Avaya Solution & Interoperability Test Lab

Configuring a Survivable SIP Gateway Solution using the Avaya Secure Router, Avaya Aura™ Session Manager 5.2, Avaya Aura™ Communication Manager 5.2.1, and Avaya Modular Messaging 5.2 in a Distributed Trunking Configuration – Issue 1.0

Abstract

These Application Notes present a sample configuration of a Survivable SIP Gateway Solution using the Avaya Secure Router, Avaya Aura™ Session Manager 5.2, Avaya Aura™ Communication Manager 5.2.1, and Avaya Modular Messaging 5.2 in a Distributed Trunking Configuration.

The Survivable SIP Gateway Solution addresses the risk of service disruption for SIP endpoints deployed at remote branch locations if connectivity to the centralized Avaya SIP call control platform is lost. Connectivity loss can be caused by WAN access problems being experienced at the branch or network problems at the central site blocking access to the Avaya SIP call control platform. The solution monitors 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 Avaya Secure Router dynamically switch to survivability mode, restoring telephony services at the branch for intra-branch and PSTN calling.

The Avaya Secure Routers 2330 and 4134 support SIP gateway capability and SIP survivability, and are intended for use as survivable SIP gateways and integrated branch routers. The results shown in this document were obtained using the SR2330 platform. The SR2330 and SR4134 share common software, interface modules, and software licenses, and the same results should be expected from the SR4134 platform.

Testing was conducted at the Avaya Solution and Interoperability Test Lab at the request of Avaya Unified Branch Product Management.
1. Introduction

These Application Notes present a sample configuration of a Survivable SIP Gateway Solution using the Avaya Secure Router, Avaya Aura™ Session Manager 5.2, Avaya Aura™ Communication Manager 5.2.1, and Avaya Modular Messaging 5.2 in a Distributed Trunking Configuration.

The Survivable SIP Gateway Solution addresses the risk of service disruption for SIP endpoints deployed at remote branch locations if connectivity to the centralized Avaya SIP call control platform is lost. Connectivity loss can be caused by WAN access problems being experienced at the branch or network problems at the centralized site blocking access to the Avaya SIP call control platform. The solution monitors connectivity health from the remote branch to the central Avaya SIP call control platform. When connectivity loss is detected, Avaya one-X Deskphone SIP 9600 Series IP Telephones as well as the Avaya Secure Router 2330 dynamically switch to survivability mode, restoring telephony services at the branch for intra-branch and PSTN calling. When connectivity from the branch to the centralized Avaya SIP call control platform is restored, SIP components can dynamically switch back to normal operation.

The Avaya Secure Routers 2330 and 4134 support SIP gateway capability and SIP survivability, and are intended for use as survivable SIP gateways and integrated branch routers. The results shown in this document were obtained using the SR2330 platform. The SR2330 and SR4134 share common software, interface modules, and software licenses, and the same results should be expected from the SR4134 platform.

2. Overview

2.1. Avaya Secure Router 2330

The Avaya Secure Router 2330, referred to as the SR2330 throughout the remainder of this document, takes on various roles based on call flows and network conditions. The following lists these roles:

- Branch router
- SIP Media Gateway (FXO interfaces to PSTN, FXS interfaces to analog endpoints)
- SIP Survivability Module (Registrar and Proxy, dynamically activated on detection of lost connectivity to Session Manager)

When the SR2330 is serving the Registrar/Proxy role, it is said to be in Survivable Mode.

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

The Avaya one-X Deskphone SIP 9600 Series IP Telephone, also referred to as Avaya 9600 SIP Phone in these Application Notes, is also a key component of the Survivable SIP Gateway Solution. The 2.5 firmware release of the Avaya 9600 SIP Phone includes feature capabilities specific to SIP survivability, enabling the phone to monitor connectivity to Session Manager and dynamically fail over to the local SR2330 as an alternate or survivable SIP server. See reference [1] for additional information on the Avaya 9600 SIP Phone.
2.3. Avaya Aura™ Communication Manager

In the sample configuration, the main Headquarters/Datacenter location includes two Communication Manager systems that serve different roles. The Communication Manager operating as a feature server (hereafter abbreviated FS) supports calling features for the SIP phones in the main location and also in the branch locations in normal mode. The Communication Manager operating as an access element (hereafter abbreviated AE) supports non-SIP telephones as well as centralized PSTN trunks. The PSTN trunks are accessible from the telephones at all locations. Unless otherwise specified in these Application Notes, the term “Communication Manager” refers to the feature server.

2.4. PSTN Trunking Configurations

The 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 by Session Manager and Communication Manager 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 the Survivable SIP Gateway Solution:

Centralized Trunking: All PSTN calls, inbound to the enterprise and outbound from the enterprise, are routed to/from PSTN media gateways centrally located at the Headquarters/Datacenter location.

Distributed Trunking: PSTN call routing can be determined based on the originating source location using Session 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 SR2330 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 Distributed Trunking call flows presented in Section 2.6 provide additional details of how calls are routed based on the location of the caller and the number being called. Incoming calls calls from the PSTN through the local branch FXO interface are routed up to Session Manager and Communication Manager FS so that the appropriate termination services can be applied to the destination phone in the branch.

The sample configuration presented in these Application Notes implements a Distributed Trunking configuration.
2.5. Network Modes

PSTN call routing is further determined within each of the trunking configurations based on the network status of each branch.

**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 communication with the Headquarters/Datacenter location, and the local branch SR2330 SIP call control is being used for all calls at that branch. Note: if the Session Manager loses connectivity to the WAN, all branches will go into survivable mode simultaneously.

2.6. Call Flows

The section presents the primary call flows for the Survivable SIP Gateway Solution in a Distributed Trunking configuration for both Normal Mode and Survivable Mode. The components included in these call flows are based on the components used in the sample configuration presented in these Application Notes.

2.6.1. Distributed Trunking – Normal Mode

**Overview:**
- **SIP Call Control:** All SIP call control and call routing is provided by the centralized Session Manager and Communication Manager.
- **Branch PSTN Outbound Local:** Session Manager Location Based Routing is used to route these calls to the local branch SR2330 FXO interface.
- **Branch PSTN Outbound Non-Local:** PSTN outbound calls from the branch to non-local numbers are routed to a centralized Avaya G650 Media Gateway controlled by the Communication Manager AE.
- **Branch PSTN Inbound:** Calls from the PSTN to a branch Listed Directory Number (LDN) enter the network at the local branch SR2330 FXO interface, then route to the Session Manager/Communication Manager for call treatment.
- **Headquarters PSTN Inbound:** Calls to Headquarters endpoints enter the network at the Headquarters Avaya G650 Media Gateway controlled by the Communication Manager AE.
Call Flows:

1. **Avaya 9600 SIP Phone at branch to H.323 IP phone at Headquarters.**

   Avaya 9600 SIP → Session Manager → Communication Manager FS → Session Manager → Communication Manager AE → H.323 IP phone

2. **Avaya 9600 SIP Phone at branch to Digital/Analog phone at Headquarters.**

   Avaya 9600 SIP → Session Manager → Communication Manager FS → Session Manager → Communication Manager AE → Avaya G650 Media Gateway → Digital/Analog phone

3. **Avaya 9600 SIP Phone at branch to PSTN endpoint – Local Number**

   Avaya 9600 SIP → Session Manager → Communication Manager FS → Session Manager → SR2330 FXO → PSTN phone

4. **Avaya 9600 SIP Phone at branch to PSTN endpoint – Long Distance Number**

   Avaya 9600 SIP → Session Manager → Communication Manager FS → Session Manager → Communication Manager AE → Avaya G650 Media Gateway → PSTN phone

5. **Avaya 9600 SIP Phone at branch to Avaya 9600 SIP phone at same branch.**

   Avaya 9600 SIP → Session Manager → Communication Manager FS → Session Manager → Communication Manager FS → Session Manager → Avaya 9600 SIP

6. **PSTN phone to Branch LDN assigned to Avaya 9600 SIP phone.**

   PSTN phone → SR2330 FXO → Session Manager → Communication Manager FS → Session Manager → Communication Manager FS → Session Manager → Avaya 9600 SIP
**2.6.2. Distributed Trunking – Survivability Mode**

*Overview:*

- **SIP Call Control:** All SIP call control and call routing is provided by the local branch SR2330.

