Avaya Solution & Interoperability Test Lab

Avaya Aura™ Session Manager Survivable SIP Gateway Solution using AudioCodes MP-118 in a Centralized Trunking Configuration – Issue 1.2

Abstract

These Application Notes present a sample configuration of the Avaya Aura™ Session Manager Survivable SIP Gateway Solution using the AudioCodes MP-118 Media Gateway in a Centralized Trunking configuration.

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 main site 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 SIP 9600 Series IP Telephones as well as the AudioCodes SIP Gateway dynamically switch to survivable mode, restoring telephony services to the branch for intra-branch and PSTN calling.

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

1. Introduction

These Application Notes present a sample configuration of the Avaya Aura™ Session Manager Survivable SIP Gateway Solution using the AudioCodes MP-118 Media Gateway in a Centralized Trunking scenario.

SIP endpoints deployed at remote branch locations risk a loss of service if a break in connectivity to the centralized SIP call control platform (Session Manager) occurs. 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 Session Manager going out of service. The survivable SIP gateway solution monitors connectivity health from the remote branch to the centralized Avaya SIP call control platform. When connectivity loss is detected, SIP endpoint and SIP gateway components within the branch dynamically switch to survivable mode restoring basic telephony services to the branch. When connectivity from the branch to the centralized Avaya SIP call control platform is restored, SIP components dynamically switch back to normal operation.

The primary components of this solution are the Avaya one-X Deskphone SIP 9600 Series IP Telephones and the AudioCodes SIP Media Gateways models MP-114 and MP-118 as well as Session Manager 5.2 which provides the centralized SIP control platform with SIP registrar and proxy functions. The sample configuration presented in these Application Notes utilizes the AudioCodes SIP Media Gateway model MP-118. Although not tested, these configuration steps can also be applied to the AudioCodes SIP Media Gateway model MP-114 using the AudioCodes firmware version specified in **Section 3**.

1.1. Interoperability Testing

The interoperability testing focused on the dynamic switch from the Normal Mode (where the network connectivity between the main site and the branch site is intact) to the 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 AudioCodes SIP Media Gateway in the Survivable Mode.

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

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 main site or at the branch sites, register to the Session Manager (the branch phones will failover to register with the AudioCodes MP-118 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.

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

1.1.2. AudioCodes SIP Media Gateway

The AudioCodes SIP Media Gateway MP-118, referred to as AudioCodes MP-118 throughout the remainder of this document, takes on various roles based on call flows and network conditions. The following lists these roles:

- SIP PSTN Media Gateway (FXO 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 centralized SIP control platform)

Note: AudioCodes labels the Survivable SIP Registrar and Proxy functionality of the MP-118 as Stand-Alone Survivability (SAS). SAS will be used throughout these Application Notes.

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

The Avaya one-X Deskphone SIP 9600 Series IP Telephone, referred to as Avaya 9600 SIP Phone throughout the remainder of this document, is a key component of the survivable SIP gateway solution. The 2.5.5.11 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 AudioCodes MP-118 as an alternate or survivable SIP server. See reference [7] for additional information on the Avaya 9600 SIP Phone.

1.1.4. 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 AudioCodes MP-118 SIP gateway with SAS 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.

1.1.5. PSTN Trunking Configurations

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 the analog trunks from the Service Provider connected to the FXO interface ports on the local AudioCodes MP-118 branch gateway.

Distributed Trunking: Outgoing PSTN call routing can be determined by the originating source location using Communication Manager Location Based Routing. Local calls from branch locations can be routed back to the same branch location and terminate on the FXO interface of the local AudioCodes MP-118 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 Centralized Trunking configuration. The sample configuration of the Session Manager Survivable SIP Gateway Solution in a Distributed Trunking configuration is described in a separate Application Notes document.

1.2. Support

For technical support for the AudioCodes MP-118 Media Gateway, contact AudioCodes via the support link at http://www.audiocodes.com/support. In case of existing support agreement please use iSupport system at https://crm.audiocodes.com/OA_HTML/jtflogin.jsp.

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

2. 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 distributed branch locations all inter-connected over a corporate WAN. While three branch locations have been included in the sample network, Branch 2 configurations are highlighted and documented in ensuing sections of these Application Notes.

The Headquarters location hosts a Session Manager (with its companion System Manager) providing enterprise-wide SIP call control, and a Communication Manager as a Feature Server providing advanced feature capabilities to Avaya 9600 SIP Phones. The Communication Manager runs inside an Avaya G-Series Media Gateway with PSTN trunks. The Avaya Aura™ Communication Manager Messaging is running co-resident with the Communication Manager to provide Voice Mail functionality[2] (Avaya Modular Messaging is also configured and tested in the sample configuration). The Headquarters location also hosts an Avaya IP Phone Configuration File Server for Avaya 9600 SIP Phones to download configuration information. The Session Manager is connected to the 10.1.2.0/24 subnet; the Communication Manager and the phone configuration file server are connected to the 10.32.2.0/24 subnet; the Avaya 9600 SIP Phones are connected to the 10.32.1.0/24 subnet.

The configuration details of the phone configuration file server, the Communication Manager Messaging application as well as Avaya Modular Messaging are considered out of scope of these Application Notes and therefore not included.

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

The branch locations consist of two Avaya 9600 SIP Phones, an AudioCodes MP-118 SIP Media Gateway with a PSTN Analog trunk on the FXO interface and two analog phones on the FXS interfaces. A flat network has been implemented at each branch.

---

[2] The voice messaging system is used in the test configuration to test voice mail access and MWI (Messaging Wait Indicator) on Avaya 9600 SIP Phones in both Normal Mode and Survivable Mode. Any compatible messaging system can be used to satisfy this test purpose, e.g., Avaya Modular Messaging can be used in the test configuration instead of Communication Manager Messaging.

Note that the Communication Manger serves as a Feature Server in the test configuration. As such, it does not support inter-working between SIP phones and non-SIP phones (H.323 and other Avaya digital and/or analog telephone sets) directly configured on the same Communication Manager[3]. This restriction will be lifted in future releases of Session Manager and Communication Manager. In the sample configuration, all phones at both the main and branch sites are SIP phones (branch analog sets are adapted by the AudioCodes MP-118 as SIP phones too).

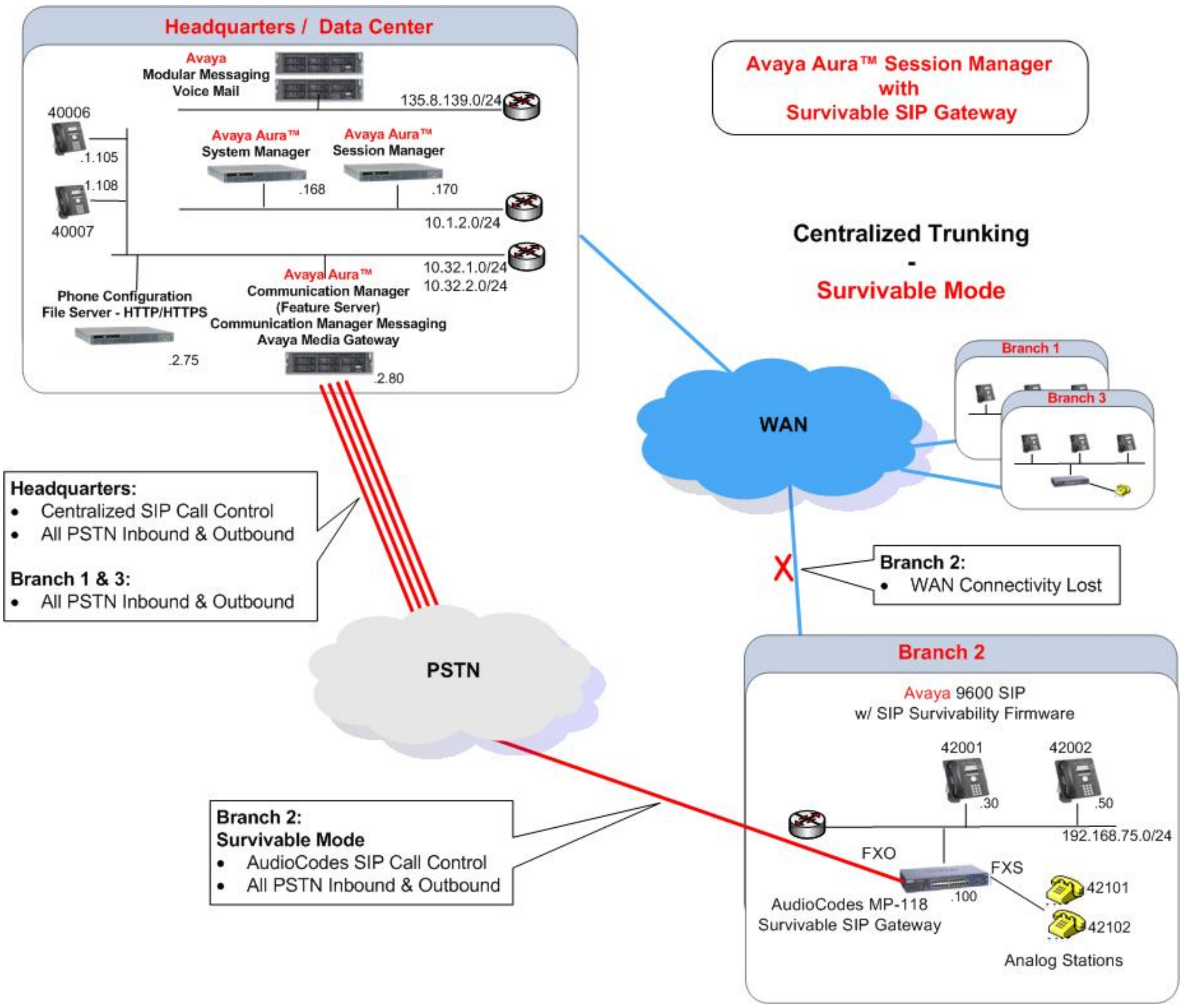


Figure 1 – Network Diagram

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

3. Components Validated

The following components were used for the sample configuration:

Component	Software/Firmware
Avaya Aura™ Session Manager	R5.2.0.1.520017
Avaya Aura™ System Manager	R5.2.0.1.5.520017
Avaya Aura™ Communication Manager (Feature Server)	5.2.1 (R015x.02.1.016.4)
Avaya Aura™ Communication Manager Messaging	Release 5.2
Avaya Modular Messaging	V5.2 with Patch 8 (9.2.15013)
Avaya 9600 Series IP Telephones Models: 9620 and 9630	Avaya one-X™ Deskphone Edition SIP 2.5.0
Avaya 6210 Analog Telephone	-
HTTPS/HTTP Phone Configuration File Server	Windows Server 2003 SP2
AudioCodes MP-118 FXS-FXO [4]	5.80A.019.003

Table 3 – Software/Hardware Version Information

[4] Although not tested, the AudioCodes MP-114 gateway can be used in the sample configuration presented in these Application Notes. The MP112 was not specifically tested. However for the functions it can perform, Avaya will support it in place of the MP-118 shown and tested in this document because the MP112 software is the same as MP-118. Please note the MP-112 has no FXO interfaces so this function is not supported on the MP-112.

4. Configure Communication Manager

This section shows the necessary steps to configure Communication Manager to support the survivable SIP gateway solution in a Centralized Trunking scenario. It is assumed that the basic configuration on Communication Manager, the required licensing, the configuration for connection to PSTN through the T1/E1 interface as well as the configuration required for accessing Communication Manager 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 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
- IP codec set
- IP network map and IP network regions
- Stations
- SIP signaling group and trunk group
- Route pattern
- Private numbering
- Automatic Alternate Routing (AAR)

4.1. 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: 800   100
           Maximum Concurrently Registered IP Stations: 18000 1
             Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
              Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 0     0
                  Maximum Video Capable H.323 Stations: 0     0
                   Maximum Video Capable IP Softphones: 0     0
                       Maximum Administered SIP Trunks: 800   252
  Maximum Administered Ad-hoc Video Conferencing Ports: 0     0
   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                             Maximum TN2501 VAL Boards: 10    1
                     Maximum Media Gateway VAL Sources: 0     0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   2
   Maximum Number of Expanded Meet-me Conference Ports: 0     0
```

4.2. Configure System Parameters Features

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

Note 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 or Class Of Service levels. Refer to the appropriate documentation in the **References** section for more details.

```
display system-parameters features                    Page   1 of  18
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? y
                                    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

   Maximum Number of Expanded Meet-me Conference Ports: 0     0
```

4.3. Configure IP Node Names

Use the "change node-names ip" command to add an entry for the Session Manager that the Communication Manager will connect to. The **Name** "sm1" and **IP Address** "10.1.2.170" are entered for the Session Manager Security Module (SM-100) interface. The configured node-name "sm1" will be used later on in the SIP Signaling Group administration (**Section 4.7.1**).

```
change node-names ip                                              Page   1 of   2
                                  IP NODE NAMES
    Name               IP Address
default               0.0.0.0
msgserver             10.32.2.90
procr                 10.32.2.80
sm1                   10.1.2.170
```

4.4. Configure IP Codec Set

Configure the IP codec set to use for SIP calls. Use the "change ip-codec-set n" command, where "n" is the codec set number to be used for interoperability. Enter the desired audio codec type in the **Audio Codec** field. Retain the default values for the remaining fields. The "G.711MU" codec was used in the test configuration.

```
display 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:
```

4.5. Configure IP Network Map and IP Network Regions

An IP address map can be used for network region assignment. The following screen illustrates a subset of the IP network map configuration used to verify these Application Notes. Branch 2 has IP Addresses in 192.168.75.0/24 assigned to network region 12. The Headquarters location has IP Addresses in 10.32.1.0/24 (for phones), 10.32.2.0/24 (for servers) and 10.1.2.0/24 (where Session Manager is assigned) configured to network region 1. Although not illustrated in these Application Notes, network region assignment can be used to vary behaviors within and between regions.

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

                                                Subnet Network      Emergency
 IP Address                                     Bits   Region VLAN Location Ext
 --------------------------------------------- ------ ------ ---- -------------
 FROM: 10.1.2.0                                 /24    1      n
   TO: 10.1.2.255
 FROM: 10.32.1.0                                /24    1      n
   TO: 10.32.1.255
 FROM: 10.32.2.0                                /24    1      n
   TO: 10.32.2.255
 FROM: 192.168.75.0                             /24    12     n
   TO: 192.168.75.255
```

Although not unique to the AudioCodes equipped branch, the following screens illustrate relevant aspects of the network region configuration used to verify these Application Notes. The **Authoritative Domain** "avaya.com" matches the SIP domain configured in the Session Manager as well as the AudioCodes gateway. The **Codec Set** for intra-region calls is set to the codec set 1 as configured in the previous step, which specifies "G.711MU". The **IP-IP Direct Audio** parameters retain the default "yes" allowing direct IP media paths both within the region, and between regions. For example, a call between two telephones at the branch will not consume bandwidth on the WAN, since the media path for a connected call will be local to the branch (i.e., directly between two SIP telephones, or from one SIP telephone to the AudioCodes gateway for a call involving an FXS station and a SIP telephone at the branch).

```
display ip-network-region 12                                     Page   1 of  19
                               IP NETWORK REGION
  Region: 12
Location:           Authoritative Domain: avaya.com
    Name: Branch 2
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                      RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

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.

```
display 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
 14
 15
```

The ip-network-region form for network region 1 is similarly configured (not shown). Network region 1 is for phones and servers as well as Session Manager at the main location as defined in the ip-network-map at the beginning of this section.

4.6. Add Stations

A station must be created on Communication Manager for each SIP User account to be created in Session Manager which includes a provisioned Communication Manager Extension. The extension assigned to the Communication Manager station must match the Communication Manager Extension assignment in Session Manager (see **Section 5.8**).

Use the "add station" command to add a station to Communication Manager. The "add station" command for an Avaya 9620 SIP Phone located at Branch 2 assigned to extension 42001 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 42001                                            Page   1 of   6
                                     STATION

Extension: 42001                        Lock Messages? n             BCC: 0
     Type: 9620SIP                      Security Code:                TN: 1
     Port:                            Coverage Path 1: 1             COR: 1
     Name: AC-Surv-BR21-LD            Coverage Path 2:               COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
              Loss Group: 19
                                                Message Lamp Ext: 42001

        Display Language: english

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

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

```
add station 42001                                            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 "9600SIP" should be used for the branch analog stations.

After all the stations have been added, use the "list off-pbx-telephone station-mapping" command to verify that all the stations have been automatically designated as OPS (Off-PBX Station) sets. In the screen shown below, extensions 40006 and 40007 are SIP phones at the main site; externsions 42001 and 42002 are SIP phones at Branch 2; extensions 42101 and 42102 are analog phones at Branch 2.

```
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

40006          OPS        40006            1  /   aar     both         all
40007          OPS        40007            1  /   aar     both         all
42001          OPS        42001            1  /   aar     both         all
42002          OPS        42002            1  /   aar     both         all
42101          OPS        42101            1  /   aar     both         all
42102          OPS        42102            1  /   aar     both         all
```

4.7. Configure SIP Signaling Group and Trunk Group

4.7.1. 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**: “tls”
- **IMS Enabled?**: “y”
- **Near-end Node Name**: “procr” node name from **Section 4.3**
- **Far-end Node Name**: “sm1” Session Manager node name from **Section 4.3**
- **Near-end Listen Port**: “5061”
- **Far-end Listen Port**: “5061”
- **Far-end Network Region**: Network region number “1” from **Section 4.5**
- **Far-end Domain**: SIP domain name from **Section 4.5** and **Section 5.1**
- **DTMF over IP**: “rtp-payload”

```
add signaling-group 42
                                SIGNALING GROUP

 Group Number: 42             Group Type: sip
                        Transport Method: tls
  IMS Enabled? y





   Near-end Node Name: procr                  Far-end Node Name: sm1
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         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
```

4.7.2. 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 as configured in **Section 4.7.1**
- **Number of Members**: Equal to the maximum number of concurrent calls supported

```
add trunk-group 42                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 42                   Group Type: sip          CDR Reports: y
  Group Name: SIP endpoints               COR: 1        TN: 1        TAC: *142
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                    Signaling Group: 42
                                                  Number of Members: 20
```

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

```
add trunk-group 42                                           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 "127" for the **Telephone Event Payload Type** field. This setting must match the configuration on AudioCodes MP-118 (see **Section 7.6**). Use default values for all other fields.

```
add trunk-group 42                                             Page   4 of  21
                              PROTOCOL VARIATIONS

                      Mark Users as Phone? n
            Prepend '+' to Calling Number? n
      Send Transferring Party Information? y

                    Send Diversion Header? n
                  Support Request History? y
             Telephone Event Payload Type: 127
```

4.8. 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.
- **Grp No**: The trunk group number from **Section 4.7.2**
- **FRL**: Facility Restriction Level that allows access to this trunk, "0" being least restrictive

```
change route-pattern 42                                           Page   1 of   3
                    Pattern Number: 42  Pattern Name: URE SIP Trunk
                             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: 42   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
```

4.9. Configure Private Numbering

Use the "change private-numbering 0" command to define the calling party number to be sent. Add an entry for the trunk group defined in **Section 4.7.2**. In the example shown below, all calls originating from a 5-digit extension beginning with 4 and routed to trunk group 42 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  4                                            5     Total Administered: 1
                                                          Maximum Entries: 540
```

4.10. Configure AAR

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

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

```
change aar analysis 4                                         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
    4                     5    5      42        aar           n
    49998                 5    5      32        aar           n
    50000                 5    5      1         aar           n
    55000                 5    5      2         aar           n
    7                     7    7      254       aar           n
    8                     7    7      254       aar           n
    9                     7    7      254       aar           n
                                                              n
                                                              n
                                                              n
                                                              n
                                                              n
                                                              n
                                                              n
                                                              n
```

5. Configure 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.

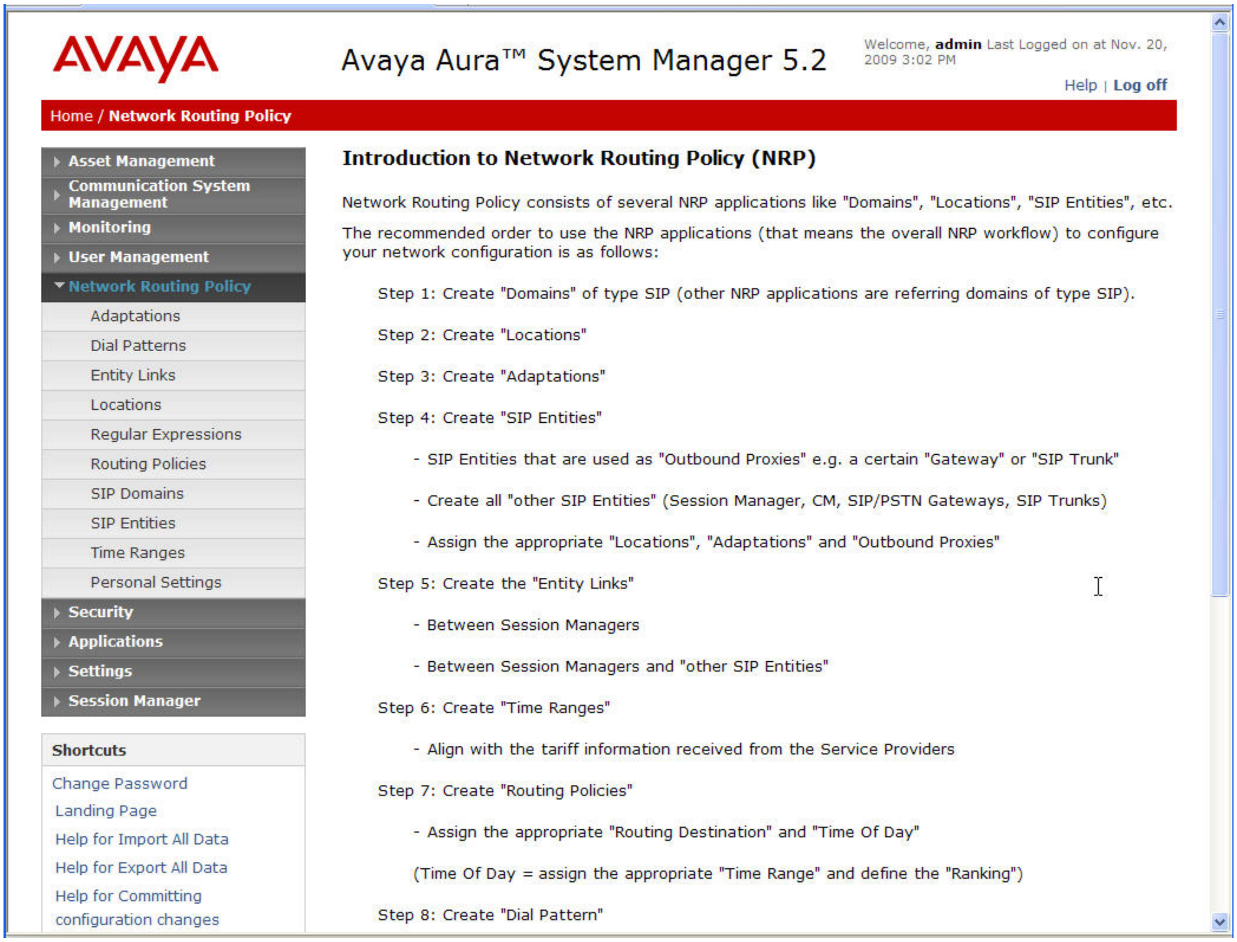
The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

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 10.1.2.170 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 10.1.2.171. 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 [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 5.1** through **5.4**).

