



Avaya Solution & Interoperability Test Lab

Applications Notes for Avaya Aura® Communication Manager 6.0.1, Avaya Aura® Session Manager 6.1 and Acme Packet Net-Net 6.2.0 with Sprint IP Toll Free SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and the Acme Packet Net-Net (models 3800 or 4500) with the Sprint IP Toll Free SIP trunk service.

Avaya Aura® Session Manager 6.1 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® Communication Manager 6.0.1 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. An Acme Packet Net-Net 6.2.0 is the point of connection between Avaya Aura® Session Manager and the Sprint IP Toll Free service and is used to not only secure the SIP trunk, but also to make adjustments to the SIP signaling for interoperability.

The Sprint IP Toll Free service is a managed Voice over IP (VoIP) communications solution that provides toll-free services over SIP trunks.

Sprint is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program.

TABLE OF CONTENTS

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	4
2.2.	Test Results	5
2.3.	Support	5
3.	Reference Configuration.....	5
3.1.	Illustrative Configuration Information	8
4.	Equipment and Software Validated	9
5.	Configure Avaya Aura® Session Manager Release 6.1	10
5.1.	SIP Domain	12
5.2.	Locations	12
5.2.1.	Location for Avaya Aura® Communication Manager	12
5.2.2.	Location for the Sprint network.....	14
5.3.	Configure Adaptations	15
5.3.1.	Adaptation for calls sent to Avaya Aura® Communication Manager.....	15
5.3.2.	Adaptation for Outbound calls from Communication Manager	16
5.4.	SIP Entities.....	17
5.4.1.	Avaya Aura® Session Manager SIP Entity	17
5.4.2.	Avaya Aura® Communication Manager SIP Entity	19
5.4.3.	Acme Packet SBC SIP Entity	20
5.5.	Entity Links	21
5.5.1.	Entity Links to Avaya Aura® Communication Manager	21
5.5.2.	Entity Link to Sprint IP Toll Free Service via Acme Packet SBC	22
5.6.	Time Ranges.....	22
5.7.	Routing Policies	23
5.7.1.	Routing Policy for Routing to Avaya Aura® Communication Manager from Sprint	23
5.7.2.	Routing Policy for Routing of outbound calls to the Acme Packet SBC for transport to Sprint.....	25
5.8.	Dial Patterns	28
5.8.1.	Matching Inbound PSTN Calls to Avaya Aura® Communication Manager	28
5.8.2.	Outbound calls from Communication Manager to the PSTN via Sprint IP Toll Free service	31
5.9.	Regular Expressions.....	33
6.	Avaya Aura® Communication Manager	35
6.1.	System Parameters	35
6.2.	Dial Plan.....	38
6.3.	IP Node Names.....	39
6.4.	IP Interface for procr	39
6.5.	IP Network Regions	40
6.5.1.	IP Network Region 1 – Local Region.....	40
6.5.2.	IP Network Region 3 – Sprint Trunk Region	41
6.6.	IP Codec Parameters	42
6.6.1.	Codecs For IP Network Region 1 (local calls)	42

6.6.2.	Codecs For IP Network Region 2	43
6.7.	SIP Trunks.....	43
6.7.1.	SIP Trunk for Sprint IP Toll Free calls.....	43
6.8.	Public Unknown Numbering.....	46
6.9.	Route Patterns	47
6.9.1.	Route Pattern for Sprint IP Toll Free SIP Trunk	47
6.10.	ARS Dialing	48
6.11.	Call Center Provisioning	49
7.	Avaya Modular Messaging.....	51
8.	Configure Acme Packet SBC.....	52
8.1.	Local Policies	52
8.2.	Network Interfaces	53
8.3.	Realms.....	55
8.4.	Session Agents	58
8.5.	SIP Configuration.....	61
8.6.	SIP Interfaces	62
8.7.	SIP Manipulations.....	65
8.8.	Steering Pools.....	65
9.	Verification Steps.....	65
9.1.	General	65
9.2.	Avaya Aura® Communication Manager	66
9.3.	Avaya Aura® Session Manager	67
9.3.1.	Call Routing Test.....	69
9.4.	Protocol Traces.....	71
9.5.	Acme Packet SBC	72
10.	Conclusion	72
11.	References.....	72
12.	Appendix A – Acme Packet Net-Net Session Director Configuration.....	73

1. Introduction

These Application Notes describe the steps for configuring Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and the Acme Packet Net-Net (models 3800 or 4500) with the Sprint IP Toll Free SIP trunk service.

Avaya Aura® Session Manager 6.1 is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya Aura® Communication Manager 6.0.1 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. An Acme Packet Net-Net 6.2.0 is the point of connection between Avaya Aura® Session Manager and the Sprint IP Toll Free service and is used to not only secure the SIP trunk, but also to make adjustments to the signaling for interoperability.

The Sprint IP Toll Free service is a managed Voice over IP (VoIP) communications solution that provides toll-free services over SIP trunks.

2. General Test Approach and Test Results

The test environment consisted of:

- A simulated enterprise with Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, Avaya phones, fax machines, Acme Packet Net-Net 3800 SBC, and Avaya Modular Messaging.
- A laboratory version of the Sprint IP Toll Free service, to which the simulated enterprise was connected via an IPSec VPN connection that emulated the Sprint MPLS network.

2.1. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound and outbound call flows between Avaya Aura® Session Manager, Avaya Aura® Communication Manager, Acme Packet Net-Net Session Director, and the Sprint IP Toll Free service.

The compliance testing was based on a test plan provided by Sprint and the standard Avaya SIP trunk test plan, for the functionality required for certification as a solution supported on the Sprint network. Calls were made to and from the PSTN across the Sprint network. The following features were tested as part of this effort:

- SIP trunking.
- T.38 Fax.
- Passing of DTMF events and their recognition by navigating automated menus.
- PBX and Sprint IP Toll Free service features such as hold, resume, conference and transfer. Alternate Destination Routing features were also tested.

2.2. Test Results

The main test objectives were to verify the following features and functionality:

- Inbound Sprint IP Toll Free service calls to Communication Manager telephones and VDNs/Vectors.
- Call and two-way talk path establishment between PSTN and Communication Manager phones via the Sprint Toll Free service.
- Basic supplementary telephony features such as hold, resume, transfer, and conference.
- G.729A and G.711MU codecs.
- T.38 fax calls between Communication Manager and the Sprint IP Toll Free service.
- DTMF tone transmission using RFC 2833 between Communication Manager and the Sprint IP Toll Free service/PSTN automated access systems.
- Inbound Sprint IP Toll Free service calls to Communication Manager that are directly routed to stations, and unanswered, can be covered to Avaya Modular Messaging.
- Long duration calls.

The test objectives stated in **Section 2.1** were verified.

2.3. Support

Sprint customers may obtain information for Sprint IP Toll Free service by going to www.sprint.com or for technical support contact Sprint Customer Care at (800) 421-3872.

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 menus. Customers may also use specific numbers (provided on <http://support.avaya.com>) to directly access specific support and consultation services based upon their Avaya support agreements.

3. Reference Configuration

The reference configuration used in these Application Notes is shown in **Figure 1** and consists of several components:

- Avaya Aura® Session Manager provides core SIP routing and integration services that enables communications between disparate SIP-enabled entities, e.g., PBXs, SIP proxies, gateways, adjuncts, trunks, applications, etc. across the enterprise. Avaya Aura® Session Manager allows enterprises to implement centralized and policy-based routing, centralized yet flexible dial plans, consolidated trunking, and centralized access to adjuncts and applications.
- Avaya Aura® System Manager provides a common administration interface for centralized management of all Avaya Aura® Session Manager instances in an enterprise.
- Avaya Aura® Communication Manager provides the voice communications services for a particular enterprise site. In the reference configuration, Avaya Aura® Communication

Manager runs on an Avaya S8800 Server in a Processor Ethernet (Procr) configuration. This solution is extensible to other Avaya S8xxx Servers.

- The Avaya Media Gateway provides the physical interfaces and resources for Avaya Aura® Communication Manager. In the reference configuration, an Avaya G450 Media Gateway is used. This solution is extensible to other Avaya Media Gateways.
- Avaya “desk” phones are represented with Avaya analog, 2420 Digital, 46x0 SW IP, 96x0, and 96x1 Series IP Telephones running H.323 or SIP software, as well as an Avaya one-X® Communicator softphone.
- The Acme Packet Net-Net 3800¹ provides SIP Session Border Controller (SBC) functionality, including address translation and SIP header manipulation, if necessary, between the Sprint IP Toll Free service and the enterprise internal network². UDP transport protocol is used between the Acme Packet Net-Net SD and the Sprint IP Toll Free service.
- An existing Avaya Modular Messaging system provides the corporate voice messaging capabilities in the reference configuration. The provisioning of Modular Messaging is beyond the scope of this document.
- Inbound calls were placed from the PSTN via the Sprint IP Toll Free service, through the Acme Packet Net-Net SD to the Session Manager which routed the call to Avaya Aura® Communication Manager. Avaya Aura® Communication Manager terminated the call to the appropriate agent/phone or fax extension. The H.323 phones on the enterprise side registered to the Avaya Aura® Communication Manager Procr. The SIP phones registered to Avaya Aura® Session Manager.

¹ Although an Acme Net-Net 3800 was used in the reference configuration, the 4250 and 4500 platforms are also supported.

² The Sprint IP Toll Free service uses SIP over UDP to communicate with enterprise edge SIP devices, e.g., the Acme Packet SBC in this sample configuration. Session Manager may use SIP over UDP, TCP, or TLS to communicate with SIP network elements, e.g., the Acme SBC and Communication Manager. In the reference configuration, Session Manager uses SIP over TCP to communicate with the Acme Packet SBC and Communication Manager.

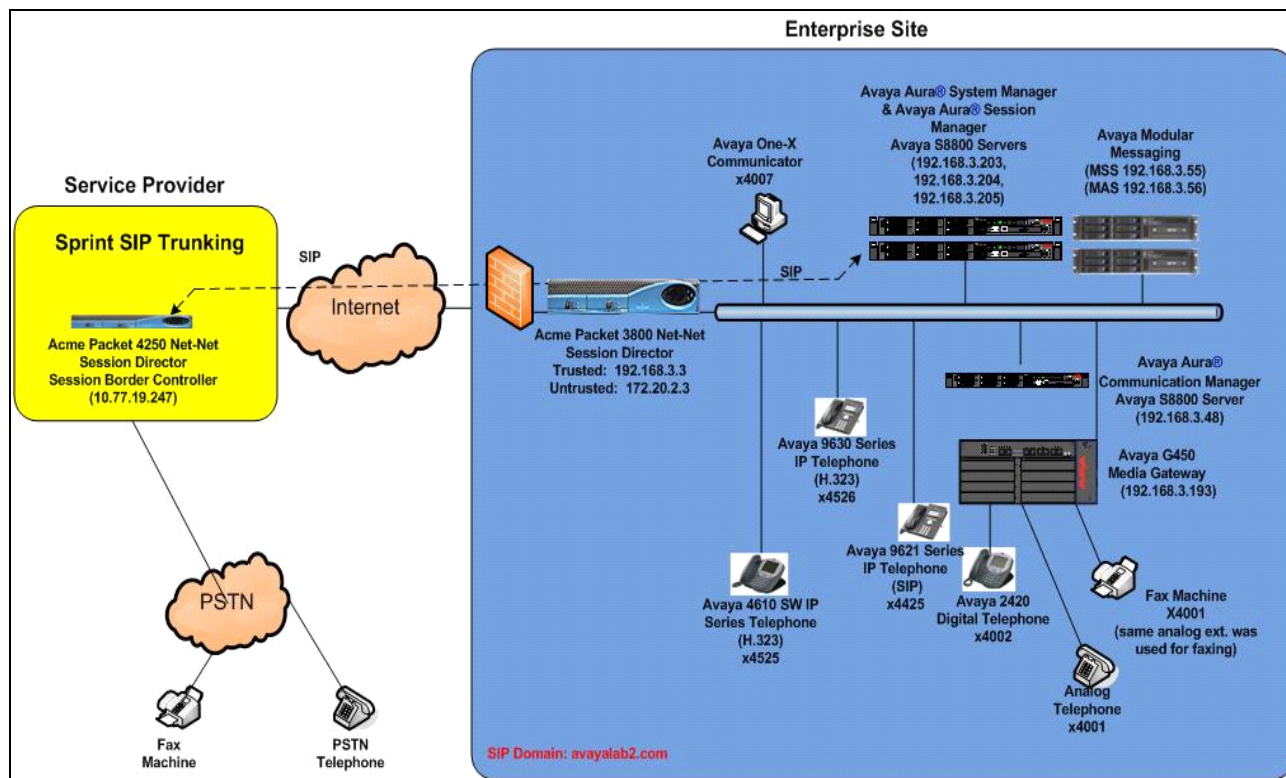


Figure 1: Reference configuration

3.1. Illustrative Configuration Information

The specific values listed in **Table 1** below and in subsequent sections are used in the reference configuration described in these Application Notes, and are **for illustrative purposes only**. Customers must obtain and use the specific values for their own specific configurations.

Note - The Sprint IP Toll Free service Border Element IP address and DNIS digits, (destination digits specified in the SIP Request URIs sent by the Sprint Toll Free service) are shown in this document as examples. Sprint will provide the actual IP addresses and DNIS digits as part of the IP Toll Free provisioning process.

Component	Illustrative Value in these Application Notes
Avaya Aura® System Manager	
Management IP Address	192.168.3.203
Avaya Aura® Session Manager	
Management IP Address	192.168.3.205
Signaling Address	192.168.3.204
Avaya Aura® Communication Manager	
Procr IP Address	192.168.3.48
Avaya Aura® Communication Manager extensions	40xx = Analog, Digital and One –X Communicator 44xx = SIP 45xx = H.323
Avaya Modular Messaging	
Messaging Application Server (MAS) IP Address	192.168.3.56
Messaging Server (MSS) IP Address	192.168.3.55
Acme Packet SBC	
IP Address of “Outside” (Public) Interface (connected to Sprint SBC/IP Toll Free Service)	172.20.2.3
IP Address of “Inside” (Private) Interface (connected to Avaya Aura® Session Manager)	192.168.3.3
Sprint IP Toll Free Service	
Border Element IP Address	10.77.19.247

Table 1: Illustrative Values Used in these Application Notes

4. Equipment and Software Validated

The following equipment and software was used for the reference configuration described in these Application Notes.

Component		Version
Avaya S8800 Server		Avaya Aura® System Manager 6.1 SP2 (6.1.0.0.7345-6.1.5.106) System Platform 6.0.3.0.3
Avaya S8800 Server		Avaya Aura® Session Manager 6.1 SP2 (6.1.2.0)
Avaya S8800 Server		Avaya Aura® Communication Manager 6.0.1 SP0 (00.1.510.1) System Platform 6.0.2.0.5
Avaya G450 Media Gateway		30.10.4
	MM711AP Analog card	HW27 FW071
	MM712AP Digital card	HW07 FW007
Avaya 9630 IP Telephone		H.323 Version S3.110b (ha96xxua3_11.bin)
Avaya 9621 IP Telephone		SIP Version 6.0.1 (S96x1_SALBR6_0_1_V452)
Avaya one-X® Communicator		6.0.1.16-SP1-25226
Avaya 4610SW IP Telephone		H323 Version 2.9.1 (a10d01b2_9_1.bin)
Avaya Analog phone		N/A
Fax device		Okidata Okifax
Acme Packet Net-Net 3800		SCX6.2.0m6p4 (Build 908)
Sprint IP Toll Free Service using an Acme Packet Net-Net Session Director		SCX6.2.0

Table 2: Equipment and Software Versions

5. Configure Avaya Aura® Session Manager Release 6.1

This section illustrates relevant aspects of the Session Manager configuration used in the verification of these Application Notes.

Note – These Application Notes assume that basic System Manager and Session Manager administration has already been performed.

This section provides the procedures for configuring Session Manager to receive calls from and route calls to the SIP trunk between Communication Manager and Session Manager, and the SIP trunk between Session Manager and the Acme SBC.

Session Manager serves as a central point for supporting SIP-based communication services in an enterprise. Session Manager connects and normalizes disparate SIP network components and provides a central point for external SIP trunking to the PSTN. The various SIP network components are represented as “SIP Entities” and the connections/trunks between Session Manager and those components are represented as “Entity Links”. Thus, rather than connecting to every other SIP Entity in the enterprise, each SIP Entity simply connects to Session Manager and relies on Session Manager to route calls to the correct destination. This approach reduces the dial plan and trunking administration needed on each SIP Entity, and consolidates administration in a central place, namely System Manager.

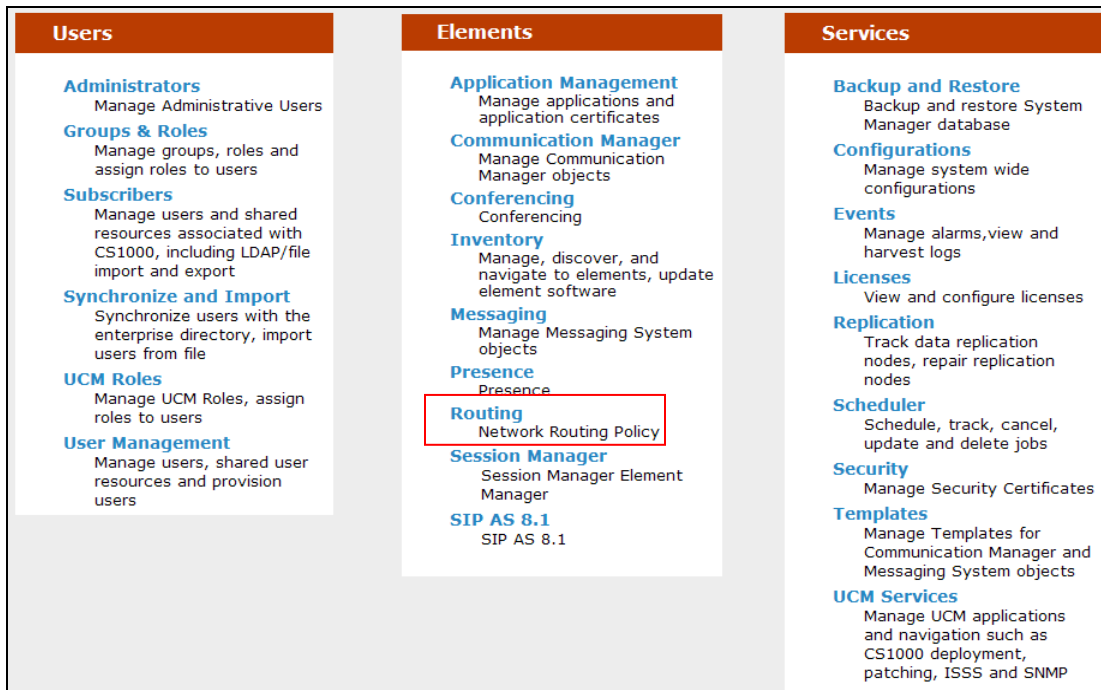
When calls arrive at Session Manager from a SIP Entity, Session Manager applies SIP protocol and numbering modifications to the calls. These modifications, referred to as “Adaptations”, are sometimes necessary to resolve SIP protocol differences between disparate SIP Entities, and also serve the purpose of “normalizing” the calls to a common or uniform numbering format, which allows for simpler administration of routing rules in Session Manager. Session Manager then matches the calls against certain criteria embodied in profiles termed “Dial Patterns”, and determines the destination SIP Entities based on “Routing Policies” specified in the matching Dial Patterns. Lastly, before the calls are routed to the respective destinations, Session Manager again applies Adaptations in order to bring the calls into conformance with the SIP protocol interpretation and numbering formats expected by the destination SIP Entities.