- **SIP Registration:** All branch Avaya 9600 SIP Phones have transitioned to use the SR2330, to which they were already registered.

- **All Branch PSTN Outbound:** Local and Non-Local: Routed to the SR2330 FXO interface.

- **Branch PSTN Inbound:** Calls from the PSTN to a branch LDN or DID enter the network at the local branch SR2330 FXO interface. The SR2330 routes the call to a phone assigned to the FXO interface or to a locally registered 9600 SIP phone.
Call Flows:
1. Avaya 9600 SIP Phone at branch to PSTN endpoint – Local & Non-Local
   Avaya 9600 SIP → SR2330 FXO → PSTN phone
2. PSTN phone to Branch LDN or DID assigned to Avaya 9600 SIP phone.
   PSTN phone → SR2330 FXO → Avaya 9600 SIP
3. Avaya 9600 SIP Phone at branch to Avaya 9600 SIP phone at same branch.¹
   Avaya 9600 SIP → SR2330 → Avaya 9600 SIP

Figure 2 presents a high level view of the Distributed Trunking Survivable Mode call flows.

¹ Note that for inter-branch calling in survivable mode, branch users would need to dial the full LDN or DID for the other branch location, since Dial Plan Transparency is not supported.
2.6.3. Detailed Call Flow: Branch PSTN Outbound Local – Normal Mode

Many of the Session Manager and Communication Manager configuration steps presented in Section 4 and Section 5 are to support the location based routing requirements of the Branch PSTN Outbound Local – Normal Mode call flow. The details of this call flow, specific to the sample configuration, are included here to illustrate the linkage of the various configuration steps. As mentioned earlier, the term “Communication Manager” refers to Communication Manager FS.

Branch PSTN Outbound Local – Normal Mode:

Branch 2 Avaya 9600 SIP Phone user dials the following local PSTN number:

9 1-908-766-1111.

1. Branch 2 Avaya 9600 SIP Phone sends SIP INVITE to Session Manager with dialed digit string of 919087661111.
2. Session Manager receives the SIP INVITE and identifies the Avaya 9600 SIP Phone user has an assigned Communication Manager Extension. Session Manager forwards the SIP INVITE to Communication Manager.
3. Communication Manager receives the SIP INVITE from Session Manager on SIP Trunk Group Number 60.
4. Communication Manager identifies the IP address of the Avaya 9600 SIP Phone in the Contact field of the SIP INVITE message as an IP address mapped to IP Network Region 10.
5. The leading 9 in the dialed digit string is identified by Communication Manager as the ARS Access Code. The 9 is removed from the dialed digit string.
6. The ARS Digit Analysis Table is queried for a match on the remaining digits 19087661111.
7. A match on 1908766 is found and Route Pattern 60 is chosen.
8. Route Pattern 60 routes the call to SIP Trunk Group Number 60.
9. Communication Manager sends a new SIP INVITE to Session Manager over SIP Trunk Group Number 60 with the dialed digits of 19087661111.
10. Session Manager matches on the digits 1908766 of the dialed number and identifies the calling phone as part of Location “Branch 2” and identifies the next hop as the Branch 2 SR2330 with IP address 20.20.20.1 using TCP port 5080.
11. Session Manager forwards the SIP INVITE with dialed digits string 19087661111 to the Branch 2 SR2330.
12. The Branch 2 SR2330 internally routes the call to an FXO interface for termination on the PSTN.
2.7. Network Topology

The network implemented for the sample configuration shown in Figure 1 and Figure 2 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 are shown, the Branch 2 configuration was implemented and is highlighted.

The Headquarters location hosts Session Manager and a Communication Manager FS running on an Avaya S8510 server, providing enterprise wide SIP call control and advanced feature capabilities. The Headquarters network is mapped to IP Network Region 1 within Communication Manager FS. The Distributed Trunking capabilities of the solution utilize the location based call routing features of Session Manager and IP codec set selection features of Communication Manager FS, and requires the information presented in Table 1.

<table>
<thead>
<tr>
<th>IP Network</th>
<th>IP Network Region</th>
<th>Location</th>
<th>Area Code &amp; Exchange</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.2.0/24</td>
<td>1</td>
<td>Basking Ridge</td>
<td>All other</td>
</tr>
<tr>
<td>20.20.20.0/24</td>
<td>10</td>
<td>Branch 2</td>
<td>908-766</td>
</tr>
</tbody>
</table>

Table 1 – Network Information

The Headquarters location also hosts the following centralized components: a Communication Manager AE, running on Avaya S8720 redundant servers controlling an Avaya G650 Media Gateway with PSTN trunks, an Avaya Modular Messaging voice mail platform, and an Avaya IP Phone Configuration File Server. The configuration details of these components are considered out of scope of these Application Notes and are 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 7 includes the parameters of the 46xxsettings.txt file used by the Avaya 9600 SIP Phone for survivability. The Avaya Modular Messaging voice mail platform can be reached by dialing the internal extension configured as the voice mail access number or pilot number, or by dialing a PSTN number that also terminates to Modular Messaging. The internal or private 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 phone is in Survivable Mode. This enables branch users to continue to access the centralized voice mail platform while in Survivable Mode via the PSTN using the Message button. Traditional Message Waiting Indication via the telephone is not available while the phone is in Survivable Mode. The messaging system, such as Avaya Modular Messaging, may enable other methods of notification that a message has been delivered.
The branch location consists of several Avaya 9600 SIP Phones and an SR2330 Secure Router with two PSTN Analog trunks on FXO interfaces and two analog phones on FXS interfaces. A flat network has been implemented at the branch. In the sample configuration (see Figure 3), the SR2330 uses its LAN side IP address (20.20.20.1) for SIP signaling. Its SIP Media Gateway Module listens for SIP requests on port 5080. Requests can come from either the Session Manager in the Headquarters location or the SIP Survivability Module within the SR2330. In survivable mode, the SIP Survivability Module listens on port 5060 for SIP requests from the branch Avaya one-X Deskphone SIP 9600 Series IP Telephones, and proxies those requests to the Media Gateway module as necessary (e.g., for calls to the FXS or FXO interfaces). In normal mode, the IP telephones signal through the SR2330 directly to Session Manager.

![Figure 3](image-url)
3. Equipment and Software Versions

The information in these Application Notes is based on the software and hardware versions listed in Table 2.