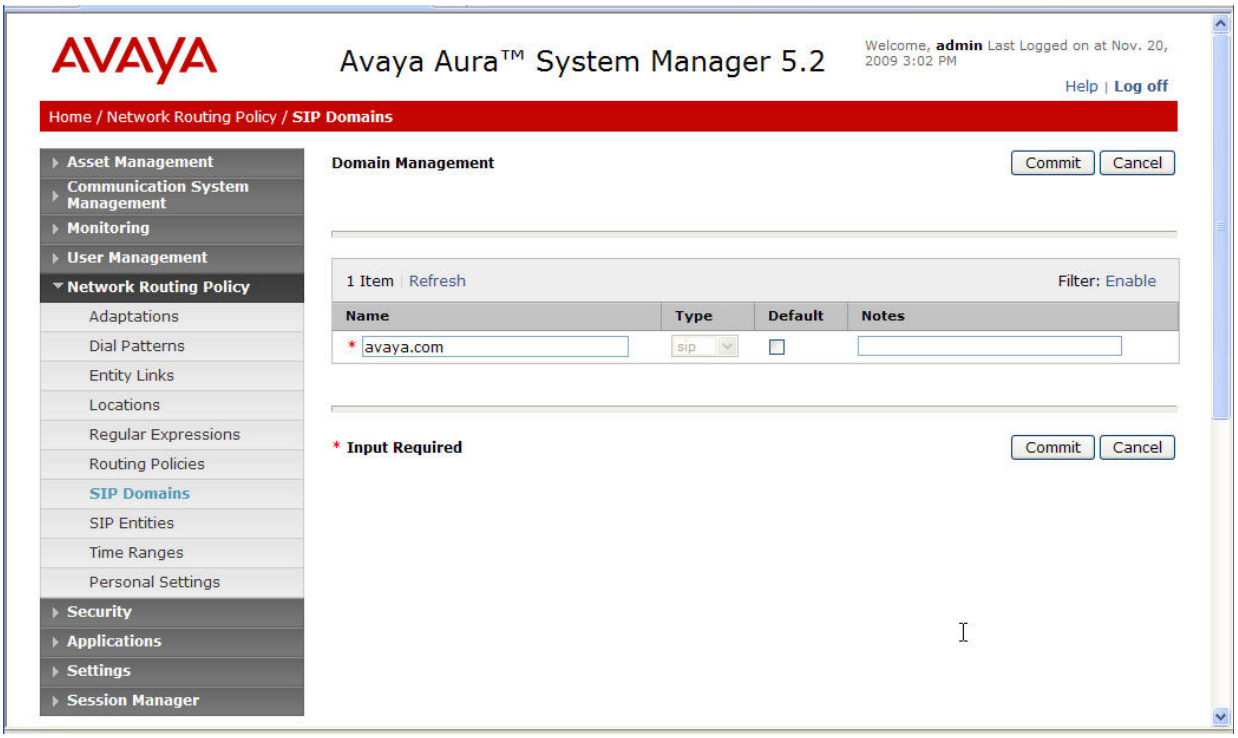

AVAYA
Avaya Aura™ System Manager 5.2
Welcome, admin Last Logged on at Nov. 20, 2009 3:02 PM
Help | Log off
Home / Network Routing Policy
Asset Management
Communication System Management
Monitoring
User Management
Network Routing Policy
Adaptations
Dial Patterns
Entity Links
Locations
Regular Expressions
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"

5.1. Specify SIP Domain

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

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

Click **Commit**.



5.2. Add Location

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:

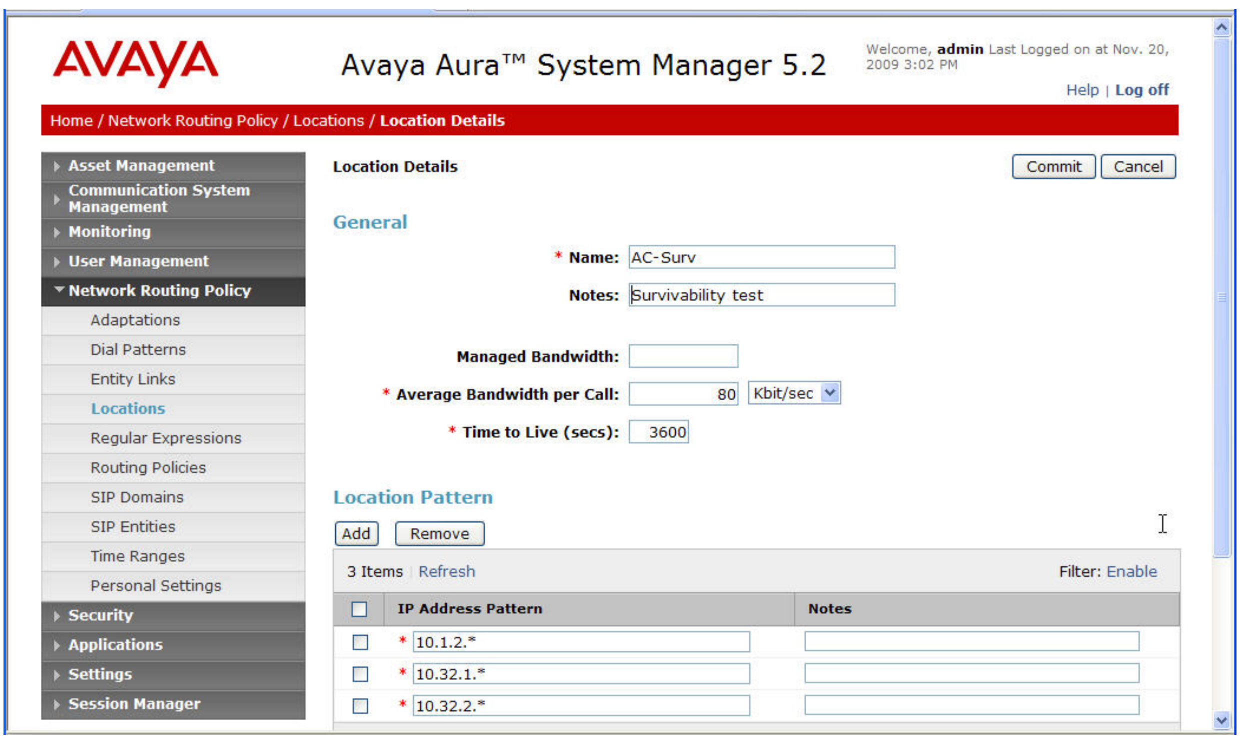
- **Name**: A descriptive name
- **Notes**: Descriptive text (optional)

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 addition of the "AC-Surv" location, which includes Session Manager (10.1.2 subnet), Communication Manager (10.32.2 subnet), and all SIP telephones located at this location (10.32.1 subnet). Click **Commit** to save the Location definition.



5.3. 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 and the Communications Manager.

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

Under *General*:

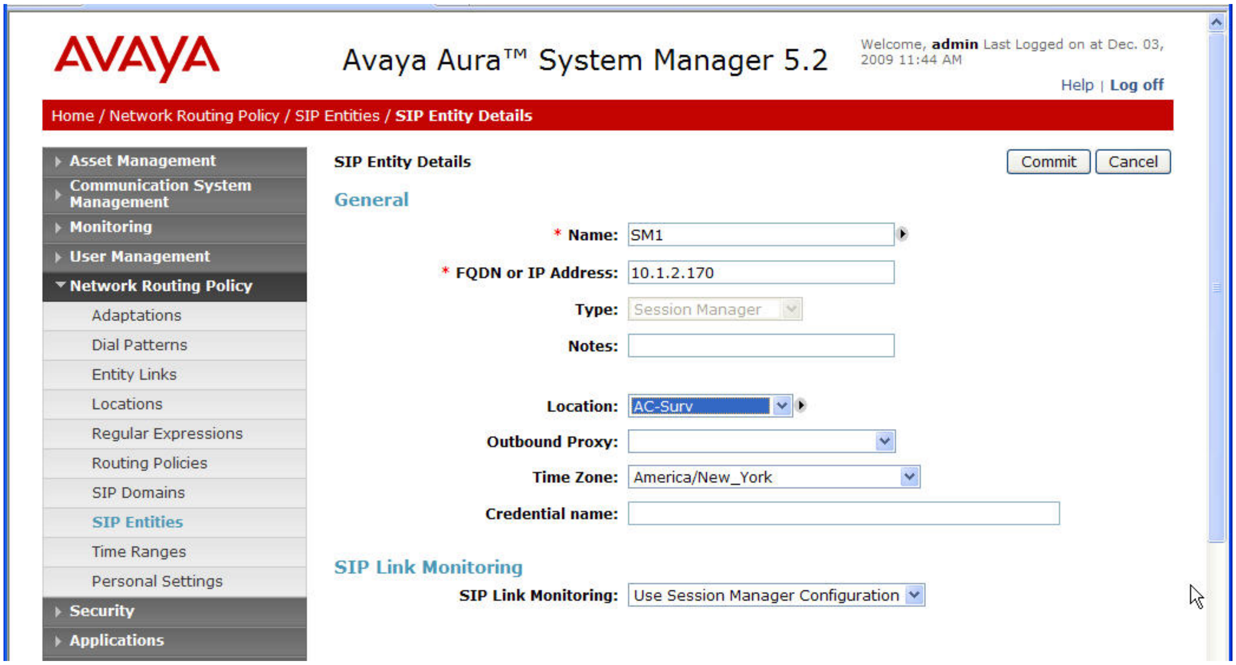
- **Name** A descriptive name
- **FQDN or IP Address**: FQDN or IP address of the Session Manager or the signaling interface on the telephony system
- **Type**: "Session Manager" for Session Manager, "CM" for Communication Manager
- **Adaptation**: Leave blank
- **Location:** Select the Location created previously
- **Time Zone:** Select the proper time zone for this installation

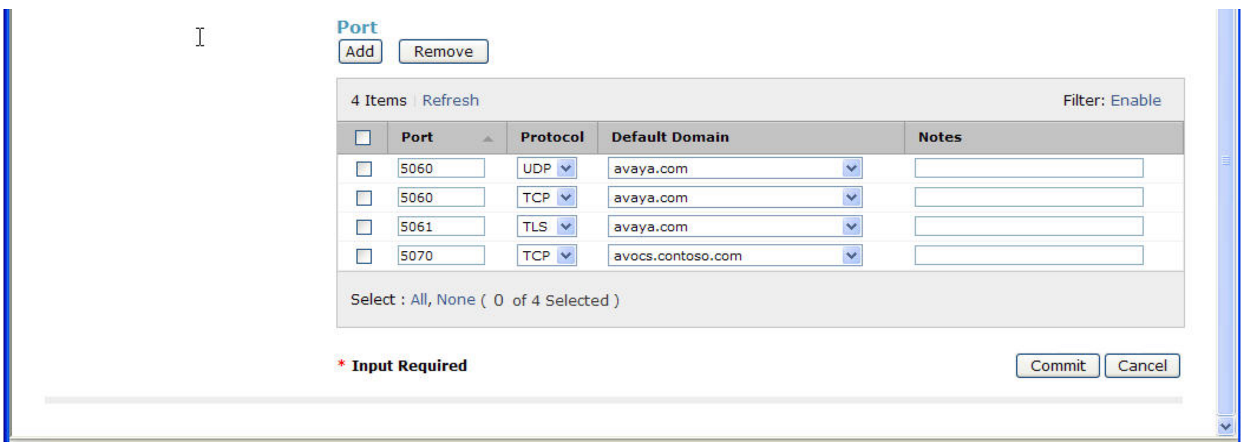
Under *Port* (for adding Session Manager Entity only), click **Add**, then edit the fields in the resulting new row as shown below:

- **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.

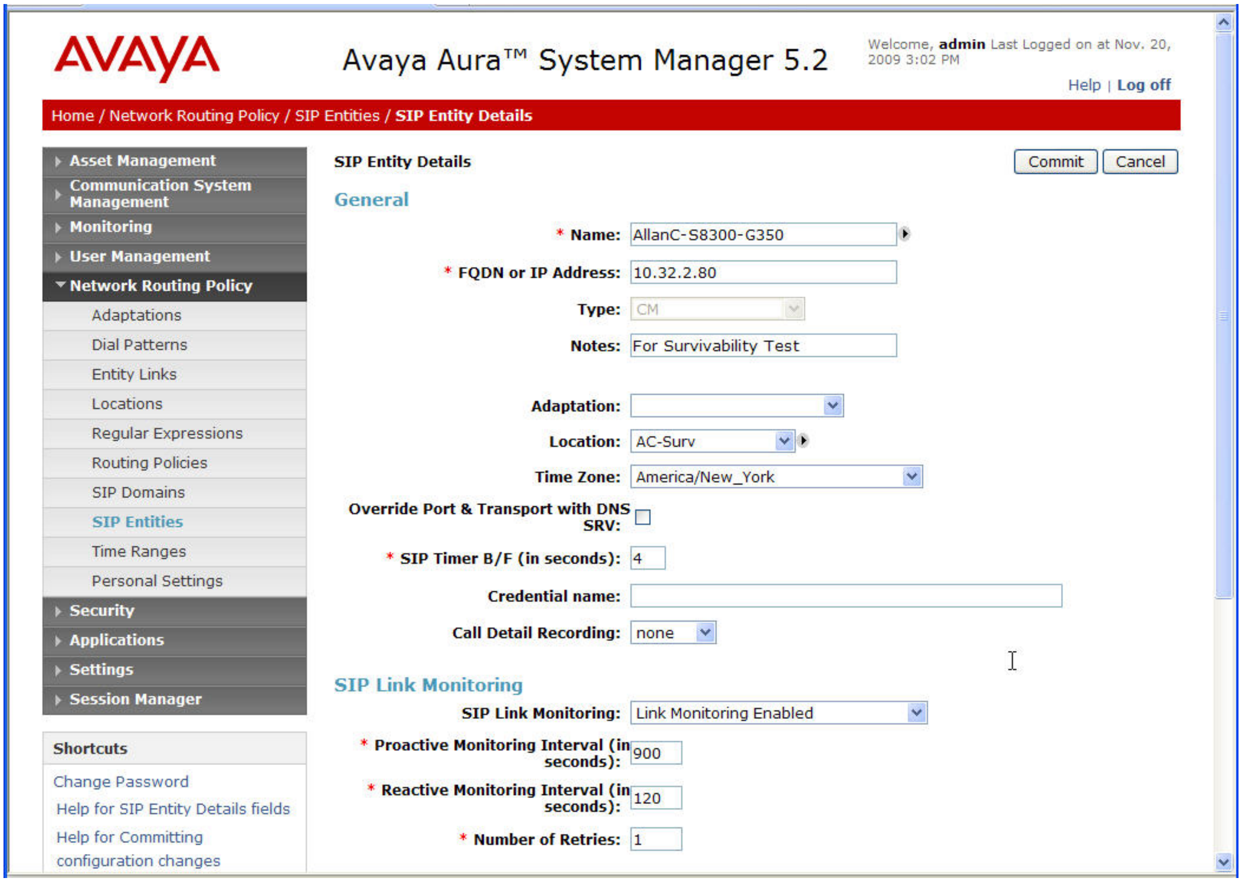
Default settings can be used for the remaining fields. Click **Commit** to save the SIP Entity definition.

The following screens show addition of Session Manager. The IP address of the SM-100 Security Module is entered for **FQDN or IP Address**. TLS port 5061 is used for communication with Communication Manager.


AVAYA
Avaya Aura™ System Manager 5.2
Welcome, admin Last Logged on at Dec. 03, 2009 11:44 AM
Help | Log off
Home / Network Routing Policy / SIP Entities / SIP Entity Details
Asset Management
Communication System Management
Monitoring
User Management
Network Routing Policy
Adaptations
Dial Patterns
Entity Links
Locations
Regular Expressions
Routing Policies
SIP Domains
SIP Entities
Time Ranges
Personal Settings
Security
Applications
SIP Entity Details
Commit
Cancel
General
* Name: SM1
* FQDN or IP Address: 10.1.2.170
Type: Session Manager
Notes:
Location: AC-Surv
Outbound Proxy:
Time Zone: America/New_York
Credential name:
SIP Link Monitoring
SIP Link Monitoring: Use Session Manager Configuration


Port
Add
Remove
4 Items | Refresh
Filter: Enable
Port
Protocol
Default Domain
Notes
5060 UDP avaya.com
5060 TCP avaya.com
5061 TLS avaya.com
5070 TCP avocs.contoso.com
Select : All, None (0 of 4 Selected)
* Input Required
Commit
Cancel

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 G350 Media Gateway has its signaling interface integrated into the Communication Manager processor. For other Avaya Media Gateways (e.g., G450 and G650), the IP address of the C-LAN board in the Media Gateway should be specified. Note the "CM" selection for **Type**.

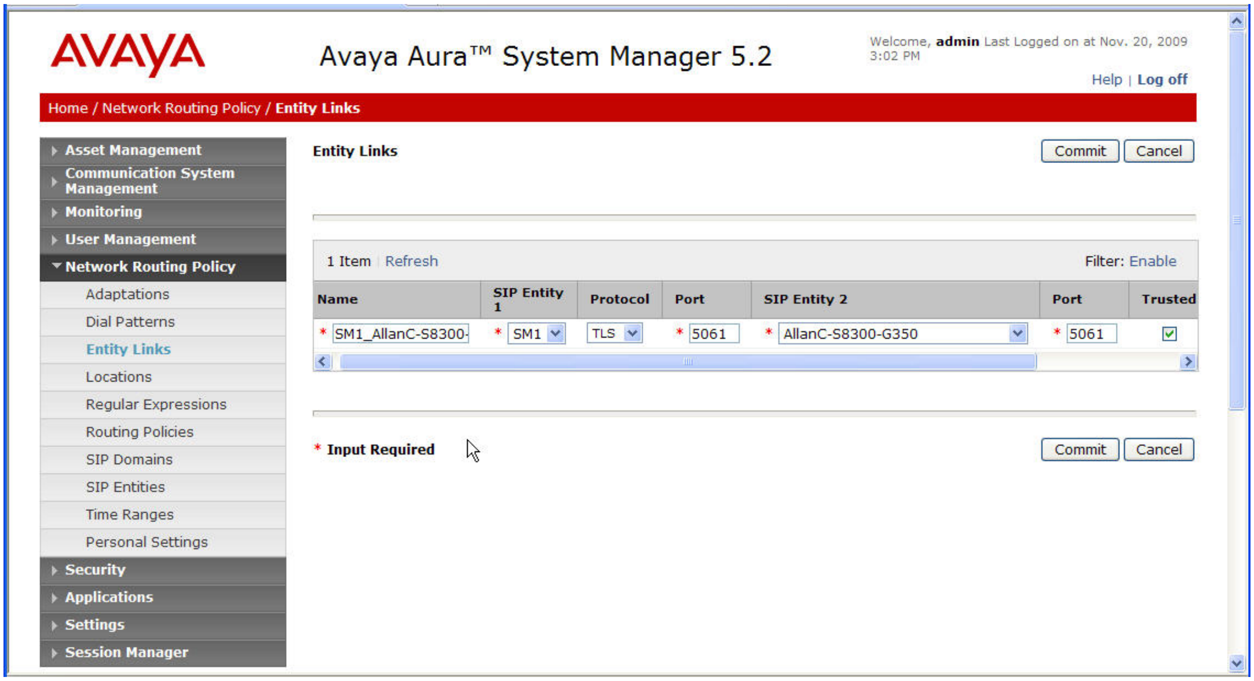


5.4. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity link. In the sample configuration, one Entity Links was created between Session Manager and Communication Manger. To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

- **Name**: A descriptive name
- **SIP Entity 1**: Select the Session Manager SIP Entity
- **Protocol**: Select "TLS"
- **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.



5.5. 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 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):

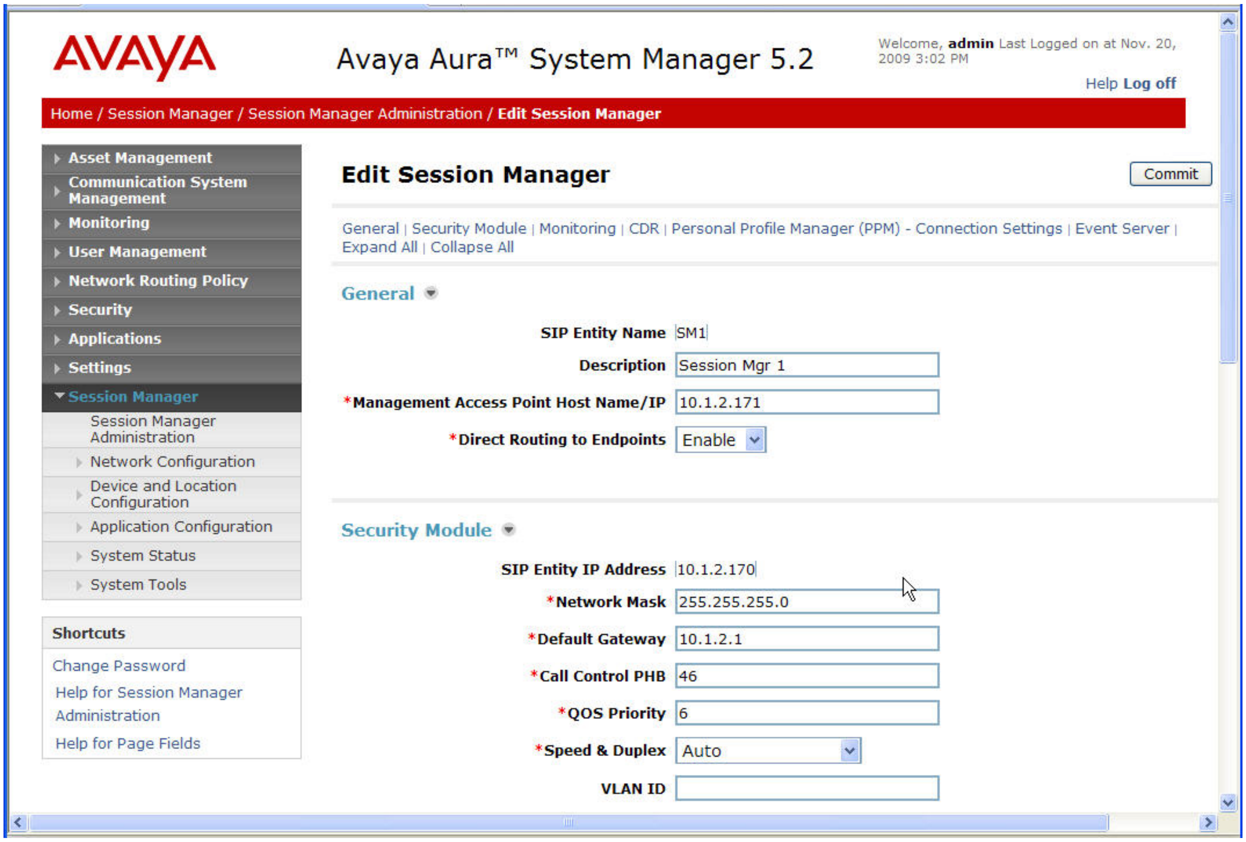
Under *General*:

- **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.

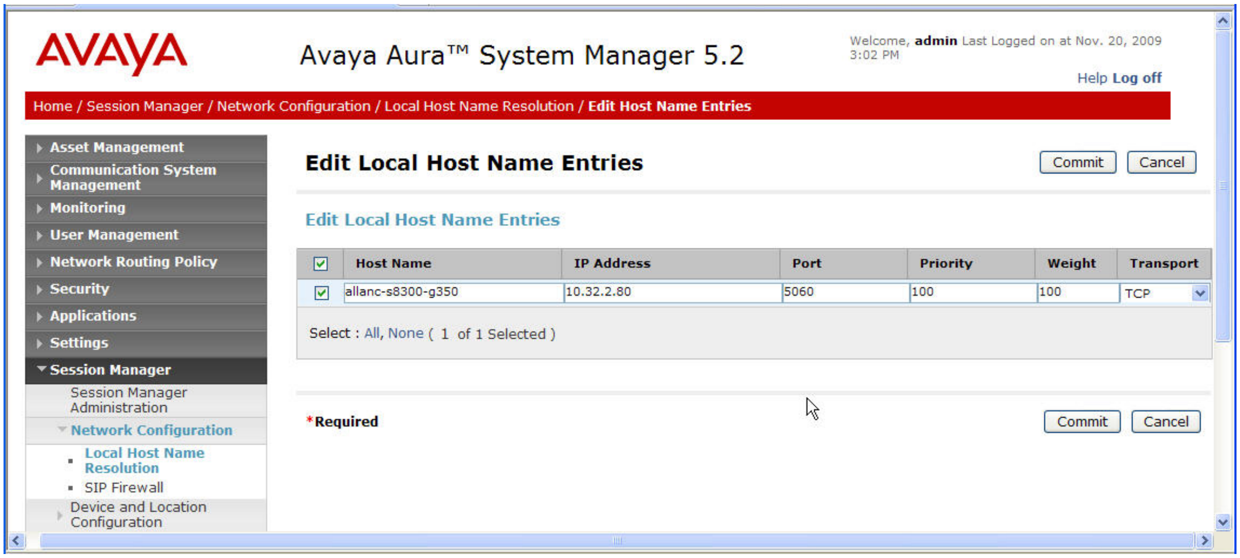


5.6. Define Local Host Name Resolution

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
- **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 entry used in the sample configuration.