The following administration activities will be described:

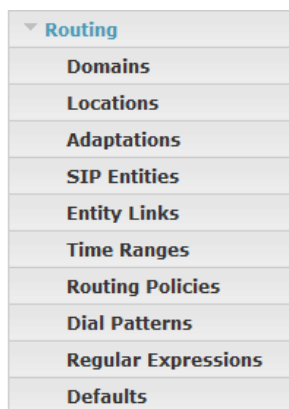
- Define SIP Domain
- Define Locations for Communication Manager, the Acme SBC, and Sprint IP Toll Free service.
- Configure the Adaptation Modules that will be associated with the SIP Entities for Communication Manager and the Acme SBC.
- Define SIP Entities corresponding to Session Manager, Communication Manager and the Acme SBC.
- Define Entity Links describing the SIP trunk between Communication Manager and Session Manager and the SIP trunk between Session Manager and the Acme SBC.
- Define Routing Policies associated with Communication Manager and the Acme SBC.
- Define Dial Patterns, which govern which routing policy will be selected for call routing.

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “**http://<Hostname>/SMGR**”, where **<Hostname>** is the short hostname of System Manager. Log in with the appropriate credentials.

At the **Log On** screen (not shown), enter appropriate **User ID** and **Password** and press the **Log On** button. Once logged in, a Release 6.1 **Home** screen like the following is displayed. From the **Home** screen below, under the **Elements** heading in the center, select **Routing**.



The screen shown below shows the various sub-headings of the left navigation menu that will be referenced in this section.



5.1. SIP Domain

Step 1 - Select **Domains** from the left navigation menu. In the reference configuration, domain “avayalab2.com” was defined.

Step 2 - Click **New** (not shown). Enter the following values and use default values for remaining fields.

- **Name** - Enter the enterprise SIP Domain Name. In the sample screen below, “avayalab2.com” is shown.
- **Type** - Verify “SIP” is selected.
- **Notes** - Add a brief description. [Optional]

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / Domains- Domain Management

Domain Management

1 Item | Refresh Filter: Enable

Name	Type	Default	Notes
* avayalab2.com	sip	<input type="checkbox"/>	

* Input Required

Commit Cancel

Step 3 - Click **Commit** to save.

Note - Multiple SIP Domains may be defined if required.

5.2. Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. Location identifiers can be defined in a broad scope (e.g. 192.168.3.x for all devices on a particular subnet), or individual devices (e.g. 192.168.3.48 for a device's IP address). In the reference configuration Communication Manager, Modular Messaging, and the Enterprise Acme SBC were all defined to be in the same Location.

5.2.1. Location for the Enterprise

Step 1 - Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name** - Enter a descriptive name for the location.
- **Notes** - Add a brief description. [Optional]

Step 2 - In the **Location Pattern** section, click **Add** and enter the following values.

- **IP Address Pattern** - Enter the IP Address used to identify the Enterprise location (e.g. 192.168.3.*).
- **Notes** - Add a brief description. [Optional]

Step 3 - Click **Commit** to save.

The screen below shows the top portion of the screen for the Location defined for the Enterprise.

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.1', and links for 'Help', 'About', 'Change Password', and 'Log off admin'. A breadcrumb trail shows 'Home / Elements / Routing / Locations- Location Details'. The left sidebar contains a tree view with 'Routing' expanded, showing sub-items like Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Location Details' and includes 'Commit' and 'Cancel' buttons. It is divided into several sections: 'General' with fields for 'Name' (set to 'Enterprise') and 'Notes'; 'Overall Managed Bandwidth' with dropdowns for 'Managed Bandwidth Units' (set to 'Kbit/sec') and input fields for 'Total Bandwidth', 'Multimedia Bandwidth', and 'Audio Calls Can Take Multimedia Bandwidth' (checked); 'Per-Call Bandwidth Parameters' with input fields for 'Maximum Multimedia Bandwidth (Intra-Location)', 'Maximum Multimedia Bandwidth (Inter-Location)', 'Minimum Multimedia Bandwidth', and 'Default Audio Bandwidth' (set to '80 Kbit/sec'); and 'Location Pattern' with 'Add' and 'Remove' buttons. Below this is a table with one item, '192.168.3.*', under the 'IP Address Pattern' column. The table has columns for 'IP Address Pattern' and 'Notes'. At the bottom, there is a 'Select : All, None' option and a '* Input Required' message. 'Commit' and 'Cancel' buttons are also present at the bottom right.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / Locations- Location Details

Location Details

Commit Cancel Help ?

General

* Name: Enterprise

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec

Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 192.168.3.*	

Select : All, None

* Input Required

Commit Cancel

5.2.2. Location for the Sprint network

Step 1 - Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name** - Enter a descriptive name for the location.
- **Notes** - Add a brief description. [Optional]

Step 2 - In the **Location Pattern** section, click **Add** and enter the following values.

- **IP Address Pattern** - Enter the IP Address or IP Address pattern used to identify the Sprint Network Acme SBC location (e.g. **10.77.19.***).
- **Notes** - Add a brief description. [Optional]

Step 3 - Click **Commit** to save.

AVAYA Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Locations- Location Details

Location Details

General

* Name: Sprint

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec

Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

Add Remove

1 Item Refresh Filter: Enable

IP Address Pattern	Notes
* 10.77.19.*	

Select : All, None

* Input Required

Commit Cancel

5.3. Configure Adaptations

Session Manager can be configured to use an Adaptation Module to convert SIP headers in messages sent by Sprint to Communication Manager, and between Communication Manager and Modular Messaging. In the reference configuration the following adaptations were used.

In the reference configuration, Adaptations are administered for the following purposes:

- Calls from Sprint (**Section 5.3.1**) - Modification of SIP messages sent to Communication Manager.
 - The IP address of Session Manager (192.168.3.204) is replaced with the Avaya CPE SIP domain (avayalab2.com) in the Request URI.
 - The Sprint called number digit strings in the Request URI are replaced with their associated Communication Manager extensions/VDNs.
- Calls from Communication Manager (**Section 5.3.2**) - Modification of SIP messages received from Communication Manager.
 - From CM – Outbound calls from Communication Manager used the “OrangeAdapter” to ensure Caller ID was being properly delivered.

5.3.1. Adaptation for calls sent to Avaya Aura® Communication Manager

The Adaptation administered in this section is used for modification of SIP messages to Communication Manager from Sprint.

Step 1 - In the left pane under **Routing**, click on “**Adaptations**”. In the **Adaptations** page, click on “**New**” (not shown).

Step 2 - In the **Adaptation Details** page, enter:

- A descriptive **Name**, (e.g. **Incoming Digit Conversion**).
- Select “**DigitConversionAdapter**” from the **Module Name** drop down menu (if no module name is present, select “<click to add module>” and enter **DigitConversionAdapter**).

The screenshot displays the Avaya Aura® System Manager 6.1 web interface. The top header includes the Avaya logo, the title 'Avaya Aura® System Manager 6.1', and links for 'Help', 'About', 'Change Password', and 'Log off admin'. Below the header is a breadcrumb trail: 'Home / Elements / Routing / Adaptations - Adaptation Details'. The left sidebar contains a navigation menu with 'Routing' expanded, showing sub-items like 'Domains', 'Locations', 'Adaptations' (highlighted), 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'Adaptation Details' and has a 'General' tab selected. It contains several input fields: 'Adaptation name' (with a red asterisk) containing 'Incoming Digit Conversion', 'Module name' (a dropdown menu) set to 'DigitConversionAdapter', 'Module parameter' (empty), 'Egress URI Parameters' (empty), and 'Notes' (empty). There are 'Commit' and 'Cancel' buttons at the top right of the form area.

Step 3 – Scroll down to the **Digit Conversion for Outgoing Calls from SM** section (the *inbound* DID digits from Sprint that need to be replaced with their associated extensions before being sent to Communication Manager).

- Example 1: 8555511818 is a digit string sent in the Request URI by Sprint IP Toll Free service that is associated with Communication Manager extension 4001. (Note: Toll free number 8555511820 is mapped to a VDN for routing calls to agents.)
 - Enter **8555511818** in the **Matching Pattern** column.
 - Enter **10** in the **Min/Max** columns.
 - Enter **10** in the **Delete Digits** column.
 - Enter **4001** string in the **Insert Digits** column.
 - Specify that this should be applied to the SIP **destination** headers in the **Address to modify** column.
 - Enter any desired notes.

Step 4 – Repeat **Step 3** for all additional Sprint DID numbers mailboxes.

Step 5 - Click on “**Commit**” (not shown).

Note - In the reference configuration no **Digit Conversion for Incoming Calls to SM** were required.

Digit Conversion for Outgoing Calls from SM

Add Remove

7 Items Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern ▲	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 7205459454	* 10	* 10		* 10	4020	destination ▼	
<input type="checkbox"/>	* 7205459455	* 10	* 10		* 10	4525	destination ▼	
<input type="checkbox"/>	* 7205459456	* 10	* 10		* 10	4526	destination ▼	
<input type="checkbox"/>	* 8555511818	* 10	* 10		* 10	4001	destination ▼	
<input type="checkbox"/>	* 8555511819	* 10	* 10		* 10	4020	destination ▼	
<input type="checkbox"/>	* 8555511820	* 10	* 10		* 10	4020	destination ▼	
<input type="checkbox"/>	* 8555511821	* 10	* 10		* 10	4526	destination ▼	

Select : All, None

* Input Required

Commit Cancel

5.3.2. Adaptation for Outbound calls from Communication Manager

Step 1 - In the left pane under **Routing**, click on “**Adaptations**”. In the **Adaptations** page, click on “**New**” (not shown).

Step 2 - In the **Adaptation Details** page, enter:

- A descriptive **Name**, (e.g. **PAI-FromHeader**).
- Select “**OrangeAdapter**” from the **Module Name** drop down menu (if no module name is present, select “<click to add module>” and enter **OrangeAdapter**). This adapter ensures proper delivery of Caller ID.

- In the **Module parameter** field enter **odstd=10.77.19.247**. The odstd parameter will replace the IP address of Session Manager (192.168.3.204) with the IP address of the Sprint SBC untrusted interface in the *outbound* Request URI.

The screenshot shows the Avaya Aura System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.1', and links for 'Help | About | Change Password | Log off admin'. Below the navigation bar, there's a breadcrumb trail: 'Home / Elements / Routing / Adaptations- Adaptation Details'. The left sidebar contains a tree view with 'Routing' expanded, showing sub-items like 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'Adaptation Details' and has a 'General' tab selected. It contains several input fields: 'Adaptation name' (PAI-FromHeader), 'Module name' (OrangeAdapter), 'Module parameter' (odstd=10.77.19.247), 'Egress URI Parameters', and 'Notes'. There are 'Commit' and 'Cancel' buttons at the bottom right of the form area.

Step 3 - Click on “**Commit**”.

Note - In the reference configuration no **Digit Conversion for Incoming or Outgoing Calls from SM** were required.

5.4. SIP Entities

In this section, SIP Entities are administered for the following SIP network elements:

- Avaya Aura® Session Manager (**Section 5.4.1**).
- Avaya Aura® Communication Manager.
- Acme Packet SBC to Sprint (**Section 5.4.4**) - This entity, and its associated entity link (using port 5060), is for both outbound and inbound calls to and from the Sprint IP Toll Free service via the Acme Packet SBC.
- Avaya Modular Messaging (**Section 5.4.5**) – This entity, and its associated entity link (using port 5060), is for local calls from Modular Messaging to Communication Manager.

Note – In the reference configuration TCP is used as the transport protocol between Session Manager and all the SIP Entities including Communication Manager. This was done to facilitate protocol trace analysis. However, Avaya best practices call for TLS (port 5061) to be used as transport protocol when possible.

5.4.1. Avaya Aura® Session Manager SIP Entity

Step 1- In the left pane under **Routing**, click on “**SIP Entities**”. In the **SIP Entities** page click on “**New**” (not shown).

Step 2 - In the **General** section of the **SIP Entity Details** page, provision the following:

- **Name** – Enter a descriptive name for Session Manager (e.g. **asm61**).

- **FQDN or IP Address** – Enter the IP address of the Session Manager network interface, (*not* the management interface), provisioned during installation (e.g. **192.168.3.204**).
- **Type** – Select “**Session Manager**”.
- **Location** – Select location “**Enterprise**” (**Section 5.2**).
- **Outbound Proxy** – (Optional) Leave blank or select another SIP Entity. For calls to SIP domains for which Session Manager is not authoritative, Session Manager routes those calls to this **Outbound Proxy** or to another SIP proxy discovered through DNS if **Outbound Proxy** is not specified.
- **Time Zone** – Select the time zone in which Session Manager resides (this will correspond to the time ranges specified in **Section 5.6**).

Step 3 - In the **SIP Monitoring** section of the **SIP Entity Details** page select:

- Select “**Link Monitoring Enabled**” for **SIP Link Monitoring**
- Use the default values for the remaining parameters.

These entries enable Session Manager to accept SIP requests on the specified ports/protocols. In addition, Session Manager will associate SIP requests containing the IP address of Session Manager (192.168.3.204) in the host part of the Request-URI.

Step 4 - In the **Port** section of the **SIP Entity Details** page, click on “**Add**” and provision an entry as follows:

- **Port** – Enter “**5060**”.
- **Protocol** – Select “**TCP**” (see note above).
- **Default Domain** – (Optional) Select a SIP domain administered in **Section 5.1**. with the selected **SIP Default Domain** (e.g. **avayalab2.com**)

Step 5 - Repeat **Step 4** to provision another entry, except with “**5060**” for **Port** and “**UDP**” for **Protocol**. This is for illustrative purposes only. In the compliance test only TCP was used as the transport protocol over port 5060.

Step 6 – Repeat **Step 4** to provision another entry, except with “**5061**” for **Port** and “**TLS**” for **Protocol**. Although TLS was not used in the reference configuration (see the note at the beginning of this section), the addition of TLS is shown for completeness.

The screenshot shows a web interface for configuring ports. At the top, there are 'Add' and 'Remove' buttons. Below them, it says '3 Items | Refresh' and 'Filter: Enable'. A table lists the configured ports:

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	avayalab2.com	
<input type="checkbox"/>	5060	UDP	avayalab2.com	
<input type="checkbox"/>	5061	TLS	avayalab2.com	

Below the table, it says 'Select : All, None'. At the bottom, there is a red asterisk and the text 'Input Required', and 'Commit' and 'Cancel' buttons.

Step 6 - Click on “**Commit**”.

Note that the **Entity Links** section of the form (not shown) will be automatically populated when the Entity Links are defined in **Section 5.5**.

5.4.2. Avaya Aura® Communication Manager SIP Entity

Step 1 - In the **SIP Entities** page, click on “**New**”.

Step 2 - In the **General** section of the **SIP Entity Details** page, provision the following:

- **Name** – Enter a descriptive name for the Communication Manager trunk (**CM601**).
- **FQDN or IP Address** – Enter the IP address of the Communication Manager Processor Ethernet (procr) described in **Section 6.4**.
- **Type** – Select “**CM**”.
- **Adaptation** – Select the Adaptation administered in **Section 5.3.1**.
- **Location** – Select a Location administered in **Section 5.2.1**.
- **Time Zone** – Select the time zone in which Communication Manager resides.
- In the **SIP Monitoring** section of the **SIP Entity Details** page select:
 - Select **Link Monitoring Enabled** for **SIP Link Monitoring**
 - Use the default values for the remaining parameters.

Step 3 - Click on “**Commit**”.

Note that the **Entity Links** section of the form (not shown) will be automatically populated when the Entity Links are defined in **Section 5.5**.

This screenshot shows the 'SIP Entity Details' configuration page for an entity named 'CM601'. The left sidebar lists various configuration categories, with 'SIP Entities' selected. The main form contains the following fields and values:

- Name:** CM601
- FQDN or IP Address:** 192.168.3.48
- Type:** CM
- Notes:** (empty)
- Adaptation:** Incoming Digit Conversion
- Location:** Enterprise
- Time Zone:** America/Denver
- Override Port & Transport with DNS SRV:** ☐
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty)
- Call Detail Recording:** none
- SIP Link Monitoring:** Use Session Manager Configuration

Buttons for 'Commit' and 'Cancel' are located in the top right corner.

5.4.3. Acme Packet SBC SIP Entity

To configure the Session Border Controller entity, repeat the Steps in **Section 5.4.2**. The **FQDN or IP Address** field is populated with the IP address of the private (inside) Acme SBC interface configured in **Section 8** and the **Type** field is set to “**SIP Trunk**”. See the figure below for the values used in the reference configuration.

Note that the **Entity Links** section of the form (not shown) will be automatically populated when the Entity Links are defined in **Section 5.5**.

This screenshot shows the 'SIP Entity Details' configuration page for an entity named 'Acme 3800'. The left sidebar lists various configuration categories, with 'SIP Entities' selected. The main form contains the following fields and values:

- Name:** Acme 3800
- FQDN or IP Address:** 192.168.3.3
- Type:** SIP Trunk
- Notes:** (empty)
- Adaptation:** PAI-FromHeader
- Location:** Sprint
- Time Zone:** America/Denver
- Override Port & Transport with DNS SRV:** ☐
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty)
- Call Detail Recording:** egress
- SIP Link Monitoring:** Use Session Manager Configuration

Buttons for 'Commit' and 'Cancel' are located in the top right corner.