<table>
<thead>
<tr>
<th>Device Description</th>
<th>Versions Tested</th>
</tr>
</thead>
<tbody>
<tr>
<td>S8720 Server with G650 Media Gateway</td>
<td>Avaya Aura™ Communication Manager 5.2.1, Service Pack 1</td>
</tr>
<tr>
<td>S8510 Server with G450 Media Gateway</td>
<td></td>
</tr>
<tr>
<td>Avaya S8510 Server</td>
<td>Session Manager 5.2 Service Pack 1, Load 5.2.1.0.52010</td>
</tr>
<tr>
<td></td>
<td>System Manager 5.2 Service Pack 1, Load 5.2.1.0.521001</td>
</tr>
<tr>
<td>Avaya Modular Messaging (MAS)</td>
<td>5.2, Build 9.2.150.13 (Patch 520008)</td>
</tr>
<tr>
<td>Avaya Modular Messaging (MSS)</td>
<td>5.2, Build 5.2-11.0</td>
</tr>
<tr>
<td>Avaya one-X Deskphone SIP 9600 Series IP Telephones</td>
<td>2.5.0</td>
</tr>
<tr>
<td>Avaya one-X Deskphone H.323 9600 Series IP Telephones</td>
<td>3.1</td>
</tr>
<tr>
<td>Avaya 6210 Analog Telephone</td>
<td>-</td>
</tr>
<tr>
<td>Avaya SR2330 Secure Router</td>
<td>10.2.1</td>
</tr>
</tbody>
</table>

Table 2 – Software/Hardware Version Information
4. Configure Avaya Aura™ Session Manager

This section describes the administration steps for Session Manager that implement the Survivable SIP Gateway Solution. The following areas are covered:

- SIP domain
- Location configuration for Branch 2
- SIP Entity configuration for the SR2330 Secure Router
- Entity Link, which defines the SIP trunk parameters used by Session Manager when routing calls to/from the SR2330 Secure Router
- Location based routing policy corresponding to the dial plan definitions
- Dial pattern configurations for routing calls to long distance and branch-local PSTN destinations
- User configuration for branch SIP and analog telephones

It is assumed that configuration of SIP trunks between Session Manager and the Communication Manager FS and AE has already been completed.

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 below will be used to configure all of the above except the SIP users (Sections 4.1 through 4.6).

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 follows:

Step 1: Create "Domains" of type SIP (other NRP applications are refining 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"
4.1. 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 (e.g., “avaya.com”)
- **Notes:** Descriptive text (optional).

Click **Commit**.

---

**Avaya Aura™ System Manager 5.2**

---

**Domain Management**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>avaya.com</em></td>
<td>15s</td>
<td>30s</td>
<td></td>
</tr>
</tbody>
</table>

* Input Required

---
4.2. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of location based routing, 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).

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 Branch 2 location, which includes the SR2330 Secure Router and the Avaya 9630 IP Telephones (SIP) in the 20.20.20.0/24 subnet. This location will be used in the configuration of routing policies for Branch 2. Click **Commit** to save the Location definition.

The fields under **General** can be filled in to specify bandwidth management parameters between Avaya Session Manager and this location. These were not used in the sample configuration, and reflect default values.

---

2 Note that even though the **WAN** interface on the SR2330 is 10.1.2.68, the **SIP signaling** interface on the SR2330 is bound to the LAN side 20.20.20.1 address. See **Section 6**.
4.3. Add SIP Entity

This section describes the configuration of the SIP Entity corresponding to the SR2330 in Branch 2. Select **SIP Entities** on the left and click on the **New** button (not shown) on the right.

Under **General**, fill in:

- **Name:** A descriptive name.
- **FQDN or IP Address:** FQDN or IP address of the SIP signaling interface on the SR2330 (See Section 6).
- **Type:** “Other”.
- **Location:** Select the location defined previously.
- **Time Zone:** Time zone for this location.

Under **SIP Link Monitoring**, fill in:

- **Proactive Monitoring Interval (in seconds):** How frequently to test the link via SIP OPTIONs messages when the link is marked in the “up” state.
- **Reactive Monitoring Interval (in seconds):** How frequently to test the link via SIP OPTIONs messages when the link is marked in the “down” state.
- **Number Of retries:** Number of attempts to send SIP OPTIONs before the link is marked “down”.
The screen below shows the resulting SIP Entity configured for the SR2330, as well as the recommended Link Monitoring values. These values are set such that when communication with the branch has been restored after a failure, there is a high probability that the link has been marked back up by Session Manager before the Avaya 9630 SIP telephones have re-registered with Session Manager. Then calls from these phones to the local PSTN will be routed to the SR2330, as opposed to being denied if the link were still marked down.

Click **Commit** to save the SIP Entity definition.
4.4. Add Entity Link

A SIP trunk between Session Manager and a telephony system is described by an Entity link. 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 desired Session Manager.
- **Protocol:** Select TCP.
- **Port:** Port number to which the SR2330 sends SIP requests.
- **SIP Entity 2:** Select the name of the SR2330.
- **Port:** Port number on which the SR2330 receives SIP requests (See Sections 2.7 and 6).
- **Trusted:** Check this box. **Note:** If this box is not checked, calls from the associated SIP Entity specified in Section 4.3 will be denied.

Click **Commit** to save the Entity Link definition. The following screen shows adding the Entity Link for the SR2330.
4.5. Add Routing Policies
Routing policies describe the conditions under which calls will be routed to SIP Entities. For the sample configuration, a routing policy has been added for routing calls to the Branch 2 SR2330. To add a routing policy, select Routing Policies on the left and click on the New button (not shown) on the right. The following screen is displayed. Fill in the following:

Under General:
Enter a descriptive name in Name.

Under SIP Entity as Destination:
Click Select, and then select the appropriate SIP entity to which this routing policy applies, in this case “SR2330”

Under Time of Day:
Select the default time range shown.

Defaults can be used for the remaining fields. Click Commit to save the Routing Policy definition. The following screen shows the Routing Policy for the Branch 2 SR2330.
4.6. Add Dial Patterns

Define dial patterns to direct calls to the Branch 2 SR2330 SIP Entity. These dial patterns affect calls from telephones at Branch 2, defined by their 20.20.20.x subnet addresses in the “Branch 2” Location (see Section 4.2). This includes the Avaya 9630 SIP telephones, as well as the analog FXS telephones connected to the SR2330, on whose behalf the SR2330 has registered with Session Manager. For the sample configuration, two dial patterns were defined for routing calls to the SR2330, which will in turn route them to its locally connected FXO analog trunks:

1-908-766-xxxx  Calls from Branch 2 telephones to local PSTN numbers

911  911 calls dialed by Branch 2 telephones.

Note that calls to Branch 2 users do not require a dial pattern, since they are directly registered to Session Manager. To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following, as shown in the screens below:

Under **General**:

- **Pattern**: Dialed number or prefix.
- **Min**: Minimum length of dialed number.
- **Max**: Maximum length of dialed number.
- **SIP Domain**: SIP domain specified in Section 4.1
- **Notes**: Comment on purpose of dial pattern.

Under **Originating Locations and Routing Policies**:

Click **Add**, and then select the “Branch 2” location and routing policy from the list.

