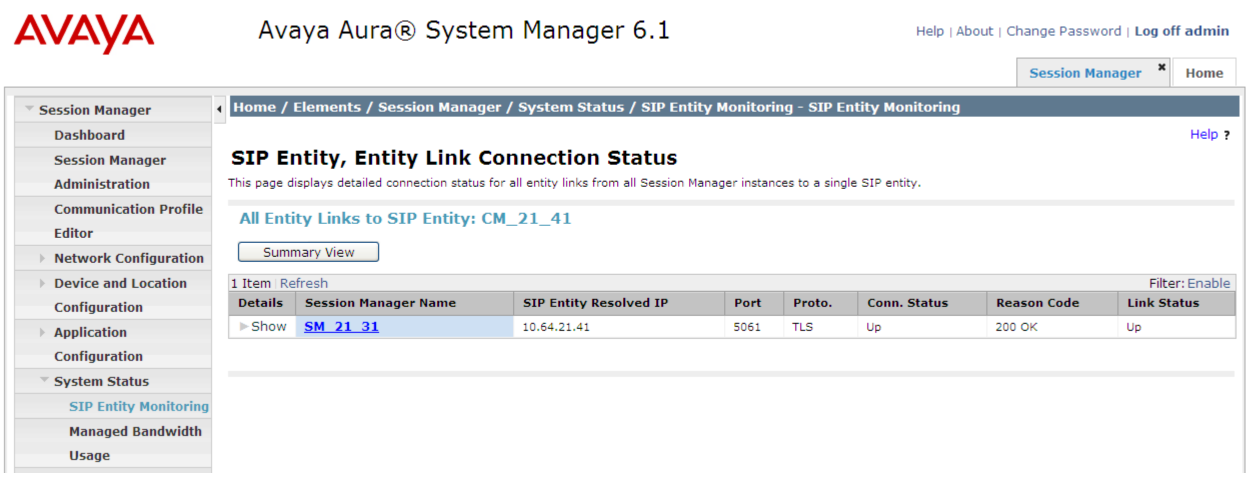
After entering Survivable Mode, enter the command again to verify the SIP phones at the branch are now registered with the HP MSR.

```
<HP>display voice sip-server register-user all
user       number                           status    address
-------------------------------------------------------------------------------
53113      53113                            offline
53114      53114                            offline
53115      53115                            online    10.64.20.17:5060
53116      53116                            online    10.64.20.188:5060
```

## 9.2. Avaya Aura® Session Manager Entity Link Status

The following 2 screens show Session Manager Entity Link statuses for the Entity Links between Session Manager and Communication Manager, and between Session Manager and the HP MSR20-40. The Entity Link status screen can be accessed by navigating to **Elements → Session Manager → System Status → SIP Entity Monitoring** on System Manger. On the *SIP Entity Link Monitoring Status Summary* page, select the relevant SIP Entity from the *All Monitored SIP Entities* list (not shown).

The screen below shows the Entity Link status between Session Manager and Communication Manager:


AVAYA
Avaya Aura® System Manager 6.1
Help | About | Change Password | Log off admin
Session Manager
Home
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
SIP Entity Monitoring
Managed Bandwidth Usage
Home / Elements / Session Manager / System Status / SIP Entity Monitoring - SIP Entity Monitoring
Help ?
Summary View
1 Item | Refresh
Filter: Enable