5.7. Add Communication Manger as a Feature Server

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

Step 1

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

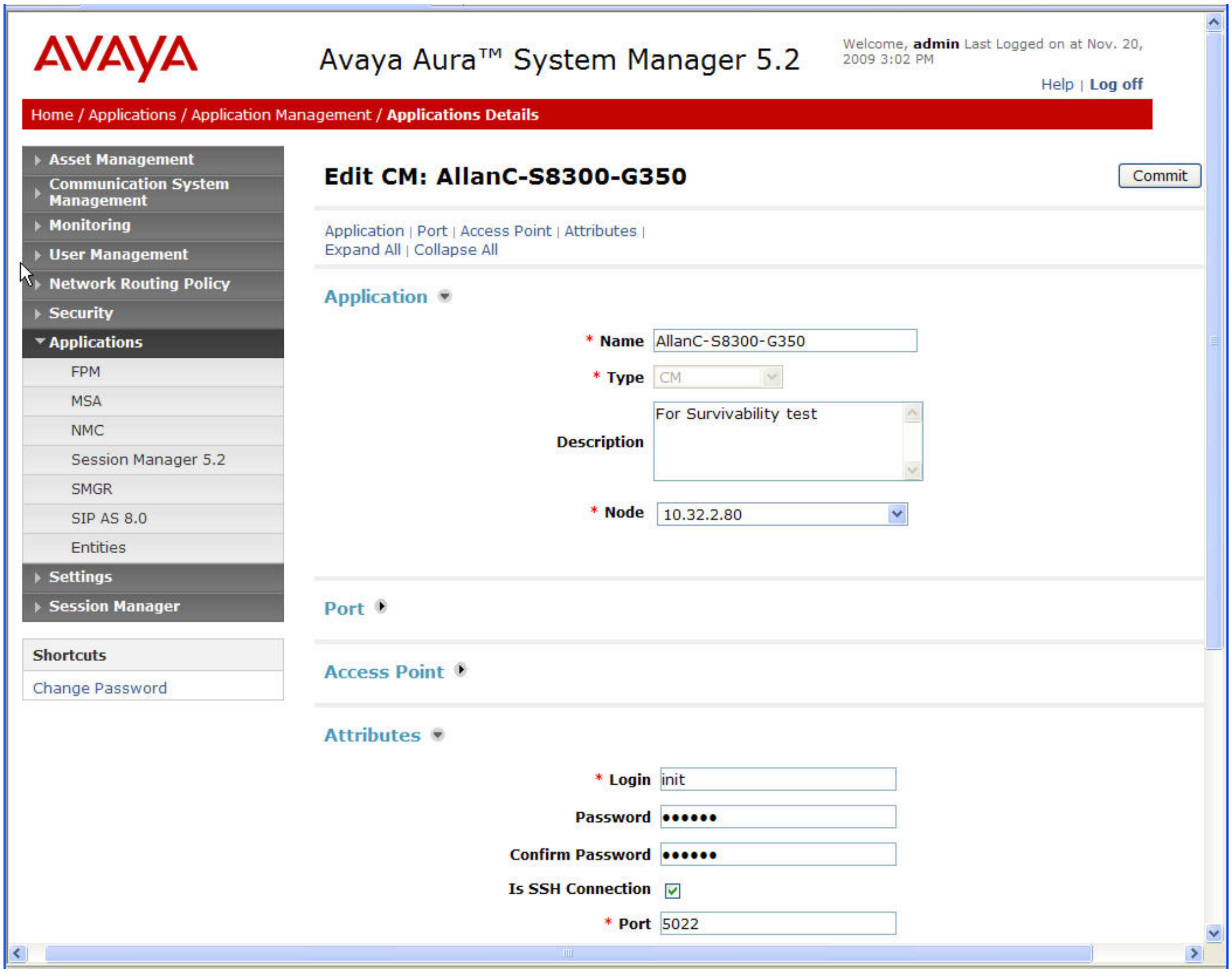
- **Name**: A descriptive name
- **Type**: Select "CM"
- **Node**: Select "Other.." and enter IP address for Communication Manager SAT access

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.



Step 2

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

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

Click on **Commit**.

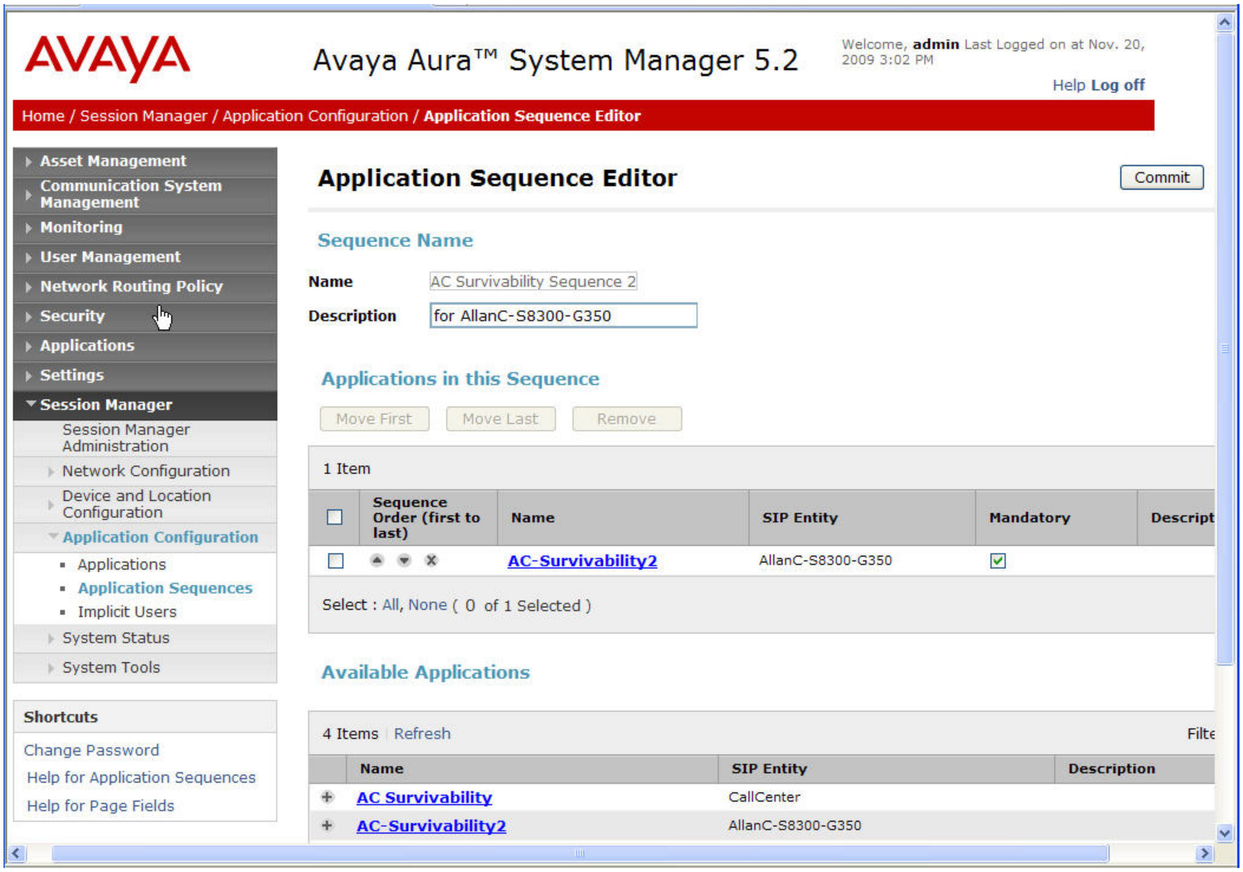
The screen shown below is the Edit screen since the Application has already been configured.

Step 3

Select **Session Manager → Application Configuration → Application Sequences** on the left. Click on **New** (not shown). Enter a descriptive Name. Click on the "+" sign next to the appropriate *Available Applications*, and the selected available application will be moved up to the *Applications in this Sequence* section. In this sample configuration, "AC-Survivability2" was selected, as shown in the screen below (which is the Edit screen since the Application Sequence has already been configured).

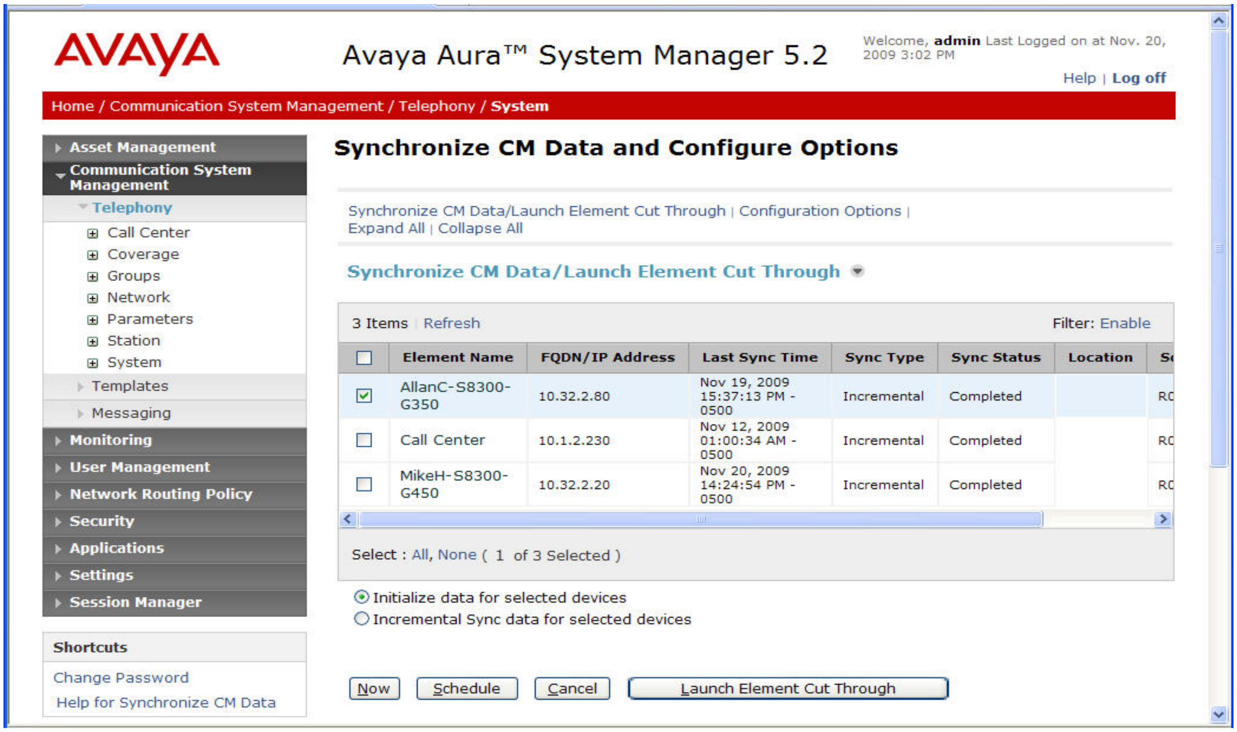
Click on **Commit**.

Note that the entry "AC-Survivability" listed in the screen was not used in the sample configuration. It was set up for other purposes.

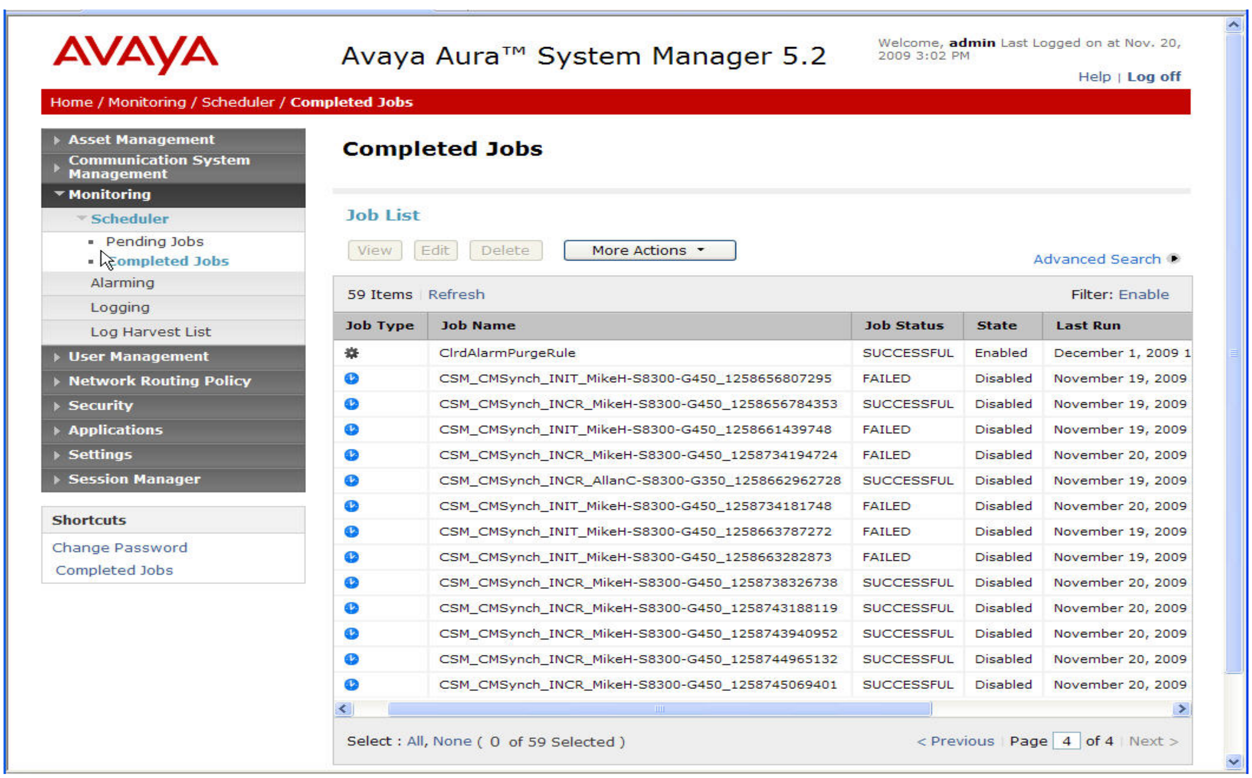


Step 4

Select **Communication System Management → Telephony** on the left. Select the appropriate Element Name ("AllanC-S8300-G350" in this case). Select **Initialize data for selected devices**. Then click on **Now**. This will cause a data synchronization task to start. This may take some time to complete.

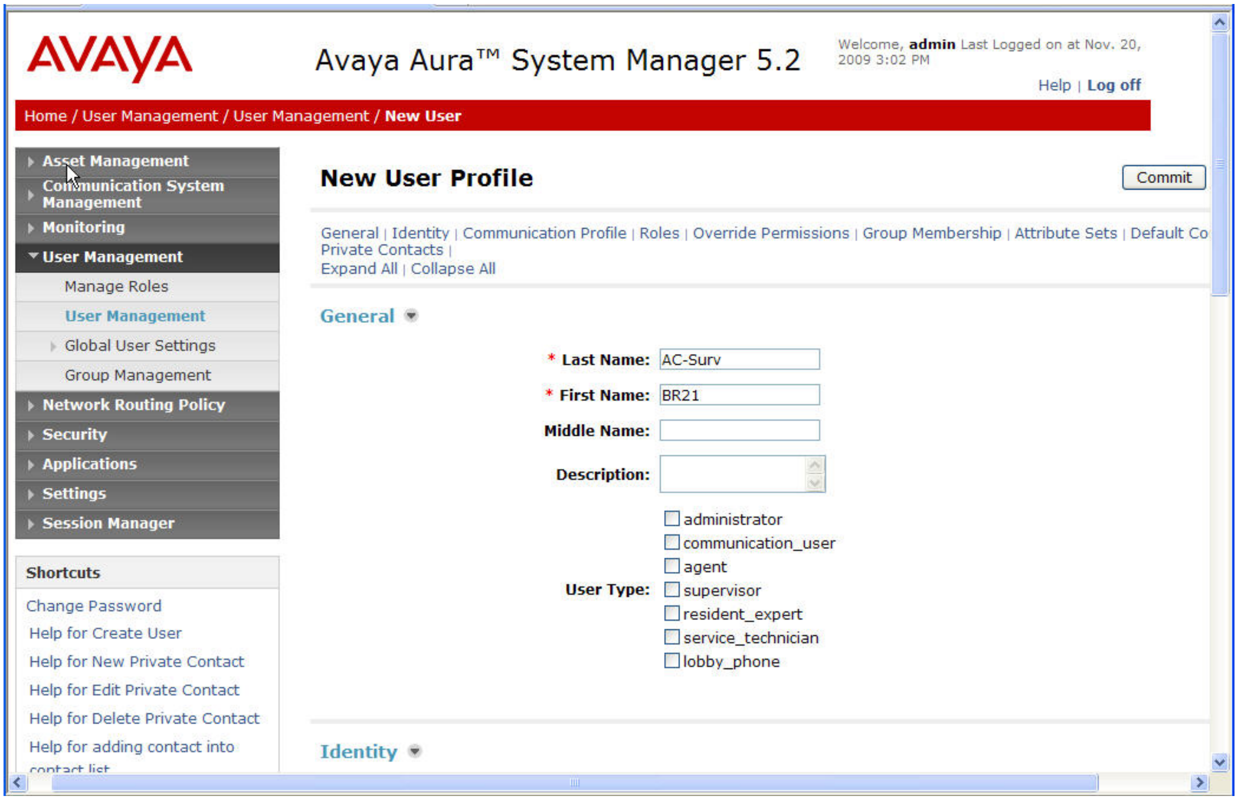


Use the menus on the left under **Monitoring → Scheduler → Completed Jobs** to determine when the task has completed, as shown below (see entry with embedded Communication Manager name - "AllanC-S8300-G350" for the sample configuration) .



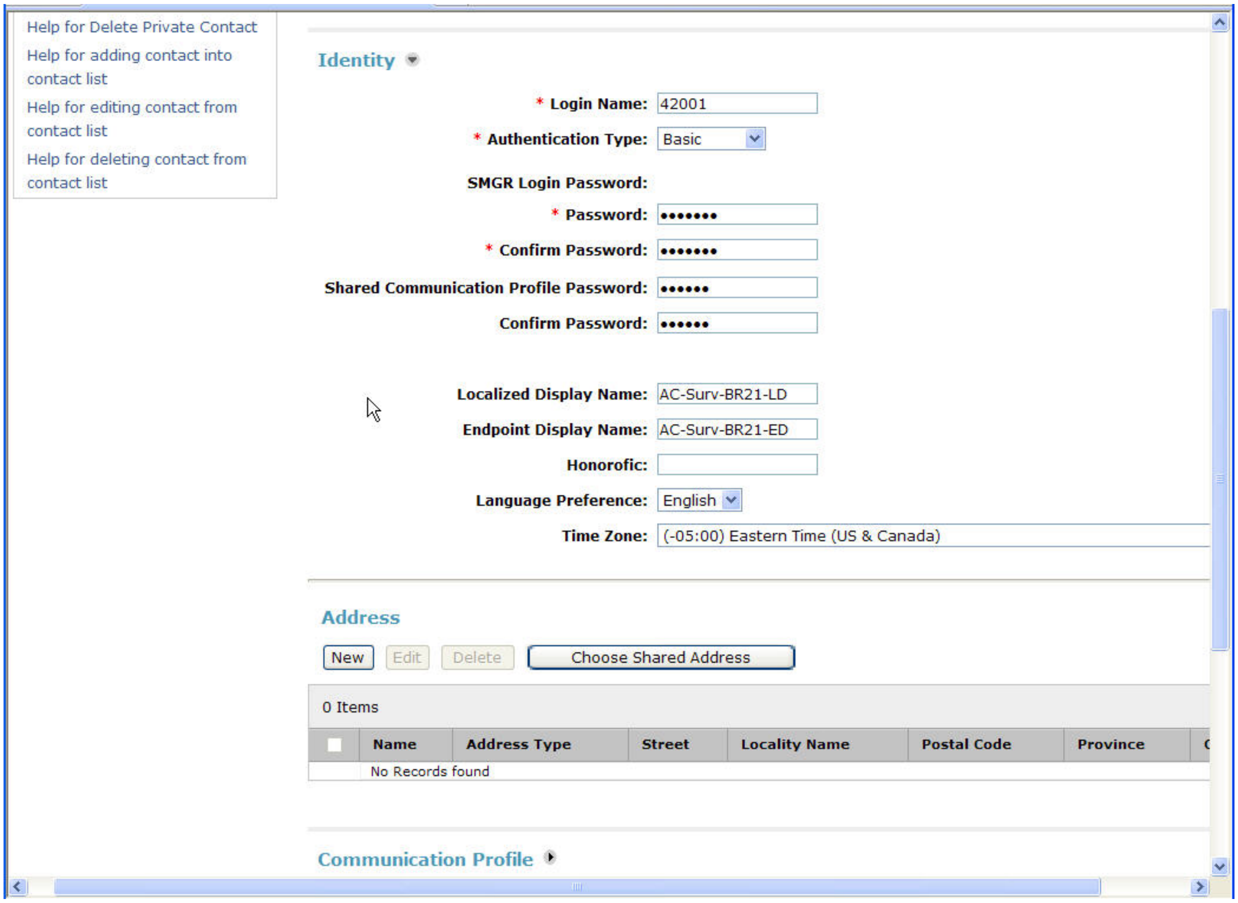
5.8. User Management for Adding SIP Telephone Users

Users must be added to Session Manager corresponding to the SIP stations added in Communication Manager (see **Section 4.6**). Select **User Management → User Management** on the left. Then click on **New** 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:

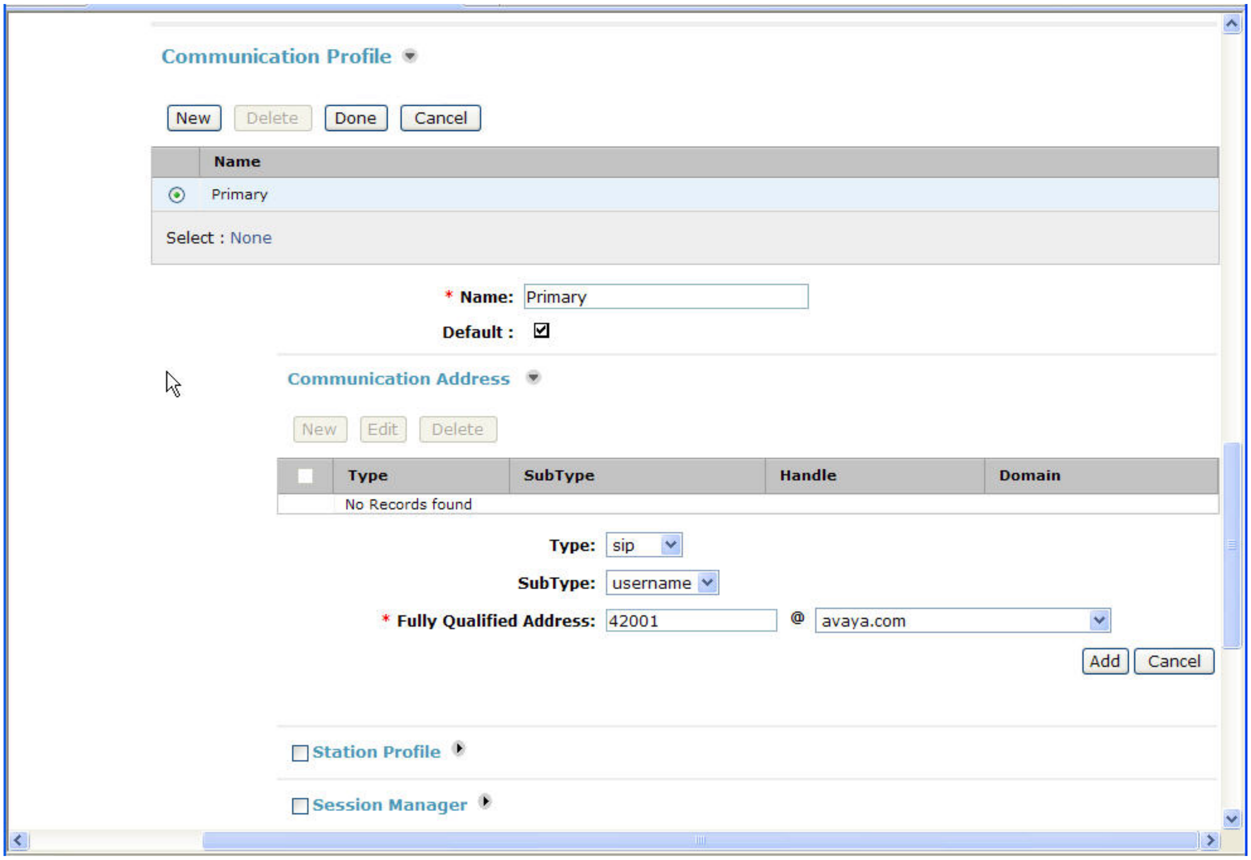
- **Login Name**: Telephone extension (see **Section 4.6**)
- **SMGR Login Password**: Password to log into System Manger
- **Shared Communication Profile Password**: Password to be entered by the user when logging into the telephone
- **Localized Display Name**: Name to be used as calling party
- **Endpoint 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 5.1**