Default values can be used for the remaining fields. Click **Commit** to save each dial pattern. The following screen shows the dial pattern definition for 1-908-766-xxxx. Repeat the above steps for the 911 dial pattern. The second screen shows the resulting display of the Routing Policy for the Branch 2 SR2330 SIP Entity and both associated dial patterns.
### Dial Pattern Details

#### General
- **Pattern**: 1908766
- **Min**: 11
- **Max**: 11
- **Emergency Call**: [Box]
- **SIP Domain**: avaya.com
- **Notes**: Local calls to PSTN via SR2330 FXO ports

#### Originating Locations and Routing Policies

<table>
<thead>
<tr>
<th>Originating Location Name</th>
<th>Originating Location Notes</th>
<th>Routing Policy Name</th>
<th>Rank</th>
<th>Routing Policy Disabled</th>
<th>Routing Policy Destination</th>
<th>Routing Policy Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch 2</td>
<td></td>
<td>avaya SR2330</td>
<td>0</td>
<td></td>
<td>SR2330</td>
<td>Gateway at Branch 2</td>
</tr>
</tbody>
</table>

Select: All, None (0 of 1 selected)
### Routing Policy Details

#### General

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Avaya SR2330</td>
</tr>
<tr>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td>Gateway at Branch 2</td>
</tr>
</tbody>
</table>

#### SIP Entity as Destination

<table>
<thead>
<tr>
<th>Name</th>
<th>FQDN or IP Address</th>
<th>Type</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SR2339</td>
<td>20.20.20.1</td>
<td>Other</td>
<td></td>
</tr>
</tbody>
</table>

#### Time of Day

<table>
<thead>
<tr>
<th>Name</th>
<th>Start Time</th>
<th>End Time</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>24/7</td>
<td>00:00</td>
<td>23:59</td>
<td>Time Range 24/7</td>
</tr>
</tbody>
</table>

#### Dial Patterns

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Min</th>
<th>Max</th>
<th>Emergency Call</th>
<th>SIP Domain</th>
<th>Originating Location</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1400746</td>
<td>11</td>
<td>11</td>
<td></td>
<td>avaya.com</td>
<td>Branch 2</td>
<td></td>
</tr>
<tr>
<td>911</td>
<td>9</td>
<td>9</td>
<td></td>
<td>avaya.com</td>
<td>Branch 2</td>
<td></td>
</tr>
</tbody>
</table>

Select: All, None (0 of 1 Selected)

#### Regular Expressions

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Rank Order</th>
<th>Deny</th>
<th>Notes</th>
</tr>
</thead>
</table>

* Input Required
4.7. SIP Users

This section describes the administration of SIP telephones in Session Manager, and applies to the 9600 series SIP telephones as well as the analog telephones connected to the FXS ports of the SR2330, which registers with Session Manager on their behalf. It is assumed that the SIP trunk between Communication Manager and Session Manager has already been provisioned. References [4] and [6] contain information on configuring SIP trunks between a Communication Manager FS and Session Manager. The following screens show a sample configuration for an Avaya 9630 SIP phone whose extension is 31003. The same procedure should be followed for all branch IP and analog telephones.

On the main configuration page, select **User Management** under **User Management**, and click **New** to administer a new telephone user.

This will create a new User Profile. In the **General** section, enter a **Last Name** and **First Name**. Note that fields marked with * are required to be filled in.
The following screen shows what was entered for extension 31003.

In the *Identity* section, enter a Login Name, for example 31003@avaya.com, and the required passwords, as shown on the next screen. Note that the *Shared Communication Profile* password is the one the telephone is required to use when registering to Session Manager. It is also recommended to enter both display names with the same data. *SMGR Login Password*, while required, was not used in this sample configuration, and can be any value.
The information below is what was entered for extension 31003. Note that the passwords are not displayed when viewing an endpoint’s configuration.

In the **Communication Profile** section, there are three sub-sections that need to be filled in: Communication Address, Session Manager, and Station Profile. Clicking on the arrow next to Communication Profile reveals the other sections.

Click **New** under **Communication Address**.
Set **Subtype** to “username”, and fill in the extension portion of the **Fully Qualified Address**, e.g., “31003”. “@avaya.com” will be automatically filled in. Then click **Add**. This will move the entry to the table as shown in the previous screen.

Click on the box next to **Session Manager**, and select the appropriate **Session Manager Instance** from the list. Select the appropriate **Origination** and **Termination Application Sequence**.

The screen below shows what was used for extension 31003.
Click on the box next to **Station Profile**, and enter the appropriate **System**, which is the Communication Manager FS supporting the telephone. Leave **Use Existing Stations** unchecked, causing Session Manager to automatically generate the station and Off-PBX station-mapping forms in Communication Manager.³ Enter an **Extension**, and select ”DEFAULT_9630SIP” for the **Template**. Leave the **Security Code** blank. Select “IP” for the **Port** field. The screen below shows what was used for extension 31003.

³ System Manager uses the **Localized Display Name** field to populate the **Name** field in the station form in Communication Manager. Additional fields can be populated in Communication Manager later, if needed. See **Section 5.6**.

⁴ This value for the **Template** also can be used for the analog telephone users supported by the FXS interfaces on the SR2330.

When done click **Commit** at the bottom of the web page. Repeat the above steps for each telephone to be configured.
5. Configure Avaya Aura™ Communication Manager

This section shows the necessary steps to configure Communication Manager FS to support the Survivable SIP Gateway Solution in a Distributed Trunking scenario. It is assumed that the basic configuration on Communication Manager and the required licensing have already been administered, as well as the SIP trunk to Session Manager. See References [3, 6] for additional information. All commands discussed in this section are executed on Communication Manager using the System Access Terminal (SAT).

5.1. IP Codec Set

The voice codec to be used is defined in the IP Codec Set form. For the sample configuration, a single codec set is used with a single codec defined. The `change ip-codec-set` command is shown below to define Codec Set 1 where the G.711MU codec is entered.

```
change ip-codec-set 1

Codec Set: 1

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

Media Encryption
1: none
2:
3:
```
5.2. IP Network Region

IP Network Regions are defined for each branch location as well as the Headquarters location as defined in Table 1 using the `change ip-network-region` command. The values used in the sample configuration for Headquarters IP Network Region 1 are shown below. The Name, Codec Set and Authoritative Domain field values shown are specific to the sample configuration. All remaining fields have been left at default values. The Authoritative Domain is the SIP domain name defined Session Manager (see Section 4.1) and used throughout the enterprise for SIP communications.

```
change ip-network-region 1
  Region: 1
  Location: HQ CM and SIP Phones
  Name: HQ CM and SIP Phones
  Authoritative Domain: avaya.com
  MEDIA PARAMETERS
    Codec Set: 1
    UDP Port Min: 2048
    UDP Port Max: 65535
  DIFFSERV/TOS PARAMETERS
    RTCP Reporting Enabled? y
  Call Control PHB Value: 46
  Audio PHB Value: 46
  Video PHB Value: 26
  802.1P/Q PARAMETERS
    Call Control 802.1p Priority: 6
    Audio 802.1p Priority: 6
    Video 802.1p Priority: 5
  AUDIO RESOURCE RESERVATION PARAMETERS
    H.323 IP ENDPOINTS
    RSVP Enabled? n
```

The values used in the sample configuration for Branch 2 IP Network Region 10 are shown below (abbreviated). The Name, Codec Set and Authoritative Domain field values shown are specific to the sample configuration. All remaining fields have been left at default values. Follow the same steps to create the IP Network Regions for other branch locations.

```
change ip-network-region 10
  Region: 10
  Location: Branch 2 SR2330
  Name: Branch 2 SR2330
  Authoritative Domain: avaya.com
  MEDIA PARAMETERS
    Codec Set: 1
    UDP Port Min: 2048
    UDP Port Max: 3029
  DIFFSERV/TOS PARAMETERS
    RTCP Reporting Enabled? y
  Call Control PHB Value: 46
  Audio PHB Value: 46
  Video PHB Value: 26
  802.1P/Q PARAMETERS
    Call Control 802.1p Priority: 6
    Audio 802.1p Priority: 6
    Video 802.1p Priority: 5
  AUDIO RESOURCE RESERVATION PARAMETERS
    H.323 IP ENDPOINTS
    RSVP Enabled? n
```
The following screen illustrates a portion of Page 3 for network region 10. The connectivity between network regions is specified under the **Inter Network Region Connection Management** heading, beginning on Page 3. For example, **codec set 1** is specified for connections between network region 10 and network region 1. If bandwidth usage is a concern, a different codec set could be defined that uses a compressed codec (e.g., G.729) between the Headquarters and Branch 2 locations, and would be specified here.