5.5. Entity Links

In this section, Entity Links are administered between Session Manager and the following SIP Entities:

- Avaya Aura® Communication Manager (**Section 5.5.1**).
- Acme Packet SBC (**Section 5.5.3**).

Note – Once the Entity Links have been committed, the link information will also appear on the associated SIP Entity pages.

Note – In the reference configuration TCP (port 5060) is used as the transport protocol between Session Manager and all the SIP Entities including Communication Manager. This was done to facilitate protocol trace analysis. However, Avaya best practices call for TLS (port 5061) to be used as transport protocol when possible.

5.5.1. Entity Links to Avaya Aura® Communication Manager

Step 1 - In the left pane under **Routing**, click on “**Entity Links**”. In the **Entity Links** page click on “**New**” (not shown).

Step 2 - Continuing in the **Entity Links** page, provision the following:

- **Name** – Enter a descriptive name for this link to Communication Manager (e.g. **ToCM**).
- **SIP Entity 1** – Select the SIP Entity administered in **Section 5.4.1** for Session Manager. SIP Entity 1 must always be a Session Manager instance.
- **SIP Entity 1 Port** – Enter “**5060**”
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.2** for the Communication Manager entity (e.g. **CM601**).
- **SIP Entity 2 Port** - Enter “**5060**”.
- **Trusted** – Check the checkbox.
- **Protocol** – Select “**TCP**”.

Step 3 - Click on “**Commit**”.

The screenshot shows the Avaya Aura® System Manager 6.1 web interface. The left navigation pane is expanded to 'Routing', and 'Entity Links' is selected. The main content area shows the 'Entity Links' configuration page. At the top, there are tabs for 'Routing' and 'Home', and a 'Help ?' link. Below the tabs, there are 'Commit' and 'Cancel' buttons. The main area contains a table with one item, 'ToCM'. The table has columns for Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Trusted, and Notes. The 'ToCM' entry has 'asm61' for SIP Entity 1, 'TCP' for Protocol, '5060' for Port, 'CM601' for SIP Entity 2, '5060' for Port, and the 'Trusted' checkbox is checked. There is a 'Filter: Enable' link at the bottom right of the table. At the bottom of the page, there is a '* Input Required' message and 'Commit' and 'Cancel' buttons.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* ToCM	* asm61	TCP	* 5060	* CM601	* 5060	<input checked="" type="checkbox"/>	

5.5.2. Entity Link to Sprint IP Toll Free Service via Acme Packet SBC

Repeat **Section 5.5.1** with the following differences:

- **Name** – Enter a descriptive name for the link to the Sprint IP Toll Free service, by way of the Acme Packet SBC.
- **SIP Entity 2** – Select the SIP Entity administered in **Section 5.4.3** for the Acme Packet SBC.

The screenshot shows the Avaya Aura System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura® System Manager 6.1", and links for "Help", "About", "Change Password", and "Log off admin". Below the navigation bar, there are tabs for "Routing" (selected) and "Home". The left sidebar contains a tree view with the following items: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links (highlighted), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled "Entity Links" and includes a "Help ?" link, "Commit", and "Cancel" buttons. Below this, there is a table with the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Note. The table contains one row with the following data: Name: * Acme_to_AT&T, SIP Entity 1: * SM61, Protocol: TCP, Port: * 5060, SIP Entity 2: * Acme_and_AT&T, Port: * 5060, Connection Policy: Trusted, and Note: (empty). The table has a "Filter: Enable" link and a "Refresh" button. At the bottom of the table, there is a "Commit" and "Cancel" button, and a note "* Input Required".

5.6. Time Ranges

Time Ranges are administered to define when routing policies are active. You can define Time Ranges by following the steps below.

Step 1 - In the left pane under **Routing**, click on “**Time Ranges**”. In the **Time Ranges** page click on “**New**” (not shown).

Step 2 - Continuing in the **Time Ranges** page, enter a descriptive **Name**, check the checkboxes for the desired day(s) of the week, and enter the desired **Start Time** and **End Time**.

Step 3 - Click on “**Commit**”.

Step 4 - Repeat **Steps 1 – 3** to provision additional time ranges.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Home

Home /Elements / Routing / Time Ranges- Time Ranges

Time Ranges

Edit New Duplicate Delete More Actions

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
<input type="checkbox"/>	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

5.7. Routing Policies

In this section, the following Routing Policies are administered:

- Sprint calls to Avaya Aura® Communication Manager (**Section 5.7.1**).
- Outbound calls from Avaya Aura® Communication Manager to Sprint via the Enterprise Acme Packet SBC.

5.7.1. Routing Policy for Routing to Avaya Aura® Communication Manager from Sprint

Step 1 - In the left pane under **Routing**, click on “**Routing Policies**”. In the **Routing Policies** page click on “**New**” (not shown).

Step 2 - In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing Sprint calls to Communication Manager (e.g. **ToCM**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.

Step 3 - In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on “**Select**” and the **SIP Entity List** page will open.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Home

Home /Elements / Routing / Routing Policies- Routing Policy Details

Routing Policy Details

Commit Cancel

General

* Name: ToCM

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM601	192.168.3.48	CM	

Step 4 - In the **SIP Entity List** page, select the SIP Entity administered in **Section 5.4.2** for Communication Manager (**CM601**), and click on “**Select**”.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Routing Policies- SIP Entity List

SIP Entity List

Select Cancel

SIP Entities

3 Items | Refresh Filter: Enable

	Name	FQDN or IP Address	Type	Notes
<input type="radio"/>	Acme 3800	192.168.3.3	SIP Trunk	
<input type="radio"/>	asm61	192.168.3.204	Session Manager	
<input checked="" type="radio"/>	CM601	192.168.3.48	CM	

Select : None

Select Cancel

Step 5 - Returning to the **Routing Policy Details** page in the **Time of Day** section, click on “**Add**”.

Step 6 - In the **Time Range List** page (not shown), check the checkbox(s) corresponding to one or more Time Ranges administered in **Section 5.6**, and click on “**Select**”.

Step 7 - Returning to the **Routing Policy Details** page in the **Time of Day** section, if multiple Time Ranges were defined, you may enter a **Ranking** (the lower the number, the higher the ranking) for each Time Range, and click on “**Commit**”.

Step 8 - Note that once the **Dial Patterns** are defined (**Section 5.8**) they will appear in the **Dial Pattern** section of this form.

Step 9 - Click on **Commit**.

AVAYA

Avaya Aura® System Manager 6.1

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Routing Policies - Routing Policy Details

Routing Policy Details

Commit

Cancel

Help ?

General

* Name:

ToCM

Disabled:

☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CM601	192.168.3.48	CM	

Time of Day

Add

Remove

View Gaps/Overlaps

1 Item | Refresh

Filter: Enable

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

Add

Remove

2 Items | Refresh

Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input type="checkbox"/>	720545945	10	10	<input type="checkbox"/>	-ALL-	-ALL-	
<input type="checkbox"/>	855	10	10	<input type="checkbox"/>	-ALL-	-ALL-	Incoming DIDs

Select : All, None

Regular Expressions

Add

Remove

0 Items | Refresh

Filter: Enable

<input type="checkbox"/>	Pattern	Rank Order	Deny	Notes
--------------------------	---------	------------	------	-------

* Input Required

Commit

Cancel

5.7.2. Routing Policy for Routing of outbound calls to the Acme Packet SBC for transport to Sprint

Step 1 - In the left pane under **Routing**, click on “**Routing Policies**”. In the **Routing Policies** page click on “**New**” (not shown).

Step 2 - In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing calls to Sprint from Communication Manager (e.g. **ToSprint**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.

Step 3 - In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on “**Select**” and the **SIP Entity List** page will open.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home /Elements / Routing / Routing Policies- SIP Entity List

SIP Entity List

Select Cancel

SIP Entities

3 Items Refresh Filter: Enable

Name	FQDN or IP Address	Type	Notes
<input checked="" type="radio"/> Acme 3800	192.168.3.3	SIP Trunk	
<input type="radio"/> asm61	192.168.3.204	Session Manager	
<input type="radio"/> CM601	192.168.3.48	CM	

Select : None

Select Cancel

Step 5 - Returning to the **Routing Policy Details** page in the **Time of Day** section, click on “**Add**”.

Step 6 - In the **Time Range List** page (not shown), check the checkbox(s) corresponding to one or more Time Ranges administered in **Section 5.6**, and click on “**Select**”.

Step 7 - Returning to the **Routing Policy Details** page in the **Time of Day** section, if multiple Time Ranges were defined, you may enter a **Ranking** (the lower the number, the higher the ranking) for each Time Range, and click on “**Commit**”.

Step 8 - Note that once the **Dial Patterns** are defined (**Section 5.8**) they will appear in the **Dial Pattern** section of this form.

Step 9 – A Regular Expression was used to define the string of possible numbers for outbound dialing rather than having an entry for each number 2 through 9. International dialing and x11 and 1x11 services were covered in the **Dial Pattern** section which is shown below in **Section 5.8**.

Step 10 - Click on **Commit**.

Routing ✕ Home

Routing

- Domains
- Locations
- Adaptations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policies
- Dial Patterns
- Regular Expressions
- Defaults

Home / Elements / Routing / Routing Policies - Routing Policy Details

Routing Policy Details

Help ?

Commit Cancel

General

* Name: ToSprint

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Acme 3800	192.168.3.3	SIP Trunk	

Time of Day

Add Remove View Gaps/Overlaps

1 Item | Refresh

Filter: Enable

<input type="checkbox"/>	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

Dial Patterns

Add Remove

7 Items Refresh							Filter: Enable
<input type="checkbox"/>	Pattern ▲	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input type="checkbox"/>	0	1	1	<input type="checkbox"/>	-ALL-	-ALL-	Operator
<input type="checkbox"/>	0	11	11	<input type="checkbox"/>	-ALL-	-ALL-	Operator Assisted
<input type="checkbox"/>	01	12	12	<input type="checkbox"/>	-ALL-	-ALL-	Operator Assisted 1+dialing
<input type="checkbox"/>	011	10	18	<input type="checkbox"/>	-ALL-	-ALL-	International
<input type="checkbox"/>	1	11	11	<input type="checkbox"/>	-ALL-	-ALL-	1+dialing
<input type="checkbox"/>	1x11	4	4	<input type="checkbox"/>	-ALL-	-ALL-	Services 1+dialing
<input type="checkbox"/>	x11	3	3	<input type="checkbox"/>	-ALL-	-ALL-	Services
Select : All, None							

Regular Expressions

Add Remove

1 Item [Refresh](#)

Filter: Enable

<input type="checkbox"/>	Pattern	Rank Order	Deny	Notes
<input type="checkbox"/>	^sip:[2-9][0-9]{9}.*	0	<input type="checkbox"/>	

Select : All, None

* Input Required

Commit Cancel

5.8. Dial Patterns

In this section, Dial Patterns are administered matching the following calls:

- Inbound PSTN calls via Sprint IP Toll Free service to Communication Manager.
- Outbound calls from Communication Manager to the PSTN via Sprint IP Toll Free service (although Sprint's IPTF service is predominantly an inbound service, outbound call functionality, including call-forwarding off-net, redirected calls and transfers out to the PSTN, were tested.).

5.8.1. Matching Inbound PSTN Calls to Avaya Aura® Communication Manager

In the reference configuration, inbound calls from the Sprint IP Toll Free service used the called digit pattern 855-551-18xx in the SIP Request URI. This pattern is matched for further call processing.

Note – Be sure to match on the digit string specified in the Request URI, not the digit string that was dialed. They may be different.

Step 1 - In the left pane under **Routing**, click on “**Dial Patterns**”. In the **Dial Patterns** page click on “**New**” (not shown).

Step 2 - In the **General** section of the **Dial Pattern Details** page, provision the following:

- **Pattern** – In the reference configuration, Sprint sends a 10 digit number in the Request URI with the format 855-551-18xx. Enter **855**. Note - The adaptation defined on Session Manager for the Communication Manager SIP entity in **Section 5.3.1** will convert the various 855-551-18xx numbers into their corresponding extensions.
- **Min** and **Max** – Enter **10**.
- **SIP Domain** – Select one of the SIP Domains defined in **Section 5.1** or “**-ALL-**”, to select all of those administered SIP Domains. Only those calls with the same domain in the Request-URI as the selected SIP Domain (or all administered SIP Domains if “**-ALL-**” is selected) can match this Dial Pattern.

AVAYA

Avaya Aura® System Manager 6.1

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing

Home

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

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

Dial Pattern Details

General

* Pattern:

855

* Min:

10

* Max:

10

Emergency Call:

☐

SIP Domain:

-ALL-

Notes:

Incoming DIDs

Originating Locations and Routing Policies

Add

Remove

1 Item

Refresh

Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	ToCM	0	<input type="checkbox"/>	CM601	

Step 3 - In the **Originating Locations and Routing Policies** section of the **Dial Pattern Details** page, click on “Add”.

Step 4 - In the **Originating Location** section of the **Originating Location and Routing Policy List** page, you can check the checkbox corresponding to the Location **Sprint** (see **Section 5.2**) or you can simply check “**Apply The Selected Routing Policies to All Originating Locations**“. Note that only those calls that originate from the selected Location(s), or all administered Locations if “**Apply The Selected Routing Policies to All Originating Locations**” is selected, can match this Dial Pattern.

Step 5 - In the **Routing Policies** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to the Routing Policy administered for routing calls to the Communication Manager trunk in **Section 5.7.1**.

Step 6 - Click on “Select”.

Originating Location

☒ Apply The Selected Routing Policies to All Originating Locations

2 Items | Refresh Filter: Enable

<input checked="" type="checkbox"/>	Name	Notes
<input type="checkbox"/>	Enterprise	
<input type="checkbox"/>	Sprint	

Select : All, None

Routing Policies

2 Items | Refresh Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input checked="" type="checkbox"/>	ToCM	<input type="checkbox"/>	CM601	
<input type="checkbox"/>	ToSprint	<input type="checkbox"/>	Acme 3800	

Select : All, None

Step 7 - Returning to the Dial Pattern Details page click on “Commit”.

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Routing * Home

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

Dial Pattern Details Help ?

General

* Pattern: 855

* Min: 10

* Max: 10

Emergency Call: ☐

SIP Domain: -ALL-

Notes: Incoming DIDs

Originating Locations and Routing Policies

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	ToCM	0	<input type="checkbox"/>	CM601	

Select : All, None

Denied Originating Locations

0 Items | Refresh Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

* Input Required

5.8.2. Outbound calls from Communication Manager to the PSTN via Sprint IP Toll Free service

In the reference configuration, outbound calls were routed from Communication Manager to the Sprint IP Toll Free service via Session Manager and the Acme Packet SBC. Dial Patterns were configured on Session Manager to route calls out to Sprint based on Dial Patterns and Regular Expressions. They are described here.

Note – Be sure to match on the digit string specified in the Request URI, not the digit string that was dialed. They may be different.

Step 1 - In the left pane under **Routing**, click on “**Dial Patterns**”. In the **Dial Patterns** page click on “**New**” (not shown).

Step 2 - In the **General** section of the **Dial Pattern Details** page, provision the following:

- **Pattern** – In the reference configuration, Communication Manager sends an 11 digit number in the Request URI and To headers. Enter as many dial patterns as necessary to support your dialing plan. In the reference configuration Dial Patterns were created for Information Services (**x11** and **1x11**) international (**011**), Operator Services (**0**), and any 11 digit dialing starting with **1**. A Regular Expression was created to support 10 digit dialing which is covered in **Section 5.9**. We will use the **x11** dial pattern as an example.
- **Min** and **Max** – Enter appropriate values, in this case **3** for both.
- **SIP Domain** – Select one of the SIP Domains defined in **Section 5.1** or “**-ALL-**”, to select all of those administered SIP Domains. Only those calls with the same domain in the Request-URI as the selected SIP Domain (or all administered SIP Domains if “**-ALL-**” is selected) can match this Dial Pattern.

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The top header includes the Avaya logo, the product name 'Avaya Aura® System Manager 6.1', and links for 'Help', 'About', 'Change Password', and 'Log off admin'. Below the header, there's a breadcrumb trail: 'Home / Elements / Routing / Dial Patterns - Dial Pattern Details'. The left sidebar contains a navigation menu with options: 'Routing', 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns' (highlighted), 'Regular Expressions', and 'Defaults'. The main content area is titled 'Dial Pattern Details' and has a 'General' tab selected. It contains several input fields: 'Pattern' with the value 'x11', 'Min' with the value '3', 'Max' with the value '3', an 'Emergency Call' checkbox which is unchecked, a 'SIP Domain' dropdown menu currently showing '-ALL-', and a 'Notes' text area with the value 'Services'. There are 'Commit' and 'Cancel' buttons at the bottom right of the form area.

Step 3 - In the **Originating Locations and Routing Policies** section of the **Dial Pattern Details** page (not shown), click on “Add”.

Step 4 - In the **Originating Location** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to the Location **Enterprise** (see **Section 5.2**). Note that only those calls that originate from the selected Location(s), or all administered Locations if “**Apply The Selected Routing Policies to All Originating Locations**” is selected, can match this Dial Pattern.

Step 5 - In the **Routing Policies** section of the **Originating Location and Routing Policy List** page, check the checkbox corresponding to the Routing Policy **ToSprint** administered for routing calls to the Sprint network.

Step 6 - Click on “Select”.

Originating Location

☐ Apply The Selected Routing Policies to All Originating Locations

2 Items RefreshFilter: Enable

<input type="checkbox"/>	Name	Notes
<input checked="" type="checkbox"/>	Enterprise	
<input type="checkbox"/>	Sprint	

Select : All, None

Routing Policies

2 Items RefreshFilter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	ToCM	<input type="checkbox"/>	CM601	
<input checked="" type="checkbox"/>	ToSprint	<input type="checkbox"/>	Acme 3800	

Select : All, None

SelectCancel

Step 7 - Returning to the Dial Pattern Details page click on “Commit”.

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Routing Home

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

Dial Pattern Details Help ?

Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name ¹	Originating Location Notes	Routing Policy Name	Rank ²	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Enterprise		ToSprint	0	<input type="checkbox"/>	Acme 3800	

Select : All, None

Denied Originating Locations

Add Remove

0 Items Refresh Filter: Enable

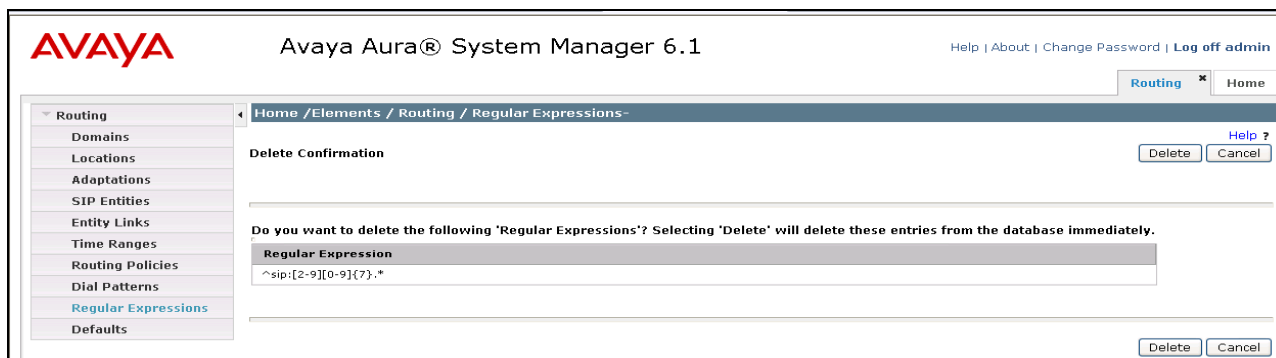
<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

* Input Required Commit Cancel

5.9. Regular Expressions

A Regular Expression was used to support 10 digit dialing without having to enter a dial pattern for every possible destination number that starting with 2 through 9. Below are the steps required to configure this Regular Expression:

Step 1 - In the left pane under **Routing**, click on “**Regular Expressions**”. In the **Regular Expressions** page click on “**New**” (not shown).



Step 2 - In the **General** section of the **Regular Expression Details** page, provision the following:

- **Pattern** – In the reference configuration, a Regular Expression was defined for all possible 10 digit dialing combinations that start with 2 thru 9 and can be followed by 9 more digits in the range of 0 to 9.
- **Rank Order** – Default value is **0** (Lower numbers have higher priority with **0** being the highest priority).

Step 3 - In the **Routing Policy** click on “Add”.

- Place a check in the **ToSprint** policy created in **Section 5.7.2**
- Click on “Select”.

Step 7 - Returning to the **Regular Expression Details** page click on “Commit”.

AVAYA

Avaya Aura® System Manager 6.1

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing

Home

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home /Elements / Routing / Regular Expressions- Regular Expression Details

Regular Expression Details

Help ?

Commit

Cancel

General

* Pattern:

^sip:[2-9][0-9]{9}.*

* Rank Order:

0

Deny:

☐

Notes:

Routing Policy

Add

Remove

1 Item

Refresh

Filter: Enable

<input type="checkbox"/>	Name	Disabled	Destination	Notes
<input type="checkbox"/>	ToSprint	<input type="checkbox"/>	Acme 3800	

Select : All, None

* Input Required

Commit

Cancel

6. Avaya Aura® Communication Manager

This section describes the administration steps for Communication Manager in support of the reference configuration described in these Application Notes. The steps are performed from the Communication Manager System Access Terminal (SAT) interface. These Application Notes assume that basic Communication Manager administration has already been performed. Consult references [5], [6] and [7] for further details if necessary.

Note – In the following sections, only the parameters that are highlighted in **bold** text are applicable to these application notes. Other parameter values may or may not match based on local configurations.

6.1. System Parameters

This section reviews the Communication Manager licenses and features that are required for the reference configuration described in these Application Notes. For required licenses that are not

enabled in the steps that follow, contact an authorized Avaya account representative to obtain the licenses.

Step 1 - Enter the **display system-parameters customer-options** command. On Page 2 of the **system-parameters customer-options** form, verify that the **Maximum Administered SIP Trunks** number is sufficient for the number of expected SIP trunks.

display system-parameters customer-options		Page	2 of	11
OPTIONAL FEATURES				
IP PORT CAPACITIES		USED		
Maximum Administered H.323 Trunks:		12000	0	
Maximum Concurrently Registered IP Stations:		18000	4	
Maximum Administered Remote Office Trunks:		12000	0	
Maximum Concurrently Registered Remote Office Stations:		18000	0	
Maximum Concurrently Registered IP eCons:		414	0	
Max Concur Registered Unauthenticated H.323 Stations:		100	0	
Maximum Video Capable Stations:		18000	1	
Maximum Video Capable IP Softphones:		18000	2	
Maximum Administered SIP Trunks:		24000	70	
Maximum Administered Ad-hoc Video Conferencing Ports:		24000	0	
Maximum Number of DS1 Boards with Echo Cancellation:		522	0	
Maximum TN2501 VAL Boards:		128	0	
Maximum Media Gateway VAL Sources:		250	1	
Maximum TN2602 Boards with 80 VoIP Channels:		128	0	
Maximum TN2602 Boards with 320 VoIP Channels:		128	0	
Maximum Number of Expanded Meet-me Conference Ports:		300	0	
(NOTE: You must logoff & login to effect the permission changes.)				

Step 2 - On Page 3 of the System-Parameters Customer-Options form, verify that the ARS feature is enabled.

display system-parameters customer-options		Page 3 of 11
OPTIONAL FEATURES		
Abbreviated Dialing Enhanced List? y	Audible Message Waiting? y	
Access Security Gateway (ASG)? y	Authorization Codes? y	
Analog Trunk Incoming Call ID? y	CAS Branch? n	
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n	
Answer Supervision by Call Classifier? y	Change COR by FAC? n	
ARS? y	Computer Telephony Adjunct Links? y	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? n	DCS (Basic)? y	
ASAI Link Core Capabilities? y	DCS Call Coverage? y	
ASAI Link Plus Capabilities? y	DCS with Rerouting? y	
Async. Transfer Mode (ATM) PNC? n		
Async. Transfer Mode (ATM) Trunking? n	Digital Loss Plan Modification? y	
ATM WAN Spare Processor? n	DS1 MSP? y	
ATMS? y	DS1 Echo Cancellation? y	
Attendant Vectoring? y		
(NOTE: You must logoff & login to effect the permission changes.)		

Step 3 - On Page 4 of the system-parameters customer-options form:

- Verify that the **Enhanced EC500?**, the **IP Stations?**, **ISDN-PRI?** and the **IP Trunks?** fields are set to “y”.

display system-parameters customer-options		Page 4 of 11
OPTIONAL FEATURES		
Emergency Access to Attendant? y	IP Stations? y	
Enable 'dadmin' Login? y		
Enhanced Conferencing? y	ISDN Feature Plus? n	
Enhanced EC500? y	ISDN/SIP Network Call Redirection? y	
Enterprise Survivable Server? n	ISDN-BRI Trunks? y	
Enterprise Wide Licensing? n	ISDN-PRI? y	
ESS Administration? y	Local Survivable Processor? n	
Extended Cvg/Fwd Admin? y	Malicious Call Trace? y	
External Device Alarm Admin? y	Media Encryption Over IP? n	
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n	
Flexible Billing? n		
Forced Entry of Account Codes? y	Multifrequency Signaling? y	
Global Call Classification? y	Multimedia Call Handling (Basic)? y	
Hospitality (Basic)? y	Multimedia Call Handling (Enhanced)? y	
Hospitality (G3V3 Enhancements)? y	Multimedia IP SIP Trunking? y	
IP Trunks? y		
IP Attendant Consoles? y		
(NOTE: You must logoff & login to effect the permission changes.)		

Step 5 - On Page 5 of the System-Parameters Customer-Options form, verify that the Private Networking and Processor Ethernet fields are set to “y”.

display system-parameters customer-options			Page	5 of	11
OPTIONAL FEATURES					
Multinational Locations? n		Station and Trunk MSP? y			
Multiple Level Precedence & Preemption? y		Station as Virtual Extension? y			
Multiple Locations? n		System Management Data Transfer? n			
Personal Station Access (PSA)? y		Tenant Partitioning? y			
PNC Duplication? n		Terminal Trans. Init. (TTI)? y			
Port Network Support? y		Time of Day Routing? y			
Posted Messages? y		TN2501 VAL Maximum Capacity? y			
		Uniform Dialing Plan? y			
Private Networking? y		Usage Allocation Enhancements? y			
Processor and System MSP? y		Wideband Switching? y			
Processor Ethernet? y		Wireless? n			
Remote Office? y					
Restrict Call Forward Off Net? y					
Secondary Data Module? y					

6.2. Dial Plan

The dial plan defines how digit strings will be used locally by Communication manager.

Step 1 - Enter the **change dialplan analysis** command to provision the dial plan. Note the following dialed strings:

- 3-digit dial access codes (indicated with a **Call Type** of “**dac**”) beginning with the digit “**1**” (e.g. Trunk Access Codes (TACs) defined for trunk groups in this reference configuration conform to this format).
- 4-digit extensions with a **Call Type** of “**ext**” beginning with the digit “**4**” (e.g. Local extensions for Communication Manager stations, agents, and Vector Directory Numbers (VDNs) in this reference configuration conform to this format).
- 1-digit facilities access code (indicated with a **Call Type** of “**fac**”) (e.g. “**9**” access code for outbound ARS dialing).
- 3-digit facilities access codes beginning with * for feature access such as caller ID blocking (e.g. *67) and also for Agent login/logoff (e.g.*56).

change dialplan analysis						Page 1 of 12			
DIAL PLAN ANALYSIS TABLE									
Location: all						Percent Full: 1			
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
1	3	dac							
4	4	ext							
5	4	ext							
6	4	ext							
7	4	ext							
8	4	ext							
9	1	fac							
*	3	fac							

6.3. IP Node Names

Node names define IP addresses to various Avaya components in the CPE.

Step 1 - Enter the **change node-names ip** command and add a node name and the IP address for the Session Manager network interface (e.g. **ASM61**)

Step 2 - A Processor Ethernet (procr) based Communication Manager platform is used in the reference configuration. Make note of the Processor Ethernet node name and IP Address (**procr** & **192.168.3.48**). These entries appear automatically based on the address defined during the Communication Manager installation.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
AA-SBC	192.168.3.217	
ASM61	192.168.3.204	
Acme	192.168.3.3	
MM	192.168.3.56	
SMGR61	192.168.3.203	
default	0.0.0.0	
procr	192.168.3.48	

6.4. IP Interface for procr

The “display ip-interface procr” command can be used to verify the Processor Ethernet (PE) parameters. The following screen shows the parameters used in the reference configuration.

- Verify the **Enable Interface?**, **Allow H.323 Endpoints?**, and **Allow H248 Gateways?** fields are set to “Y”.
- Assign a network region (e.g. **1**)..
- Use default values for the remaining parameters.

display ip-interface procr		Page 1 of 2
IP INTERFACES		
Type: PROCR	Target socket load: 19660	
Enable Interface? y	Allow H.323 Endpoints? y	Allow H.248 Gateways? y
Network Region: 1	Gatekeeper Priority: 5	
IPV4 PARAMETERS		
Node Name: procr	IP Address: 192.168.3.48	
Subnet Mask: /24		

6.5. IP Network Regions

Network Regions are used to group various Communication Manager Resources such as codecs, UDP port ranges, and inter-region communication. In the reference configuration two network regions are used, one for local enterprise calls and one for Sprint calls.

6.5.1. IP Network Region 1 – Local Region

In the reference configuration, Communication Manager elements (e.g. procr) as well as other local Avaya devices (e.g. IP phones, Modular Messaging, etc.) are assigned to ip-network-region 1.

Step 1 – Enter **change ip-network-region x**, where x is the number of an unused IP network region (e.g. region 1). This IP network region will be used to represent the devices within the enterprise site. Populate the form with the following values:

- Enter a descriptive name (e.g. **Enterprise**).
- Enter **avayalab2.com** in the **Authoritative Domain** field.
- Enter **1** for the **Codec Set** parameter.
- **Intra IP-IP Audio Connections** – Set to “yes”, indicating that the RTP paths should be optimized to reduce the use of media resources when possible within the same region.
- **Inter IP-IP Audio Connections** – Set to “yes”, indicating that the RTP paths should be optimized to reduce the use of media resources when possible between regions.
- **UDP Port Min**: - Left at the default value of **16384**.
- **UDP Port Max**: - Left at the default value of **32767**.

change ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1		
Location: 1 Authoritative Domain: avayalab2.com		
Name: Enterprise		
MEDIA PARAMETERS		
Codec Set: 1		Intra-region IP-IP Direct Audio: yes
UDP Port Min: 16384		Inter-region IP-IP Direct Audio: yes
UDP Port Max: 32767		IP Audio Hairpinning? n
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46		
Audio PHB Value: 46		
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5		
		AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS		RSVP Enabled? n
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

Step 2 - On Page 4 of the form:

- Verify that next to region **1** in the **dst rgn** column, the codec set is **1**.
- Next to region **3** in the **dst rgn** column, enter **3** (this means Region 1 is permitted to talk to region 3 and they will use codec set 3 to do so). The **WAN** and **Units** columns will self populate with **Y** and **No Limit**.
- Let all other values default for this form.

change ip-network-region 1										Page 4 of 20		
Source Region: 1										Inter Network Region Connection Management		
										I	M	
										G	A	t
dst	codec	direct	WAN-BW-limits	Video	Intervening	Dyn	A	G	c			
rgn	set	WAN	Units	Total Norm	Prio Shr	Regions	CAC	R	L	e		
1	1									all		
2												
3	3	y	NoLimit						n	t		
4												

6.5.2. IP Network Region 3 – Sprint Trunk Region

In the reference configuration Sprint SIP trunk calls are assigned to ip-network-region 3.

Step 1 - Repeat the steps in Section 6.5.1 with the following changes:

- Page 1
 - Enter a descriptive name (e.g. **Sprint IPTF**)
 - Enter **3** for the **Codec Set** parameter.

change ip-network-region 3		Page 1 of 20	
IP NETWORK REGION			
Region: 3			
Location:		Authoritative Domain: 10.77.19.247	
Name: Sprint IPTF			
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes	
Codec Set: 3		Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 16384		IP Audio Hairpinning? n	
UDP Port Max: 32767			
DIFFSERV/TOS PARAMETERS			
Call Control PHB Value: 46			
Audio PHB Value: 46			
Video PHB Value: 26			
802.1P/Q PARAMETERS			
Call Control 802.1p Priority: 6			
Audio 802.1p Priority: 6			
Video 802.1p Priority: 5			
H.323 IP ENDPOINTS		AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 Link Bounce Recovery? y		RSVP Enabled? n	
Idle Traffic Interval (sec): 20			
Keep-Alive Interval (sec): 5			
Keep-Alive Count: 5			

Step 2 – On **Page 4** of the form:

- Verify that codec **3** is listed for **dst rgn 1** and **3**.

change ip-network-region 3										Page	4 of	20
Source Region: 3		Inter Network Region Connection Management							I	M		
dst rgn	codec set	direct WAN Units	WAN-BW-limits	Video	Intervening	Dyn	A	G	c			
1	3	y	NoLimit	Total Norm	Prio Shr	Regions	CAC	R	L	e	t	
2												
3	3									all		
4												

6.6. IP Codec Parameters

6.6.1. Codecs For IP Network Region 1 (local calls)

In the reference configuration, IP Network Region 1 uses codec set 1.

Step 1 - Enter the **change ip-codec-set x** command, where **x** is the number of an IP codec set used for internal calls. On **Page 1** of the **ip-codec-set** form, ensure that “**G.711MU**” and “**G.729A**” are included in the codec list. Note that the packet interval size will default to 20ms.

change ip-codec-set 1					Page	1 of	2
IP Codec Set							
Codec Set: 1							
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size (ms)				
1: G.711MU	n	2	20				
2: G.729A	n	2	20				
3:							

Step 2 - On **Page 2** of the **ip-codec-set** form, set **FAX Mode** to “**t.38-standard**”.

change ip-codec-set 1			Page	2 of	2
IP Codec Set					
Allow Direct-IP Multimedia? y					
Maximum Call Rate for Direct-IP Multimedia: 384:Kbits					
Maximum Call Rate for Priority Direct-IP Multimedia: 384:Kbits					
FAX	Mode	Redundancy			
Modem	t.38-standard	0			
TDD/TTY	off	0			
Clear-channel	US	3			
	n	0			

6.6.2. Codecs For IP Network Region 2

In the reference configuration, IP Network Region 3 uses codec set 3 for calls from Sprint.

Step 1 - Enter the **change ip-codec-set x** command, where **x** is the number of an unused IP codec set (e.g. **3**). This IP codec set will be used for inbound and outbound Sprint IP Toll Free calls. On **Page 1** of the **ip-codec-set** form, provision the codecs in the order shown below.

change ip-codec-set 3		Page 1 of 2	
IP Codec Set			
Codec Set: 3			
Audio	Silence	Frames	Packet
Codec	Suppression	Per Pkt	Size (ms)
1: G.729A	n	2	30
2: G.711MU	n	2	30
3:			

Step 2 - On **Page 2** of the **ip-codec-set** form, set **FAX Mode** to “**t.38-standard**”.

change ip-codec-set 2		Page 2 of 2	
IP Codec Set			
Allow Direct-IP Multimedia? n			
	Mode	Redundancy	
FAX	t.38-standard	0	
Modem	off	0	
TDD/TTY	off	0	
Clear-channel	n	0	

6.7. SIP Trunks

A SIP trunk is defined on Communication Manager in the reference configuration:

- Sprint access – SIP Trunk 2
 - Note that this trunk uses TCP port 5060 as described in **Section 5.5.1**.

SIP trunks are defined on Communication Manager by provisioning a Signaling Group and a corresponding Trunk Group.

Note – In the reference configuration TCP (port 5060) is used as the transport protocol between Session Manager and all the SIP Entities including Communication Manager. This was done to facilitate protocol trace analysis. However, Avaya best practices call for TLS (port 5061) to be used as transport protocol in customer environments whenever possible.

6.7.1. SIP Trunk for Sprint IP Toll Free calls

This section describes the steps for administering the SIP trunk used for Sprint IP Toll Free calls. This trunk corresponds to the “**CM601**” Entity defined in **Section 5.4.2**.

Step 1 - Enter the **add signaling-group x** command, where **x** is the number of an unused signaling group (e.g. **2**), and provision the following:

- **Group Type** – Set to “**sip**”.