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

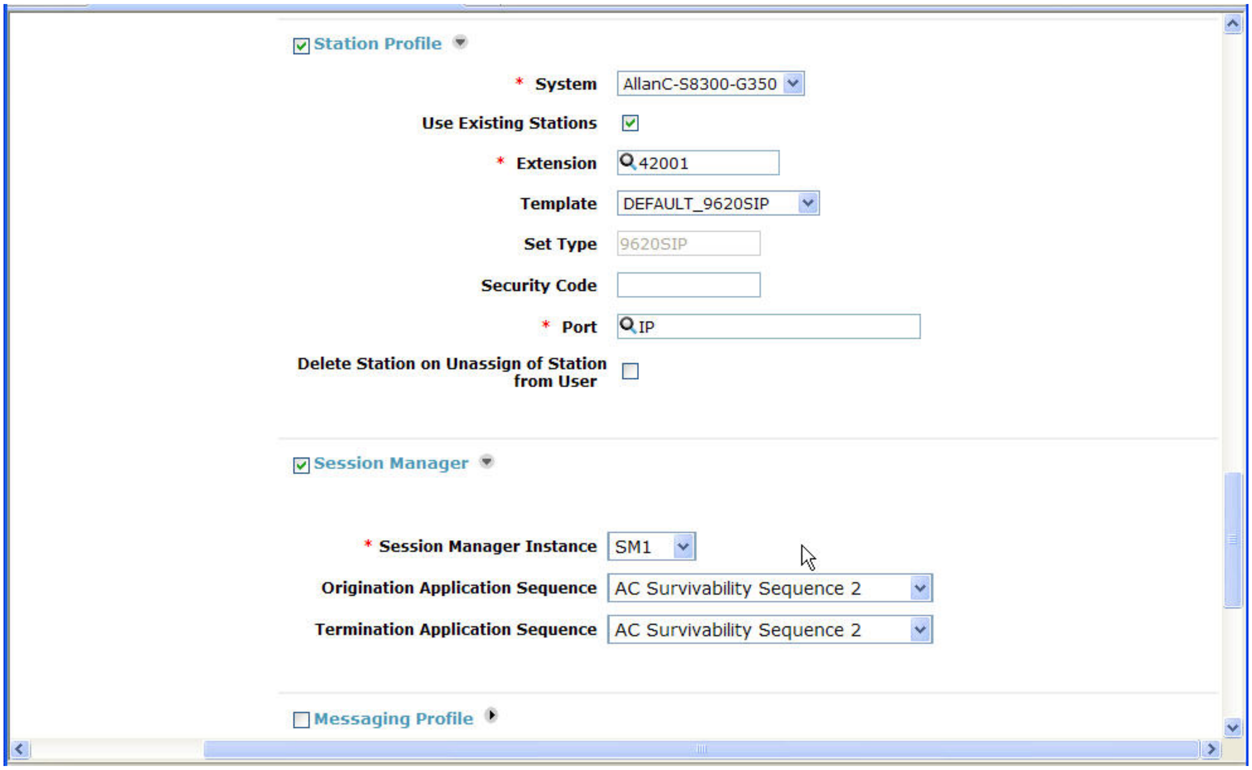


Click on *Station Profile* to expand that section. Enter the following fields and use defaults for the remaining fields:

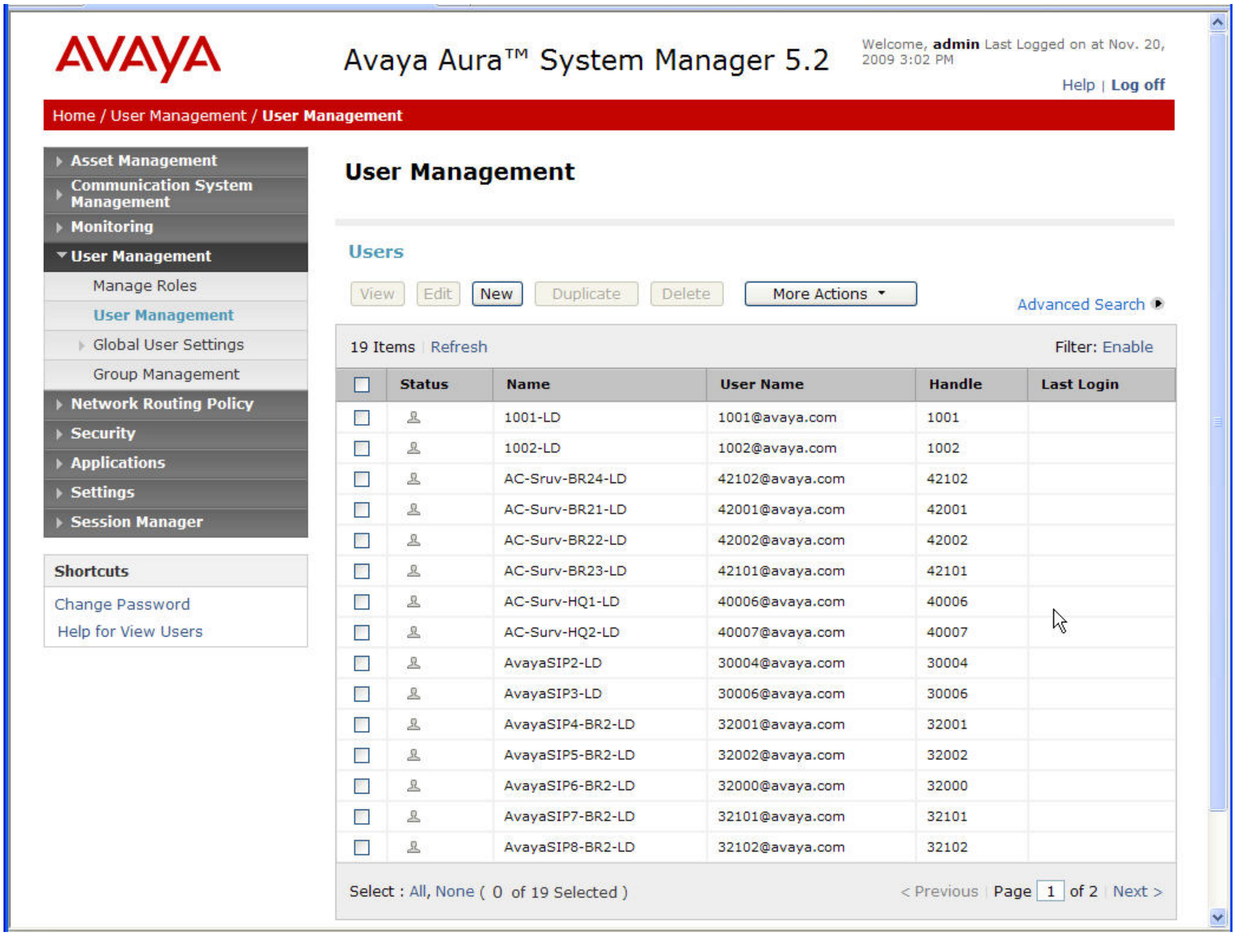
• **System**:	Select the Communication Manager entity
• **Use Existing Stations**:	Check this box
• **Extension**:	Enter the extension
• **Template**:	Select an appropriate template matching the telephone type as configured on Communication Manger (see **Section 4.6**)
• **Port**:	Click on the Search icon to pick a port (in this case "IP")

Click on *Session Manager* to expand that section. Select the appropriate Session Manager server for **Session Manager Instance**. For **Origination Application Sequence** and **Termination Application Sequence**, select the Application Sequence configured in **Section 5.7 Step 3**.

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



Repeat the above procedures to add each SIP telephone user for the Headquarters site as well as the branch site (including the analog phones connected to the FXS interface ports on the MP-118). The follow User Management screen shows the SIP telephone users configured in the sample configuration for the Headquarters site and Branch 2 (40006 and 40007 are Headquarters Avaya 9600 SIP Phone users; 42001 and 42002 are Avaya 9600 SIP Phone users at Branch 2; 42101 and 42102 are analog phones connected to the MP-118 FXS ports at Branch 2).



6. Configure Avaya 9600 SIP Phones

The Avaya 9600 SIP Phones at all sites will use the Session Manager (10.1.2.170) as the SIP Proxy Server. The Avaya 9600 SIP Phones at the branch sites will also configure the on-site MP-118 (192.168.75.100 for Branch 2) as an additional call server for survivability. The table below shows an example of the SIP telephone configuration settings for the Headquarters and Branch 2.

	Headquarters	**Branch 2**
Extension	40006	42002
IP Address	10.32.1.105	192.168.75.50
Subnet Mask	255.255.255.0	255.255.255.0
Router	10.32.1.1	192.168.75.1
File Server	10.32.2.75	10.32.2.75
DNS Server	0.0.0.0	0.0.0.0
SIP Domain	avaya.com	avaya.com
SIP Proxy Server	10.1.2.170	10.1.2.170
Alternate SIP Proxy Server		192.168.75.100

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

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

46xxsettings.txt Parameter Name	Value Used in Sample Configuration	Description
SIP_CONTROLLER_LIST	10.1.2.170:5060 ;transport=tcp, 192.168.75.100: 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 setting used in the sample configuration shows the values used for this parameter for a phone in Branch 2. The Session Manager is the first priority SIP Server listed using port and transport of 5060 and TCP. Separated by a comma, the Branch 2 AudioCodes MP-118 is the next priority SIP Server using port 5060 and TCP transport. The SIP Server list for each branch would require different values for the SIP_CONTROLLER_LIST, e.g. the list for Branch 1 phones will include the Session Manager and the Branch 1 AudioCodes MP-118 while the list for Branch 2 phones will include the Session Manager and the Branch 2 AudioCodes MP-118. To accomplish this, the GROUP system value mechanism can be implemented as described in [7].
FAILBACK_POLICY	Auto	While in Survivable Mode, determines the mechanism to use to fail back to the centralized SIP Server. **Auto** = the phone periodically checks the availability of the primary controller and dynamically fails back.

FAST_RESPONSE_TIMEOUT	2	The timer terminates SIP INVITE transactions if no SIP response is received within the specified number of seconds after sending the request. Useful when a phone goes off-hook after connectivity to the centralized SIP Server is lost, but before the phone has detected the connectivity loss. The default value of 4 seconds may be retained if desired. After the SIP INVITE is terminated, the phone immediately transitions to Survivable Mode.
MSGNUM	5000	The number dialed when the Message button is pressed and the phone is in Normal Mode.
PSTN_VM_NUM	919081235000	The number dialed when the Message button is pressed and the phone is in Survivable Mode.
RECOVERYREGISTERWAIT	60	A Reactive Monitoring Interval. If no response to a "maintenance check" REGISTER request is received within the timeout period, the phone will retry the monitoring attempt after a randomly selected delay of 50% - 90% of this parameter.
DIALPLAN	40xxx|41xxx|42xxx|43xxx|911|9911|91xxxxxxxxxx|9011x.T	Enables the acceleration of dialing when the WAN is down and the AudioCodes SAS 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. The dialplan values used in the phone will generally match the values used by the AudioCodes MP-118 in **Section 7.6**. See [7] for additional format details on the DIALPLAN parameter.
DISCOVER_AVAYA_ENVIRONMENT	1	Automatically determines if the active SIP Server is an Avaya server or not.
SIPREGPROXYPOLICY	alternate	A policy to control how the phone treats a

		list of proxies in the SIP_CONTROLLER_LIST parameter **alternate** = remain registered with only the active controller **simultaneous** = remain registered with all available controllers
SIPDOMAIN	avaya.com	The enterprise SIP domain. Must be the same for all SIP controllers in the configuration. SIPDOMAIN is set to "avaya.com" in the sample configuration.

7. Configure AudioCodes MP-118

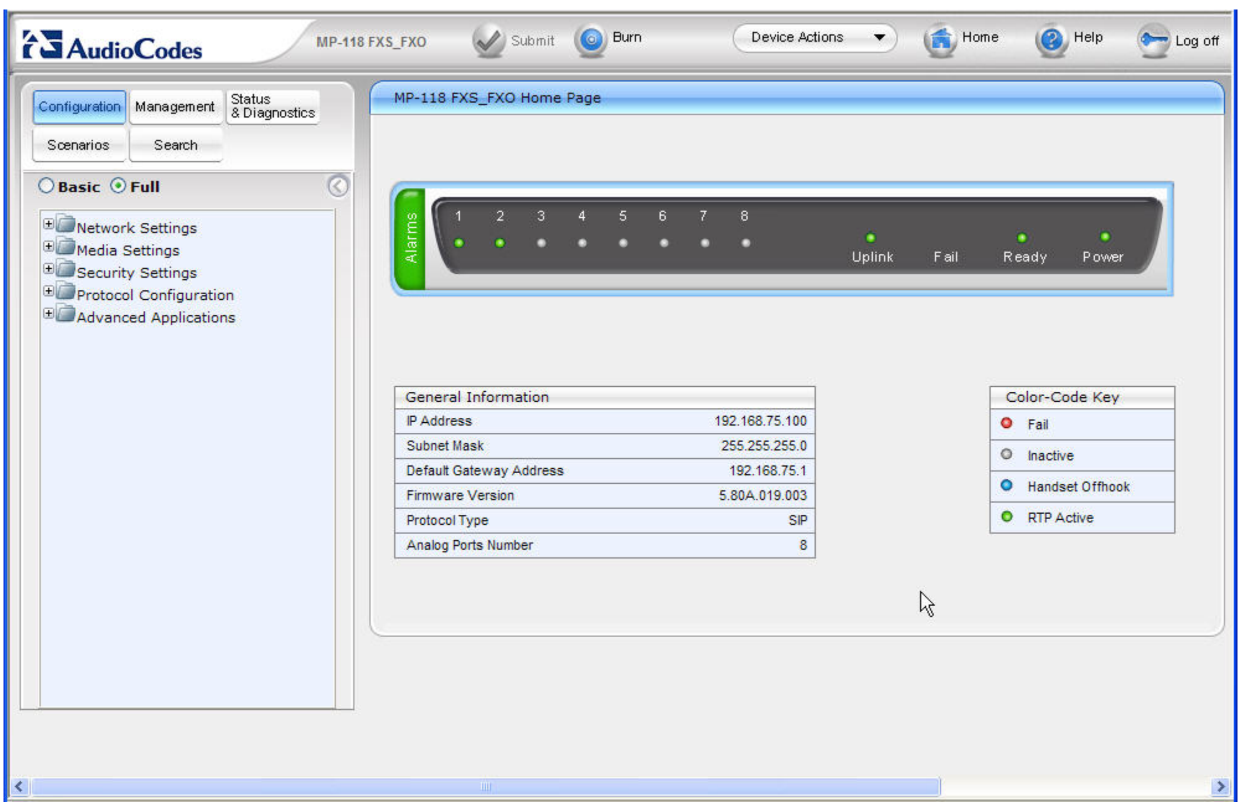
This section shows the necessary steps to configure the AudioCodes MP-118 Gateway to support the Avaya Session Manager Survivable SIP Gateway Solution in a Centralized Trunking scenario. It is assumed that the basic configuration of the AudioCodes MP-118 has already been administered. See [11] and [12] for additional information.

The icon  on the AudioCodes MP-118 configuration screens contained in this section indicates the corresponding parameter value has been changed. All parameters with this icon shown in the following screens are relevant to the Avaya Session Manager Survivable SIP Gateway Solution. In some cases, the parameter values used are specific to the sample configuration and may not apply to all environments.

7.1. MP-118 Access

From a web browser, enter the AudioCodes MP-118 IP address in the URL. A pop-up login window will appear (not shown) to allow entering the appropriate User Name and Password to gain access to the MP-118 administration web pages (default username is “Admin”; default password is “Admin”).

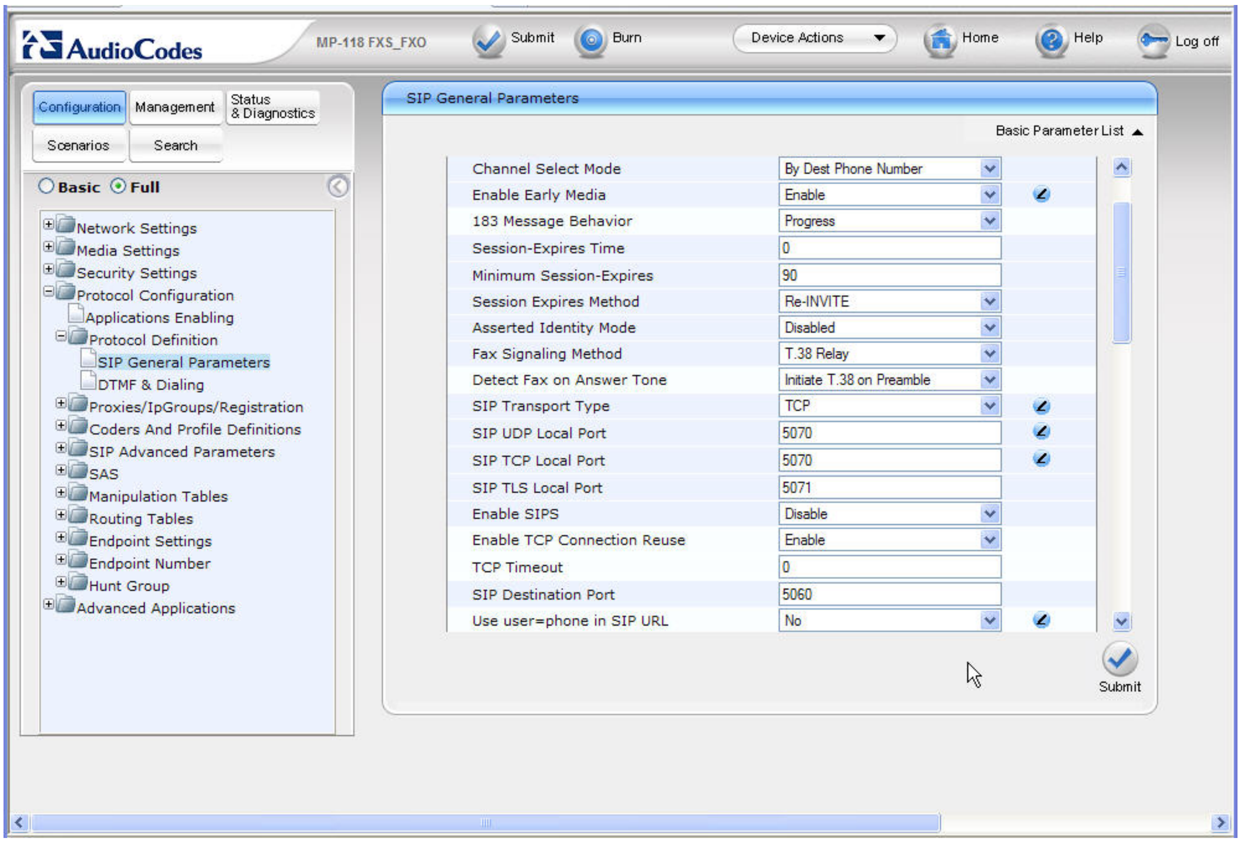
Once logged in, select the **Full** radio button and **Configuration** from the left navigation panel. The example screen below was captured when two calls were up. Each call was between an Avaya 9600 SIP Phone at the branch and an analog FXS port. This is the reason that ports 1 and 2 show green for “RTP Active”. The FXO line on port 5 was idle. Other ports were not assigned/used in the sample configuration.



7.2. SIP General Parameters

From the left navigation panel, navigate to the SIP General Parameters screen by selecting **Protocol Configuration → Protocol Definition → SIP General Parameters**. The values of the fields with an adjacent icon have changed from the default.

These key parameter values on this screen instruct the AudioCodes MP-118, when functioning as a media gateway, to use TCP as the transport and listen on port 5070 for SIP messages.

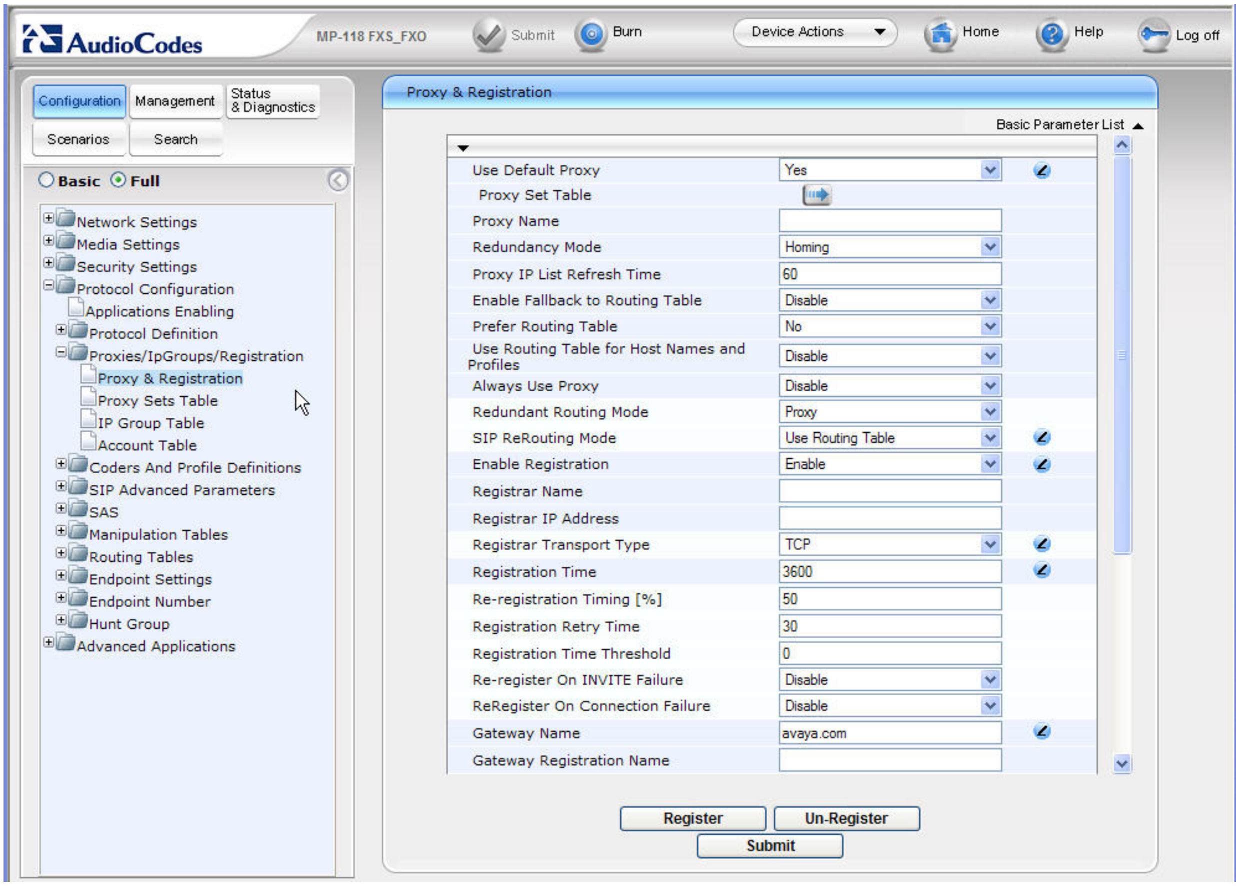


The remaining fields of the SIP General Parameters screens maintain the default values.

7.3. Proxy & Registration

From the left navigation panel, navigate to the Proxy & Registration screen by selecting **Protocol Configuration → Proxies/IpGroups/Registration → Proxy & Registration**. The values of the fields with an adjacent icon have changed from the default.

The value of “avaya.com” specified for the **Gateway Name** parameter is the SIP Domain name used in the sample configuration and matches the SIP Domain name configured on Session Manager and Communication Manager. This and other configured parameters instruct the AudioCodes MP-118 to register each FXS station with the SIP registrar using TCP transport, refreshing every 3600 seconds.