<table>
<thead>
<tr>
<th>change ip-network-region 10</th>
<th>Page 3 of 19</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Region: 10</td>
<td>Inter Network Region Connection Management</td>
</tr>
<tr>
<td>dst codec direct WAN-BW-limits Video Intervening Dyn A G a</td>
<td></td>
</tr>
<tr>
<td>rgn set WAN Units Total Norm Prio Shr Regions CAC R L s</td>
<td></td>
</tr>
<tr>
<td>1 l y NoLimit</td>
<td>n</td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

### 5.3. IP Network Map

IP addresses are used to associate a device with a specific IP Network Region. The **change ip-network-map** command is used to perform the IP address to IP Network Region mapping. The IP Address Mapping used in the sample configuration is shown below based on the information from Table 1. In this case, the full subnet for Branch 2 is entered with the corresponding IP Network Region number.

<table>
<thead>
<tr>
<th>change ip-network-map</th>
<th>Page 1 of 63</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP ADDRESS MAPPING</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>Subnet</td>
</tr>
<tr>
<td>FROM: 10.1.2.0</td>
<td>/24</td>
</tr>
<tr>
<td>TO: 10.1.2.255</td>
<td></td>
</tr>
<tr>
<td>FROM: 20.20.20.0</td>
<td>/24</td>
</tr>
<tr>
<td>TO: 20.20.20.255</td>
<td></td>
</tr>
</tbody>
</table>
5.4. Automatic Route Selection (ARS)
The ARS entries highlighted in this section focus on the local and long distance dialing from branch locations.

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

<table>
<thead>
<tr>
<th>change feature-access-codes</th>
<th>Page 1 of 9</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEATURE ACCESS CODE (FAC)</td>
<td></td>
</tr>
<tr>
<td>Abbreviated Dialing List1 Access Code: 621</td>
<td></td>
</tr>
<tr>
<td>Abbreviated Dialing List2 Access Code: 622</td>
<td></td>
</tr>
<tr>
<td>Abbreviated Dialing List3 Access Code: 623</td>
<td></td>
</tr>
<tr>
<td>Abbreviated Dial - Prgm Group List Access Code:</td>
<td></td>
</tr>
<tr>
<td>Announcement Access Code: 626</td>
<td></td>
</tr>
<tr>
<td>Answer Back Access Code: 625</td>
<td></td>
</tr>
<tr>
<td>Attendant Access Code:</td>
<td></td>
</tr>
<tr>
<td>Auto Alternate Routing (AAR) Access Code: 8</td>
<td></td>
</tr>
<tr>
<td>Auto Route Selection (ARS) - Access Code 1: 9</td>
<td></td>
</tr>
<tr>
<td>Access Code 2:</td>
<td></td>
</tr>
<tr>
<td>Automatic Callback Activation: *5 Deactivation: #5</td>
<td></td>
</tr>
<tr>
<td>Call Forwarding Activation Busy/DA: *2 All: 612 Deactivation: #2</td>
<td></td>
</tr>
<tr>
<td>Call Forwarding Enhanced Status: Act: Deactivation:</td>
<td></td>
</tr>
<tr>
<td>Call Park Access Code: 624</td>
<td></td>
</tr>
<tr>
<td>Call Pickup Access Code: *6</td>
<td></td>
</tr>
<tr>
<td>CAS Remote Hold/Answer Hold-Unhold Access Code: #6</td>
<td></td>
</tr>
<tr>
<td>CDR Account Code Access Code:</td>
<td></td>
</tr>
<tr>
<td>Change COR Access Code:</td>
<td></td>
</tr>
<tr>
<td>Change Coverage Access Code:</td>
<td></td>
</tr>
<tr>
<td>Conditional Call Extend Activation: Deactivation:</td>
<td></td>
</tr>
<tr>
<td>Contact Closure Open Code: Close Code:</td>
<td></td>
</tr>
</tbody>
</table>

5.4.2. ARS Digit Analysis
The change ars analysis y command is used to make global routing entries where “y” is the dialed digit string to match. The global ARS table used in the sample configuration is shown below. Calls to 1 + 10 digits, and emergency 911 calls will select Route Pattern 60, which will select the SIP trunk to Session Manager, not described in these Application Notes. Note that since the Communication Manager in the sample configuration is a Feature Server and has no PSTN gateways under its control, all PSTN numbers are configured to route to Session Manager, which can use location based routing to determine which gateway in the network should handle this call.

<table>
<thead>
<tr>
<th>change ars analysis 19</th>
<th>Page 1 of 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARS DIGIT ANALYSIS TABLE</td>
<td>Percent Full: 0</td>
</tr>
<tr>
<td>Location: all</td>
<td></td>
</tr>
<tr>
<td>Dialed String</td>
<td>Total Min</td>
</tr>
<tr>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>911</td>
<td>3</td>
</tr>
</tbody>
</table>
### 5.5. Route Pattern

Use the **change route-pattern** command to modify the route pattern for calls routed to Session Manager. The changes made to Route Pattern 60 in the sample configuration are highlighted below. Route Pattern 60 uses SIP Trunk Group 60. In the case of the sample configuration, this causes all digits to be sent to Session Manager. This is required to match the Dial Patterns for routing calls to the SR2330 in Branch 2 as described in **Section 4.6**.

<table>
<thead>
<tr>
<th>Grp</th>
<th>FRL</th>
<th>NPA</th>
<th>Pfx</th>
<th>Hop</th>
<th>Toll No.</th>
<th>Inserted</th>
<th>Digits</th>
<th>Intw</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:</td>
<td>60</td>
<td>0</td>
<td></td>
<td></td>
<td>0</td>
<td>n user</td>
<td>0</td>
<td>n user</td>
</tr>
<tr>
<td>2:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>n user</td>
<td></td>
<td>n user</td>
</tr>
<tr>
<td>3:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>n user</td>
<td></td>
<td>n user</td>
</tr>
<tr>
<td>4:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>n user</td>
<td></td>
<td>n user</td>
</tr>
<tr>
<td>5:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>n user</td>
<td></td>
<td>n user</td>
</tr>
<tr>
<td>6:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>n user</td>
<td></td>
<td>n user</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BCC VALUE</th>
<th>TSC</th>
<th>CA-TSC</th>
<th>ITC</th>
<th>BCIE Service/Feature</th>
<th>PARM</th>
<th>No. Numbering</th>
<th>LAR</th>
<th>Dgts Format</th>
<th>Subaddress</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 1 2 M 4 W</td>
<td>Request</td>
<td>Dgts Format</td>
<td>Subaddress</td>
<td>none</td>
<td>none</td>
<td>none</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1: y y y y n n</td>
<td>rest</td>
<td></td>
<td></td>
<td>none</td>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2: y y y y n n</td>
<td>rest</td>
<td></td>
<td></td>
<td>none</td>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3: y y y y n n</td>
<td>rest</td>
<td></td>
<td></td>
<td>none</td>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4: y y y y y n n</td>
<td>rest</td>
<td></td>
<td></td>
<td>none</td>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5: y y y y y n n</td>
<td>rest</td>
<td></td>
<td></td>
<td>none</td>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6: y y y y y n n</td>
<td>rest</td>
<td></td>
<td></td>
<td>none</td>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5.6. Modify Stations

A station must exist on Communication Manager for each SIP user account created in Session Manager. The extension assigned to the Communication Manager station must match the Extension under the Station Profile for the corresponding Session Manager user. As described in Section 4.7, Session Manager will automatically create the station and Off-PBX station-mapping forms when the Session Manager user is created. The forms generated for the user added in Section 4.7 are shown below, and are sufficient for basic calling features. Additional fields can be entered or existing fields edited by using the change station command. Typical fields modified are Coverage Path 1 on Page 1, MWI Served User Type on Page 2, and various feature BUTTON ASSIGNMENTS on Page 3. Note that feature buttons are only supported on the Avaya 9600 SIP phones, and not on the analog telephones connected to the FXS ports of the SR2330.