- **Transport Method** – Set to “**tcp**”. Note – Although TCP is used as the transport protocol between the Avaya CPE components, the transport protocol used between the Acme Packet SBC and the Sprint IP Toll Free service is UDP.
- Verify the **IMS Enabled?** Is set to **N**.
- Verify that **Peer Detection Enabled** is “**y**” and that **Peer Server** is **SM**.
- **Near-end Node Name** – Set to the node name of the Procr noted in **Section 6.3**
- **Far-end Node Name** – Set to the node name of Session Manager as administered in **Section 6.3** (e.g. **ASM61**).
- **Near-end Listen Port** and **Far-end Listen Port** – set to “**5060**” (see Transport Method note above).
- **Far-end Network Region** – Set to the IP network region **3**, as defined in **Section 6.5.2**.
- **Far-end Domain** – Enter **avayalab2.com** (Note: An IP address can be used here instead of FQDN). This is the domain used by Session Manager in **Section 5.1**.
- **DTMF over IP** – Set to “**rtp-payload**” to enable Communication Manager to use DTMF according to RFC 2833.
- **Direct IP-IP Audio Connections** – Set to “**y**”, indicating that the RTP paths should be optimized to reduce the use of MedPro resources when possible (known as “shuffling”).
- **Enable Layer 3 Test** – Set to “**y**”. This initiates Communication Manager to send OPTIONS “pings” to Session Manager to provide link status.

add signaling-group 2		Page 1 of 1
SIGNALING GROUP		
Group Number: 2	Group Type: sip	
IMS Enabled? n	Transport Method: tcp	
Q-SIP? n		SIP Enabled LSP? n
IP Video? n		Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y	Peer Server: SM	
Near-end Node Name: procr	Far-end Node Name: ASM61	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 3	
	Far-end Secondary Node Name:	
Far-end Domain: avayalab2.com		
	Bypass If IP Threshold Exceeded? n	
Incoming Dialog Loopbacks: eliminate	RFC 3389 Comfort Noise? n	
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? y	
Session Establishment Timer(min): 3	IP Audio Hairpinning? n	
Enable Layer 3 Test? Y	Initial IP-IP Direct Media? n	
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6	

Step 2 - Enter the **add trunk-group x** command, where **x** is the number of an unused trunk group (e.g. 2). On Page 1 of the **trunk-group** form, provision the following:

- **Group Type** – Set to “**sip**”.
- **Group Name** – Enter a descriptive name (e.g. **Sprint IPTF**).
- **TAC** – Enter a trunk access code that is consistent with the dial plan (e.g. **102**).
- **Direction** – Set to “**two-way**”.
- **Service Type** – Set to “**public-ntwrk**”.

- **Signaling Group** – Enter the number of the signaling group administered in **Step 1** above (e.g. 2).
- **Number of Members** – Enter the maximum number of simultaneous calls permitted on this trunk group (e.g. 14).

add trunk-group 2		Page 1 of 21	
TRUNK GROUP			
Group Number: 2	Group Type: sip	CDR Reports: y	
Group Name: Sprint IPTF	COR: 1	TN: 1	TAC: 102
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? N		
		Member Assignment Method: auto	
		Signaling Group: 2	
		Number of Members: 14	

Step 3 - On Page 2 of the Trunk Group form:

- Set the **Preferred Minimum Session Refresh Interval(sec):** to **900**. This entry will actually cause a value of 1800 to be generated in the SIP header.

add trunk-group 2		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
SCCAN? n		Redirect On OPTIM Failure: 5000	
		Digital Loss Group: 18	
Preferred Minimum Session Refresh Interval(sec): 900			
Disconnect Supervision - In? y Out? y			
XOIP Treatment: auto		Delay Call Setup When Accessed Via IGAR? n	

Step 4 - On Page 3 of the Trunk Group form:

- Set **Numbering Format:** to **public**

add trunk-group 2		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n		Measured: none	
		Maintenance Tests? y	
Numbering Format: public			
		UII Treatment: service-provider	
		Replace Restricted Numbers? n	
		Replace Unavailable Numbers? n	
Modify Tandem Calling Number: no			
Show ANSWERED BY on Display? y			
DSN Term? n			

Step 5 - On Page 4 of the Trunk Group form:

- Set the “**Mark Users as Phone?**” field to “y”.
- Set “**Telephone Event Payload Type**” to the RTP payload type required by the Sprint IP Toll Free service (e.g. 100).

- Use default for all other values.

```

add trunk-group 2
                                Page 4 of 21
                                PROTOCOL VARIATIONS

                                Mark Users as Phone? y
                                Prepend '+' to Calling Number? n
                                Send Transferring Party Information? n
                                Network Call Redirection? y
                                Send Diversion Header? y
                                Support Request History? y
                                Telephone Event Payload Type: 100

                                Convert 180 to 183 for Early Media? n
                                Always Use re-INVITE for Display Updates? n
                                Identity for Calling Party Display: P-Asserted-Identity
                                Enable Q-SIP? n

```

6.8. Public Unknown Numbering

In the public unknown numbering form, Communication Manager local extensions are converted to Sprint numbers (previously identified by Sprint) and directed to the trunk defined in **Section 6.7.1**.

Step 1 - Using the **change public-unknown-numbering 0** command, enter.

- **Ext Len** – Enter the total number of digits in the local extension range (e.g. 4).
- **Ext Code** – Enter the Communication Manager extension (e.g. 4425).
- **Trk Grp(s)** – Enter the number of the Sprint trunk group (e.g. 2).
- **CPN Prefix** – Enter the corresponding Sprint P Toll Free number (e.g. 7205559453).
(For the compliance test Sprint had provided local DIDs for the extensions but you could use an 800 number here for all extensions instead, e.g. 800-555-1234).
- **CPN Len** – Enter the total number of digits after the digit conversion (e.g. 10).

Step 2 – Repeat **Step 1** for all corresponding Sprint numbers/Communication Manager extensions.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp(s)	CPN Prefix	Total CPN Len	
4	4425	2	7205559453	10	Total Administered: 3
4	4525	2	7205559454	10	Maximum Entries: 9999
4	4526	2	7205559456	10	

6.9. Route Patterns

A route pattern is required to direct calls to the Sprint SIP trunk.

6.9.1. Route Pattern for Sprint IP Toll Free SIP Trunk

This form defines the SIP trunk, based on the route-pattern selected by the ARS table in **Section 6.10**.

Step 1 – Enter the **change route-pattern 2** command and enter the following:

- Enter a descriptive **Pattern Name** (e.g. **Sprint IPTF**).
- In the **Grp No** column enter **2** for SIP trunk 2 (The Sprint trunk).
- In the **FRL** column enter **0** (zero).

change route-pattern 2															Page 1 of 3			
Pattern Number: 2 Pattern Name: Sprint IPTF																		
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:	2	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				next				
2:	y	y	y	y	y	n	n			rest				none				
3:	y	y	y	y	y	n	n			rest				none				
4:	y	y	y	y	y	n	n			rest				none				
5:	y	y	y	y	y	n	n			rest				none				
6:	y	y	y	y	y	n	n			rest				none				

6.10. ARS Dialing

Automatic Route Selection (ARS) is used to direct calls to the Sprint network via the route pattern defined in **Section 6.10**.

Step 1 – Enter the **change ars analysis 0** command and enter the following:

- **Dialed String** enter all appropriate combinations of NPA-NXX numbers, international numbers and any services such as Operator or Information services.
- **Min & Max** enter an appropriate value
- **Route Pattern** enter 2
- **Call Type** enter the appropriate call type (e.g. **op**, **int**, **natl**, **hnpa**, **fnpa**).

Step 2 – Repeat **Step 1** for all valid and acceptable destination numbers. The bottom part of the screen shot below shows examples of how to configure the ARS table to support 7 and 10 digit dialing.

change ars analysis 0							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 1
Dialed String	Min	Max	Route Pattern	Call Type	Node Num	ANI Req'd	
0	1	1	2	op		n	
0	8	8	2	op		n	
0	11	11	2	op		n	
00	2	2	2	op		n	
01	9	17	2	iop		n	
011	10	18	2	intl		n	
-----Output Omitted-----							
130	11	11	2	hnpa		n	
1300	11	11	deny	fnpa		n	
131	11	11	2	fnpa		n	
132	11	11	2	fnpa		n	
133	11	11	2	fnpa		n	
134	11	11	2	fnpa		n	
135	11	11	2	fnpa		n	
136	11	11	2	fnpa		n	
137	11	11	2	fnpa		n	
138	11	11	2	fnpa		n	
139	11	11	2	fnpa		n	
140	11	11	2	fnpa		n	
1400	11	11	deny	fnpa		n	
141	11	11	2	fnpa		n	
1411	4	4	2	natl		n	
-----Output Omitted-----							
2	7	7	2	hnpa		n	
3	7	7	2	hnpa		n	
3	10	10	2	hnpa		n	
4	7	7	2	hnpa		n	
411	3	3	2	svcl		n	
5	7	7	2	hnpa		n	
555	7	7	deny	hnpa		n	
6	7	7	2	hnpa		n	
611	3	3	2	svcl		n	
7	7	7	2	hnpa		n	
7	10	10	2	hnpa		n	
8	7	7	2	hnpa		n	
8	10	10	2	fnpa		n	
811	3	3	2	svcl		n	
9	7	7	2	hnpa		n	

6.11. Call Center Provisioning

The administration of Communication Manager Call Center elements – agents, skills (hunt groups), vectors, and Vector Directory Numbers (VDNs) are beyond the scope of these Application Notes. Consult references [5], [6], and [7] for further details if necessary. The samples that follow are provided for reference purposes only and are not meant to be prescriptive.

- Agent form – Page 1

display agent-loginID 8011		Page 1 of 3
AGENT LOGINID		
Login ID: 8011	AAS? n	
Name: Agent 86	AUDIX? n	
TN: 1	LWC Reception: spe	
COR: 1	LWC Log External Calls? n	
Coverage Path: 1	AUDIX Name for Messaging:	
Security Code: 1234	LoginID for ISDN/SIP Display? y	
	Password: 1234	
	Password (enter again): 1234	
	Auto Answer: none	
	MIA Across Skills: system	
	ACW Agent Considered Idle: system	
	Aux Work Reason Code Type: system	
	Logout Reason Code Type: system	
	Maximum time agent in ACW before logout (sec): system	
	Forced Agent Logout Time: :	
WARNING: Agent must log in again before changes take effect		

- Agent form – Page 2. This agent belongs to two different Skill groups (1 and 2) as well as a SuperGroup 4.

display agent-loginID 8011		Page 2 of 3
AGENT LOGINID		
Direct Agent Skill:	Service Objective? n	
Call Handling Preference: skill-level	Local Call Preference? n	
SN RL SL	SN RL SL	
1: 1 1	16: 31: 46:	
2: 2 1	17: 32: 47:	
3: 4 1	18: 33: 48:	

- Skill 2 Hunt Group form – Page 1

display hunt-group 2		Page 1 of 4
HUNT GROUP		
Group Number: 2		ACD? y
Group Name: Skill 2		Queue? y
Group Extension: 4010		Vector? y
Group Type: ucd-mia		
TN: 1		
COR: 1		MM Early Answer? n
Security Code:		Local Agent Preference? n
ISDN/SIP Caller Display:		
Queue Limit: unlimited		
Calls Warning Threshold:	Port:	
Time Warning Threshold:	Port:	

- Skill 2 VDN form – Page 1

display vdn 4020		Page 1 of 3
VECTOR DIRECTORY NUMBER		
Extension: 4020		
Name*: Sprint IPTF		
Destination: Vector Number	2	
Attendant Vectoring?	n	
Meet-me Conferencing?	n	
Allow VDN Override?	n	
COR:	1	
TN*:	1	
Measured: internal		
Acceptable Service Level (sec):	20	
VDN of Origin Annc. Extension*:		
1st Skill*:		
2nd Skill*:		
3rd Skill*:		
* Follows VDN Override Rules		

- Skill 2 Vector form – Page 1

display vector 2

Page 1 of 6

CALL VECTOR

Number: 2

Name: Sprint IPTF

Multimedia? n

Attendant Vectoring? n

Meet-me Conf? n

Lock? n

Basic? y

EAS? y

G3V4 Enhanced? y

ANI/II-Digits? y

ASAI Routing? y

Prompting? y

LAI? y

G3V4 Adv Route? y

CINFO? y

BSR? y

Holidays? y

Variables? y

3.0 Enhanced? y

01 wait-time 2 secs hearing ringback

02 collect 1 digits after announcement 7000 for none

03 goto step 8 if digits = 1

04 goto step 10 if digits = 2

05 goto step 12 if digits = 3

06 goto step 14 if digits = 4

07 stop

08 route-to number ~r13035381932 with cov y if unconditionally

09 stop

10 queue-to skill 2 pri h

11 stop

12 queue-to skill 3 pri h

13 stop

14 queue-to skill 4 pri h

15

16 route-to number ~r13035551932 with cov n if unconditionally

7. Avaya Modular Messaging

In this reference configuration, Avaya Modular Messaging was used to verify DTMF, Message Waiting Indicator (MWI), as well as basic call coverage functionality. The administration for Modular Messaging is beyond the scope of these Application Notes. Consult references [8] and [9] for further details.

8. Configure Acme Packet SBC³

These Application Notes assume that basic Acme Packet SBC administration has already been performed. In the reference configuration, an Acme Packet 3800 Net-Net Session Director SBC was used. The Enterprise Acme Packet SBC configuration used in the reference configuration is provided below as a reference. The notable settings are highlighted in bold and brief annotations are provided on the pertinent settings. Consult with Acme Packet Support [10] for further details and explanations on the configuration below.

Note - The Sprint IP Toll Free service border element IP addresses shown in this document are examples. Sprint will provide the actual IP addresses as part of the IP Toll Free provisioning process.

³ Although an Acme Net-Net SD 3800 was used in the reference configuration, these configurations also apply to the 4250 and 4500 platforms.

8.1. Local Policies

ANNOTATION: The local policy below governs the routing of SIP messages from elements on the network on which the Avaya elements, e.g., Session Manager, Communication Manager, etc., reside to the Sprint IP Toll Free service. The Session Agents are defined here.

```
local-policy
  from-address          *
  to-address            *
  source-realm          Enterprise
  description
  activate-time         N/A
  deactivate-time       N/A
  state                enabled
  policy-priority       none
  last-modified-by      admin@135.x.x.x
  last-modified-date    2010-09-08 19:18:51
  policy-attribute
    next-hop            10.77.19.247
    realm               Sprint
    action              none
    terminate-recursion disabled
    carrier
    start-time          0000
    end-time            2400
    days-of-week        U-S
    cost                0
    app-protocol        SIP
```

state	enabled
methods	
media-profiles	
lookup	single
next-key	
eloc-str-lkup	disabled
eloc-str-match	local-policy

ANNOTATION: The local policy below governs the routing of SIP messages from the Sprint IP Toll Free service to Session Manager.

```

local-policy
  from-address
    *
  to-address
    *
  source-realm
    Sprint
  description
  activate-time      N/A
  deactivate-time    N/A
  state
    enabled
  policy-priority    none
  last-modified-by   admin@135.x.x.x
  last-modified-date 2010-09-08 19:20:48
  policy-attribute
    next-hop
      192.168.3.204
    realm
      Enterprise
    action
      none
    terminate-recursion
      disabled
    carrier
    start-time        0000
    end-time           2400
    days-of-week       U-S
    cost               0
    app-protocol
      SIP
    state
      enabled
    methods
    media-profiles
    lookup
      single
    next-key
    eloc-str-lkup      disabled
    eloc-str-match     local-policy

```

8.2. Network Interfaces

ANNOTATION: The network interface below defines the IP addresses on the interface connected to the network on which the Sprint IP Toll Free service resides.

```

network-interface
  name
    s0p1
  sub-port-id
    0

```

```

description
hostname
ip-address                172.20.2.3
pri-utility-addr
sec-utility-addr
netmask                  255.255.255.0
gateway                  172.20.2.190
sec-gateway
gw-heartbeat
    state                    disabled
    heartbeat                0
    retry-count              0
    retry-timeout            1
    health-score             0
dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout                  11
hip-ip-list              172.20.2.3
ftp-address
icmp-address             172.20.2.3
snmp-address
telnet-address
ssh-address

```

ANNOTATION: The network interface below defines the IP addresses on the interface connected to the network on which the Avaya elements reside.

```

network-interface
    name                    s0p0
    sub-port-id             0
description
hostname
ip-address                192.168.3.3
pri-utility-addr
sec-utility-addr
netmask                  255.255.255.0
gateway                  192.168.3.1
sec-gateway
gw-heartbeat
    state                    disabled
    heartbeat                0
    retry-count              0
    retry-timeout            1
    health-score             0
dns-ip-primary            192.168.3.9
dns-ip-backup1
dns-ip-backup2
dns-domain

```

dns-timeout	11
hip-ip-list	192.168.3.3
ftp-address	
icmp-address	192.168.3.3
snmp-address	
telnet-address	
ssh-address	

8.3. Realms

ANNOTATION: The realm configuration “**Sprint**” below represents the external network on which the Sprint IP Toll Free service resides.

realm-config	
identifier	Sprint
description	
addr-prefix	0.0.0.0
network-interfaces	s0p1:0
mm-in-realm	enabled
mm-in-network	enabled
mm-same-ip	enabled
mm-in-system	enabled
bw-cac-non-mm	disabled
msm-release	disabled
generate-UDP-checksum	disabled
max-bandwidth	0
fallback-bandwidth	0
max-priority-bandwidth	0
max-latency	0
max-jitter	0
max-packet-loss	0
observ-window-size	0
parent-realm	
dns-realm	
media-policy	
media-sec-policy	
in-translationid	
out-translationid	
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
class-profile	
average-rate-limit	0
access-control-trust-level	none
invalid-signal-threshold	0
maximum-signal-threshold	0
untrusted-signal-threshold	0
nat-trust-threshold	0
deny-period	30
ext-policy-svr	
diam-e2-address-realm	

symmetric-latching	disabled
pai-strip	disabled
trunk-context	
early-media-allow	
enforcement-profile	
additional-prefixes	
restricted-latching	none
restriction-mask	32
accounting-enable	enabled
user-cac-mode	none
user-cac-bandwidth	0
user-cac-sessions	0
icmp-detect-multiplier	0
icmp-advertisement-interval	0
icmp-target-ip	
monthly-minutes	0
net-management-control	disabled
delay-media-update	disabled
refer-call-transfer	disabled
dyn-refer-term	disabled
codec-policy	
codec-manip-in-realm	disabled
constraint-name	
call-recording-server-id	
xnq-state	xnq-unknown
hairpin-id	0
stun-enable	disabled
stun-server-ip	0.0.0.0
stun-server-port	3478
stun-changed-ip	0.0.0.0
stun-changed-port	3479
match-media-profiles	
qos-constraint	
sip-profile	
sip-isup-profile	
block-rtcp	disabled
hide-egress-media-update	disabled

<p>ANNOTATION: The realm configuration “Enterprise” below represents the internal network on which the Avaya elements reside.</p>
--

realm-config	
identifier	Enterprise
description	
addr-prefix	0.0.0.0
network-interfaces	
	s0p0:0
mm-in-realm	enabled
mm-in-network	enabled
mm-same-ip	enabled
mm-in-system	enabled
bw-cac-non-mm	disabled
msm-release	disabled

generate-UDP-checksum	disabled
max-bandwidth	0
fallback-bandwidth	0
max-priority-bandwidth	0
max-latency	0
max-jitter	0
max-packet-loss	0
observ-window-size	0
parent-realm	
dns-realm	
media-policy	
media-sec-policy	
in-translationid	
out-translationid	
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
class-profile	
average-rate-limit	0
access-control-trust-level	none
invalid-signal-threshold	0
maximum-signal-threshold	0
untrusted-signal-threshold	0
nat-trust-threshold	0
deny-period	30
ext-policy-svr	
diam-e2-address-realm	
symmetric-latching	disabled
pai-strip	disabled
trunk-context	
early-media-allow	
enforcement-profile	
additional-prefixes	
restricted-latching	none
restriction-mask	32
accounting-enable	enabled
user-cac-mode	none
user-cac-bandwidth	0
user-cac-sessions	0
icmp-detect-multiplier	0
icmp-advertisement-interval	0
icmp-target-ip	
monthly-minutes	0
net-management-control	disabled
delay-media-update	disabled
refer-call-transfer	disabled
dyn-refer-term	disabled
codec-policy	
codec-manip-in-realm	disabled
constraint-name	
call-recording-server-id	
xnq-state	xnq-unknown
hairpin-id	0

stun-enable	disabled
stun-server-ip	0.0.0.0
stun-server-port	3478
stun-changed-ip	0.0.0.0
stun-changed-port	3479
match-media-profiles	
qos-constraint	
sip-profile	
sip-isup-profile	
block-rtcp	disabled
hide-egress-media-update	disabled

8.4. Session Agents

ANNOTATION: The **session agent** below represents the Sprint IP Toll Free service network border element. The Acme will attempt to send calls to the border element based on successful responses to the OPTIONS "ping-method". Redundant network session-agents may be defined.