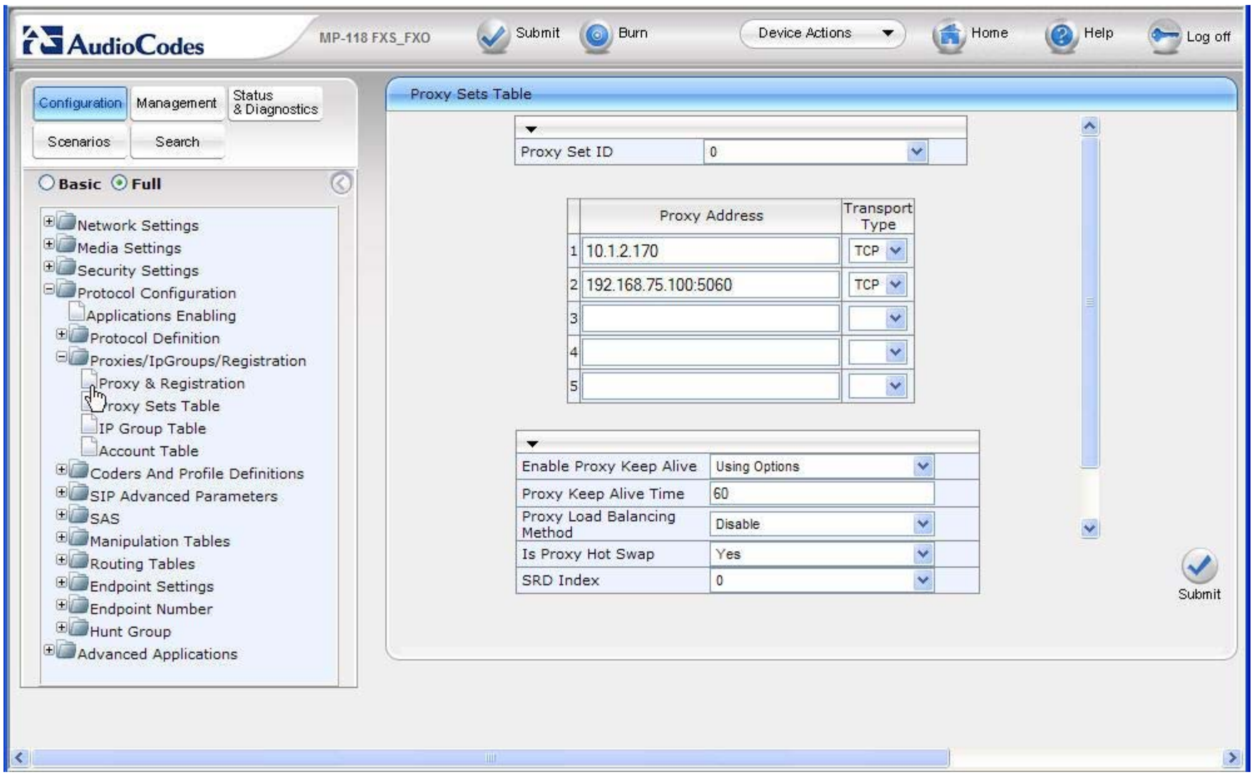
7.4. Proxy Sets Table

From the left navigation panel, navigate to the Proxy Sets Table screen by selecting **Protocol Configuration → Proxies/IpGroups/Registration → Proxy Sets Table**. The values of the fields with an adjacent icon have changed from the default.

The Proxy Sets Table specifies the SIP Proxy server the AudioCodes MP-118 is going to monitor for connectivity health to determine when to become active as a Survivability Server. In this case, the SIP Proxy server is the Session Manager with IP 10.1.2.170. The Proxy Sets Table also contains an entry specifying the Survivability Server (the AudioCodes MP-118 itself) with IP 192.168.75.100.

The mechanism used to monitor the Session Manager is also specified. SIP Options is used in the sample configuration with the AudioCodes MP-118 default Proxy Keep Alive Time of 60 seconds. This results in the AudioCodes MP-118 sending SIP Options messages to the Session Manager and using the response as an acknowledgement that the Session Manager is accessible from the branch location. If a response to a SIP Options message is not received, the AudioCodes MP-118 will continue to attempt to contact the Session Manager for 60 seconds, the Proxy Keep Alive Time value, and then activate its SAS survivable SIP server feature.

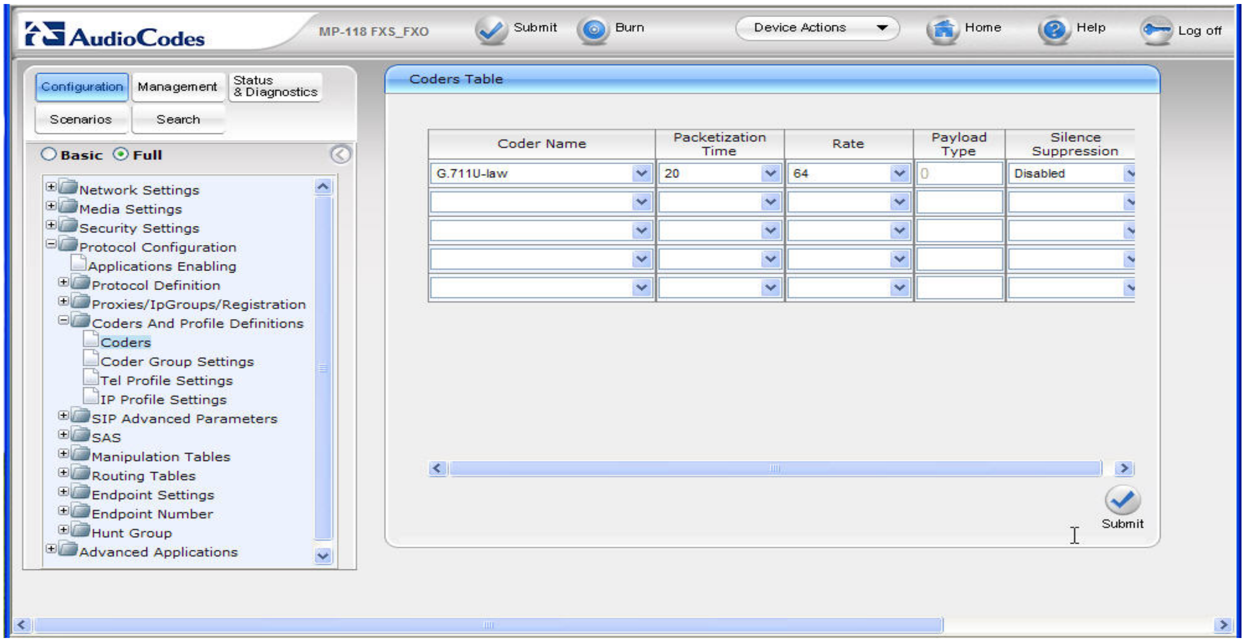
Enter the IP addresses of the Session Manager and the AudioCodes MP-118 in the **Proxy Address** table as shown below. Select TCP from the **Transport Type** drop-down list for both entries. For **Enable Proxy Keep Alive**, select "Using Options" from the drop-down list. Select "Yes" for **Is Proxy Hot Swap**.



7.5. Coders Table

From the left navigation panel, navigate to the Coders Table screen by selecting **Protocol Configuration → Coders And Profile Definitions → Coders**.

Select the codec from the drop-down list that matches the codec configured on Communication Manager (see **Section 4.4**).



7.6. DTMF & Dialing

From the left navigation panel, navigate to the DTMF & Dialing screen by selecting **Protocol Configuration → Protocol Definition → DTMF & Dialing**. The values of the fields with an adjacent  icon have changed from the default.

The value of the **RFC 2833 Payload Type** field must match the value configured for **Telephone Event Payload Type** for the Communication Manager SIP Trunks (see **Section 4.7.2**).

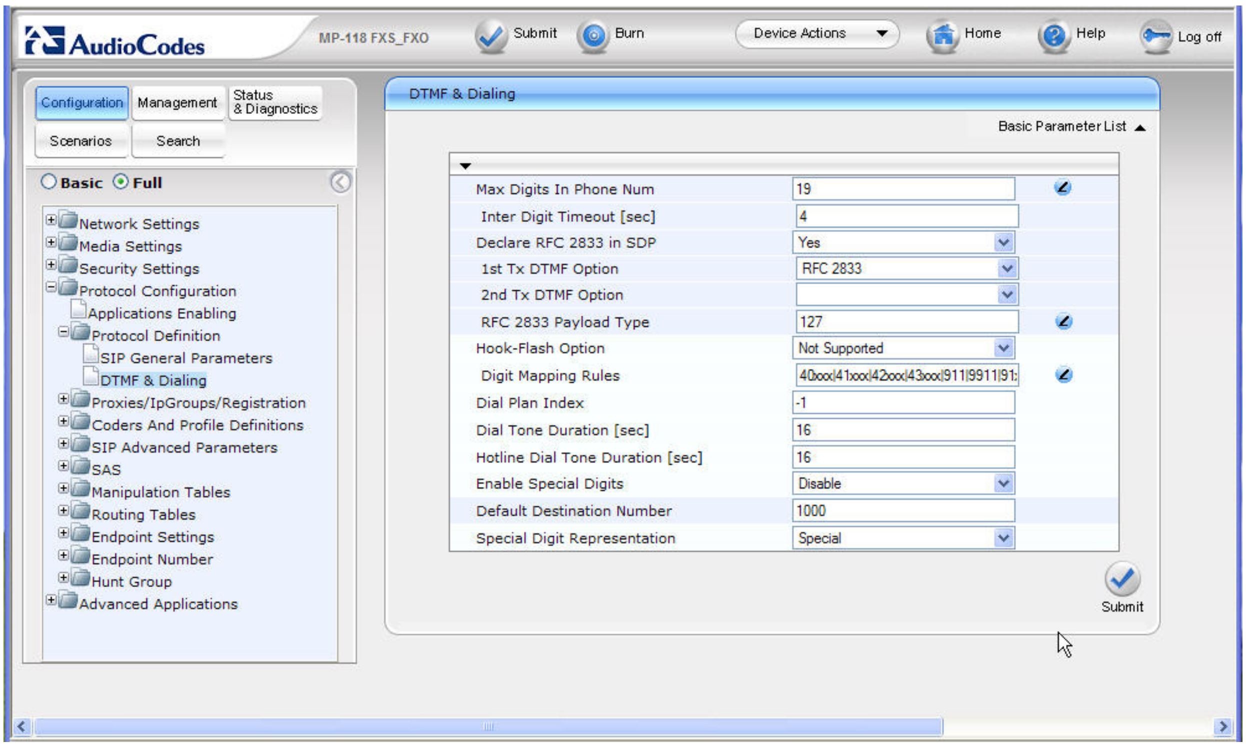
Because the full value of the **Digit Mapping Rules** field is not viewable in the screenshot, the full rule used in the sample configuration for Branch 2 is shown below:

40xxx|41xxx|42xxx|43xxx|911|9911|91xxxxxxxxxx|9011x.T

The details of the Digit Mapping Rule are captured in **Table 2** below. Refer to [12] for additional information on digit mapping rules.

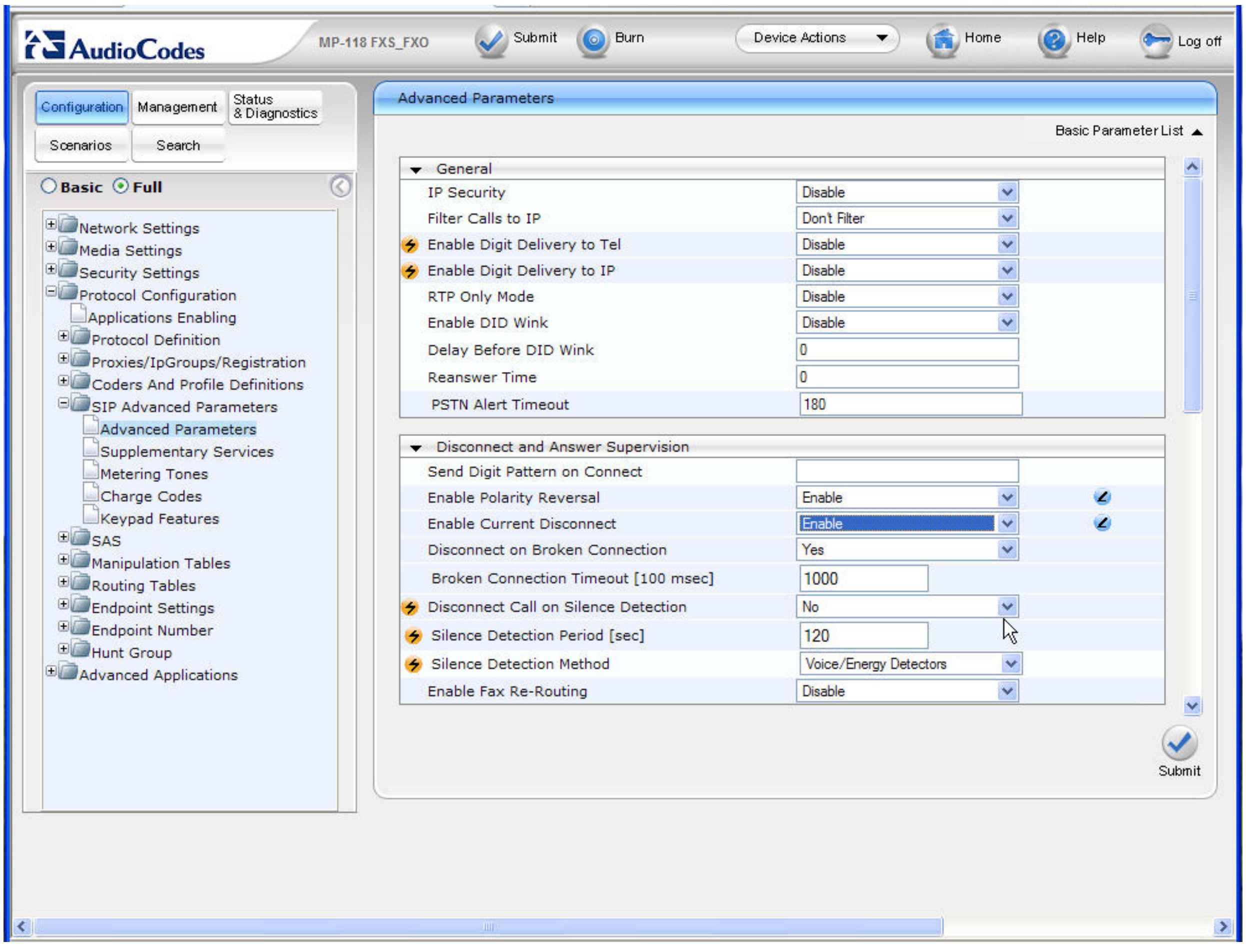
Digit String To Match	Sample Configuration Use
40xxx	HQ extensions
41xxx|42xxx|43xxx	Branch extensions (for Branches 1, 2, and 3)
911|9911	Emergency dialing
91xxxxxxxxxx	North American Numbering Plan
9011x.T	International dialing

Table 2 – Digit Mapping Rule used in Sample Configuration



7.7. Advanced Parameters

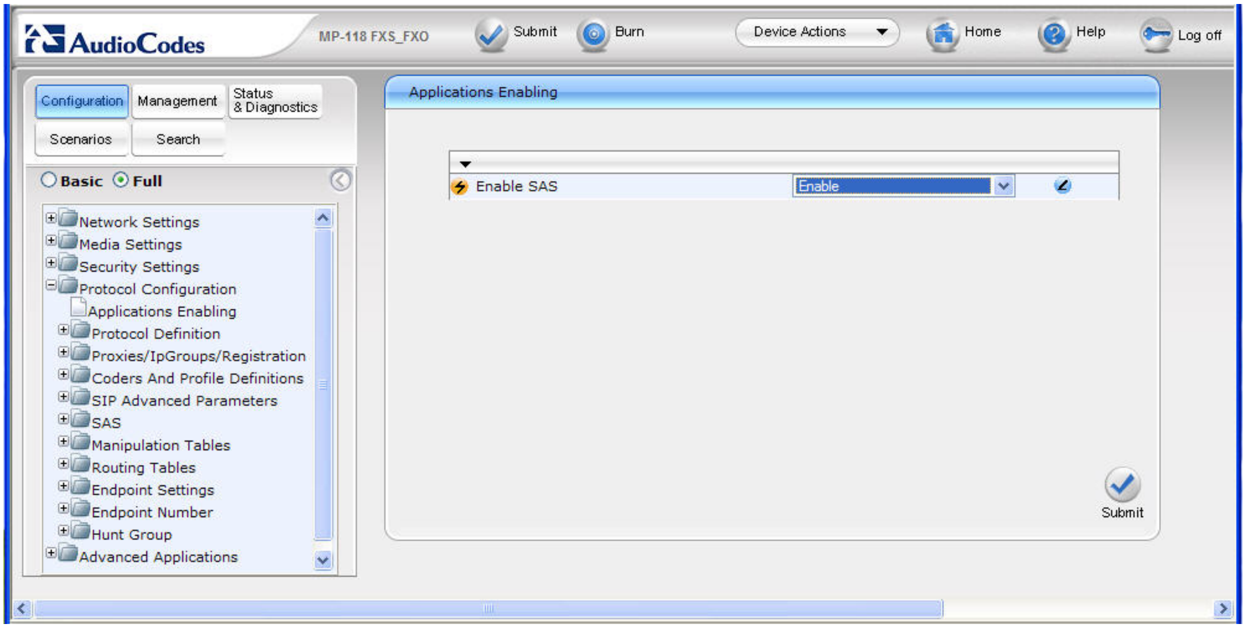
From the left navigation panel, navigate to the Advanced Parameters screen by selecting **Protocol Configuration → SIP Advanced Parameters → Advanced Parameters**. The values of the fields with an adjacent icon have changed from the default.



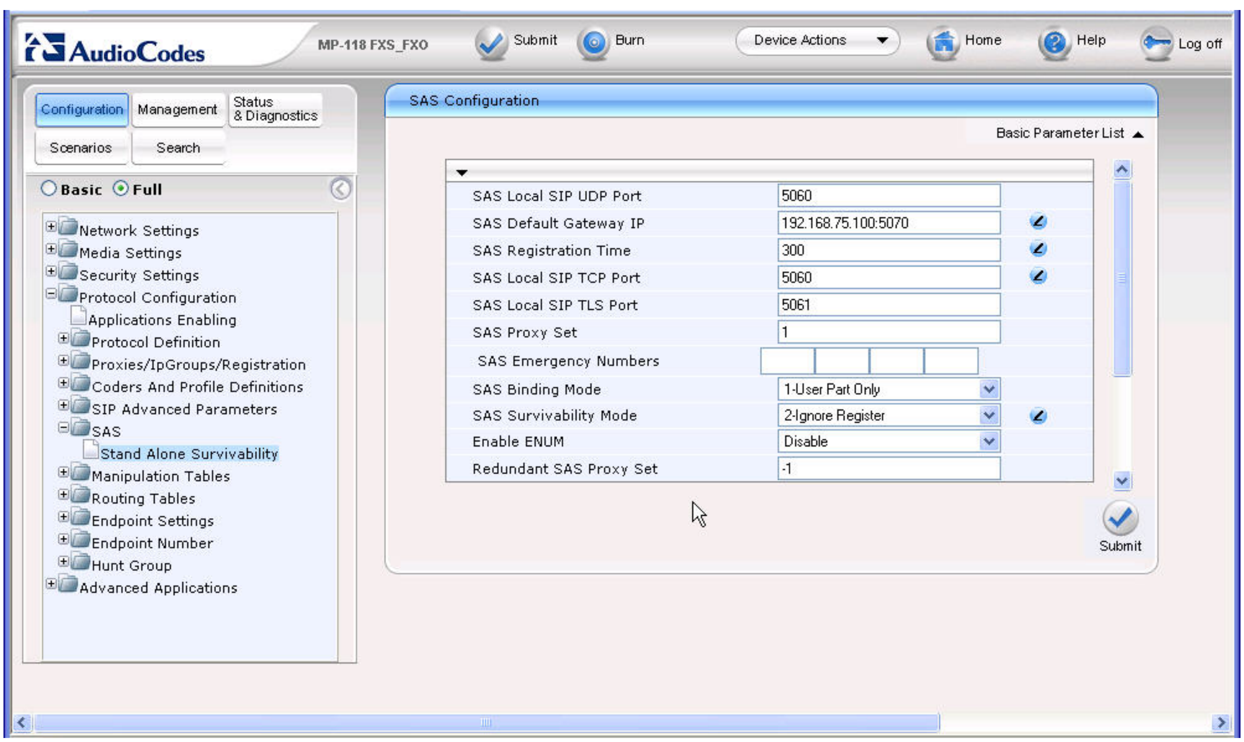
The remaining fields of the SIP General Parameters screens maintain the default values.

7.8. Stand-Alone Survivability

From the left navigation panel, navigate to the Application Enabling screen by selecting **Protocol Configuration → Application Enabling**. Select "Enable" for **Enable SAS**.



From the left navigation panel, navigate to the Stand-Alone Survivability screen by selecting **Protocol Configuration → SAS → Stand-Alone Survivability**. The values of the fields with an adjacent icon have changed from the default. Note the SAS SIP Proxy and SIP Registrar IP address specified for the **SAS Default Gateway IP** field.

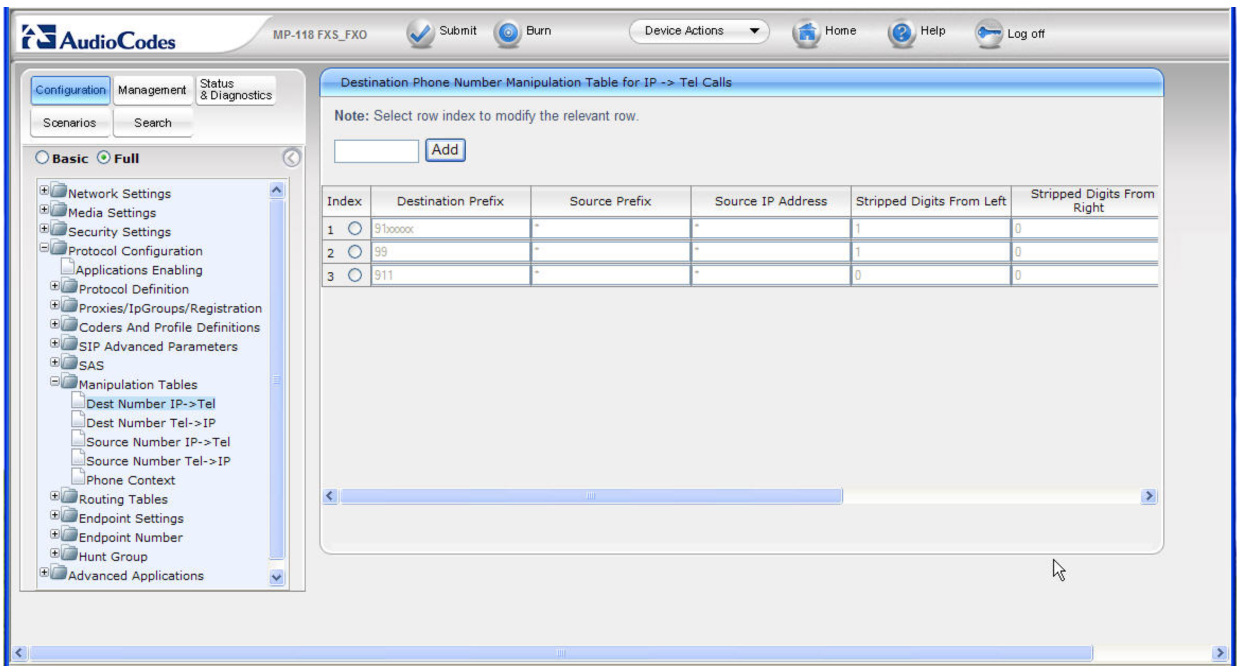


7.9. Dest Number IP → Tel

From the left navigation panel, navigate to **Protocol Configuration → Manipulation Tables → Dest Number IP->Tel**.

The entry in this table strips the leading 9 from the dialed digit strings (for numbers matching the **Destination Prefix**) for IP to PSTN calls while in Survivable Mode. In Normal Mode, this is done by Communication Manager.

As an example, the leading digit "9" would be stripped in the dialed number "9 1-732-555-1111" leaving "1-732-555-1111" presented to the PSTN via the AudioCodes MP-118 FXO interface. Similarly, the dialed emergency number "9 911" would be presented to the PSTN as "911". However, if the user simply dials "911", the AudioCodes MP-118 FXO interface will pass it along to the PSTN as is.