<table>
<thead>
<tr>
<th>change station 31003</th>
<th></th>
<th></th>
<th>Page 1 of 6</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>STATION</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extension: 31003</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type: 9630SIP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port: S00092</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name: SIP3 SR2330</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>STATION OPTIONS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss Group: 19</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display Language: english</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Survivable COR: internal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Survivable Trunk Dest? y</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>STATION OPTIONS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time of Day Lock Table:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message Lamp Ext: 31003</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Button Modules: 0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>STATION OPTIONS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>FEATURE OPTIONS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LWC Reception: spe</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LWC Activation? y</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CDR Privacy? n</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bridged Call Alerting? n</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Station Ringing: single</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H.320 Conversion? n</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Per Station CPN - Send Calling Number?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EC500 State: enabled</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coverage After Forwarding? s</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct IP-IP Audio Connections? y</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emergency Location Ext: 31003</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Precedence Call Waiting? y</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>change station 31003</th>
<th></th>
<th></th>
<th>Page 2 of 6</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>STATION</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lock Messages? n</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Code:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coverage Path 1: 60</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COR: 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coverage Path 2:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COS: 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hunt-to Station:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>STATION OPTIONS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss Group: 19</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display Language: english</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Survivable COR: internal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Survivable Trunk Dest? y</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>STATION OPTIONS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time of Day Lock Table:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message Lamp Ext: 31003</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Button Modules: 0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>STATION OPTIONS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>FEATURE OPTIONS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LWC Reception: spe</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LWC Activation? y</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CDR Privacy? n</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bridged Call Alerting? n</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Station Ringing: single</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H.320 Conversion? n</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Per Station CPN - Send Calling Number?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EC500 State: enabled</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Coverage After Forwarding? s</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct IP-IP Audio Connections? y</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emergency Location Ext: 31003</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Precedence Call Waiting? y</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The following screen shows the **off-pbx-telephone station-mapping** screen automatically generated by Session Manager. No changes to this form are typically required.

```
change off-pbx-telephone station-mapping 31003

STATIONS WITH OFF-PBX TELEPHONE INTEGRATION

<table>
<thead>
<tr>
<th>Station Extension</th>
<th>Application</th>
<th>Dial</th>
<th>Call</th>
<th>Mapping</th>
<th>Calls</th>
<th>Bridged</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>31003</td>
<td>OPS</td>
<td>-</td>
<td>31003</td>
<td>aar</td>
<td>both</td>
<td>all</td>
<td></td>
</tr>
</tbody>
</table>
```

Repeat any desired modifications to stations added by Session Manager. The following list command output summarizes the configuration relevant to the sample configuration. Each Avaya SIP Telephone at the branch (e.g., 31003 and 31004), each analog device connected to an FXS port on the SR2330 (e.g., 31001 and 31002) can be observed. The corresponding registration of these users to Session Manager is shown in **Section 8.3**.

```
list off-pbx-telephone station-mapping 3100*

STATION TO OFF-PBX TELEPHONE MAPPING

<table>
<thead>
<tr>
<th>Station Extension</th>
<th>Appl</th>
<th>CC</th>
<th>Phone Number</th>
<th>Config Set</th>
<th>Trunk Select</th>
<th>Mapping Mode</th>
<th>Calls Allowed</th>
</tr>
</thead>
<tbody>
<tr>
<td>31001</td>
<td>OPS</td>
<td>31001</td>
<td>31001</td>
<td>1</td>
<td>aar</td>
<td>both</td>
<td>all</td>
</tr>
<tr>
<td>31002</td>
<td>OPS</td>
<td>31002</td>
<td>31002</td>
<td>1</td>
<td>aar</td>
<td>both</td>
<td>all</td>
</tr>
<tr>
<td>31003</td>
<td>OPS</td>
<td>31003</td>
<td>31003</td>
<td>1</td>
<td>aar</td>
<td>both</td>
<td>all</td>
</tr>
<tr>
<td>31004</td>
<td>OPS</td>
<td>31004</td>
<td>31004</td>
<td>1</td>
<td>aar</td>
<td>both</td>
<td>all</td>
</tr>
</tbody>
</table>
```
6. Configure Avaya SR2330 Secure Router

Presented below is an annotated version of the Avaya SR2330 Secure Router configuration used in Branch 2 for Distributed Trunking. There are two main SIP components in the SR2330 as used in the survivable SIP Gateway solution: the SIP Media Gateway and the SIP Survivability Module (SSM). The SIP Media Gateway implements a Back-to-Back User Agent (B2BUA) and provides call processing support for locally connected FXS and FXO ports, as well as SIP to PSTN gateway capabilities. It registers on behalf of its configured FXS ports to Session Manager in normal mode. The 9630 SIP telephones register through the secure router to Session Manager as their primary SIP registrar, and simultaneously to the SSM as the secondary registrar. See Section 2.7 and Figure 3 for more details on the SIP signaling configuration implemented below.

# SR2330 system configuration file (.CFG).

system logging
  console
    priority crit
    no enable
    exit console
  syslog
    # syslog target for debug messages
    host_ipaddr 10.1.2.49
    module alarms local0 none
    module dos local0 none
    module forwarding local0 none
    module voip-ssm-cdr local0 none
    module voip-cdr local0 none
    enable
    exit syslog
  exit logging
hostname SR

# WAN side Ethernet interface
interface ethernet 0/1
  ip address 10.1.2.68 255.255.255.0
  exit ethernet

# LAN side Ethernet interface
interface ethernet 0/2
  ip address 20.20.20.1 255.255.255.0
  # The following command is required - When SR2330 receives an Ethernet frame (from the WAN) of size 1514 bytes and it also contains an FCS header (4 bytes), then "ip tcp-mss 1452" is needed to be configured on the LAN interface such that the forwarded Ethernet frame is not dropped because its size exceeds 1514 bytes
  ip tcp-mss 1452
  exit ethernet

ftp_server
telnet_server
telnet_timeout 0
# Required to support domain lookup in survivable mode.
# Avaya 9630 IP Telephones use the domain name (avaya.com) in the
# Refer-To header of REFER messages during transfer scenarios.
# This entry allows the SR2330 to resolve the domain name to its
# private side IP address.
ip host_add avaya.com 20.20.20.1

# Default route is toward the WAN
ip route 0.0.0.0/0 10.1.2.1

# Dialed digit translations used in survivable mode to strip the first 9
# before sending out on the local FXO trunk
voice translation-rule 1
    rule 1 /9.........../ //
    rule 2 /9911/ /911/
exit translation-rule
voice translation-profile strip9
    translate called 1
exit translation-profile

voice service voip
    # sip signaling options
    # Configure the SIP Media Gateway to listen on port 5080
    sip
        bind all ipv4:20.20.20.1:5080
    exit sip
    # One single codec must be configured for calls
    # to be supported from FXS analog phones to 9630 SIP phones
    # in survivable mode.
    codec 1 g711ulaw 160
    # Support for RFC 2833 DTMF
    dtmf-relay rtp-nte