NOTE - The **ping-method OPTIONS;hops=70** parameter shown below was a setting used in the reference test environment. Acme Packet best practices recommends a setting of **OPTIONS;hops=0** in customer deployments.

session-agent	
hostname	10.77.19.247
ip-address	10.77.19.247
port	5060
state	enabled
app-protocol	SIP
app-type	
transport-method	UDP
realm-id	Sprint
egress-realm-id	
description	
carriers	
allow-next-hop-lp	enabled
constraints	disabled
max-sessions	0
max-inbound-sessions	0
max-outbound-sessions	0
max-burst-rate	0
max-inbound-burst-rate	0
max-outbound-burst-rate	0
max-sustain-rate	0
max-inbound-sustain-rate	0
max-outbound-sustain-rate	0
min-seizures	5
min-asr	0
time-to-resume	0
ttr-no-response	0
in-service-period	0
burst-rate-window	0
sustain-rate-window	0

req-uri-carrier-mode	None
proxy-mode	
redirect-action	
loose-routing	enabled
send-media-session	enabled
response-map	
ping-method	OPTIONS ; hops=70
ping-interval	60
ping-send-mode	keep-alive
ping-all-addresses	disabled
ping-in-service-response-codes	
out-service-response-codes	
media-profiles	
in-translationid	
out-translationid	
trust-me	enabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	
invalidate-registrations	disabled
rfc2833-mode	none
rfc2833-payload	0
codec-policy	
enforcement-profile	
refer-call-transfer	disabled
reuse-connections	NONE
tcp-keepalive	none
tcp-reconn-interval	0
max-register-burst-rate	0
register-burst-window	0
sip-profile	
sip-isup-profile	

ANNOTATION: The session agent below represents the Avaya Aura® Session Manager used in the reference configuration.

session-agent	
hostname	192.168.3.204
ip-address	192.168.3.204
port	5060
state	enabled
app-protocol	SIP

app-type	
transport-method	StaticTCP
realm-id	Enterprise
egress-realm-id	
description	
carriers	
allow-next-hop-lp	enabled
constraints	disabled
max-sessions	0
max-inbound-sessions	0
max-outbound-sessions	0
max-burst-rate	0
max-inbound-burst-rate	0
max-outbound-burst-rate	0
max-sustain-rate	0
max-inbound-sustain-rate	0
max-outbound-sustain-rate	0
min-seizures	5
min-asr	0
time-to-resume	0
ttr-no-response	0
in-service-period	0
burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	Proxy
loose-routing	enabled
send-media-session	enabled
response-map	
ping-method	OPTIONS
ping-interval	60
ping-send-mode	keep-alive
ping-all-addresses	disabled
ping-in-service-response-codes	
out-service-response-codes	
media-profiles	
in-translationid	
out-translationid	
trust-me	enabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	

invalidate-registrations	disabled
rfc2833-mode	none
rfc2833-payload	0
codec-policy	
enforcement-profile	
refer-call-transfer	disabled
reuse-connections	NONE
tcp-keepalive	none
tcp-reconn-interval	0
max-register-burst-rate	0
register-burst-window	0
sip-profile	
sip-isup-profile	

8.5. SIP Configuration

ANNOTATION: The sip-config defines global sip-parameters, including SIP timers, SIP options, which realm to send requests to if not specified elsewhere, and enabling the SD to collect statistics on requests other than REGISTERs and INVITEs.

sip-config	
state	enabled
operation-mode	dialog
dialog-transparency	enabled
home-realm-id	Enterprise
egress-realm-id	Enterprise
nat-mode	None
registrar-domain	
registrar-host	
registrar-port	0
register-service-route	always
init-timer	500
max-timer	4000
trans-expire	32
invite-expire	180
inactive-dynamic-conn	32
enforcement-profile	
pac-method	
pac-interval	10
pac-strategy	PropDist
pac-load-weight	1
pac-session-weight	1
pac-route-weight	1
pac-callid-lifetime	600
pac-user-lifetime	3600
red-sip-port	1988
red-max-trans	10000
red-sync-start-time	5000
red-sync-comp-time	1000
add-reason-header	disabled
sip-message-len	4096
enum-sag-match	disabled

extra-method-stats	enabled
registration-cache-limit	0
register-use-to-for-lp	disabled
options	max-udp-length=65535
	set-inv-exp-at-100-resp
refer-src-routing	disabled
add-ucid-header	disabled
proxy-sub-events	
pass-gruu-contact	disabled
sag-lookup-on-redirect	disabled
set-disconnect-time-on-bye	disabled

8.6. SIP Interfaces

ANNOTATION: The SIP interface below is used to communicate with the Sprint IP Toll Free service, and specifies the "**Sprint**" realm. Note that the connection between the Acme SBC and the Sprint border element uses UDP.

sip-interface	
state	enabled
realm-id	Sprint
description	
sip-port	
address	172.20.2.3
port	5060
transport-protocol	UDP
tls-profile	
allow-anonymous	all
ims-aka-profile	
carriers	
trans-expire	0
invite-expire	0
max-redirect-contacts	0
proxy-mode	
redirect-action	
contact-mode	none
nat-traversal	none
nat-interval	30
tcp-nat-interval	90
registration-caching	disabled
min-reg-expire	300
registration-interval	3600
route-to-registrar	disabled
secured-network	disabled
teluri-scheme	disabled
uri-fqdn-domain	
trust-mode	all
max-nat-interval	3600
nat-int-increment	10
nat-test-increment	30
sip-dynamic-hnt	disabled
stop-recurse	401,407
port-map-start	0

port-map-end	0
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
sip-ims-feature	disabled
operator-identifier	
anonymous-priority	none
max-incoming-conns	0
per-src-ip-max-incoming-conns	0
inactive-conn-timeout	0
untrusted-conn-timeout	0
network-id	
ext-policy-server	
default-location-string	
charging-vector-mode	pass
charging-function-address-mode	pass
ccf-address	
ecf-address	
term-tgrp-mode	none
implicit-service-route	disabled
rfc2833-payload	101
rfc2833-mode	transparent
constraint-name	
response-map	
local-response-map	
ims-aka-feature	disabled
enforcement-profile	
route-unauthorized-calls	
tcp-keepalive	none
add-sdp-invite	disabled
add-sdp-profiles	
sip-profile	
sip-isup-profile	

ANNOTATION: The SIP interface below is used to communicate with the Avaya elements and references the "**Enterprise**" realm. Note that TCP is used between the Acme SBC and Session Manager. See the note in **Section 5.5** regarding the use of TCP and TLS.

sip-interface	
state	enabled
realm-id	Enterprise
description	
sip-port	
address	192.168.3.3
port	5060
transport-protocol	TCP
tls-profile	
allow-anonymous	all
ims-aka-profile	
carriers	

trans-expire	0
invite-expire	0
max-redirect-contacts	0
proxy-mode	
redirect-action	
contact-mode	none
nat-traversal	none
nat-interval	30
tcp-nat-interval	90
registration-caching	disabled
min-reg-expire	300
registration-interval	3600
route-to-registrar	disabled
secured-network	disabled
teluri-scheme	disabled
uri-fqdn-domain	
trust-mode	all
max-nat-interval	3600
nat-int-increment	10
nat-test-increment	30
sip-dynamic-hnt	disabled
stop-recurse	401,407
port-map-start	0
port-map-end	0
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
sip-ims-feature	disabled
operator-identifier	
anonymous-priority	none
max-incoming-conns	0
per-src-ip-max-incoming-conns	0
inactive-conn-timeout	0
untrusted-conn-timeout	0
network-id	
ext-policy-server	
default-location-string	
charging-vector-mode	pass
charging-function-address-mode	pass
ccf-address	
ecf-address	
term-tgrp-mode	none
implicit-service-route	disabled
rfc2833-payload	101
rfc2833-mode	transparent
constraint-name	
response-map	
local-response-map	
ims-aka-feature	disabled
enforcement-profile	
route-unauthorized-calls	
tcp-keepalive	none
add-sdp-invite	disabled


```
add-sdp-profiles
sip-profile
sip-isup-profile
```

8.7. SIP Manipulations

ANNOTATION: Due to Adaptations performed on Session Manager, no SIP Manipulations were necessary on the Acme SBC.

8.8. Steering Pools

ANNOTATION: The steering pools below define the IP Addresses and RTP port ranges on the respective realms. The "Sprint" realm IP Address will be used as the CPE media traffic IP Address to communicate with Sprint (Note: The RTP port range should be obtained from Sprint). Likewise, the IP Address and RTP port range defined for the "Enterprise" realm steering pool will be used to communicate with the Avaya elements. Please note that the "INSIDE" realm port range does not have to be within the range specified below.

```
steering-pool
  ip-address          172.20.2.3
  start-port          16384
  end-port            32767
  realm-id            Sprint
  network-interface   s0p1:0
```

```
steering-pool
  ip-address          192.168.3.3
  start-port          16384
  end-port            32767
  realm-id            Enterprise
  network-interface   s0p0:0
```

Note: The entire Acme Packet SBC configuration can be found in the Appendix at the end of this document.

9. Verification Steps

The following steps may be used to verify the configuration:

9.1. General

1. Place an inbound call, answer the call, and verify that two-way talk path exists. Verify that the call remains stable for several minutes and disconnect properly.
2. Place an inbound call to an agent or phone, but do not answer the call. Verify that the call is redirected back out to Sprint via a SIP 302 Redirect message.
3. Place an inbound call to an agent or phone, press the appropriate IVR option ("1" in the compliance test) to be redirected back out to the PSTN via a SIP REFER message. Verify

that the call is redirected back out to Sprint via SIP REFER message, that there is two way audio, and that the call has been released from the enterprise PBX.

9.2. Avaya Aura® Communication Manager

The following examples are only a few of the monitoring commands available on Communication Manager. See reference [5] and [6] for more information.

1. From the Communication Manager console connection enter the command ***list trace tac xxx***, where xxx is a trunk access code defined for the SIP trunk to Sprint (e.g. 102). Note that in the trace below Session Manager has converted the Sprint IPTF number dialed by the PSTN (855-551-1820) to the Communication Manager VDN extension 4020, before sending the INVITE to Communication Manager.

list trace previous

Page 1

LIST TRACE

time data

```
14:32:19 TRACE STARTED 10/11/2011 CM Release String
14:32:23 SIP<INVITE sip:4020@avayalab2.com:5060;transport=tcp;dt
14:32:23 SIP<g=tl2trga SIP/2.0
14:32:23 active trunk-group 2 member 1 cid 0xc9
14:32:23 SIP>SIP/2.0 180 Ringing
14:32:23 dial 4020
14:32:23 ring vector 2 cid 0xc9
14:32:23 G729 ss:off ps:20
          rgn:3 [192.168.3.3]:16438
          rgn:1 [192.168.3.193]:16388
14:32:23 xoip options: fax:T38 modem:off tty:US uid:0x5001d
          xoip ip: [192.168.3.193]:16388
14:32:24 SIP<PRACK sip:192.168.3.48;transport=tcp SIP/2.0
14:32:24 SIP>SIP/2.0 200 OK
14:32:25 SIP>SIP/2.0 200 OK
14:32:25 active announcement 7000 cid 0xc9
14:32:25 hear annc board 001V9 ext 7000 cid 0xc9
14:32:26 SIP<ACK sip:192.168.3.48;transport=tcp SIP/2.0
14:32:26 SIP>UPDATE sip:SDrejd1-8rdpnmmkrtclf3216rvih0t7hvvvg0jov
14:32:26 SIP>fro9g9c4v9s9400020e0@192.168.3.3:5060;transport=tcp S
14:32:26 SIP>IP/2.0
14:32:26 SIP<SIP/2.0 200 OK
14:32:31 SIP>REFER sip:SDrejd1-8rdpnmmkrtclf3216rvih0t7hvvvg0jovf
14:32:31 SIP>ro9g9c4v9s9400020e0@192.168.3.3:5060;transport=tcp SI
14:32:31 SIP>P/2.0
14:32:31 SIP<SIP/2.0 202 Accepted
14:32:31 SIP<BYE sip:4020@192.168.3.48;transport=tcp SIP/2.0
14:32:31 SIP>SIP/2.0 200 OK
14:32:31 idle trunk-group 2 member 1 cid 0xc9
14:32:46 TRACE COMPLETE trunk-group 2 cid 0x0
```

Command successfully completed

Command:

2. Similar Communication Manager commands are, *list trace station*, *list trace vdn*, and *list trace vector*. Other useful commands are *status trunk* and *status station*.

9.3. Avaya Aura® Session Manager

Step 1 - Access the System Manager GUI, using the URL “<http://<Hostname>/SMGR>”, where **<Hostname>** is the short hostname of System Manager. Log in with the appropriate credentials. Once logged in, the **Home** screen is displayed. Under the **Elements** heading in the center, select **Session Manager**.

Users	Elements	Services
Administrators Manage Administrative Users	Application Management Manage applications and application certificates	Backup and Restore Backup and restore System Manager database
Groups & Roles Manage groups, roles and assign roles to users	Communication Manager Manage Communication Manager objects	Configurations Manage system wide configurations
Subscribers Manage users and shared resources associated with CS1000, including LDAP/file import and export	Conferencing Conferencing	Events Manage alarms, view and harvest logs
Synchronize and Import Synchronize users with the enterprise directory, import users from file	Inventory Manage, discover, and navigate to elements, update element software	Licenses View and configure licenses
UCM Roles Manage UCM Roles, assign roles to users	Messaging Manage Messaging System objects	Replication Track data replication nodes, repair replication nodes
User Management Manage users, shared user resources and provision users	Presence Presence	Scheduler Schedule, track, cancel, update and delete jobs
	Routing Network Routing Policy	Security Manage Security Certificates
	Session Manager Session Manager Element Manager	Templates Manage Templates for Communication Manager and Messaging System objects
	SIP AS 8.1 SIP AS 8.1	UCM Services Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

Step 2 - Expand System Status → SIP Entity Monitoring.

Avaya Aura® System Manager 6.1

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Session Manager

Home

Session Manager

Dashboard

Session Manager

Administration

Communication Profile Editor

Network Configuration

Device and Location Configuration

Application Configuration

System Status

SIP Entity Monitoring

Managed Bandwidth Usage

Security Module Status

Registration Summary

User Registrations

SIP Performance

System Performance

System Tools

Home / Elements / Session Manager / System Status / SIP Entity Monitoring- SIP Entity Monitoring

SIP Entity Link Monitoring Status Summary

This page provides a summary of Session Manager SIP entity link monitoring status.

Entity Link Status for All Session Manager Instances

Run Monitor

1 Item | Refresh

<input type="checkbox"/>	Session Manager Name	Entity Links Down/Total	Entity Links Partially Down	SIP Entities - Monitoring Not Started	SIP Entities - Not Monitored
<input type="checkbox"/>	asm61	0/2	0	0	0

Select : All, None

All Monitored SIP Entities

Run Monitor

2 Items | Refresh | Show ALL | Filter: Enable

<input type="checkbox"/>	SIP Entity Name
<input type="checkbox"/>	Acme 3800
<input type="checkbox"/>	CM601

Select : All, None

Step – 3 From the list of monitored entities, select an entity of interest, such as “**Acme 3800**”. Under normal operating conditions, the **Link Status** should be “**Up**” as shown in the example screen below. The **Reason Code** column indicates that the SBC has responded to SIP OPTIONS from Session Manager with a SIP “**200 OK**” message, which tells Session Manager’s SIP Link Monitoring to consider the link up (Note: Other SIP responses such as “483 Too Many Hops” will also keep the link up. Even though it is considered an error message, it is valid as a response to SIP OPTIONS).