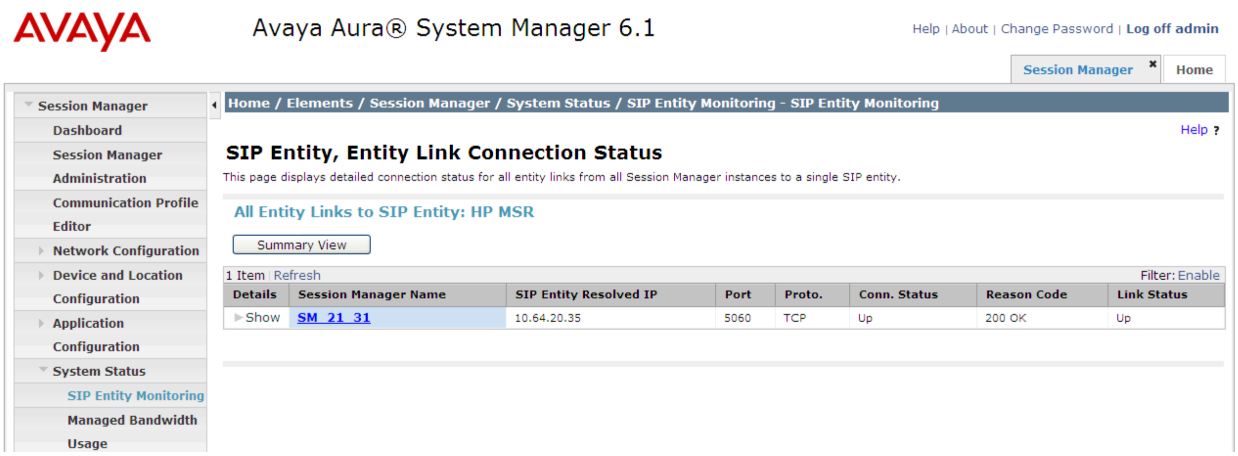
SIP Entity, Entity Link Connection Status

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

All Entity Links to SIP Entity: CM_21_41

| Details | Session Manager Name | SIP Entity Resolved IP | Port | Proto. | Conn. Status | Reason Code | Link Status |
|---|---|---|---|---|---|---|---|
| ▸Show | SM_21_31 | 10.64.21.41 | 5061 | TLS | Up | 200 OK | Up |

The screen below shows the Entity Link status between Session Manager and the HP MSR20-40.


AVAYA
Avaya Aura® System Manager 6.1
Help | About | Change Password | Log off admin
Session Manager
Home
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
SIP Entity Monitoring
Managed Bandwidth Usage
Home / Elements / Session Manager / System Status / SIP Entity Monitoring - SIP Entity Monitoring
Help ?
Summary View
1 Item | Refresh
Filter: Enable

SIP Entity, Entity Link Connection Status

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

All Entity Links to SIP Entity: HP MSR

| Details | Session Manager Name | SIP Entity Resolved IP | Port | Proto. | Conn. Status | Reason Code | Link Status |
|---|---|---|---|---|---|---|---|
| ▸Show | SM_21_31 | 10.64.20.35 | 5060 | TCP | Up | 200 OK | Up |

## 9.3. Verify Basic Calls

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

In the Survivable Mode, make calls between the branch phones; verify that the calls are successful with a two-way talk-path.  Make calls between the PSTN and the branch through the FXO interfaces on the HP MSR20-40. Verify that the calls are successful with a two-way talk-path

# 10. Conclusion

SIP endpoints deployed at remote branch locations risk a loss of service if a break in connectivity to the centralized SIP call control platform occurs. Connectivity loss can be caused by WAN access issues being experienced at the branch or network problems at the centralized site blocking access to the Avaya SIP call control platform. These Application Notes present the configuration steps to implement the Avaya Aura® Session Manager Survivable SIP Gateway Solution using the HP MSR20-40 to minimize service disruption impact to the remote branch SIP endpoints.  All compliance test cases passed successfully with the exceptions/observations noted in **Section 2.2**.

# 11. Additional References

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

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

[2] *Administering Avaya Aura® Session Manager,* Doc ID 03-603324, July 2012.

[3] *Maintaining and Troubleshooting Avaya Aura® Session Manager,* Doc ID 03-603325, November 2011.

[4] *Administering Avaya Aura® Communication Manager*, Doc ID 03-300509, March 2012.

[5] *Avaya one-X™ Deskphone SIP Administrator Guide*, Doc ID 16-603838, February 2011.

[6] *Avaya one-X™ Deskphone SIP for 9600 Series IP Telephones Administrator Guide*, Doc ID 16-601944, November 2010.

HP Networking support and documentation can be found at: http://www.hp.com/networking/supportnav.

[7] *MSR20 Series Datasheets* - http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA3-0761ENW.pdf

[8] *MSR20-1x Series Datasheets* **-** http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA3-0762ENW.pdf

[9] MSR30 Compliance Testing Report - https://devconnect.avaya.com/public/download/dyn/HP_MSR-30.pdf

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.