7.10. IP to Hunt Group Routing

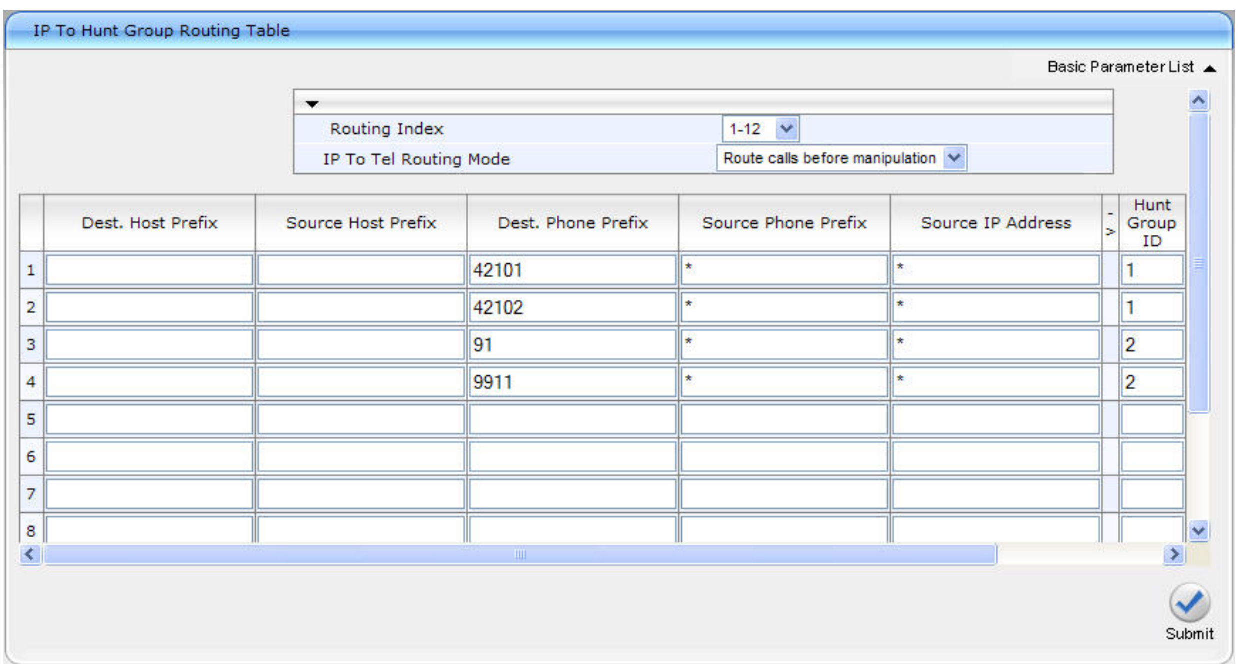
From the left navigation panel, navigate to the IP to Hunt Group Routing Table screen by selecting **Protocol Configuration → Routing Tables → IP to Trunk Group Routing**.

The entries in this table are used by the AudioCodes MP-118 to route calls originating on IP and terminating on the gateway. Note that the AudioCodes “Hunt Group” concept is not the same as a “Hunt Group” in Communication Manager. The leading digits of the called numbers are used to determine the selected AudioCodes MP-118 Hunt Group. In the sample configuration, the FXS analog phone numbers are entered explicitly and route to Hunt Group ID 1. Calls to PSTN starting with “91” (including 911 call and 91xxxxxxxxxx conforming to North American Numbering Plan) as well as 911 call with a PSTN access digit “9” will route to Hunt Group ID 2.

Hunt Group ID 1 consists of two FXS interfaces and Hunt Group ID 2 consists of one FXO interface. Hunt Group to Channel assignments are configured in **Section 7.14. Table 3** below shows a summary of the Hunt Group assignments.

Channel	Hunt Group ID
FXS 1, 2	1
FXS 3, 4	Un-assigned
FXO 5	2
FXO 6, 7, 8	Un-assigned

Table 3 – Hunt Group Assignments


IP To Hunt Group Routing Table

Basic Parameter List

Routing Index: 1-12

IP To Tel Routing Mode: Route calls before manipulation

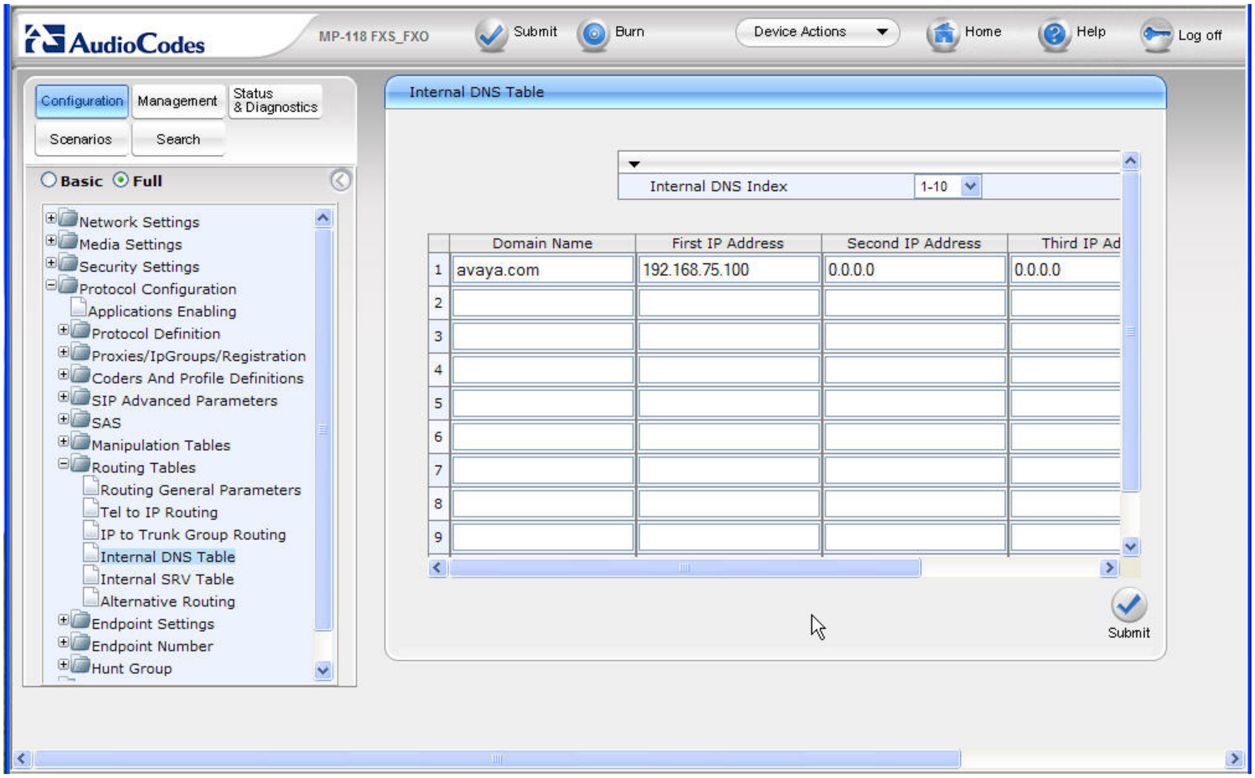
	Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	->	Hunt Group ID
1			42101	*	*		1
2			42102	*	*		1
3			91	*	*		2
4			9911	*	*		2
5							
6							
7							
8							

Submit

7.11. Internal DNS Table

From the left navigation panel, navigate to the Internal DNS Table screen by selecting **Protocol Configuration → Routing Tables → Internal DNS Table**.

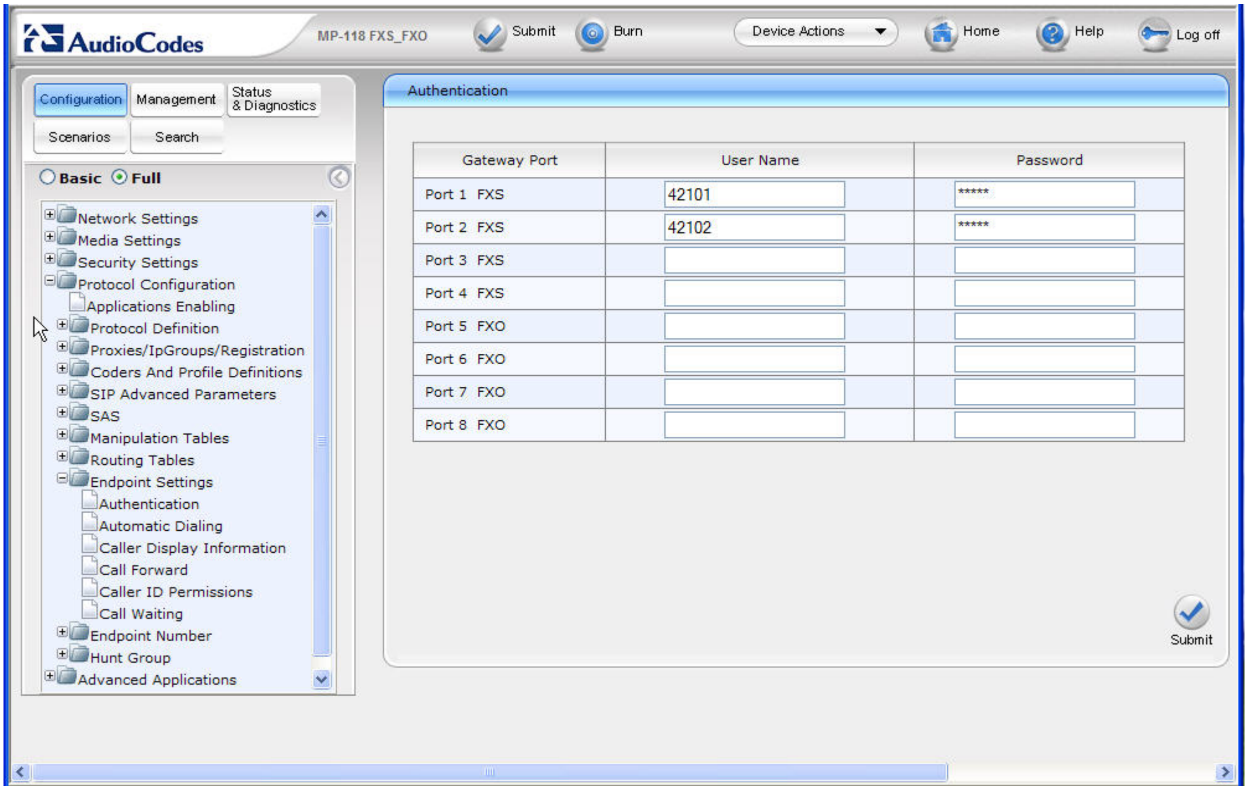
Enter the SIP domain and the IP address of the on-site branch AudioCodes MP-118 in the first table entry. Enter “0.0.0.0” for **Second IP Address**, **Third IP Address**, and **Fourth IP Address** (not shown)..



7.12. Authentication

From the left navigation panel, navigate to the Authentication screen by selecting **Protocol Configuration → Endpoint Settings → Authentication**.

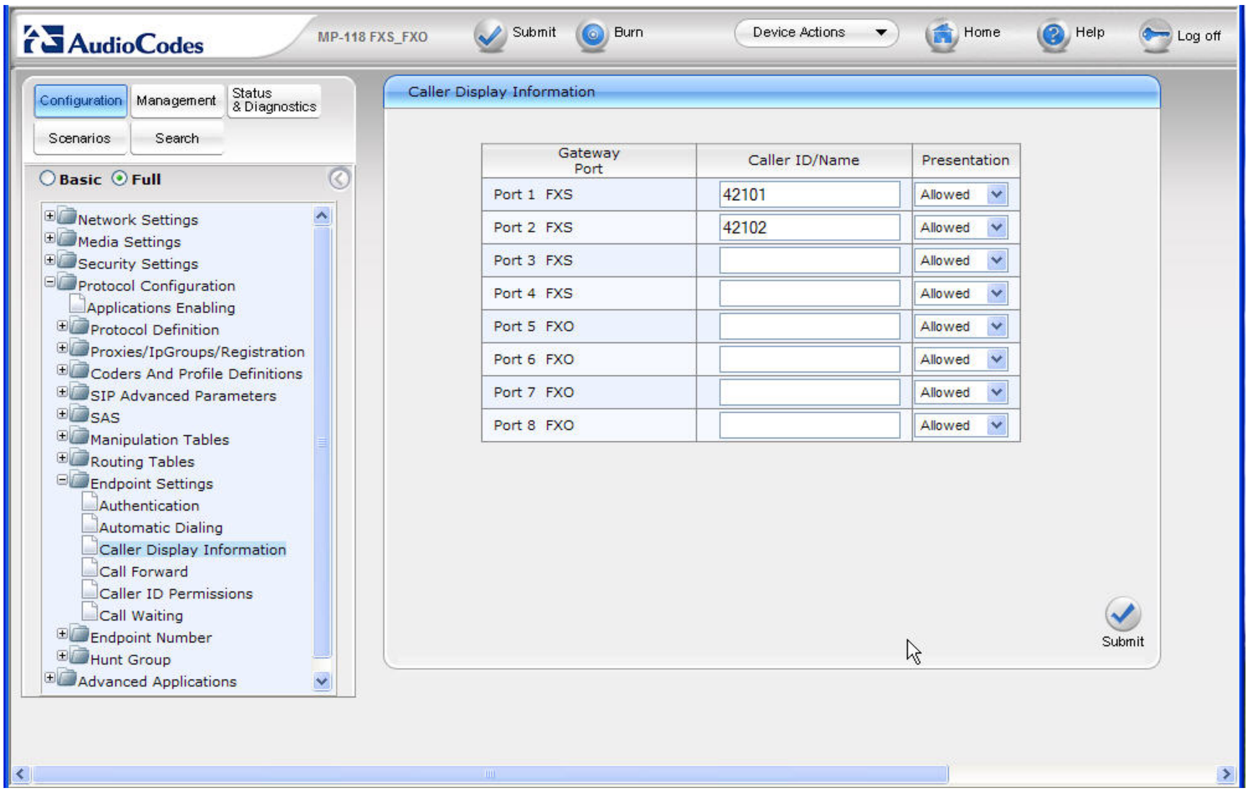
Enter the SIP user name and password that match the AudioCodes MP-118 FXS Analog Phone User Account created on Session Manager in **Section 5.8**.



7.13. Caller Display Information

From the left navigation panel, navigate to the Caller Display Information screen by selecting **Protocol Configuration → Endpoint Settings → Caller Display Information**.

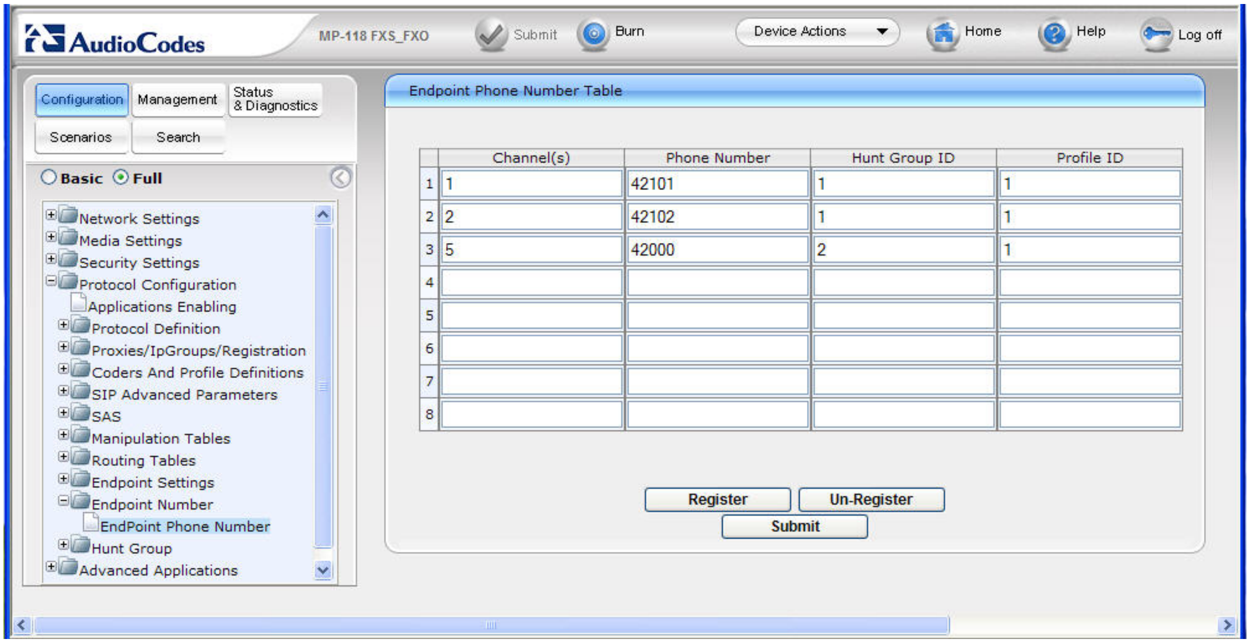
Enter the name/number to be displayed on the called station in Survivable Mode for each interface. The FXS extension numbers are used in the sample configuration. In Normal Mode, the display information is controlled by the name and number configuration in Communication Manager.



7.14. Endpoint Phone Number

From the left navigation panel, navigate to the Endpoint Phone Number Table screen by selecting **Protocol Configuration → Endpoint Number → Endpoint Phone Number**.

Enter the phone number assignment for each channel of the AudioCodes MP-118 as well as the associated Hunt Group ID. On AudioCodes MP-118, Channels 1 through 4 are the FXS interfaces; Channels 5 through 8 are the FXO interfaces. The sample configuration used Channels 1, 2 (FXS) and 5 (FXO) only.



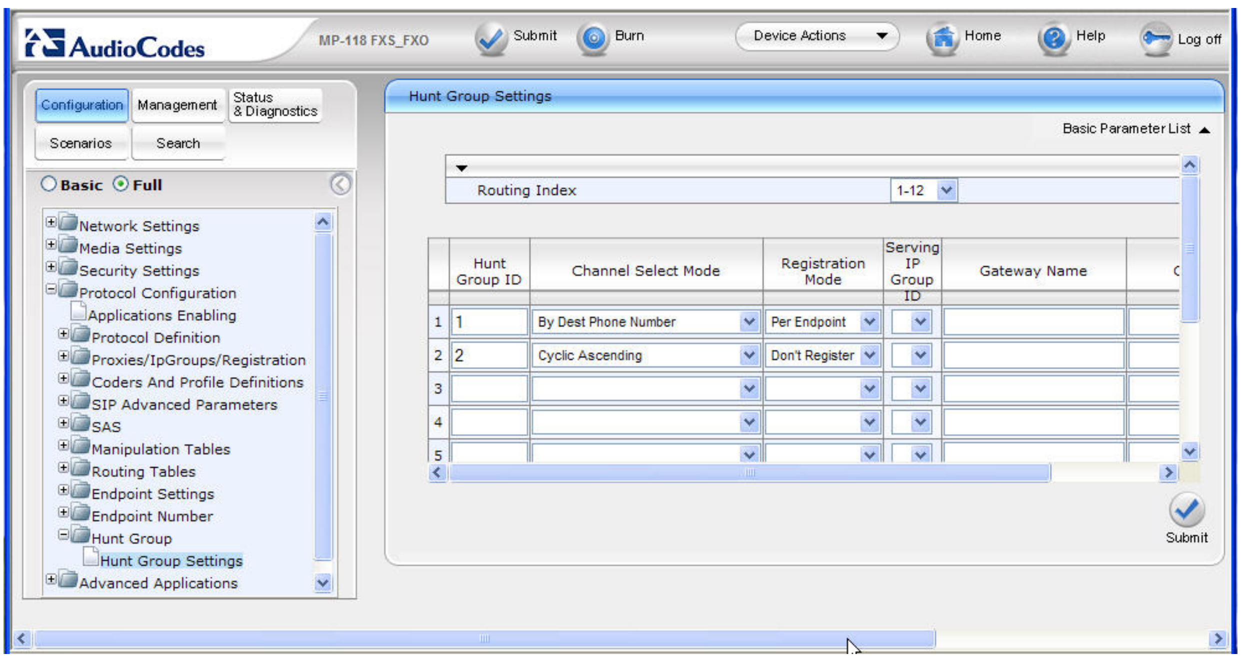
7.15. Hunt Group Settings

From the left navigation panel, navigate to the Hunt Group Settings screen by selecting **Protocol Configuration → Hunt Group → Hunt Group Settings**.

The settings on this screen configure the method in which calls originating on IP and terminating on the gateway are assigned to channels within each Hunt Group.

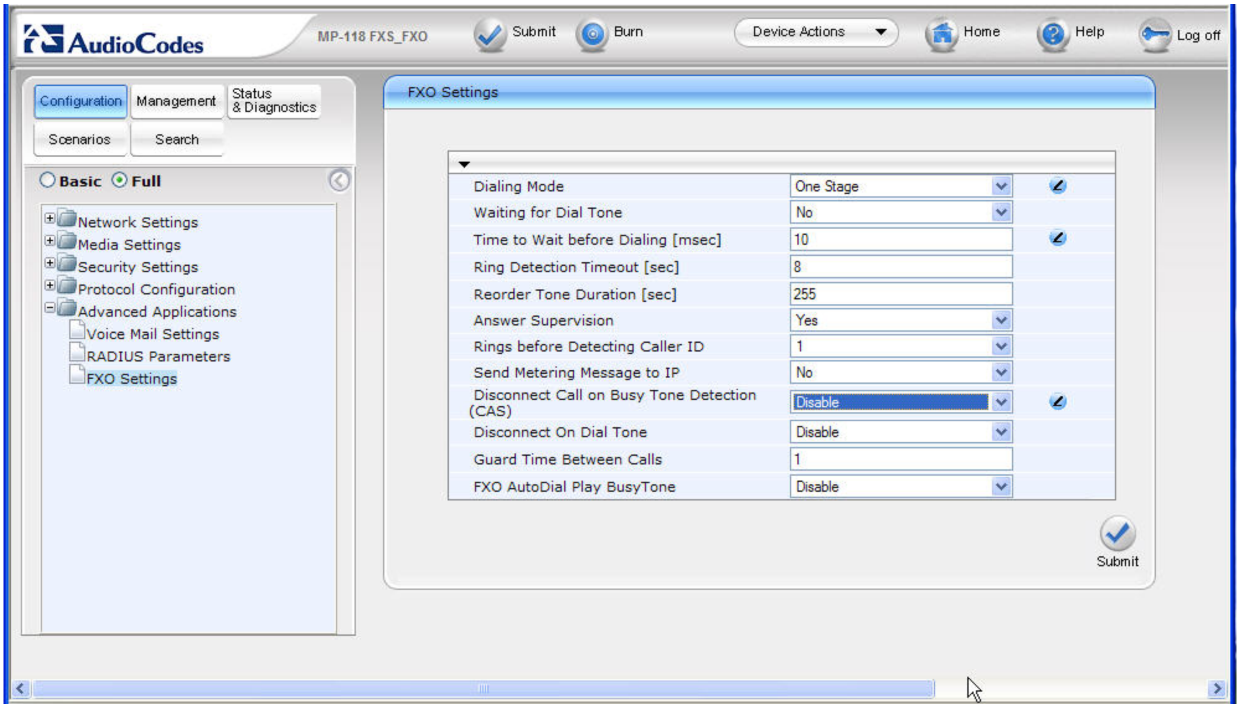
Hunt Group 1, containing 2 FXS interfaces for analog phones, is configured to select the proper FXS interface to terminate calls based on the destination phone number.

Hunt Group 2, containing 1 FXO interface to the PSTN, is configured to select any interface in this Hunt Group in a Cyclic Ascending order. Cyclic Ascending is the default. Since only one FXO interface is configured for Hunt Group 2 in the sample configuration, no channel cycling is occurring.



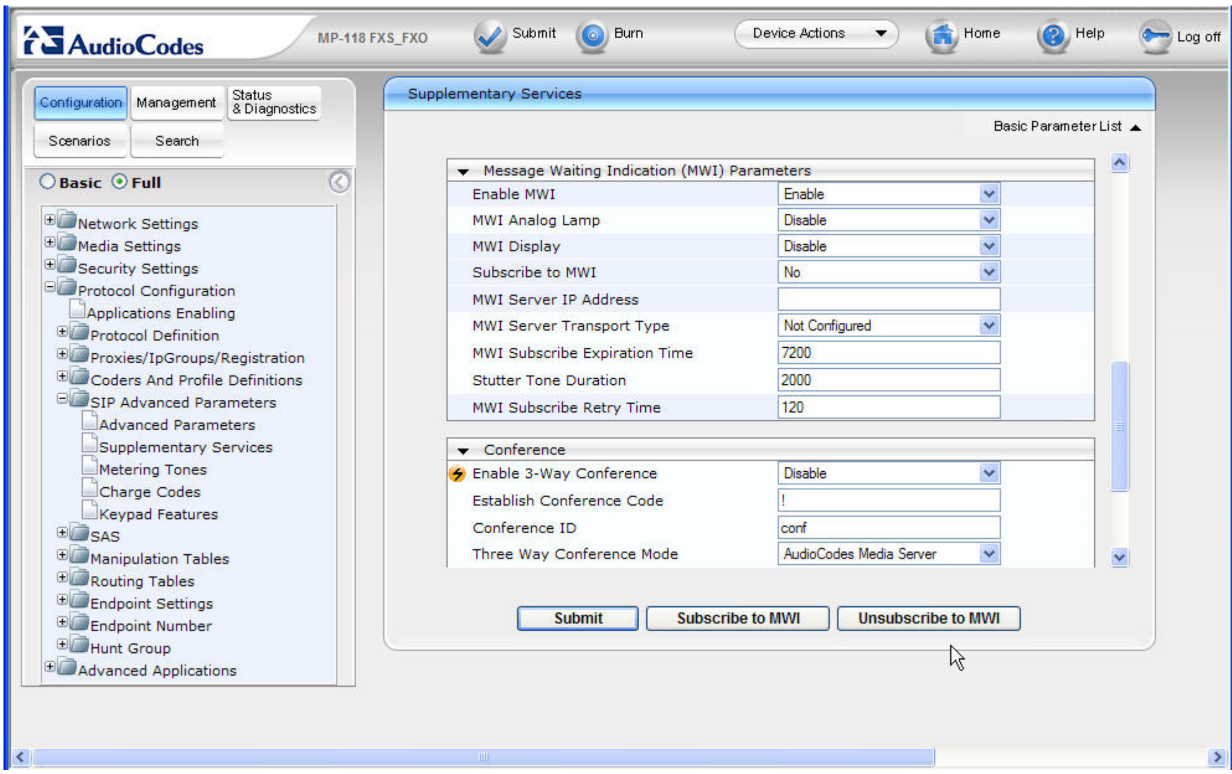
7.16. Advanced Applications → FXO Settings

From the left navigation panel, navigate to the FXO Settings screen by selecting **Advanced Applications → FXO Settings**. The values of the fields with an adjacent  icon have changed from the default.