SIP Entity, Entity Link Connection Status

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

All Entity Links to SIP Entity: Acme 3800

Summary View

1 Item | Refresh | Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	asm61	. .3.3	5060	TCP	Up	200 OK	Up

9.3.1. Call Routing Test

The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, expand **Elements** → **Session Manager** → **System Tools** → **Call Routing Test**. The following example shows an inbound call to Communication Manager from the Sprint IP Toll Free service. Note that the Request URI called number was 855-551-1820 and Session Manager converts this to Communication Manager VDN extension 4020 before routing the call to Communication Manager

Step 1 – Called Party URI field = the information passed in the Request URI from Sprint to the enterprise Acme SBC (e.g. **8555511820@avayalab2.com**)

Step 2 – Calling Party Address field = the IP address of the WAN interface of the Sprint SBC (e.g. **192.168.3.3**).

Step 3 – Calling Party URI field = The contents of the From header (e.g. **3035551682@10.77.19.247**).

Step 4 – Session Manager Listening Port = **5060** and **Transport protocol** = **TCP** (see the note in **Section 5.5** regarding the use of TCP).

Step 5 – Populate the **Day of Week** and **Time (UTC)** fields, or let them default to current.

Step 6 – Verify that the **Called Session Manager** instance is correct (if multiple ones are defined).

Step 7 - Click on “Execute Test”.

[Home](#) / [Elements](#) / [Session Manager](#) / [System Tools](#) / [Call Routing Test- Call Routing Test](#)[Help ?](#)

Call Routing Test

This page allows you to test SIP routing algorithms on Session Manager instances. Enter information about a SIP INVITE to learn how it will be routed based on current administration.

SIP INVITE Parameters

Called Party URI <input type="text" value="8555511820@avayalab2.com"/>	Calling Party Address <input type="text" value="10.77.19.247"/>
Calling Party URI <input type="text" value="3035551682@10.77.19.247"/>	Session Manager Listen Port <input type="text" value="5060"/>
Day Of Week <input type="text" value="Tuesday"/>	Time (UTC) <input type="text" value="13:52"/>
Called Session Manager Instance <input type="text" value="asm61"/>	Transport Protocol <input type="text" value="TCP"/>
<div>Execute Test</div>	

The results of the test are shown below. The ultimate routing decision is displayed under the heading **Routing Decisions**. The example shows that a PSTN call to Sprint IP Toll Free service, delivering 8555511820 in the Request URI, is sent to Communication Manager extension **4020**. Further down, the **Routing Decision Process** steps are displayed (depending on the complexity of the routing, multiple pages may be generated). Verify that the test results are consistent with the expected results of the routing administered on Session Manager in **Section 5**.

Routing Decisions

Route < sip:4020@avayalab2.com > to SIP Entity CM601 (.3.48). Terminating Location is Enterprise.

Routing Decision Process

BEGIN EMERGENCY CALL CHECK: Determining if this is a call to an emergency number.

Originating Location is Sprint. Using digits < 8555511820 > and host < avayalab2.com > for routing.

NRP Dial Patterns: No matches for digits < 8555511820 > and domain < avayalab2.com >.

NRP Dial Patterns: No matches for digits < 8555511820 > and domain < null >.

NRP Dial Patterns: No matches found for Sprint. Trying again using NRP Dial Patterns that specify -ALL- NRP Locations.

NRP Dial Patterns: No matches for digits < 8555511820 > and domain < avayalab2.com >.

NRP Dial Patterns: Found a Dial Pattern match for pattern < 855 > Min/Max length 10/10 and domain < null >.

NRP Routing Policies: Ranked destination NRP Sip Entities: CM601.

NRP Routing Policies: Removing disabled routes.

NRP Routing Policies: Ranked destination NRP Sip Entities: CM601.

END EMERGENCY CALL CHECK: This is not an emergency call.

Adapting and proxying for SIP Entity CM601.

NRP Entity Links: Found direct link to destination. Link uses TCP to port 5060.

NRP Adaptations: Incoming Digit Conversion applied.

NRP Adaptations: Request-URI set to sip:4020@avayalab2.com

< Previous

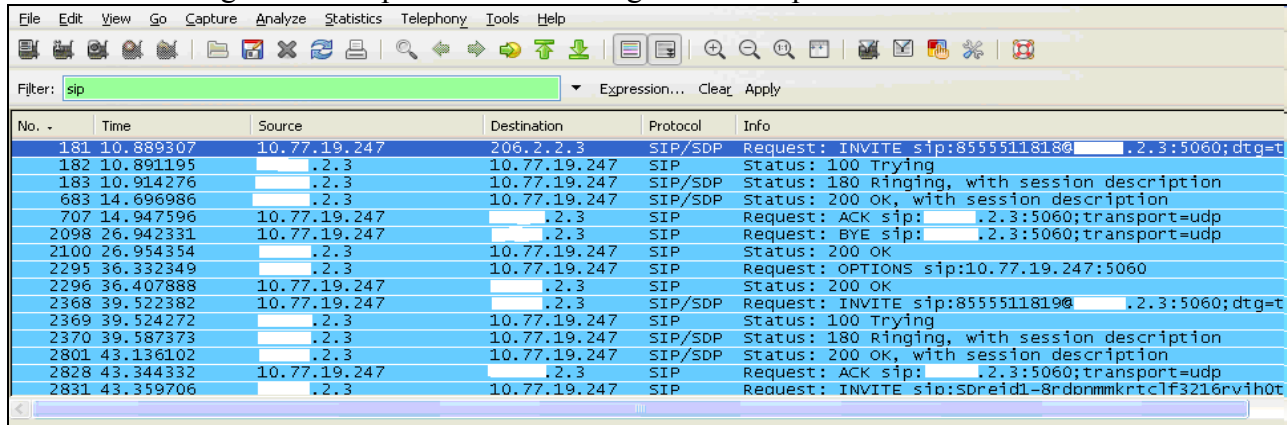
Page 1 of 2

Next >

9.4. Protocol Traces

Using a SIP protocol analyzer (e.g. Wireshark), monitor the SIP traffic at the Acme SBC public “outside” interface connection to the Sprint IP Toll Free service.

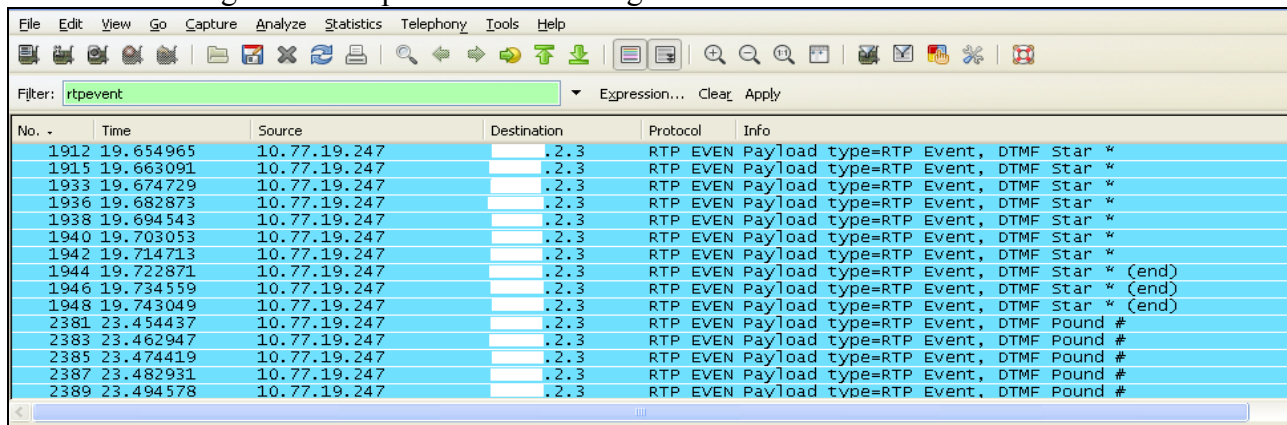
The following is an example of a call filtering on the SIP protocol.



Wireshark interface showing a filter of 'sip'. The packet list displays SIP messages between 10.77.19.247 and 206.2.2.3. The packet details pane shows the selected packet's structure.

No.	Time	Source	Destination	Protocol	Info
181	10.889307	10.77.19.247	206.2.2.3	SIP/SDP	Request: INVITE sip:8555511818@.2.3:5060;dtg=t
182	10.891195	.2.3	10.77.19.247	SIP	Status: 100 Trying
183	10.914276	.2.3	10.77.19.247	SIP/SDP	Status: 180 Ringing, with session description
683	14.696986	.2.3	10.77.19.247	SIP/SDP	Status: 200 OK, with session description
707	14.947596	10.77.19.247	.2.3	SIP	Request: ACK sip:.2.3:5060;transport=udp
2098	26.942331	10.77.19.247	.2.3	SIP	Request: BYE sip:.2.3:5060;transport=udp
2100	26.954354	.2.3	10.77.19.247	SIP	Status: 200 OK
2295	36.332349	.2.3	10.77.19.247	SIP	Request: OPTIONS sip:10.77.19.247:5060
2296	36.407888	10.77.19.247	.2.3	SIP	Status: 200 OK
2368	39.522382	10.77.19.247	.2.3	SIP/SDP	Request: INVITE sip:8555511819@.2.3:5060;dtg=t
2369	39.524272	.2.3	10.77.19.247	SIP	Status: 100 Trying
2370	39.587373	.2.3	10.77.19.247	SIP/SDP	Status: 180 Ringing, with session description
2801	43.136102	.2.3	10.77.19.247	SIP/SDP	Status: 200 OK, with session description
2828	43.344332	10.77.19.247	.2.3	SIP	Request: ACK sip:.2.3:5060;transport=udp
2831	43.359706	.2.3	10.77.19.247	SIP	Request: INVITE sip:Spreid1-8rdonmmkrtclf3216rvihot

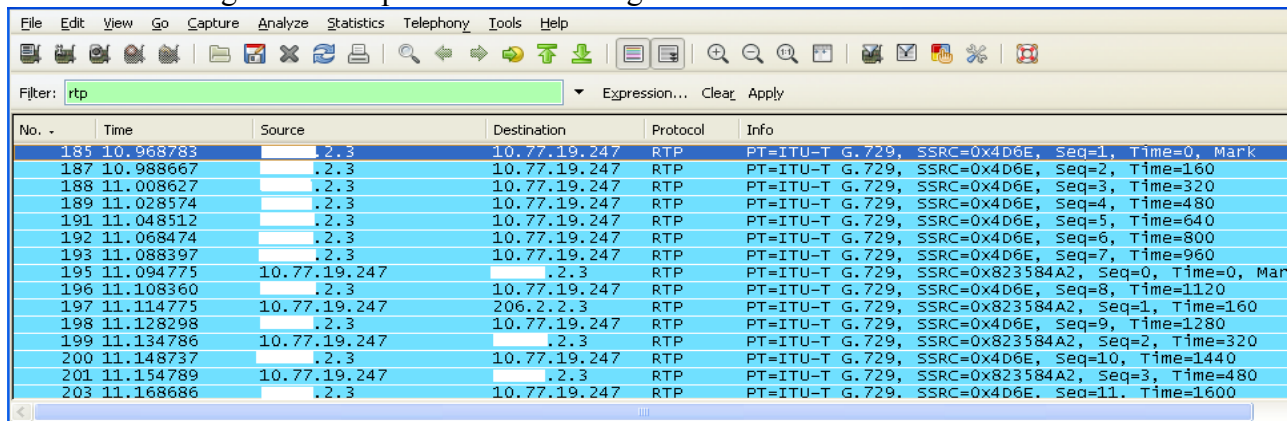
The following is an example of a call filtering on DTMF.



Wireshark interface showing a filter of 'rtpevent'. The packet list displays RTP events between 10.77.19.247 and .2.3. The packet details pane shows the selected packet's structure.

No.	Time	Source	Destination	Protocol	Info
1912	19.654965	10.77.19.247	.2.3	RTP EVEN	Payload type=RTP Event, DTMF Star *
1915	19.663091	10.77.19.247	.2.3	RTP EVEN	Payload type=RTP Event, DTMF Star *
1933	19.674729	10.77.19.247	.2.3	RTP EVEN	Payload type=RTP Event, DTMF Star *
1936	19.682873	10.77.19.247	.2.3	RTP EVEN	Payload type=RTP Event, DTMF Star *
1938	19.694543	10.77.19.247	.2.3	RTP EVEN	Payload type=RTP Event, DTMF Star *
1940	19.703053	10.77.19.247	.2.3	RTP EVEN	Payload type=RTP Event, DTMF Star *
1942	19.714713	10.77.19.247	.2.3	RTP EVEN	Payload type=RTP Event, DTMF Star *
1944	19.722871	10.77.19.247	.2.3	RTP EVEN	Payload type=RTP Event, DTMF Star * (end)
1946	19.734559	10.77.19.247	.2.3	RTP EVEN	Payload type=RTP Event, DTMF Star * (end)
1948	19.743049	10.77.19.247	.2.3	RTP EVEN	Payload type=RTP Event, DTMF Star * (end)
2381	23.454437	10.77.19.247	.2.3	RTP EVEN	Payload type=RTP Event, DTMF Pound #
2383	23.462947	10.77.19.247	.2.3	RTP EVEN	Payload type=RTP Event, DTMF Pound #
2385	23.474419	10.77.19.247	.2.3	RTP EVEN	Payload type=RTP Event, DTMF Pound #
2387	23.482931	10.77.19.247	.2.3	RTP EVEN	Payload type=RTP Event, DTMF Pound #
2389	23.494578	10.77.19.247	.2.3	RTP EVEN	Payload type=RTP Event, DTMF Pound #

The following is an example of a call filtering on RTP.



Wireshark interface showing a filter of 'rtp'. The packet list displays RTP packets between 10.77.19.247 and .2.3. The packet details pane shows the selected packet's structure.

No.	Time	Source	Destination	Protocol	Info
185	10.968783	.2.3	10.77.19.247	RTP	PT=ITU-T G.729, SSRC=0x4D6E, Seq=1, Time=0, Mark
187	10.988667	.2.3	10.77.19.247	RTP	PT=ITU-T G.729, SSRC=0x4D6E, Seq=2, Time=160
188	11.008627	.2.3	10.77.19.247	RTP	PT=ITU-T G.729, SSRC=0x4D6E, Seq=3, Time=320
189	11.028574	.2.3	10.77.19.247	RTP	PT=ITU-T G.729, SSRC=0x4D6E, Seq=4, Time=480
191	11.048512	.2.3	10.77.19.247	RTP	PT=ITU-T G.729, SSRC=0x4D6E, Seq=5, Time=640
192	11.068474	.2.3	10.77.19.247	RTP	PT=ITU-T G.729, SSRC=0x4D6E, Seq=6, Time=800
193	11.088397	.2.3	10.77.19.247	RTP	PT=ITU-T G.729, SSRC=0x4D6E, Seq=7, Time=960
195	11.094775	10.77.19.247	.2.3	RTP	PT=ITU-T G.729, SSRC=0x823584A2, Seq=0, Time=0, Mar
196	11.108360	.2.3	10.77.19.247	RTP	PT=ITU-T G.729, SSRC=0x4D6E, Seq=8, Time=1120
197	11.114775	10.77.19.247	206.2.2.3	RTP	PT=ITU-T G.729, SSRC=0x823584A2, Seq=1, Time=160
198	11.128298	.2.3	10.77.19.247	RTP	PT=ITU-T G.729, SSRC=0x4D6E, Seq=9, Time=1280
199	11.134786	10.77.19.247	.2.3	RTP	PT=ITU-T G.729, SSRC=0x823584A2, Seq=2, Time=320
200	11.148737	.2.3	10.77.19.247	RTP	PT=ITU-T G.729, SSRC=0x4D6E, Seq=10, Time=1440
201	11.154789	10.77.19.247	.2.3	RTP	PT=ITU-T G.729, SSRC=0x823584A2, Seq=3, Time=480
203	11.168686	.2.3	10.77.19.247	RTP	PT=ITU-T G.729, SSRC=0x4D6E, Seq=11, Time=1600

9.5. Acme Packet SBC

The Acme Packet SBC provisioning can be checked by entering the command “*verify-config*”. Acme maintenance manuals may be found at [10].

10. Conclusion

As illustrated in these Application Notes, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, and the Acme Packet Net-Net can be configured to interoperate successfully with the Sprint IP Toll Free service. This solution provides users of Avaya Aura® Communication Manager the ability to support inbound toll free calls over a Sprint IP Toll Free SIP trunk service connection.

The reference configuration shown in these Application Notes is representative of a basic enterprise customer configuration and is intended to provide configuration guidance to supplement other Avaya product documentation. It is based upon formal interoperability compliance testing as part of the Avaya DevConnect Service Provider program.

11. References

The Avaya product documentation is available at <http://support.avaya.com> unless otherwise noted.

- [1] *Administering Avaya Aura® Session Manager*, Doc ID 03-603324, Issue 4, Feb 2011
- [2] *Installing and Configuring Avaya Aura® Session Manager*, Doc ID 03-603473 Issue 2, November 2010
- [3] *Maintaining and Troubleshooting Avaya Aura® Session Manager*, Doc ID 03-603325, Issue 3.1, March 2011
- [4] *Administering Avaya Aura® System Manager*, Document Number 03-603324, June 2010
- [5] *Administering Avaya Aura® Communication Manager*, Release 6.003-300509, Issue 6.0, June 2010
- [6] *Administering Avaya Aura® Call Center Features*, Release 6.0, June 2010
- [7] *Programming Call Vectors in Avaya Aura® Call Center*, 6.0, June 2010
- [8] *Modular Messaging Multi-Site Guide Release 5.1*, June 2009
- [9] *Modular Messaging Messaging Application Server (MAS) Administration Guide*, July 2011

Acme Packet Support (login required):

- [10] <http://support.acmepacket.com>

Sprint IP Toll Free Service Descriptions:

- [11] *Sprint IP Toll Free Service description* - <http://www.sprint.com/>

12. Appendix A – Acme Packet Net-Net Session Director Configuration

Below is the complete configuration for the Acme Packet 3800 Net-Net Session Director used in this compliance test. This is provided as reference material for configuring the Acme Packet SBC and is not meant to be prescriptive.