    # SIP Survivable Module
    ssm
    #To configure the SIP Survivability Module, bind the IP interface
    # for SIP traffic using default port 5060
    bind ip ipv4:20.20.20.1
    # Enable the SSM
    enable
    sip-server
        # Specify the SSM domain name to be used with Session Manager
        domain dns:avaya.com
    exit sip-server
    # Point the SSM to the SIP Media Gateway IP interface as the
    # default gateway (specifying the non-default port)
    default-gateway ipv4:20.20.20.1:5080 transport tcp
exit ssm
exit voip
# SIP user registration parameters
sip-ua
  # Primary Registrar is Session Manager, secondary is SSM
  sip-server ipv4:10.1.2.170
  sip-server ipv4:20.20.20.1:5060 secondary
  transport tcp
  registrar ipv4:10.1.2.170 expires 3600
  # Enable SIP OPTIONS messages for keepalives
  keepalive target sip-server
  keepalive target sip-server secondary
  keepalive timer 30
exit sip-ua

# FXO trunk group name (will include 3/1 and 3/2)
trunk group pstn

# FXO ports

voice-port 3/1
  signal loop-start
  ring-number 2
  caller-id enable 1
  station number 9087661000
  no shutdown
  # Calls into this FXO port are routed to this extension (via Session
  # Manager or SMM depending on normal or survivable mode, respectively
  connection plar 31003
  trunk-group pstn
exit voice-port

voice-port 3/2
  signal loop-start
  ring-number 2
  caller-id enable 1
  station number 9087662000
  no shutdown
  # Calls into this FXO port are routed to this extension (via Session
  # Manager or SMM depending on normal or survivable mode, respectively
  connection plar 31002
  trunk-group pstn
exit voice-port

# FXS ports for the two analog phones
voice-port 1/1
  signal loop-start
  # User name
  station name fxs1
  # Extension number
  station number 31001
  no shutdown
  # Interdigit timeout governs how fast call is launched when user stops
  # dialing
  timeouts interdigit 3
exit voice-port

voice-port 1/2
  signal loop-start
  station name fxs2
station number 31002
no shutdown
timeouts interdigit 3
exit voice-port

# Routing for 1-AAA-NNN-CCCC calls dialed by branch phones that are delivered
# by Session Manager
dial-peer voice pots 6
  destination-pattern 1.%
  # Send out local FXO ports
  trunkgroup pstn
  # Send all digits
  forward-digits all
  no shutdown
  exit pots

# Routing for calls to the local analog phones on FXS ports
dial-peer voice pots 1
  # Extension as known by ACM & ASM
  destination-pattern 31001
  port 1/1
  forward-digits all
  no shutdown
  # Userid and password used to register to Session Manager on behalf
  # of the phone
  authentication 31001 31001
  register e164
  exit pots
dial-peer voice pots 2
  destination-pattern 31002
  port 1/2
  forward-digits all
  no shutdown
  # Userid and password used to register to Session Manager on behalf
  # of the phone
  authentication 31002 31002
  register e164
  exit pots
dial-peer voice pots 5
  destination-pattern 91.%
  trunkgroup pstn
  forward-digits all
  no shutdown
  # Strip the "9"
  translation-profile outgoing strip9
  exit pots

# Same routing as for dial peer pots #6, except it handles dialing the
# initial "9"
7. Configure Avaya 9600 Series IP Telephone (SIP)

The following 46xxsettings.txt file parameters/values were used for the testing:

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Value Used in Sample Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SIP_CONTROLLER_LIST</strong></td>
<td>10.1.2.170:5060;transport=tcp, 20.20.20.1:5060;transport=tcp</td>
<td>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 Avaya SR2330 Secure Router 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 Avaya SR2330 Secure Router while the list for Branch 2 phones will include the Session Manager and the Branch 2 Avaya SR2330 Secure Router. To accomplish this, the GROUP system value mechanism can be implemented as described in [8].</td>
</tr>
<tr>
<td><strong>FAILBACK_POLICY</strong></td>
<td>Auto</td>
<td>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.</td>
</tr>
<tr>
<td><strong>FAST_RESPONSE_TIMEOUT</strong></td>
<td>2</td>
<td>The timer terminates SIP INVITE transactions if no SIP response is received within the</td>
</tr>
</tbody>
</table>

FS; Reviewed: SPOC 06/08/2010 ©2010 Avaya Inc. All Rights Reserved. SR2330SMMCMM5_2
<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Value Used in Sample Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>46xxsettings.txt</td>
<td></td>
<td>specified number of seconds after sending the request. Useful when a phone goes off-hook after connectivity to the centralized SIP Server is lost, but before the phone has detected the connectivity loss. The default value is 4 seconds. After the SIP INVITE is terminated, the phone immediately transitions to Survivable Mode.</td>
</tr>
<tr>
<td>MSGNUM</td>
<td>33000</td>
<td>The number dialed when the Message button is pressed and the phone is in Normal Mode.</td>
</tr>
<tr>
<td>PSTN_VM_NUM</td>
<td>19088485960</td>
<td>The number dialed when the Message button is pressed and the phone is in Survivable Mode.</td>
</tr>
<tr>
<td>RECOVERYREGISTERWAIT</td>
<td>60</td>
<td>A Reactive Monitoring Interval. If no response to a &quot;maintenance check&quot; 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.</td>
</tr>
<tr>
<td>DIALPLAN</td>
<td>[2-8]xxxx</td>
<td>91xxxxxxxxxxx</td>
</tr>
<tr>
<td>PHNEMERGNUM</td>
<td>911</td>
<td>Number dialed when emergency soft key is pressed.</td>
</tr>
<tr>
<td>DISCOVER_AVAYA_ENVIRONMENT</td>
<td>1</td>
<td>Automatically determines if the active SIP Server is an Avaya server or not.</td>
</tr>
</tbody>
</table>
| SIPREGPROXYPOLICY          | simultaneous                      | A policy to control how the phone treats a list of proxies in...
### 46xxsettings.txt

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Value Used in Sample Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>the SIP_CONTROLLER_LIST parameter</td>
<td>alternate = remain registered with only the active controller simultaneous = remain registered with all available controllers</td>
<td></td>
</tr>
</tbody>
</table>

| SIPDOMAIN | avaya.com | The enterprise SIP domain. Must be the same for all SIP controllers in the configuration. SIPDOMAIN is set to “avaya.com” in the sample configuration. |

## 8. Verification and Troubleshooting

### 8.1. Session Manager/Secure Router 2330 Link Status

From the left navigation panel of the browser-based GUI of System Manager, select **System Status → SIP Entity Monitoring**. The SIP entities monitored by Session Manager are listed on the lower portion of the page as shown below. Select the entity corresponding to the SR2330, in this case “SR2330”.

**All Monitored SIP Entities**

![All Monitored SIP Entities](image)

- RobertIP500
- 88300-C250-JRWB
- 88300-C430
- 88300-C450-BR1
- SR2330
- Victor-88300-WM1
- VZ-807x0-PE
The next screen displayed will show the entity link status, which is determined by the SR2330 response to a SIP OPTIONS message periodically sent by Session Manager. In this case the “404 Not Found” response by the SR2330 indicates that SIP signaling on the SR2330 is functional, and so the **Conn. Status** is shown as “Up”. An indication of “Down” would imply that the SR 2330 is most likely in survivable mode, since the SR2330 uses the same OPTIONs method to determine if Session Manager is accessible, and the interval is the same as that configured for Session Manager (30 sec).