7.17. Message Waiting Indication via Stutter Dial Tone for Analog FXS

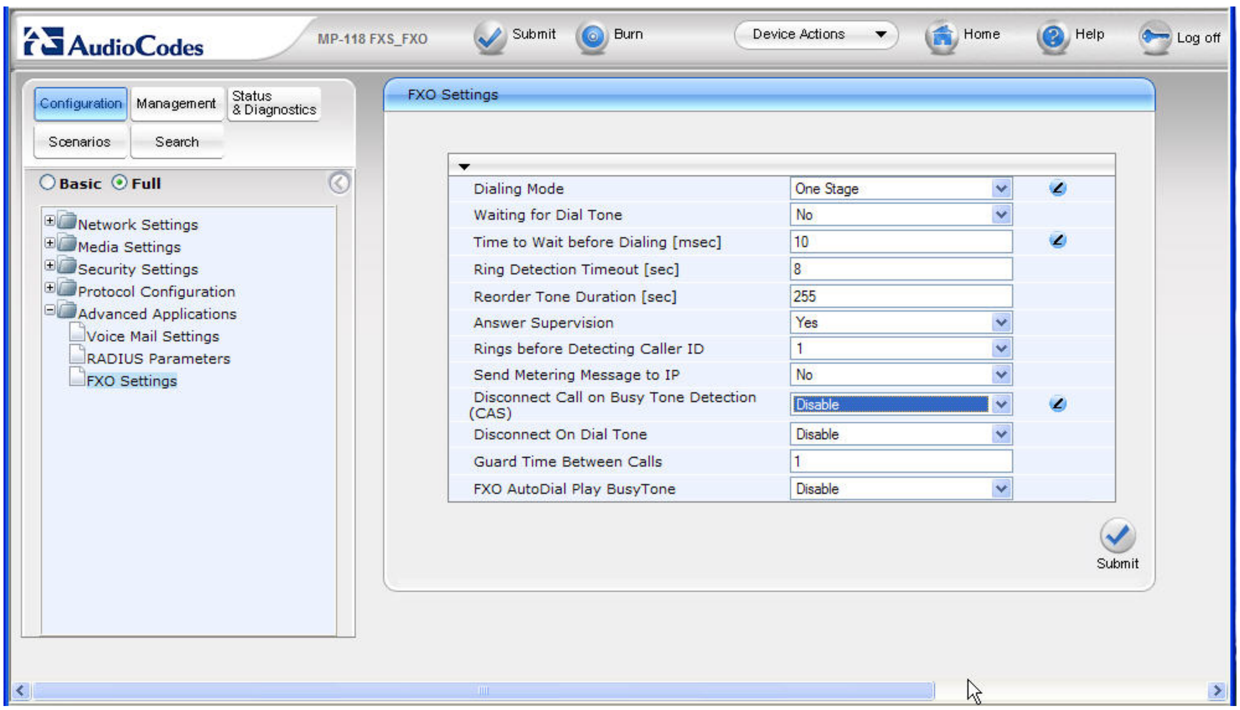
To enable analog stations connected to the FXS ports to receive stutter dial tone for audible message waiting notification, navigate to **Protocol Configuration → SIP Advanced Parameters → Supplementary Services**. Verify that "Enable" from the **Enable MWI** drop-down is selected, as shown in the following screen. When a SIP user registers, or the message waiting status of a registered user changes, Session Manager will send SIP NOTIFY messages to update the message waiting status. The AudioCodes Gateway can process these NOTIFY messages, and provide normal dial tone to the FXS ports when there is no message waiting, and stutter dial tone when there is a message waiting (e.g., a new message in a Communication Manager Messaging or Avaya Modular Messaging mailbox). It is not necessary that the AudioCodes Gateway subscribe to MWI, but this option (**Subscribe to MWI**) is also available. Observe that **Stutter Tone Duration** can also be configured.



7.18. Disable FXO Disconnect on Busy Tone Detection (Optional)

The AudioCodes Gateway can automatically detect when a call is connected to busy tone from the PSTN on an FXO line, and disconnect the call if desired. For the sample configuration, it is recommended that this feature be disabled. If the feature remains enabled, and an Avaya SIP Telephone in the branch makes a call to a PSTN number (in Survivable Mode) that is busy (e.g., a standard home telephone that is in use with no call waiting and no voice mail), the Avaya SIP Telephone will hear busy tone for a few seconds, and then the call appearance will be cleared. Although this frees the FXO more quickly, it may be perceived by the telephone user as a problem with the system. With the feature disabled as shown below, the Avaya SIP Telephone would simply hear busy tone until hanging up the telephone.

Navigate to **Advanced Applications → FXO Settings**. Use the drop-down menu to select "Disable" for the **Disconnect Call on Busy Tone Detection (CAS)** parameter.



7.19. .ini File

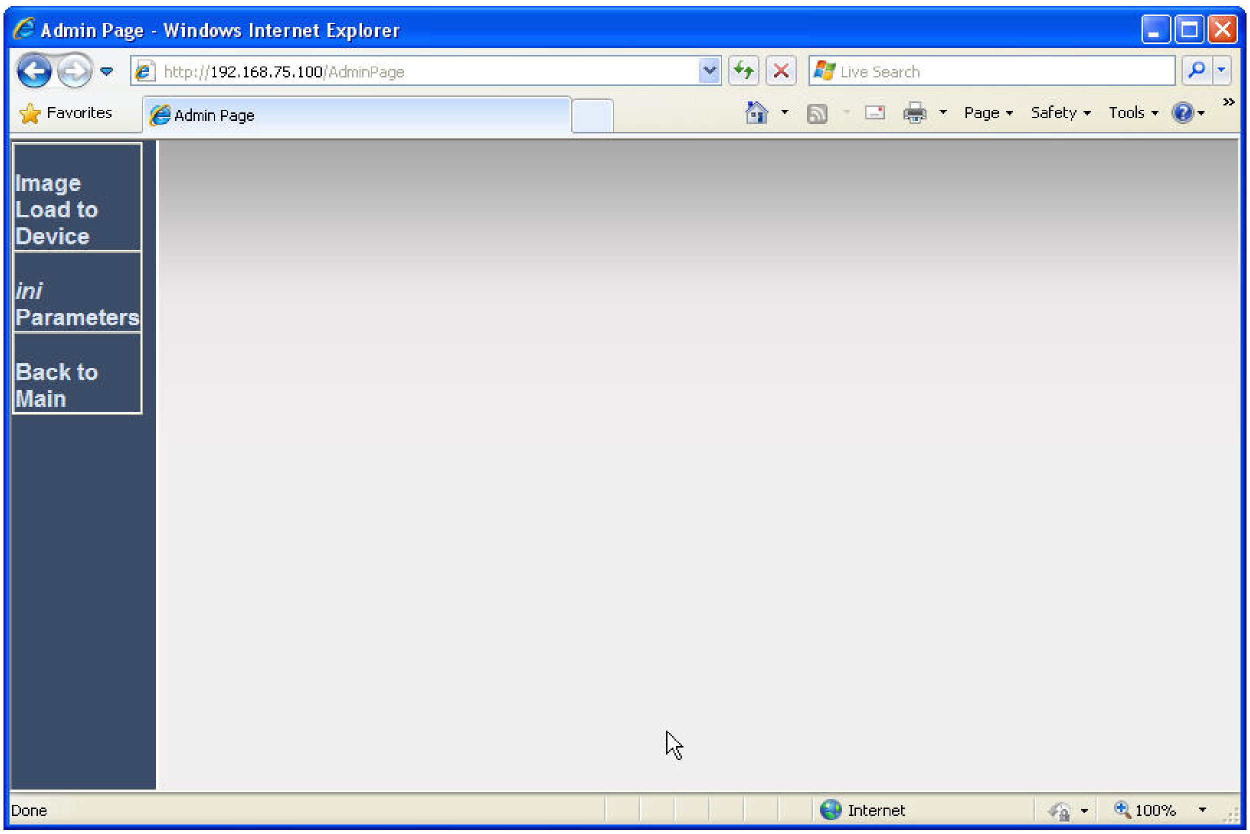
The AudioCodes MP-118 utilizes an initialization text file with a .ini extension. The .ini file contains MP-118 parameters that have been set by the WebUI, such as the parameters described in the previous sections. See [12] for additional information on the ini configuration file.

As of the AudioCodes MP-118 firmware version listed in **Table 1**, the following parameters are not configurable from the WebUI and must be modified directly in the .ini file.

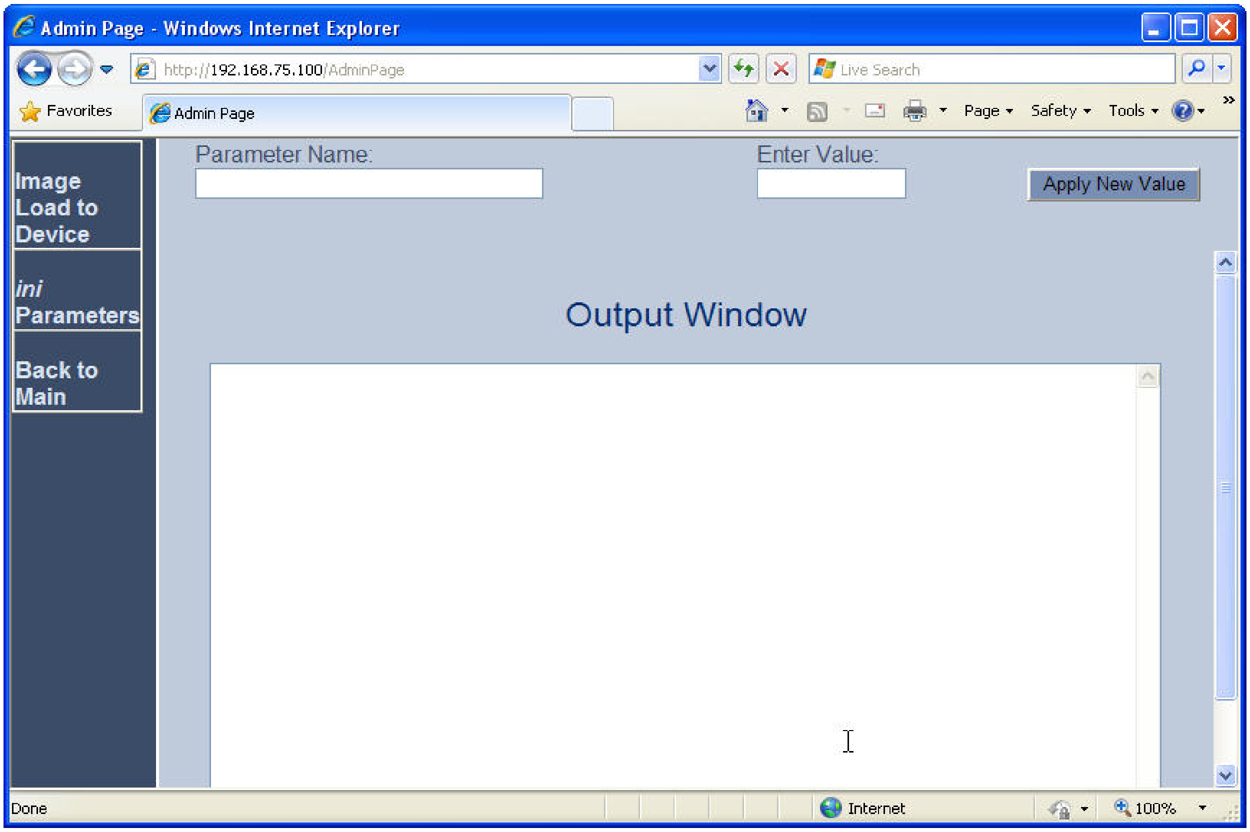
- ReliableConnectionPersistentMode
- CurrentDisconnectDuration

While the .ini file can be edited directly with a text editor, it is recommended to use the .ini file editing capability of the AudioCodes Web AdminPage. The AdminPage can be accessed from a browser by entering the following URL: http://<MP-118 IP Address>/**AdminPage**.

The AdminPage, similar to the one shown below, will be displayed. Select **ini Parameters** to access the .ini parameter editing screen.



The .ini editing screen, similar to the one shown below, will be displayed.



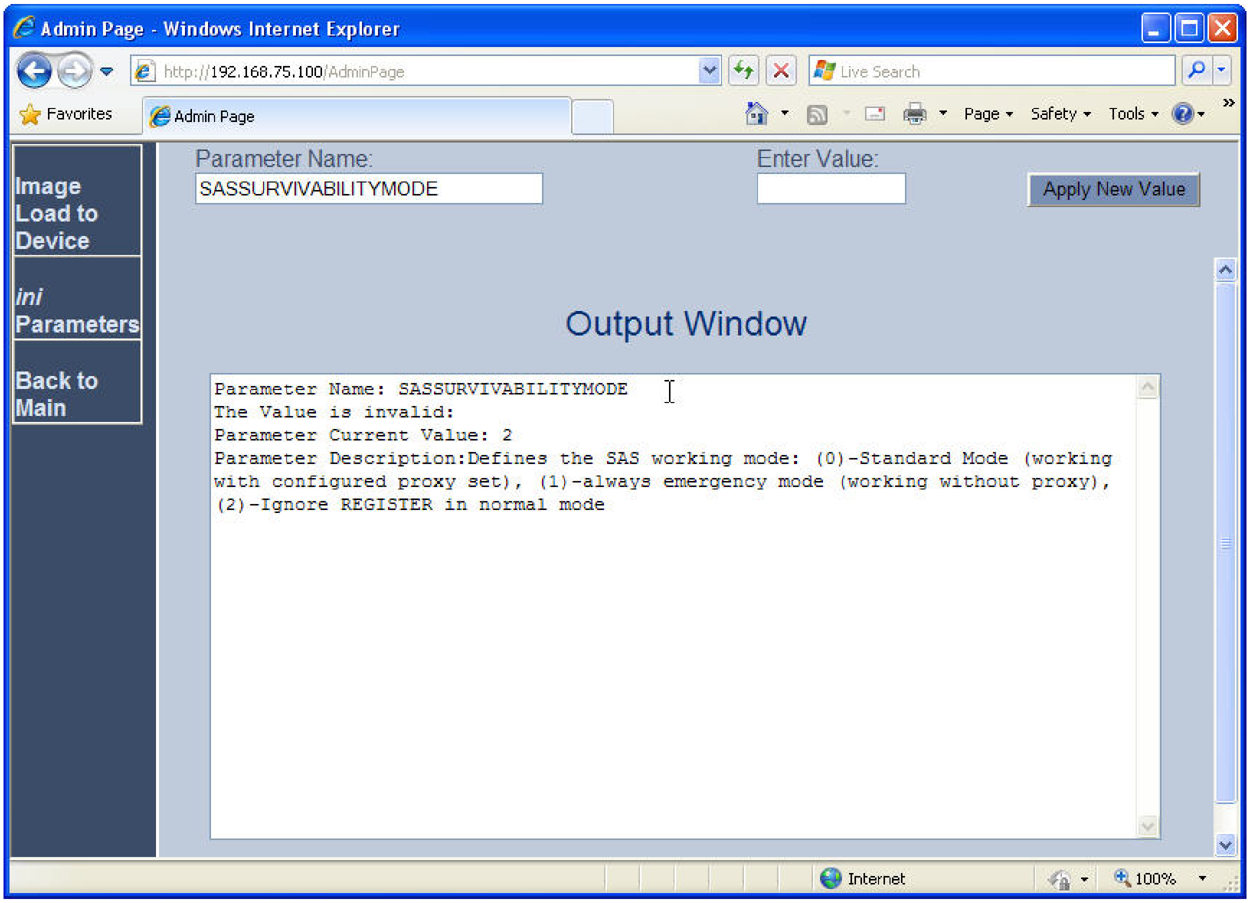
7.19.1. SASSurvivabilityMode

The **SASSurvivabilityMode** parameter is accessible from **Configuration→ Protocol Configuration→ SAS→ Stand Alone Survivability** of the MP-118 web administrative interface. This important setting is included here as a verification point.

The **SASSurvivabilityMode** parameter determines how the SAS feature of the AudioCodes MP-118 will operate. By default, **SASSurvivabilityMode** is set to a value of 0 which enables SAS to be able to accept SIP Registrations while the AudioCodes MP-118 can simultaneously communicate with Session Manager.

SASSurvivabilityMode ***must be changed from the default value of 0 to a value of 2.*** This sets SAS to become active and only accept SIP Registrations when it is not able to communicate with Session Manager.

To verify the current value of a parameter using the AdminPage, enter the parameter name in the top "Parameter Name" field and leave the "Enter Value" field blank. Click the adjacent "Apply New Value" button. The "Output Window" will display the current setting for the parameter entered in the Parameter Name field. The screen below shows that the **SASSurvivabilityMode** parameter is currently set to the required value of 2 as previously administered.



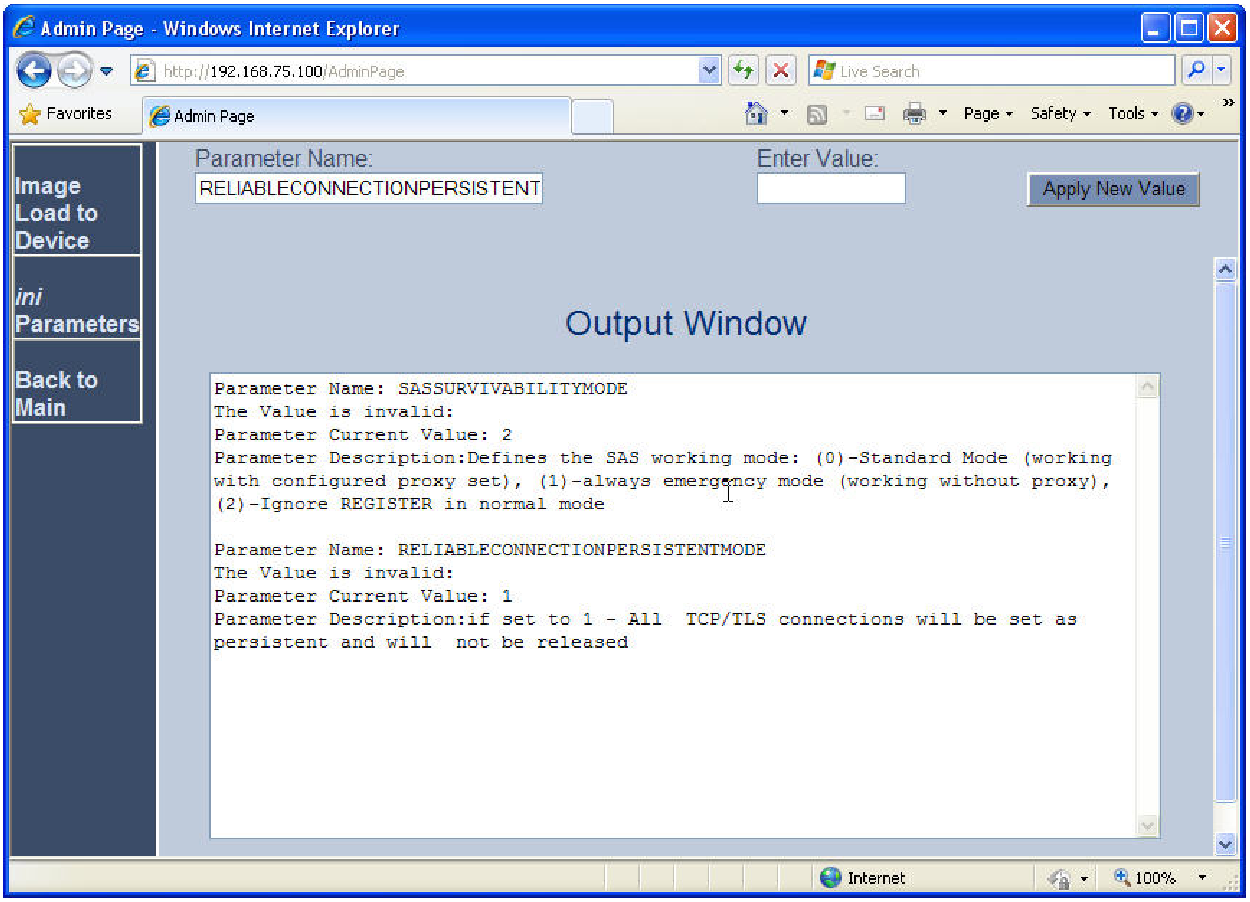
To change the value of a parameter, enter the new parameter value in the "Enter Value" field, then click the adjacent "Apply New Value" button. The resulting screen will show both the old and new settings.

7.19.2. ReliableConnectionPersistentMode

The **ReliableConnectionPersistentMode** parameter determines how the AudioCodes MP-118 establishes TCP connections. When **ReliableConnectionPersistentMode** is set to the default value of 0, all TCP/TLS connections established by the AudioCodes MP-118 are non-persistent connections.

ReliableConnectionPersistentMode ***must be changed from the default value of 0 to a value of 1***. This configures the AudioCodes MP-118 to establish all TCP connections as persistent connections that will not be prematurely released.

The following screen shows the value of the **ReliableConnectionPersistentMode** parameter is currently set to the required value of 1 as previously administered.



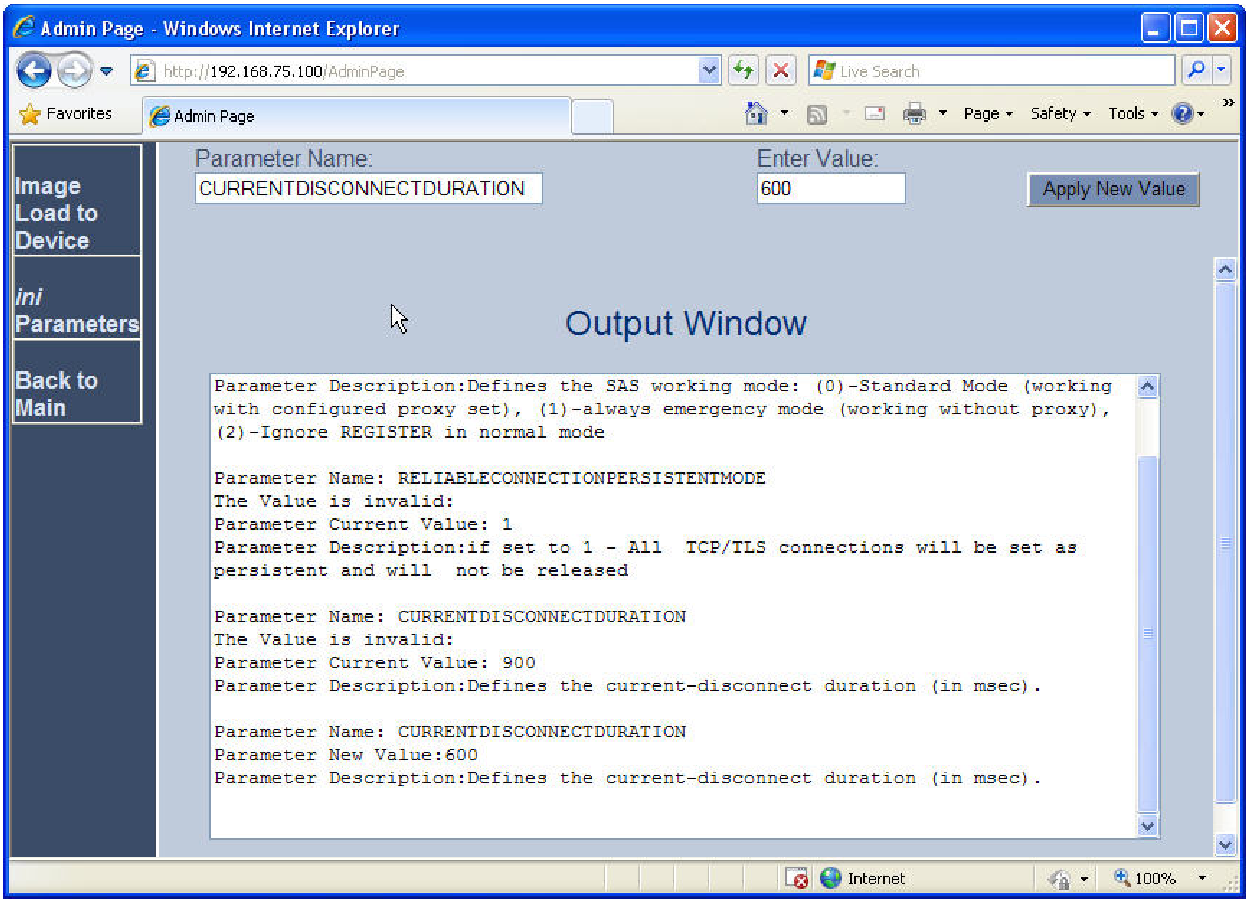
7.19.3. CurrentDisconnectDuration

The **CurrentDisconnectDuration** parameter determines the duration of time in milliseconds the analog line current is dropped indicating a disconnect pulse to the AudioCodes MP-118 FXO interfaces. For the sample configuration, this parameter was changed from the default value of 900ms to 600ms. This was required to obtain a proper disconnect on the AudioCodes MP-118 FXO Analog Trunk from the PSTN service provider.

Note: The need to change **CurrentDisconnectDuration** may not apply to all environments and will be determined by the PSTN service provider configuration of the analog trunk.

Also, the parameters **EnableReversalPolarity** and **EnableCurrentDisconnect** must both be enabled for **CurrentDisconnectDuration** to be active. The **EnableReversalPolarity** and **EnableCurrentDisconnect** parameters are both configured on the Advanced Parameters screen as shown in **Section 7.7**.

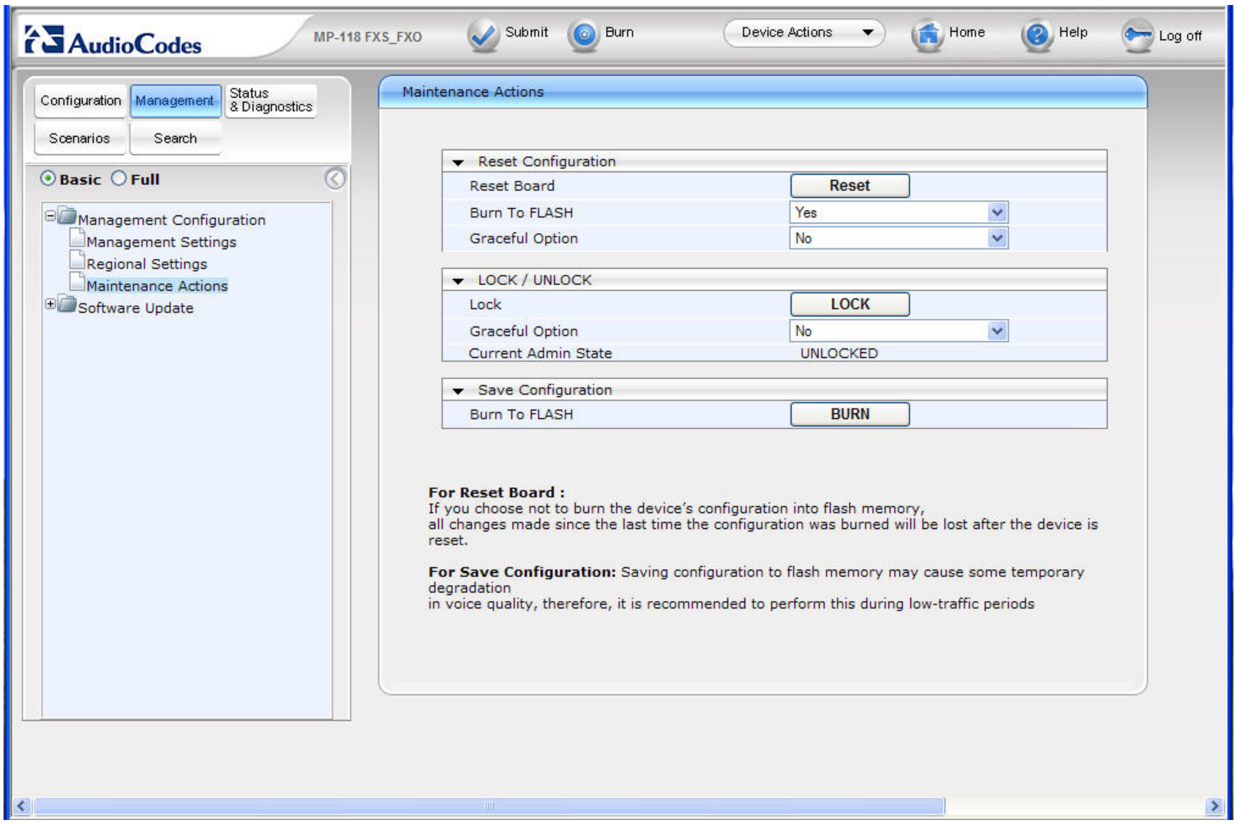
The following screen shows the value of the **CurrentDisconnectDuration** parameter was successfully set to a value of 600.



7.20. Saving Changes to the AudioCodes Gateway

The  button on the screens in the **Configuration** tab will save changes to the volatile memory (RAM) only. To save settings to non-volatile memory (flash), the  button at the top of the screen can be used. Only configuration "burned" to non-volatile memory will be available after a hardware reset or power fail.

An alternate means to access the "burn" function is via the **Management** tab. Navigate to **Management Configuration → Maintenance Actions**. The **BURN** button illustrated in the following screen may be used. The on-screen text below should be self-explanatory.



8. General Test Approach and Test Results

This section describes the testing used to verify the sample configuration for the Avaya Session Manager Survivable SIP Gateway Solution using the AudioCodes MP-118 Media Gateway in a Centralized Trunking scenario. This section covers the general test approach and the test results.

8.1. General Test Approach

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

- When network connectivity is broken, the branch AudioCodes MP-118 gateway automatically assumes the SIP proxy and SIP registrar functions. In this Survivable Mode, the branch phones can still call each other and reach PSTN through the AudioCodes MP-118 FXO trunk interface.
- When network connectivity is restored, SIP proxy and registrar functions are automatically switched back to the Session Manager at the headquarters location for providing centralized SIP call control. In this Normal Mode, PSTN access by phones at both the headquarters and branch sites are through the T1/E1 connection on the Avaya Media Gateway at the central location.

8.2. Test Results

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

- In Normal Mode, branch phones register to the Session Manager located at the central site; in Survivable Mode, branch phones register to the AudioCodes MP-118 located at the branch location.
- Switching between the Normal and the Survivable Modes is automatic and within a reasonable time span (within one to two minutes).
- In Normal Mode, calls can be placed between phones at the main site and the branch site, and among phones within the site.
- 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 AudioCodes MP-118 located at the branch site.
- PBX features including Hold, Transfer, Call Waiting, Call Forwarding and Conference on Avaya 9600 SIP Phones in both Normal and Survivable Modes.
- Analog phones connected to the FXS ports on the AudioCodes MP-118 are properly adapted as SIP phones in both Normal and Survivable Modes.
- Messaging system access by branch phones (through internal access number in Normal Mode and PSTN call in Survivable Mode) and proper function of MWI (Messaging Waiting Indicator) on Avaya 9600 IP Phones.
- Proper system recovery after AudioCodes MP-118 restart and loss/restoration of IP connection.

The following observation was made during the testing using the sample configuration:

- **Call Waiting on analog phones connected to AudioCodes MP-118 FXS ports does not work after initial Flash button press**: when a new call arrives at the analog phone already in call with an Avaya 9600 SIP IP Phone, the first Flash button press correctly switches to the new call while placing the existing call on hold. However, subsequent Flash button presses do not switch between the two calls. Traces on SIP messages in this call scenario seemed to indicate the problem was with the Avaya 9600 SIP IP Phone: on second Flash button press to switch back to the original call with the Avaya 9600 SIP IP Phone, the IP phone sends the 200 OK message which contains SDP contents with an indication that the phone status is *inactive* .

- **Delayed ring-back for PSTN calls in Survivable Mode**: when branch phones call into PSTN through the FXO interface on the AudioCodes MP-118, there is a pause of about 3 to 4 seconds between end of dialing and start of ring-back. AudioCodes support and development engineers investigated and determined that this behavior is due to the interface between the MP-118 FXO and the specific Service Provider analog trunk used in the testing to verify the sample configuration.

- **In Survivable Mode, no secondary dial-tone for branch phones after dialing PSTN access digit**: currently there is no configuration on AudioCodes MP-118 that will enable a secondary dial-tone after a PSTN access digit is dialed for both IP and analog phones in the branch. Some specific configuration can enable the secondary dial-tone for the analog phones but not for IP phones.

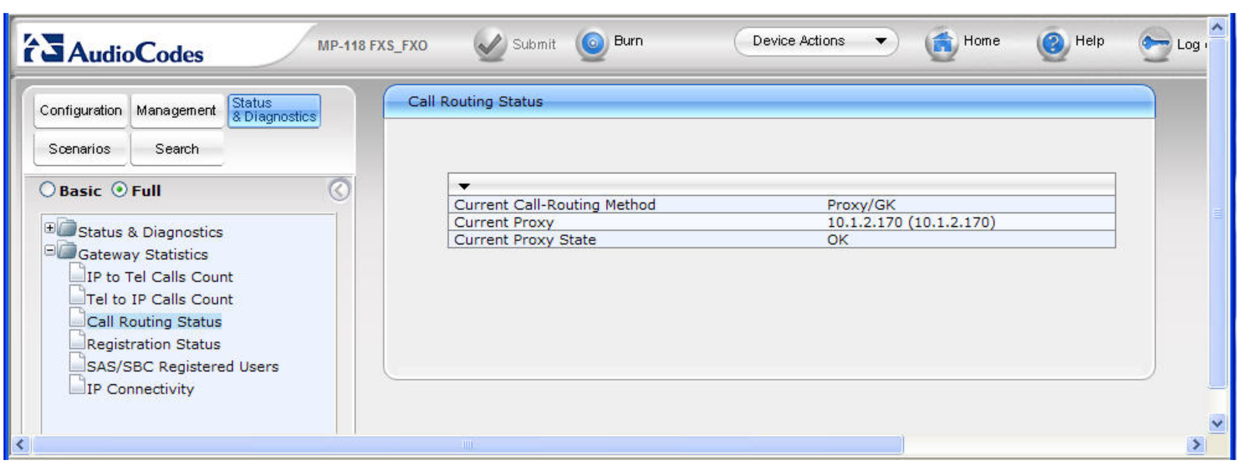
9. Verification

9.1. AudioCodes MP-118 Call Routing Status

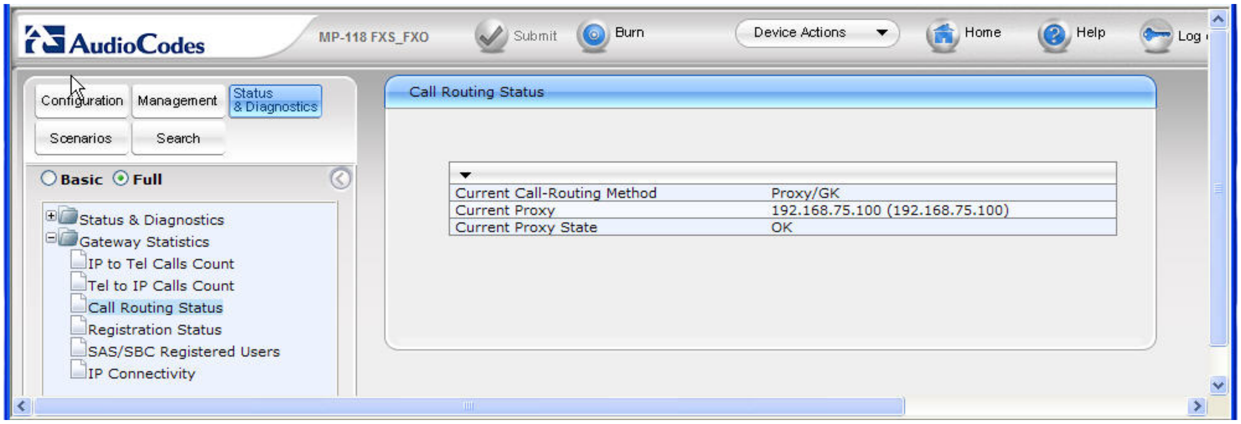
From the left navigation panel, select the **Status & Diagnostics** tab, then navigate to the Call Routing Status screen by selecting **Gateway Statistics → Call Routing Status**.

The Call Routing Status screens from the Branch 2 AudioCodes MP-118 while in Normal Mode and Survivable Mode are shown below.

Normal Mode:
The status shows all call routing is using the centralized Session Manager IP address which is in an “OK” state.



Survivable Mode:
The status shows all call routing is using the internal AudioCodes SAS Proxy IP address which is in an “OK” state.

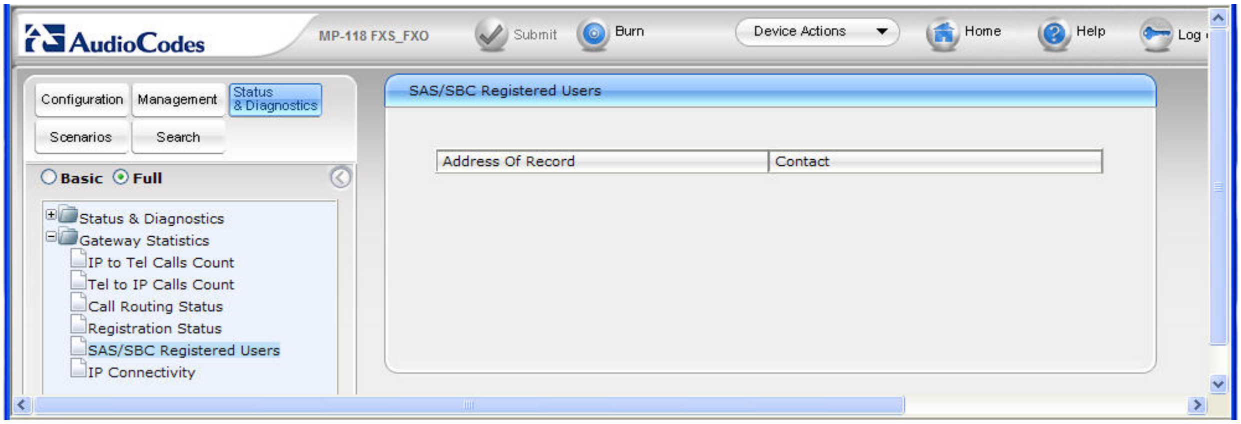


9.2. SAS/SBC Registered Users

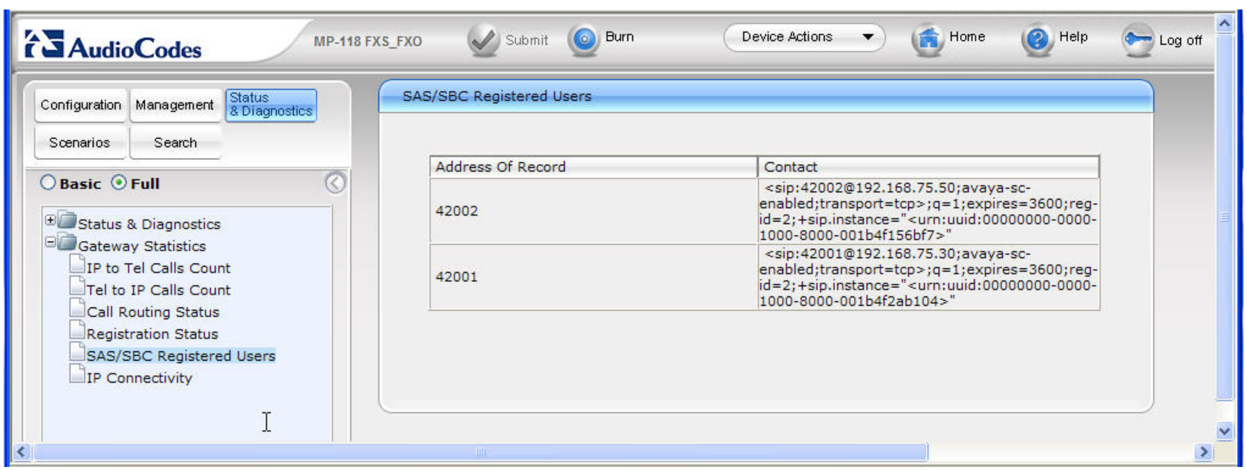
From the left navigation panel, select **Status & Diagnostics** then navigate to the SAS/SBC Registered Users screen by selecting **Gateway Statistics → SAS/SBC Registered Users**.

The SAS Registered Users screens from the Branch 2 AudioCodes MP-118 while in Normal Mode and Survivable Mode are shown below.

Normal Mode:
The screen shows no active SAS users.



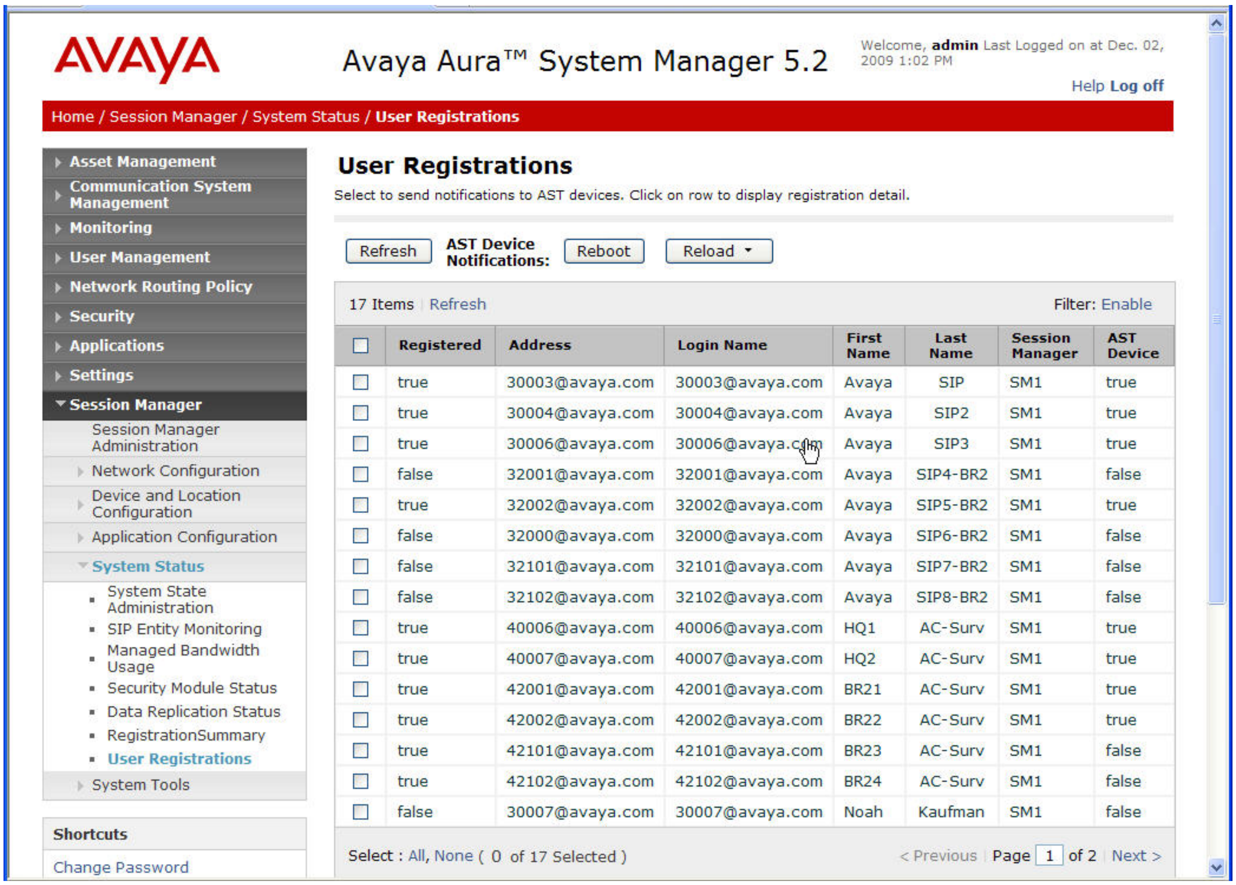
Survivable Mode:
The screen shows two Branch 2 Avaya 9600 SIP Phones actively registered to the AudioCodes MP-118 SAS.



9.3. Session Manager Registered Users

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

Note the user registrations for the 2 Avaya 9600 SIP Phones (42001 and 42002) and the two FXS stations (42101 and 42102) at the Branch 2 location. Also note the user registrations for the main site Avaya 9600 SIP Phones (40006 and 40007). 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
true	30003@avaya.com	30003@avaya.com	Avaya	SIP	SM1	true
true	30004@avaya.com	30004@avaya.com	Avaya	SIP2	SM1	true
true	30006@avaya.com	30006@avaya.com	Avaya	SIP3	SM1	true
false	32001@avaya.com	32001@avaya.com	Avaya	SIP4-BR2	SM1	false
true	32002@avaya.com	32002@avaya.com	Avaya	SIP5-BR2	SM1	true
false	32000@avaya.com	32000@avaya.com	Avaya	SIP6-BR2	SM1	false
false	32101@avaya.com	32101@avaya.com	Avaya	SIP7-BR2	SM1	false
false	32102@avaya.com	32102@avaya.com	Avaya	SIP8-BR2	SM1	false
true	40006@avaya.com	40006@avaya.com	HQ1	AC-Surv	SM1	true
true	40007@avaya.com	40007@avaya.com	HQ2	AC-Surv	SM1	true
true	42001@avaya.com	42001@avaya.com	BR21	AC-Surv	SM1	true
true	42002@avaya.com	42002@avaya.com	BR22	AC-Surv	SM1	true
true	42101@avaya.com	42101@avaya.com	BR23	AC-Surv	SM1	false
true	42102@avaya.com	42102@avaya.com	BR24	AC-Surv	SM1	false
false	30007@avaya.com	30007@avaya.com	Noah	Kaufman	SM1	false

9.4. Timing Expectations for Fail-over to AudioCodes SAS Mode

This section is intended to set *approximate* expectations for the length of time before Avaya 9600 SIP Telephones in the branch will acquire service from the AudioCodes Gateway, 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 register to the AudioCodes Gateway for SAS service before others, with the earliest registering 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 AudioCodes Gateway approximately two minutes after the branch is isolated by a WAN failure.

9.5. Timing Expectations for Fail-back to Normal Mode

This section is intended to set *approximate* expectations for the length of time before Avaya 9600 SIP Telephones registered to the AudioCodes Gateway in SAS 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 in 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.

10. Conclusion

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

11. References

Avaya Aura™ Session Manager:
[1] *Avaya Aura™ Session Manager Overview*, Doc ID 03-603473, available at http://support.avaya.com.
[2] *Installing and Upgrading Avaya Aura™ Session Manager*, Doc ID 03-603324, available at http://support.avaya.com.

[3] *Maintaining and Troubleshooting Avaya Aura™ Session Manager*, Doc ID 03-603325, available at http://support.avaya.com.
[4] *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:
[5] *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.
[6] *Administering Avaya Aura™ Communication Manager*, Doc ID 03-300509, May 2009, available at http://support.avaya.com.

Avaya one-X Deskphone Edition 9600 Series SIP IP Telephones:
[7] *Avaya one-X Deskphone Edition for 9600 SIP IP Telephones Administrator Guide*, Doc ID 16-601944, December 2009, available at http://support.avaya.com.

Avaya Messaging Applications
[8] *Avaya Aura™ Communication Manager Messaging Installation and Initial Configuration*, Doc ID 03-603353, May 2009, available at http://support.avaya.com.
[9] *Modular Messaging Admin Guide Release 5.2 with Avaya MSS*, November 2009, available at http://support.avaya.com.

Avaya Application Notes:
[10] *Front-Ending Nortel Communication Server 1000 with an AudioCodes Mediant 1000 Modular Media Gateway to Support SIP Trunks to Avaya Aura™ Session Manager with Avaya Aura™ Communication Manager 5.2 as an Access Element – Issue 1.1*, available at http://www.avaya.com.

AudioCodes MP-118:
[11] *AudioCodes SIP MP-11x & MP-124 Release Notes*, Version 5.8, Document #: LTRT-65614, October 09, available at http://www.audiocodes.com.
[12] *AudioCodes SIP MP-11x & MP-124 SIP User's Manual*, Version 5.8, Document #: LTRT-65412, October 09, available at http://www.audiocodes.com.