ACME_SP# show running-config

```
host-routes
  dest-network      192.168.3.48
  netmask           255.255.255.255
  gateway           192.168.3.1
  description
  last-modified-by  admin@135.x.x.x
  last-modified-date 2011-04-20 13:51:47
local-policy
  from-address      *
  to-address         *
  source-realm      Enterprise
  description
  activate-time     N/A
  deactivate-time   N/A
  state             enabled
  policy-priority   none
  last-modified-by  admin@135.x.x.x
  last-modified-date 2010-09-08 19:18:51
  policy-attribute
    next-hop        10.77.19.247
    realm            Sprint
    action           none
    terminate-recursion disabled
    carrier
    start-time       0000
    end-time         2400
    days-of-week     U-S
    cost             0
    app-protocol     SIP
    state            enabled
    methods
    media-profiles
    lookup           single
    next-key
    eloc-str-lkup    disabled
    eloc-str-match
```

local-policy	
from-address	*
to-address	*
source-realm	Sprint
description	
activate-time	N/A
deactivate-time	N/A
state	enabled
policy-priority	none
last-modified-by	admin@135.x.x.x
last-modified-date	2010-09-08 19:20:48
policy-attribute	
next-hop	192.168.3.204
realm	Enterprise
action	none
terminate-recursion	disabled
carrier	
start-time	0000
end-time	2400
days-of-week	U-S
cost	0
app-protocol	SIP
state	enabled
methods	
media-profiles	
lookup	single
next-key	
eloc-str-lkup	disabled
eloc-str-match	
media-manager	
state	enabled
latching	enabled
flow-time-limit	86400
initial-guard-timer	300
subsq-guard-timer	300
tcp-flow-time-limit	86400
tcp-initial-guard-timer	300
tcp-subsq-guard-timer	300
tcp-number-of-ports-per-flow	2
hnt-rtcp	disabled
algd-log-level	NOTICE
mbcd-log-level	NOTICE
red-flow-port	1985
red-mgcp-port	1986
red-max-trans	10000
red-sync-start-time	5000
red-sync-comp-time	1000
media-policing	enabled
max-signaling-bandwidth	10000000
max-untrusted-signaling	100

min-untrusted-signaling	30
app-signaling-bandwidth	0
tolerance-window	30
rtcp-rate-limit	0
trap-on-demote-to-deny	disabled
min-media-allocation	2000
min-trusted-allocation	4000
deny-allocation	32000
anonymous-sdp	disabled
arp-msg-bandwidth	32000
fragment-msg-bandwidth	0
rfc2833-timestamp	disabled
default-2833-duration	100
rfc2833-end-pkts-only-for-non-sig	enabled
translate-non-rfc2833-event	disabled
media-supervision-traps	disabled
dnalg-server-failover	disabled
last-modified-by	admin@135.x.x.x
last-modified-date	2010-09-08 19:23:20
network-interface	
name	wancom0
sub-port-id	0
description	
hostname	
ip-address	135.x.x.251
pri-utility-addr	
sec-utility-addr	
netmask	255.255.255.0
gateway	135.x.x.254
sec-gateway	
gw-heartbeat	
state	disabled
heartbeat	0
retry-count	0
retry-timeout	1
health-score	0
dns-ip-primary	
dns-ip-backup1	
dns-ip-backup2	
dns-domain	
dns-timeout	11
hip-ip-list	
ftp-address	
icmp-address	
snmp-address	
telnet-address	
ssh-address	
last-modified-by	admin@console
last-modified-date	2011-08-22 14:04:52
network-interface	
name	s0p0
sub-port-id	0
description	

hostname	
ip-address	192.168.3.3
pri-utility-addr	
sec-utility-addr	
netmask	255.255.255.0
gateway	192.168.3.1
sec-gateway	
gw-heartbeat	
state	disabled
heartbeat	0
retry-count	0
retry-timeout	1
health-score	0
dns-ip-primary	192.168.3.9
dns-ip-backup1	
dns-ip-backup2	
dns-domain	
dns-timeout	11
hip-ip-list	192.168.3.3
ftp-address	
icmp-address	192.168.3.3
snmp-address	
telnet-address	
ssh-address	
last-modified-by	admin@135.x.x.x
last-modified-date	2010-09-02 18:20:58
network-interface	
name	s0p1
sub-port-id	0
description	
hostname	
ip-address	172.20.2.3
pri-utility-addr	
sec-utility-addr	
netmask	255.255.255.0
gateway	172.20.2.190
sec-gateway	
gw-heartbeat	
state	disabled
heartbeat	0
retry-count	0
retry-timeout	1
health-score	0
dns-ip-primary	
dns-ip-backup1	
dns-ip-backup2	
dns-domain	
dns-timeout	11
hip-ip-list	172.20.2.3
ftp-address	
icmp-address	172.20.2.3
snmp-address	
telnet-address	

ssh-address	
last-modified-by	admin@135.x.x.x
last-modified-date	2011-08-22 15:56:13
ntp-config	
server	192.168.3.9
last-modified-by	admin@135.x.x.x
last-modified-date	2010-09-08 19:26:51
phy-interface	
name	wancom0
operation-type	Control
port	0
slot	1
virtual-mac	
wancom-health-score	50
overload-protection	disabled
last-modified-by	admin@console
last-modified-date	2010-04-20 12:15:56
phy-interface	
name	s0p0
operation-type	Media
port	0
slot	0
virtual-mac	
admin-state	enabled
auto-negotiation	enabled
duplex-mode	FULL
speed	100
overload-protection	disabled
last-modified-by	admin@135.x.x.x
last-modified-date	2010-04-20 12:31:37
phy-interface	
name	s0p1
operation-type	Media
port	1
slot	0
virtual-mac	
admin-state	enabled
auto-negotiation	enabled
duplex-mode	FULL
speed	100
overload-protection	disabled
last-modified-by	admin@135.x.x.x
last-modified-date	2011-08-22 15:54:58
realm-config	
identifier	Sprint
description	
addr-prefix	0.0.0.0
network-interfaces	s0p1:0
mm-in-realm	enabled
mm-in-network	enabled
mm-same-ip	enabled
mm-in-system	enabled
bw-cac-non-mm	disabled

msm-release	disabled
generate-UDP-checksum	disabled
max-bandwidth	0
fallback-bandwidth	0
max-priority-bandwidth	0
max-latency	0
max-jitter	0
max-packet-loss	0
observ-window-size	0
parent-realm	
dns-realm	
media-policy	
media-sec-policy	
in-translationid	
out-translationid	
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
class-profile	
average-rate-limit	0
access-control-trust-level	none
invalid-signal-threshold	0
maximum-signal-threshold	0
untrusted-signal-threshold	0
nat-trust-threshold	0
deny-period	30
ext-policy-svr	
diam-e2-address-realm	
symmetric-latching	disabled
pai-strip	disabled
trunk-context	
early-media-allow	
enforcement-profile	
additional-prefixes	
restricted-latching	none
restriction-mask	32
accounting-enable	enabled
user-cac-mode	none
user-cac-bandwidth	0
user-cac-sessions	0
icmp-detect-multiplier	0
icmp-advertisement-interval	0
icmp-target-ip	
monthly-minutes	0
net-management-control	disabled
delay-media-update	disabled
refer-call-transfer	disabled
dyn-refer-term	disabled
codec-policy	
codec-manip-in-realm	disabled
constraint-name	
call-recording-server-id	

xnq-state	xnq-unknown
hairpin-id	0
stun-enable	disabled
stun-server-ip	0.0.0.0
stun-server-port	3478
stun-changed-ip	0.0.0.0
stun-changed-port	3479
match-media-profiles	
qos-constraint	
sip-profile	
sip-isup-profile	
block-rtcp	disabled
hide-egress-media-update	disabled
last-modified-by	admin@135.x.x.x
last-modified-date	2011-08-24 12:49:17
realm-config	
identifier	Enterprise
description	
addr-prefix	0.0.0.0
network-interfaces	s0p0:0
mm-in-realm	enabled
mm-in-network	enabled
mm-same-ip	enabled
mm-in-system	enabled
bw-cac-non-mm	disabled
msm-release	disabled
generate-UDP-checksum	disabled
max-bandwidth	0
fallback-bandwidth	0
max-priority-bandwidth	0
max-latency	0
max-jitter	0
max-packet-loss	0
observ-window-size	0
parent-realm	
dns-realm	
media-policy	
media-sec-policy	
in-translationid	
out-translationid	
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
class-profile	
average-rate-limit	0
access-control-trust-level	none
invalid-signal-threshold	0
maximum-signal-threshold	0
untrusted-signal-threshold	0
nat-trust-threshold	0
deny-period	30
ext-policy-svr	

diam-e2-address-realm	
symmetric-latching	disabled
pai-strip	disabled
trunk-context	
early-media-allow	
enforcement-profile	
additional-prefixes	
restricted-latching	none
restriction-mask	32
accounting-enable	enabled
user-cac-mode	none
user-cac-bandwidth	0
user-cac-sessions	0
icmp-detect-multiplier	0
icmp-advertisement-interval	0
icmp-target-ip	
monthly-minutes	0
net-management-control	disabled
delay-media-update	disabled
refer-call-transfer	disabled
dyn-refer-term	disabled
codec-policy	
codec-manip-in-realm	disabled
constraint-name	
call-recording-server-id	
xnq-state	xnq-unknown
hairpin-id	0
stun-enable	disabled
stun-server-ip	0.0.0.0
stun-server-port	3478
stun-changed-ip	0.0.0.0
stun-changed-port	3479
match-media-profiles	
qos-constraint	
sip-profile	
sip-isup-profile	
block-rtcp	disabled
hide-egress-media-update	disabled
last-modified-by	admin@135.x.x.x
last-modified-date	2011-08-24 12:49:39
session-agent	
hostname	192.168.3.204
ip-address	192.168.3.204
port	5060
state	enabled
app-protocol	SIP
app-type	
transport-method	StaticTCP
realm-id	Enterprise
egress-realm-id	
description	
carriers	
allow-next-hop-ip	enabled

constraints	disabled
max-sessions	0
max-inbound-sessions	0
max-outbound-sessions	0
max-burst-rate	0
max-inbound-burst-rate	0
max-outbound-burst-rate	0
max-sustain-rate	0
max-inbound-sustain-rate	0
max-outbound-sustain-rate	0
min-seizures	5
min-asr	0
time-to-resume	0
ttr-no-response	0
in-service-period	0
burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	Proxy
loose-routing	enabled
send-media-session	enabled
response-map	
ping-method	OPTIONS
ping-interval	60
ping-send-mode	keep-alive
ping-all-addresses	disabled
ping-in-service-response-codes	
out-service-response-codes	
media-profiles	
in-translationid	
out-translationid	
trust-me	enabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	
invalidate-registrations	disabled
rfc2833-mode	none
rfc2833-payload	0
codec-policy	
enforcement-profile	
refer-call-transfer	disabled

reuse-connections	NONE
tcp-keepalive	none
tcp-reconn-interval	0
max-register-burst-rate	0
register-burst-window	0
sip-profile	
sip-isup-profile	
last-modified-by	admin@135.x.x.x
last-modified-date	2011-08-24 15:32:34
session-agent	
hostname	10.77.19.247
ip-address	10.77.19.247
port	5060
state	enabled
app-protocol	SIP
app-type	
transport-method	UDP
realm-id	Sprint
egress-realm-id	
description	
carriers	
allow-next-hop-lp	enabled
constraints	disabled
max-sessions	0
max-inbound-sessions	0
max-outbound-sessions	0
max-burst-rate	0
max-inbound-burst-rate	0
max-outbound-burst-rate	0
max-sustain-rate	0
max-inbound-sustain-rate	0
max-outbound-sustain-rate	0
min-seizures	5
min-asr	0
time-to-resume	0
ttr-no-response	0
in-service-period	0
burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	
loose-routing	enabled
send-media-session	enabled
response-map	
ping-method	OPTIONS;hops=70
ping-interval	60
ping-send-mode	keep-alive
ping-all-addresses	disabled
ping-in-service-response-codes	
out-service-response-codes	
media-profiles	
in-translationid	

out-translationid	
trust-me	enabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
li-trust-me	disabled
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	
invalidate-registrations	disabled
rfc2833-mode	none
rfc2833-payload	0
codec-policy	
enforcement-profile	
refer-call-transfer	disabled
reuse-connections	NONE
tcp-keepalive	none
tcp-reconn-interval	0
max-register-burst-rate	0
register-burst-window	0
sip-profile	
sip-isup-profile	
last-modified-by	admin@135.x.x.x
last-modified-date	2011-08-24 15:32:55
sip-config	
state	enabled
operation-mode	dialog
dialog-transparency	enabled
home-realm-id	Enterprise
egress-realm-id	Enterprise
nat-mode	None
registrar-domain	
registrar-host	
registrar-port	0
register-service-route	always
init-timer	500
max-timer	4000
trans-expire	32
invite-expire	180
inactive-dynamic-conn	32
enforcement-profile	
pac-method	
pac-interval	10
pac-strategy	PropDist
pac-load-weight	1
pac-session-weight	1

pac-route-weight	1
pac-callid-lifetime	600
pac-user-lifetime	3600
red-sip-port	1988
red-max-trans	10000
red-sync-start-time	5000
red-sync-comp-time	1000
add-reason-header	disabled
sip-message-len	4096
enum-sag-match	disabled
extra-method-stats	enabled
registration-cache-limit	0
register-use-to-for-lp	disabled
options	max-udp-length=65535 set-inv-exp-at-100-resp
refer-src-routing	disabled
add-ucid-header	disabled
proxy-sub-events	
pass-gruu-contact	disabled
sag-lookup-on-redirect	disabled
set-disconnect-time-on-bye	disabled
last-modified-by	admin@135.x.x.x
last-modified-date	2010-09-09 16:43:20
sip-interface	
state	enabled
realm-id	Sprint
description	
sip-port	
address	172.20.2.3
port	5060
transport-protocol	UDP
tls-profile	
allow-anonymous	all
ims-aka-profile	
carriers	
trans-expire	0
invite-expire	0
max-redirect-contacts	0
proxy-mode	
redirect-action	
contact-mode	none
nat-traversal	none
nat-interval	30
tcp-nat-interval	90
registration-caching	disabled
min-reg-expire	300
registration-interval	3600
route-to-registrar	disabled
secured-network	disabled
teluri-scheme	disabled
uri-fqdn-domain	
trust-mode	all
max-nat-interval	3600

nat-int-increment	10
nat-test-increment	30
sip-dynamic-hnt	disabled
stop-recurse	401,407
port-map-start	0
port-map-end	0
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
sip-ims-feature	disabled
operator-identifier	
anonymous-priority	none
max-incoming-conns	0
per-src-ip-max-incoming-conns	0
inactive-conn-timeout	0
untrusted-conn-timeout	0
network-id	
ext-policy-server	
default-location-string	
charging-vector-mode	pass
charging-function-address-mode	pass
ccf-address	
ecf-address	
term-tgrp-mode	none
implicit-service-route	disabled
rfc2833-payload	101
rfc2833-mode	transparent
constraint-name	
response-map	
local-response-map	
ims-aka-feature	disabled
enforcement-profile	
route-unauthorized-calls	
tcp-keepalive	none
add-sdp-invite	disabled
add-sdp-profiles	
sip-profile	
sip-isup-profile	
last-modified-by	admin@135.x.x.x
last-modified-date	2011-06-07 12:24:20
sip-interface	
state	enabled
realm-id	Enterprise
description	
sip-port	
address	192.168.3.3
port	5060
transport-protocol	UDP
tls-profile	
allow-anonymous	all
ims-aka-profile	
sip-port	

address	192.168.3.3
port	5060
transport-protocol	TCP
tls-profile	
allow-anonymous	all
ims-aka-profile	
carriers	
trans-expire	0
invite-expire	0
max-redirect-contacts	0
proxy-mode	
redirect-action	
contact-mode	none
nat-traversal	none
nat-interval	30
tcp-nat-interval	90
registration-caching	disabled
min-reg-expire	300
registration-interval	3600
route-to-registrar	disabled
secured-network	disabled
teluri-scheme	disabled
uri-fqdn-domain	
trust-mode	all
max-nat-interval	3600
nat-int-increment	10
nat-test-increment	30
sip-dynamic-hnt	disabled
stop-recurse	401,407
port-map-start	0
port-map-end	0
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
sip-ims-feature	disabled
operator-identifier	
anonymous-priority	none
max-incoming-conns	0
per-src-ip-max-incoming-conns	0
inactive-conn-timeout	0
untrusted-conn-timeout	0
network-id	
ext-policy-server	
default-location-string	
charging-vector-mode	pass
charging-function-address-mode	pass
ccf-address	
ecf-address	
term-tgrp-mode	none
implicit-service-route	disabled
rfc2833-payload	101
rfc2833-mode	transparent

constraint-name	
response-map	
local-response-map	
ims-aka-feature	disabled
enforcement-profile	
route-unauthorized-calls	
tcp-keepalive	none
add-sdp-invite	disabled
add-sdp-profiles	
sip-profile	
sip-isup-profile	
last-modified-by	admin@135.x.x.x
last-modified-date	2011-08-24 15:31:02
steering-pool	
ip-address	172.20.2.3
start-port	16384
end-port	32767
realm-id	Sprint
network-interface	s0p1:0
last-modified-by	admin@135.x.x.x
last-modified-date	2011-08-24 15:38:17
steering-pool	
ip-address	192.168.3.3
start-port	16384
end-port	32767
realm-id	Enterprise
network-interface	s0p0:0
last-modified-by	admin@135.x.x.x
last-modified-date	2011-08-24 15:25:39
system-config	
hostname	Enterprise-Acme
description	
location	
mib-system-contact	
mib-system-name	
mib-system-location	
snmp-enabled	enabled
enable-snmp-auth-traps	disabled
enable-snmp-syslog-notify	disabled
enable-snmp-monitor-traps	disabled
enable-env-monitor-traps	disabled
snmp-syslog-his-table-length	1
snmp-syslog-level	WARNING
system-log-level	WARNING
process-log-level	NOTICE
process-log-ip-address	0.0.0.0
process-log-port	0
collect	
sample-interval	5
push-interval	15
boot-state	disabled
start-time	now
end-time	never

red-collect-state	disabled
red-max-trans	1000
red-sync-start-time	5000
red-sync-comp-time	1000
push-success-trap-state	disabled
call-trace	disabled
internal-trace	disabled
log-filter	all
default-gateway	172.20.2.190
restart	enabled
exceptions	
telnet-timeout	0
console-timeout	0
remote-control	enabled
cli-audit-trail	enabled
link-redundancy-state	disabled
source-routing	disabled
cli-more	disabled
terminal-height	24
debug-timeout	0
trap-event-lifetime	0
default-v6-gateway	::
ipv6-support	disabled
cleanup-time-of-day	00:00
last-modified-by	admin@135.x.x.x
last-modified-date	2010-09-02 18:44:49

task done
ACME_SP# exit
ACME_SP> exit
Closing Session

©2011 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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