### 8.2. Secure Router 2330 Registered Users

The command line interface of the SR2330 can be used to determine the registration state of the Analog phones connected to the FXS interfaces of the SIP Media Gateway Module. Below are shown the command and the output, which indicates that the two FXS interfaces configured with extensions 31001 and 31002 have successfully registered with Session Manager.

```
SR# show sip-ua register status
Line   peer      expires(sec)  registered
 4      31001    3600          yes
 5      31002    3600          yes
```

The following command shows the Avaya 9600 SIP phones registered to the SSM, simultaneously with their registration to Session Manager:

```
SR# show ssm subscriber all
Subscriber Destination Alias Identity
 31004   avaya.com
 31003   avaya.com
```
8.3. Session Manager Registered Users (Normal Mode)

To verify registration of the SR2330 supported analog stations connected to the FXS interfaces and the Avaya 9630 IP phones, navigate to Session Manager → System Status → User Registrations. The following abridged screens show the last four users listed to correspond to those users; extensions 31001 and 31002 correspond to the analog stations and 31003 and 31004 correspond to the Avaya 9630 IP phones.

<table>
<thead>
<tr>
<th>Registered</th>
<th>Address</th>
<th>Login Name</th>
<th>First Name</th>
<th>Last Name</th>
<th>Session Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td><a href="mailto:30042@avaya.com">30042@avaya.com</a></td>
<td><a href="mailto:30042@avaya.com">30042@avaya.com</a></td>
<td>Nortel</td>
<td></td>
<td>SMI</td>
</tr>
<tr>
<td>false</td>
<td><a href="mailto:30014@avaya.com">30014@avaya.com</a></td>
<td><a href="mailto:30014@avaya.com">30014@avaya.com</a></td>
<td>One-K</td>
<td></td>
<td>SIP</td>
</tr>
<tr>
<td>false</td>
<td><a href="mailto:30001@avaya.com">30001@avaya.com</a></td>
<td><a href="mailto:30001@avaya.com">30001@avaya.com</a></td>
<td>UA1</td>
<td></td>
<td>SRLAB</td>
</tr>
<tr>
<td>false</td>
<td><a href="mailto:30002@avaya.com">30002@avaya.com</a></td>
<td><a href="mailto:30002@avaya.com">30002@avaya.com</a></td>
<td>UA2</td>
<td></td>
<td>SRLAB</td>
</tr>
<tr>
<td>false</td>
<td><a href="mailto:30063@avaya.com">30063@avaya.com</a></td>
<td><a href="mailto:30063@avaya.com">30063@avaya.com</a></td>
<td>UA3</td>
<td></td>
<td>SRLAB</td>
</tr>
<tr>
<td>false</td>
<td><a href="mailto:30064@avaya.com">30064@avaya.com</a></td>
<td><a href="mailto:30064@avaya.com">30064@avaya.com</a></td>
<td>UA4</td>
<td></td>
<td>SRLAB</td>
</tr>
<tr>
<td>false</td>
<td><a href="mailto:30065@avaya.com">30065@avaya.com</a></td>
<td><a href="mailto:30065@avaya.com">30065@avaya.com</a></td>
<td>UA5</td>
<td></td>
<td>SRLAB</td>
</tr>
<tr>
<td>false</td>
<td><a href="mailto:30081@avaya.com">30081@avaya.com</a></td>
<td><a href="mailto:30081@avaya.com">30081@avaya.com</a></td>
<td>GWUA1</td>
<td></td>
<td>SRLAB</td>
</tr>
<tr>
<td>false</td>
<td><a href="mailto:30082@avaya.com">30082@avaya.com</a></td>
<td><a href="mailto:30082@avaya.com">30082@avaya.com</a></td>
<td>GWUA2</td>
<td></td>
<td>SRLAB</td>
</tr>
<tr>
<td>false</td>
<td><a href="mailto:30083@avaya.com">30083@avaya.com</a></td>
<td><a href="mailto:30083@avaya.com">30083@avaya.com</a></td>
<td>GWUA3</td>
<td></td>
<td>SRLAB</td>
</tr>
<tr>
<td>false</td>
<td><a href="mailto:30084@avaya.com">30084@avaya.com</a></td>
<td><a href="mailto:30084@avaya.com">30084@avaya.com</a></td>
<td>GWUA4</td>
<td></td>
<td>SRLAB</td>
</tr>
<tr>
<td>false</td>
<td><a href="mailto:30085@avaya.com">30085@avaya.com</a></td>
<td><a href="mailto:30085@avaya.com">30085@avaya.com</a></td>
<td>GWUA5</td>
<td></td>
<td>SRLAB</td>
</tr>
<tr>
<td>false</td>
<td><a href="mailto:30012@avaya.com">30012@avaya.com</a></td>
<td><a href="mailto:30012@avaya.com">30012@avaya.com</a></td>
<td>Fred</td>
<td></td>
<td>SIP3</td>
</tr>
<tr>
<td>true</td>
<td><a href="mailto:31001@avaya.com">31001@avaya.com</a></td>
<td><a href="mailto:31001@avaya.com">31001@avaya.com</a></td>
<td>SIP1</td>
<td></td>
<td>SR2330</td>
</tr>
<tr>
<td>true</td>
<td><a href="mailto:31002@avaya.com">31002@avaya.com</a></td>
<td><a href="mailto:31002@avaya.com">31002@avaya.com</a></td>
<td>SIP2</td>
<td></td>
<td>SR2330</td>
</tr>
<tr>
<td>true</td>
<td><a href="mailto:31003@avaya.com">31003@avaya.com</a></td>
<td><a href="mailto:31003@avaya.com">31003@avaya.com</a></td>
<td>SIP3</td>
<td></td>
<td>SR2330</td>
</tr>
<tr>
<td>true</td>
<td><a href="mailto:31004@avaya.com">31004@avaya.com</a></td>
<td><a href="mailto:31004@avaya.com">31004@avaya.com</a></td>
<td>SIP4</td>
<td></td>
<td>SR2330</td>
</tr>
</tbody>
</table>
8.4. Timing Expectations for Fail-over to Survivable 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 Secure Router 2330 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 9600 SIP phones in the branch will typically display the “Acquiring Service…” screen in approximately 75-120 seconds. With multiple identical idle phones in the same branch, it would not be unusual for some phones to register to the SR2330 before others, with the earliest registering in approximately one minute and the latest registering in approximately two minutes.

Note that attempting to place a call from a branch phone during this time will trigger acquisition of service from the SR2330 immediately. Likewise, if a phone receives an intra-branch call before it has acquired service, it will do so immediately and then the call will be successfully delivered.

In other words, the Avaya SIP Telephones in the branch can typically place and receive calls processed by the SR2330 approximately two minutes after the branch is isolated by a WAN failure.

8.5. 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 phones registered to the SR2330 in survivable mode will re-acquire service from Session Manager for normal service, once branch communication 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 9600 SIP phones in the branch will typically be registered with Session Manager 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 15 seconds, others within 30 seconds, with others registering in approximately one minute.
9. 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 Survivable SIP Gateway Solution based on the Avaya Secure Router to minimize service disruptions to these remote branch SIP endpoints.

10. References

Avaya Application Notes and additional resources can be found at the following web address http://www.avaya.com/usa/resources/. Product documentation for Avaya products may be found at http://support.avaya.com/.

The following Avaya references are relevant to these Application Notes:


