



Avaya Solution & Interoperability Test Lab

Application Notes for Avaya Voice Portal, Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Acme Packet Net-Net Session Border Controller with Verizon Business IP Trunk Service – Issue 1.0

Abstract

These Application Notes describe a sample configuration consisting of Avaya Voice Portal 5.1, Avaya Aura® Communication Manager 6.0, Avaya Aura® Session Manager 6.0, and an Acme Packet Net-Net Session Border Controller. The enterprise equipment is integrated with the Verizon Business IP Trunk Service. The Verizon Business IP Trunk service supports inbound and outbound PSTN calling via SIP trunks. Using the sample configuration, calls to Verizon IP Trunk DID numbers can be delivered to Avaya Voice Portal self-service applications, which can transfer the callers to Avaya Aura® Communication Manager agents if necessary.

Verizon Business is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted in the Avaya Interoperability Test Lab, utilizing a Verizon Business Private IP (PIP) circuit connection to the production Verizon Business IP Trunk Service.

Avaya Voice Portal has not been independently certified by Verizon Business. These Application Notes may be used to facilitate Avaya Voice Portal customer engagements via the Verizon Business field trial process.

TABLE OF CONTENTS

1.	Introduction.....	4
1.1.	Interoperability Compliance Testing.....	4
1.2.	Support.....	4
1.3.	Known Limitations.....	5
2.	Sample Configuration.....	6
2.1.	Illustrative Configuration Information.....	8
2.2.	Call Flows.....	9
3.	Equipment and Software Validated.....	11
4.	Avaya Voice Portal.....	11
4.1.	Background.....	11
4.2.	Log In to Avaya Voice Portal.....	12
4.3.	Voice Portal Home Screen.....	13
4.4.	VoIP Connection.....	13
4.5.	Application References.....	15
4.6.	MPP Servers and VoIP Settings.....	18
4.7.	Configuring RFC2833 Event Value Offered by Avaya Voice Portal.....	19
5.	Avaya Aura® Communication Manager.....	20
5.1.	Processor Ethernet Configuration on S8800 Server.....	20
5.2.	Verify Licensed Features.....	24
5.3.	Dial Plan.....	26
5.4.	Node Names.....	27
5.5.	IP Interface for procr.....	27
5.6.	Network Regions for Gateway, Telephones.....	28
5.7.	IP Codec Sets.....	32
5.8.	SIP Signaling Groups.....	33
5.9.	SIP Trunk Groups.....	36
5.10.	Contact Center Configuration.....	39
5.11.	Public Numbering.....	43
5.12.	Incoming Call Handling Treatment for Incoming Calls.....	43
5.13.	Uniform Dial Plan (UDP) Configuration.....	44
5.14.	Route Pattern for Internal Calls via Avaya Aura® Session Manager.....	44
5.15.	Private Numbering.....	45
5.16.	Avaya Aura® Communication Manager Stations.....	45
5.17.	Coverage Path.....	46
5.18.	Saving Avaya Aura® Communication Manager Configuration Changes.....	47
6.	Avaya Aura® Session Manager Configuration.....	47
6.1.	Domains.....	52
6.2.	Locations.....	53
6.3.	Adaptations.....	57
6.3.1.	Adaptation for Avaya Aura® Session Manager to Avaya Voice Portal.....	58
6.3.2.	Adaptation for Avaya Aura® Session Manager to Acme Packet Net-Net SBC.....	58
6.3.3.	Adaptation for Avaya Aura® Session Manager to Avaya Aura® Communication Manager.....	60
6.4.	SIP Entities.....	60

6.4.1.	SIP Entity for Avaya Voice Portal.....	61
6.4.2.	SIP Entity for Acme Packet Net-Net SBC.....	62
6.4.3.	SIP Entity for Avaya Aura® Session Manager	63
6.4.4.	SIP Entity for Avaya Aura® Communication Manager (Not Specific to Verizon).....	65
6.4.5.	SIP Entity for Avaya Aura® Communication Manager (Specific to Verizon)	66
6.5.	Entity Links	67
6.5.1.	Entity Link for Avaya Aura® Session Manager and Avaya Voice Portal	67
6.5.2.	Entity Link for Avaya Aura® Session Manager and Acme Packet Net-Net SBC ..	67
6.5.3.	Entity Links for Avaya Aura® Session Manager to Avaya Aura® Communication Manager	67
6.6.	Time Ranges.....	69
6.7.	Routing Policies	70
6.7.1.	Routing Policy for Avaya Voice Portal	70
6.7.2.	Verizon-Specific Routing Policy for Avaya Aura® Communication Manager	71
6.7.3.	General Routing Policy for Avaya Aura® Communication Manager.....	72
6.8.	Dial Patterns	73
6.8.1.	Dial Pattern for Calls from Verizon Directly to Avaya Voice Portal	73
6.8.2.	Dial Pattern for Calls Transferred by Avaya Voice Portal to an Avaya Aura® Communication Manager Extension.....	74
6.8.3.	Dial Patterns for Calls from Verizon Directly to Avaya Aura® Communication Manager	74
7.	Acme Packet Net-Net Session Border Controller.....	75
7.1.	Session Agent Change for Avaya Aura® Session Manager Release 6.....	75
7.2.	SIP Manipulation For To Header Towards Avaya Voice Portal	76
7.3.	SIP Manipulation to Preserve User-to-User Information for REFER-based Transfers to Avaya Aura® Communication Manager	76
8.	Verizon Business IP Trunk Configuration.....	80
8.1.	Fully Qualified Domain Name (FQDN)s.....	80
8.2.	Service Access information.....	80
9.	General Test Approach and Test Results.....	81
10.	Verification Steps.....	81
10.1.	Verification Tests	81
10.2.	Avaya Aura® System Manager and Avaya Aura® Session Manager Verifications ..	81
10.2.1.	Verify SIP Entity Link Status.....	82
10.2.2.	Call Routing Test	83
10.3.	Avaya Voice Portal Verifications.....	85
10.4.	Troubleshooting Tools.....	88
11.	Conclusion	88
12.	References.....	88
12.1.	Avaya.....	88
12.2.	Acme Packet.....	89
12.3.	Verizon Business	89

1. Introduction

These Application Notes describe a sample configuration consisting of Avaya Voice Portal 5.1, Avaya Aura® Communication Manager 6.0, Avaya Aura® Session Manager 6.0, and an Acme Packet Net-Net Session Border Controller. The enterprise equipment is integrated with the Verizon Business IP Trunk Service. The Verizon Business IP Trunk service supports inbound and outbound PSTN calling via SIP trunks. Using the sample configuration, calls to Verizon IP Trunk DID numbers can be delivered to Avaya Voice Portal self-service applications, which can transfer the callers to Avaya Aura® Communication Manager agents if necessary.

Avaya Voice Portal has not been independently certified by Verizon Business. These Application Notes may be used to facilitate Avaya Voice Portal customer engagements via the Verizon Business field process.

Access to the IP Trunk Service may use Internet Dedicated Access (IDA) or Private IP (PIP). PIP was used for the sample configuration described in these Application Notes.

In the sample configuration, an Acme Packet 4250 Net-Net Session Border Controller (SBC) is used as an edge device between the Avaya CPE and Verizon Business. The Acme Packet 3800 or 4500 Session Border Controller platforms may be used with similar configuration. The Acme Packet SBC performs SIP header manipulation and provides Network Address Translation (NAT) functionality to convert the private Avaya CPE IP addressing to IP addressing appropriate for the Verizon access method.

Avaya Aura® Session Manager is used as the Avaya SIP trunking “hub” connecting to Avaya Voice Portal, Avaya Aura® Communication Manager, the Acme Packet Session Border Controller, and other applications such as Avaya Modular Messaging. Avaya Voice Portal SIP Connections, Avaya Aura® Communication Manager SIP trunks, and Acme Packet SBC “session-agents” are configured to terminate at Avaya Aura® Session Manager.

1.1. Interoperability Compliance Testing

The interoperability compliance testing focused on verifying inbound call flows to Avaya Voice Portal and subsequent Avaya Voice Portal call transfers to Avaya Aura® Communication Manager skills and agents. Additional test objectives are listed in **Section 8**. See **Section 2.2** for an overview of key call flows.

1.2. Support

Verizon Business customers may obtain support for the Verizon Business IP Trunk service by visiting online support at <http://www.verizonbusiness.com/us/customer/>.

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.

1.3. Known Limitations

The following limitations are noted for the sample configuration described in these Application Notes:

- Avaya Voice Portal 5.1 requires the host portion of the To header of an inbound SIP INVITE message to match the SIP domain configured in Avaya Voice Portal. In the sample configuration, Verizon IP Trunk service sends the SIP domain known to Verizon as the host portion of the To header. Since the SIP domain configured in Avaya Voice Portal may or may not match the SIP domain known to Verizon, the Acme Packet SBC can be used to manipulate the To header so that the To header received by Avaya Voice Portal contains the SIP domain configured in Avaya Voice Portal. While the use of this SIP header manipulation does not present a problem, it is listed here to highlight the SIP header manipulation shown in **Section 7**.
- After Avaya Voice Portal answers an inbound Verizon IP Trunk Service call with a self-service application, Avaya Voice Portal can transfer the call to an Avaya Aura® Communication Manager resource such as a skill and contact center agent, if desired by the caller or application. Depending on the configuration, after the transfer, the PSTN caller may not hear ring back tone while the transferred-to target (e.g., an agent) is ringing. (Acme Packet is investigating this issue via PD00017338.) To ensure that ring back tone is heard, the call vector associated with the transferred-to Vector Directory Number (VDN) can include an announcement step prior to the “queue-to skill” step as described in **Section 5.10**. Again, this announcement configuration does not present a problem, but is listed here to call attention to a benefit of having the transferred-to vector answer the call prior to ringing an agent.
- If an Avaya Voice Portal transfer (occurring on the inside interface of the SBC) results in two consecutive re-INVITE messages sent to the Verizon IP Trunk Service, the Verizon IP Trunk Service will respond to the second INVITE with a 491 Request Pending. This response may beget additional re-INVITE/491 sequences that add to the messaging used to complete a call. Such extra messaging can be avoided if Avaya Voice Portal transfers the call to a VDN that includes an announcement step prior to the “queue-to skill” step as described in **Section 5.10**. For consultative transfers to a VDN involving IP Trunk Service, the Avaya Voice Portal configurable behavior for Consultative Transfer may be set to REFER to avoid extra messaging, as shown in **Section 4.4**.
- When using Verizon IP Trunk service, G.729a will always be used for incoming calls, while the call is connected to Avaya Voice Portal. While it is possible to disable the use of G.729 for outbound calls from Avaya Voice Portal, incoming calls to Avaya Voice Portal that list G.729 as the first audio codec will be answered by Avaya Voice Portal using G.729. Since Verizon IP Trunk service always lists G.729a as the first audio codec on the production circuit used for testing, inbound calls to Avaya Voice Portal always used G.729a in the sample configuration. Calls transferred to Avaya Aura® Communication Manager may use G.729a or G.711MU after the transfer, subject to the Avaya Aura® Communication Manager configuration. An enhancement request to

Avaya Voice Portal (wi00830274) has been entered to ask for greater configurability in the codec selection for an incoming call to Avaya Voice Portal. If it is desired that inbound calls from Verizon use G.711 while in Avaya Voice Portal, the SBC can be used to strip G.729a from the SDP of the INVITE from Verizon, so that Avaya Voice Portal receives only G.711 in the SDP offer.

- Verizon Business IP Trunk Service does not support the History Info Header.
- Verizon Business IP Trunk Services suite does not support G.729B codec.

2. Sample Configuration

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

- Voice Portal provides interactive voice response services to inbound callers. Voice Portal can consist of one or more Media Processing Platform (MPP) servers and a Portal Management System (VPMS) server. Voice Portal also supports MPP and VPMS co-resident on the same server. The co-resident MPP and VPMS configuration was used in the sample configuration.
- Communication Manager provides the enterprise voice communications services. In the sample configuration, Communication Manager runs on an Avaya S8800 Server. This solution is extensible to other Avaya S8xxx Servers.
- The Avaya Media Gateway provides the physical interfaces and resources for enterprise voice communications. For example, announcements and call progress tones can be sourced from the media gateway. In the sample configuration, an Avaya G450 Media Gateway is used. This solution is extensible to other Avaya Media Gateways.
- Avaya “office” phones are represented with Avaya 9600 Series IP Telephones running H.323 and SIP software. Avaya 9600 Series IP Telephones running H.323 firmware are used as contact center agents to staff Communication Manager skills.
- Session Manager routes SIP traffic within the enterprise. In the sample configuration, Session Manager runs on an Avaya S8800 Server.
- System Manager manages Session Manager and Communication Manager. In the sample configuration, System Manager runs on an Avaya S8800 Server.
- The Acme Packet Net-Net provides SIP Session Border Controller (SBC) functionality between the Verizon Business IP Trunk service and the enterprise internal network. The Acme Packet Net-Net 4250 will be referred to as the Acme Packet SBC in these Application Notes. The solution is extensible to other Acme Packet Net-Net models, including the 3800 and 4500.
- The Apache Tomcat Application Server¹ hosts the VXML and CCXML applications that provide the directives for handling the inbound calls to Voice Portal. Voice Portal references those applications.
- Optionally, a Speech Server may be used Automatic Speech Recognition (ASR) and Text-To-Speech (TTS) capabilities. The focus of these Application Notes is protocol compatibility, and a Speech Server was not utilized.

¹ During testing, the Apache Tomcat Application Server, Avaya MPP and VPMS software were installed on the same server. Separate servers may be used.

Figure 1 illustrates the sample configuration. As also noted in **Section 8.2**, the Verizon IP Trunk number listed with a “*” is the number illustrated via screens in these Application Notes. The sample configuration is similar to the configuration previously documented in reference [JRR-VZIPT], with Voice Portal added. Although the Verizon IP Trunk Service is capable of supporting toll-free numbers (e.g., IP Trunk with dedicated 8xx numbers), the DID numbers assigned to the Verizon IP Trunk circuit used for testing did not include any toll-free numbers.

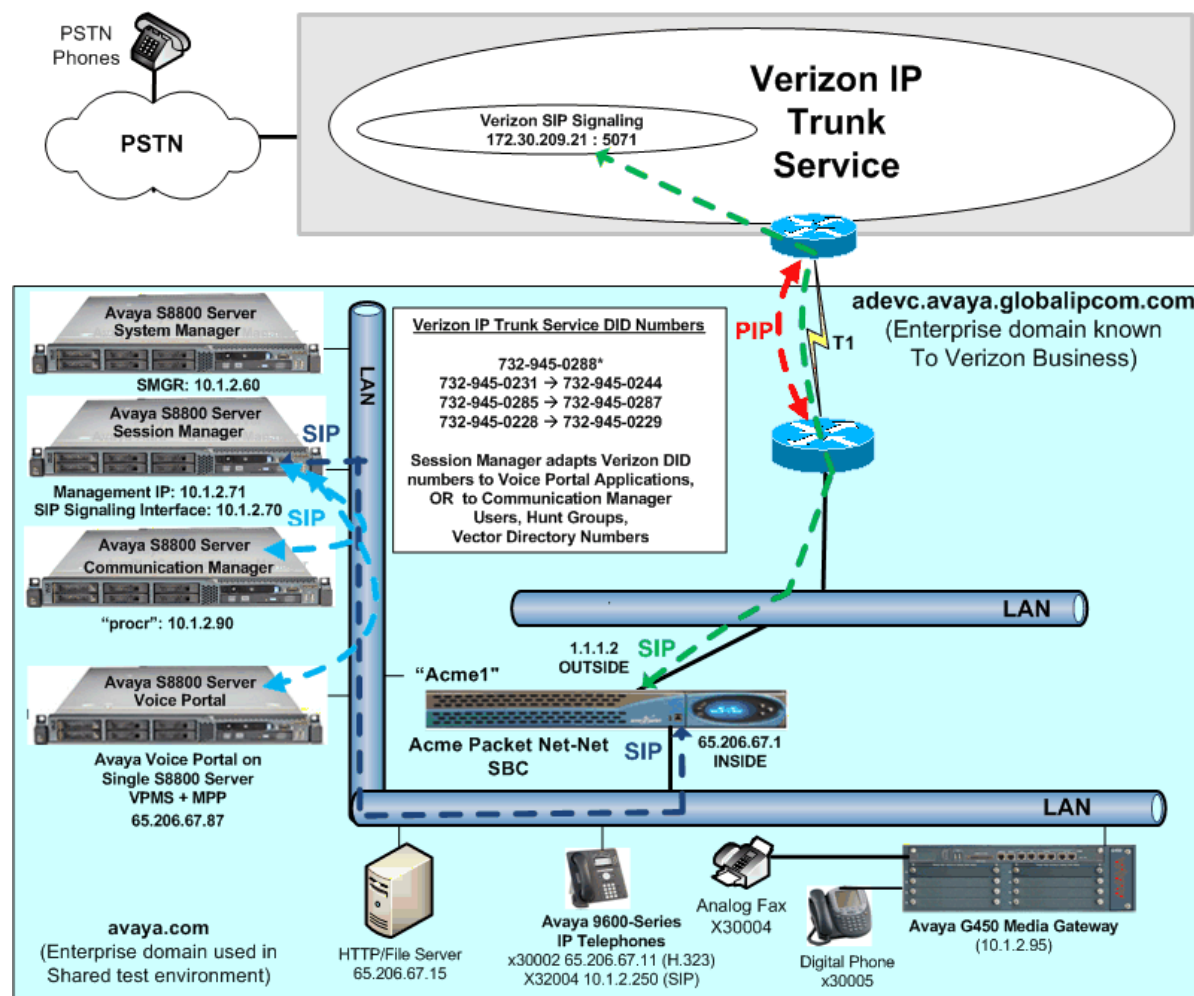


Figure 1: Sample Configuration

2.1. Illustrative Configuration Information

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

Component	Illustrative Value in these Application Notes
Avaya Voice Portal	
MPP Server IP Address	65.206.67.87
Number Triggering Voice Portal Application	44000 as illustrated. Other number to application mappings can be configured similarly.
Avaya Aura® Session Manager	
Signaling Interface	10.1.2.70
Avaya Aura® Communication Manager	
Processor Ethernet IP Address	10.1.2.90
Avaya G450 Media Gateway	10.1.2.95
Vector Directory Number (VDN) Extensions	36880 illustrated, others as needed
Skill (Hunt Group) Extensions	36680 illustrated, others as needed
Agent Extensions (Agent Login-Ids)	46880 illustrated, others as needed
Telephone Extensions	3000x
Acme Packet Net-Net SBC	
IP Address of “Outside” Interface (towards Verizon Business)	1.1.1.2
IP Address of “Inside” Interface (towards Avaya elements)	65.206.67.1
Verizon Business IP Trunk Service	
Border Element IP Address and Port	172.30.209.21:5071 (UDP)
Digits Passed to Avaya Voice Portal	As illustrated, 732-945-0288 (IP Trunk DID) mapped to 44000 by Session Manager Adaptation. Other mappings of Verizon DID numbers to Voice Portal application triggers can be configured similarly.

Table 1: Illustrative Values Used in these Application Notes

2.2. Call Flows

To understand how inbound Verizon Business IP Trunk inbound calls are handled by Voice Portal, several call flows are described in this section.

One type of call scenario, illustrated in **Figure 2**, is an inbound call arriving and remaining on Voice Portal.

1. A PSTN phone originates a call to a Verizon Business IP Trunk DID number.
2. The PSTN routes the call to the Verizon Business IP Trunk service network.
3. The Verizon Business IP Trunk service routes the call to the Acme Packet SBC.
4. The Acme Packet SBC performs SIP Network Address Translation (NAT) and any necessary SIP header modifications, and routes the call to Session Manager.
5. Session Manager routes the call to Voice Portal.
6. Voice Portal matches the called party number to a VXML and/or CCXML application, answers the call, and handles the call according to the directives specified in the application.
7. In this scenario, the application sufficiently meets the caller's needs or requests, and thus the call does not need to be transferred to Communication Manager.

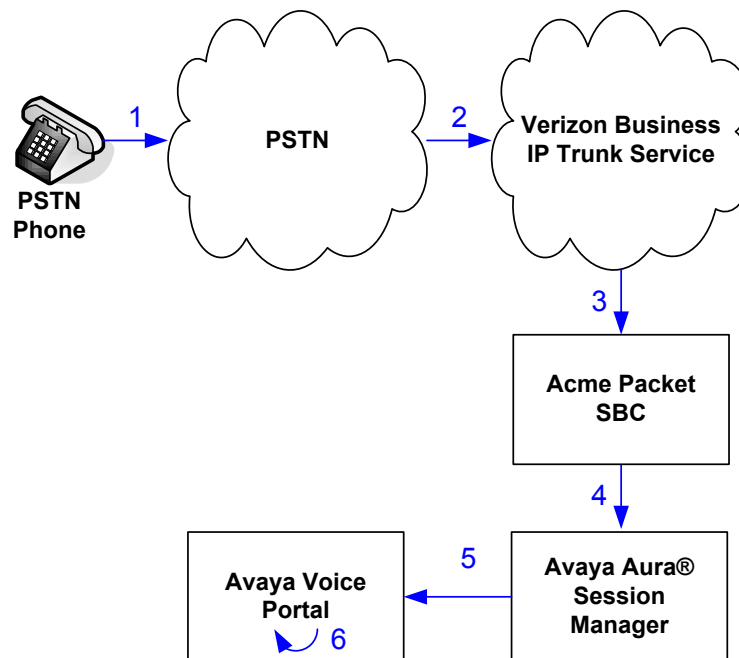


Figure 2: Inbound Call Handled Entirely by Avaya Voice Portal

Another type of call scenario, illustrated in **Figure 3**, is an inbound call arriving on Voice Portal and subsequently transferred by Voice Portal to a Communication Manager skill via a Communication Manager Vector Directory Number (VDN). Although the Voice Portal application logic can in general check for agent availability prior to transferring the call, in this

case, assume that Voice Portal transfers the call to the Communication Manager VDN without first checking whether agents are available.

The steps depicted below are intended to be a high-level representation of the call flow.

1. Same as the first five steps from the first call scenario.
2. In this scenario, the application is not sufficient to meet the caller's needs or requests, and thus the call needs to be transferred to a Communication Manager agent via Session Manager. Voice Portal instructs the Acme Packet SBC to transfer the inbound call to a Communication Manager skill.
3. The Acme Packet SBC transfers the inbound call to the aforementioned skill on Communication Manager via Session Manager.
4. An agent becomes available.
5. Communication Manager routes the call to the agent.

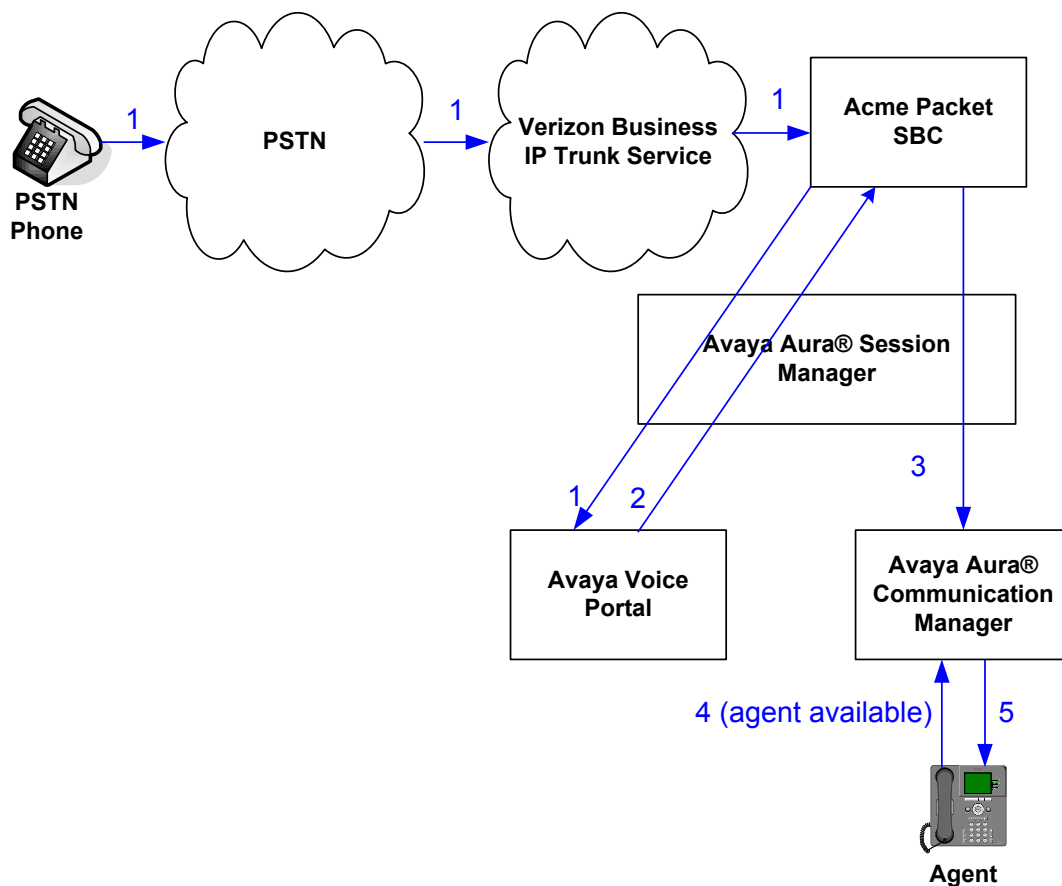


Figure 3: Inbound Call Transferred by Avaya Voice Portal to Avaya Aura® Communication Manager

3. Equipment and Software Validated

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

Component	Version
Avaya S8800 Server	Avaya Voice Portal 5.1 Voice Portal Management System (VPMS) 5.1.0.0.4201 Media Processing Platform (MPP) Application Server 5.1.0.0.4206
Avaya S8800 Server	Avaya Aura® Communication Manager R6.0 (345.0 + patch 18444)
Avaya S8800 Server	Avaya Aura® System Manager R6.0 SP1
Avaya S8800 Server	Avaya Aura® Session Manager (6.0.1.0.601013)
Avaya G450 Media Gateway	30.13.2
Avaya 9630 IP Telephone (H.323)	3.1.1
Avaya 2420 Digital Telephone	---
Apache Tomcat Application Server	6.0.18
Acme Packet Net-Net 4250 ²	SC6.2.0m3p5.xz

Table 2: Equipment and Software Versions

4. Avaya Voice Portal

These Application Notes assume that the necessary Voice Portal licenses have been installed and basic Voice Portal administration has already been performed. Consult [1], [2], [3], and [4] for further details if necessary.

4.1. Background

Voice Portal handles inbound calls according to the directives specified by Voice XML (VXML) and/or Call Control XML (CCXML) applications. References to these applications are administered on Voice Portal, along with one or more called numbers for each application reference. When an inbound call arrives at Voice Portal, the called party number (URI) is matched against the administered called numbers. If a match is found, then the corresponding application is accessed to handle the call.

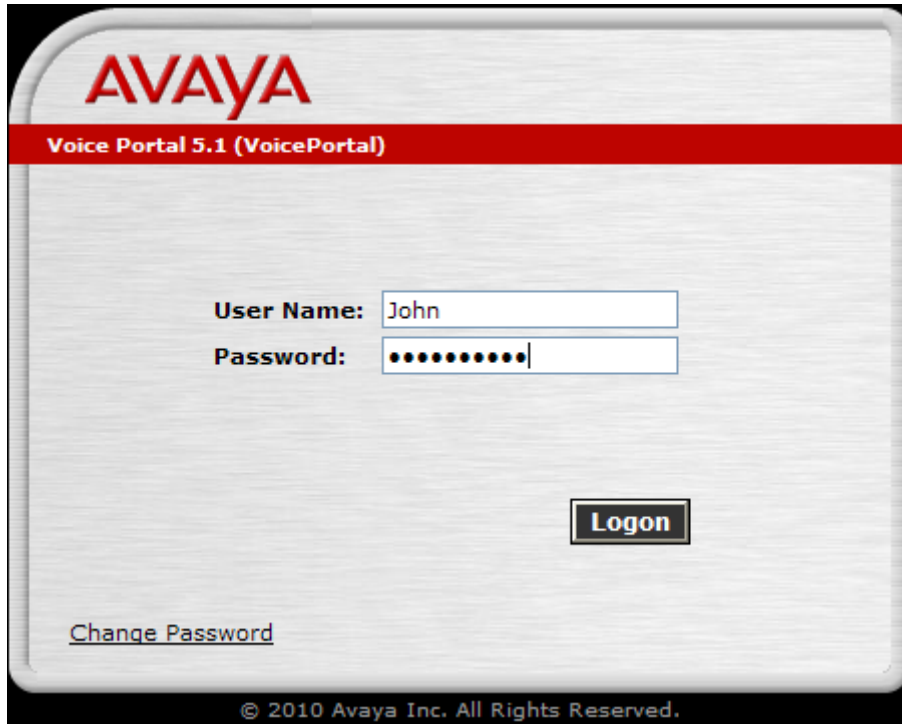
For the sample configuration described in these Application Notes, a simple VXML test application was used to exercise various SIP call flow scenarios with the Verizon Business IP Trunk service. In production, enterprises can develop their own VXML and/or CCXML applications to meet specific customer self-service needs, or consult Avaya Professional Services

² Although an Acme Packet Net-Net 4250 was used in the sample configuration, the 3800, 4500, and 9200 platforms may also be used.

and/or authorized Avaya Business Partners. The development and deployment of VXML and CCXML applications is beyond the scope of these Application Notes. Consult [1], [2], and [4] for further details if necessary.

4.2. Log In to Avaya Voice Portal

Launch a web browser, enter `https://65.206.67.87/VoicePortal` in the URL, where 65.206.67.87 is the IP Address of Voice Portal Management System (VPMS) in the sample configuration. Enter the appropriate credentials as shown in the example screen below. Click **Logon**.



The screenshot shows the Avaya Voice Portal 5.1 login interface. At the top, the Avaya logo is displayed in red. Below it, a red banner reads "Voice Portal 5.1 (VoicePortal)". The main area is white and contains a login form. The form has two fields: "User Name:" with the value "John" and "Password:" with a masked password represented by ten dots. A "Logon" button is positioned to the right of the password field. Below the login fields, there is a link labeled "Change Password". At the bottom of the page, a copyright notice reads "© 2010 Avaya Inc. All Rights Reserved."

4.3. Voice Portal Home Screen

After logging in successfully, the **Home** screen will appear, as shown below.

AVAYA

Welcome, John

Last logged in 10/11/10 at 10:34:44 AM EDT

Voice Portal 5.1 (VoicePortal)

Expand All | Collapse All

User Management

Roles

Users

Login Options

Real-Time Monitoring

System Monitor

Active Calls

Port Distribution

System Maintenance

Audit Log Viewer

Trace Viewer

Log Viewer

Alarm Manager

System Management

MPP Manager

Software Upgrade

System Backup

System Configuration

Alarm Codes

Alarm/Log Options

Applications

MPP Servers

Report Data

SNMP

Speech Servers

VoIP Connections

VPMS Servers

Security

Certificates

Licensing

Reports

Standard

Custom

Scheduled

You are here: Home

Voice Portal Management System Version 5.1.0.0.4201

Voice Portal Management System (VPMS) is the consolidated web-based application for administering Voice Portal. Through the VPMS interface, you can configure Voice Portal, check the status of a Voice Portal component, and generate reports related to system operation.

Legal Notice

© 2005 - 2010 Avaya Inc. All Rights Reserved.

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims,

Last Login: 10/11/10 10:34:44 AM EDT

4.4. VoIP Connection

This section illustrates the procedure for administering a SIP connection from Voice Portal to Session Manager. From the left pane of the **Home** screen shown in **Section 4.3**, expand **System Configuration** → **VoIP Connections**. In the resultant screen, select the **SIP** tab. To add a new SIP connection, click **Add**. To view or edit an existing connection, click the **Name** of the connection. In the example screen shown below, a SIP connection named “SessionManager” had been added previously.

You are here: [Home](#) > System Configuration > VoIP Connections

VoIP Connections

This page displays a list of Voice over Internet Protocol (VoIP) servers that Voice Portal communicates with. You can configure multiple SIP connections, but only one SIP connection can be enabled at any one given time.

H.323SIP

<input type="checkbox"/>	Name	Enable	Proxy Transport	Proxy/DNS Server Address	Proxy Server Port	Listener Port	SIP Domain	Maximum Simultaneous Calls	Inbound Calls Allowed	Outbound Calls Allowed
<input type="checkbox"/>	SessionManager	Yes	TCP	10.1.2.70	5060	5060	avaya.com	10	10	10

Add

Delete

Help

After clicking **Add** to add a new connection, or the name of an existing connection, a screen like the following is displayed. Configure the SIP connection to Session Manager as follows, and then click **Save**:

- **Name** – When adding, enter a descriptive name, such as “SessionManager”.
- **Enable** – Select “Yes”.
- **Proxy Transport** – Select “TCP”.
- Click the **Proxy Servers** radio button.
- **Proxy Server Address** – Enter the IP address of the Session Manager SIP signaling interface, such as “10.1.2.70” in the sample configuration.
- **Proxy Server Port** – Enter “5060”.
- **Listener Port** – Enter “5060”
- **SIP Domain** – Enter the enterprise SIP domain, such as “avaya.com”
- **P-Asserted-Identity**: This field may be left blank for the call flows illustrated in these Application Notes. If calls made by Voice Portal should include a PAI header in the INVITE, specify a full SIP URI. For example, if an inbound call from IP Trunk Service to Voice Portal may be bridge transferred back out to the PSTN via the IP Trunk Service, then the P-Asserted-Identity field can be configured to a DID known to Verizon on the circuit (e.g., sip:7329450287@avaya.com) to allow Verizon to admit and route the outbound call to the transferred-to destination. However, note that Voice Portal would include this configured PAI (unless overridden by the application) for all transfer scenarios using INVITE (e.g., bridged transfer or consultative transfer when “INVITE with REPLACES” is selected below). For example, if this field is populated with a Verizon DID, if a call is bridged transferred to a Communication Manager extension, the Communication Manager extension will ring and display the configured PAI as the caller id, rather than the true caller’s identity.
- **Maximum Simultaneous Calls** – Enter the number of calls this SIP connection can handle, taking capacity and license considerations into account.
- **Consultative Transfer**: “INVITE with REPLACES” and “REFER” were tested successfully with Verizon IP Trunk Service. The screen shows “REFER” selected because additional signaling message exchanges were observed when INVITE with REPLACES was used with the Verizon IP Trunk Service. See **Section 1.3**.

You are here: [Home](#) > [System Configuration](#) > [VoIP Connections](#) > [Change SIP Connection](#)

Change SIP Connection

Use this page to change the configuration of a SIP connection.

Name: SessionManager

Enable: ☒ Yes ☐ No

Proxy Transport: TCP

☒ Proxy Servers ☐ DNS SRV Domain

Address	Port	Priority	Weight	
10.1.2.70	5060	0	0	Remove

[Additional Proxy Server](#)

Listener Port: 5060

SIP Domain: avaya.com

P-Asserted-Identity:

Maximum Redirection Attempts: 0

Consultative Transfer: ☐ INVITE with REPLACES ☒ REFER

Call Capacity

Maximum Simultaneous Calls: 10

☒ All Calls can be either inbound or outbound

☐ Configure number of inbound and outbound calls allowed

4.5. Application References

This section illustrates the procedure for administering a reference to a VXML and/or CCXML application residing on an application server. In the sample configuration, the applications were co-resident on one Voice Portal server, with IP Address 65.206.67.87.

From the left pane of the **Home** screen shown in **Section 4.3**, expand **System Configuration** → **Applications**. To add a new application, click **Add**. To view or edit an existing connection, click the **Name** of the application. In the example screen shown below, a sample application named “SampleApp” had been added previously.

Voice Portal 5.1 (VoicePortal)

Expand All | Collapse All

You are here: [Home](#) > System Configuration > Applications

Applications

This page displays the VoiceXML and CCXML applications that are currently deployed on the Voice Portal system. When a call comes in, Voice Portal compares the called number or URI with the values in the Launch column, starting with the first application in the list and proceeding down the list in order. As soon as it finds a match, it invokes that application to handle the call. If two or more applications have launch values that overlap or duplicate each other, make sure that the application you want Voice Portal to use appears first in the list. To move an application, click Change Launch Order.

<input type="checkbox"/>	Name	Enable	Type	URL	Launch	ASR	Languages	TTS	Voices	Con Ap V
<input type="checkbox"/>	SampleApp	Yes	VoiceXML	http://65.206.67.87/mpp/misc/avptestapp/intro.vxml	44000, 44000@avaya.com	No ASR		No TTS		

Add **Delete** **Help**

After clicking **Add** to add a new application, or the name of an existing application, a screen like the following is displayed. Configure an application as follows, and then click **Save**.

- **Name** – Enter a descriptive name.
- **Enable** – Select “Yes”.
- **Type** – Select “VoiceXML”, “CCXML”, or “CCXML/VoiceXML” according to the application type.
- **VoiceXML and/or CCXML URL** – Enter the necessary URL(s) to access the VXML and/or CCXML application(s) on the application server. In the sample screen below, the Voice Portal test application on the single server Voice Portal is referenced.
- **Speech Servers ASR and TTS** – Select the appropriate ASR and/or TTS servers as necessary.
- **Application Launch** – Select “Inbound”.
- Select the **Number** radio button to add a number or the **URI** radio button to add a URI.
- **Called Number** – Enter the number to match against an inbound SIP INVITE message, and click **Add**. In the sample configuration illustrated in these Application Notes, the dialed Verizon IP Trunk DID number 732-945-0288 was adapted by Session Manager to 44000. Repeat to define additional called party numbers as needed. Inbound Verizon Business calls with these called party numbers will be handled by the application defined in this section.

You are here: [Home](#) > [System Configuration](#) > [Applications](#) > [Change Application](#)

Change Application

Use this page to change the configuration of a VoiceXML or CCXML application.

Name: SampleApp

Enable: ☒ Yes ☐ No

Type:

URL

☒ Single ☐ Fail Over ☐ Load Balance

VoiceXML URL:

Verify

Mutual Certificate Authentication: ☐ Yes ☒ No

Basic Authentication: ☐ Yes ☒ No

Speech Servers

ASR:

TTS:

Application Launch

☒ Inbound ☐ Inbound Default ☐ Outbound

☒ Number ☐ Number Range ☐ URI

Called Number:

Add

44000
44000@avaya.com

Remove

Speech Parameters ▶

Add additional application references using the procedures in this section as needed.

4.6. MPP Servers and VoIP Settings

This section illustrates the procedure for viewing or changing the MPP Settings. From the left pane of the **Home** screen shown in **Section 4.3**, expand **System Configuration** → **MPP Servers**. In the sample configuration, the MPP Server is co-resident on a single server with the Voice Portal Management System (VPMS), and therefore the same **Host Address** “65.206.67.87” is used for both the MPP and VPMS.

You are here: [Home](#) > System Configuration > MPP Servers

MPP Servers

This page displays the list of Media Processing Platform (MPP) servers in the Voice Portal system. When an MPP receives a call from a PBX, it invokes a VoiceXML application on an application server and communicates with ASR and TTS servers as necessary to process the call.

<input type="checkbox"/>	Name	Host Address	Network Address (VoIP)	Network Address (MRCP)	Network Address (AppSvr)	Maximum Simultaneous Calls	Trace Level
<input type="checkbox"/>	MPP1	65.206.67.87	<Default>	<Default>	<Default>	10	Use MPP Settings
<input type="button" value="Add"/> <input type="button" value="Delete"/>							

[MPP Settings](#) [Browser Settings](#) [Event Handlers](#) [Video Settings](#) [VoIP Settings](#) [Help](#)

Click the **VoIP Settings** button to view or change Voice over IP parameters. The following screen illustrates the default configuration retained in the sample configuration. With this configuration, inbound calls from Verizon IP Trunk service that remain in Voice Portal for self-service will use the G.729a codec. Inbound calls from Verizon IP Trunk service to Voice Portal that are subsequently transferred to Communication Manager may use G.729a or G.711MU, depending on the Communication Manager codec set configuration.

You are here: [Home](#) > System Configuration > [MPP Servers](#) > VoIP Settings

VoIP Settings

Voice over Internet Protocol (VoIP) is the process of sending voice data through a network using one or more standard protocols such as H.323 and Real-time Transfer Protocol (RTP). Use this page to configure parameters that affect how voice data is transferred through the network. Note that if you make any changes to this page, you must restart all MPPs.

Port Ranges

	Low	High
UDP:	<input type="text" value="23000"/>	<input type="text" value="30999"/>
TCP:	<input type="text" value="31000"/>	<input type="text" value="31999"/>
MRCP:	<input type="text" value="32000"/>	<input type="text" value="32999"/>
H.323 Station:	<input type="text" value="35000"/>	<input type="text" value="50000"/>

RTCP Monitor Settings

Host Address:

Port:

VoIP Audio Formats

MPP Native Format:

Audio Codecs

Packet Time:

G729: ☒ Yes ☐ No

Reduced Complexity Encoder: ☒ Yes ☐ No

Discontinuous Transmission: ☒ Yes ☐ No

First Offered:

4.7. Configuring RFC2833 Event Value Offered by Avaya Voice Portal

The configuration change example noted in this section is not required for any of the call flows illustrated in these Application Notes. For incoming calls from Verizon services to Voice Portal, Verizon specifies the value 101 for the RFC2833 telephone-events that signal DTMF digits entered by the user. When Voice Portal answers, the SDP from Voice Portal matches this Verizon offered value.

When Voice Portal sends an INVITE with SDP as part of an INVITE-based transfer (e.g., bridged transfer), Voice Portal offers the SDP. By default, Voice Portal specifies the value 127 for the RFC2833 telephone-events. Optionally, the value that is offered by Voice Portal can be changed, and this section outlines the procedure that can be performed by an Avaya authorized representative.

- Access Voice Portal via the command line interface.
- Navigate to the following directory: /opt/Avaya/VoicePortal/MPP/config
- Edit the file mppconfig.xml.
- Search for the parameter “mpp.sip.rfc2833.payload”. If there is no such parameter specified, add a line such as the following to the file, where the value 101 is the value to be used for the RFC2833 events. If the parameter is already specified in the file, simply edit the value assigned to the parameter.
`<parameter name="mpp.sip.rfc2833.payload">101</parameter>`
- In the verification of these Application Notes, the line was added directly above the line where the sip.session.expires parameter is configured.

After saving the file with the change, restart the MPP server for the change to take effect. As shown below, the MPP may be restarted using the **Restart** button available via the Voice Portal GUI at **System Management → MPP Manager**.

You are here: [Home](#) > System Management > MPP Manager

MPP Manager (11/23/10 11:16:19 AM EST)

This page displays the current state of each MPP in the Voice Portal system. To enable the state and mode commands, select one or more MPPs. selected MPPs must also be stopped.

Last Poll: 11/23/10 11:16:06 AM EST

<input checked="" type="checkbox"/>	Server Name	Mode	State	Config	Auto Restart	Restart Schedule		Active Calls	
						Today	Recurring	In	Out
<input checked="" type="checkbox"/>	MPP1	Online	Running	OK	Yes	No	None	1	1

State Commands

Mode Commands

Restart/Reboot Options

☐ One server at a time

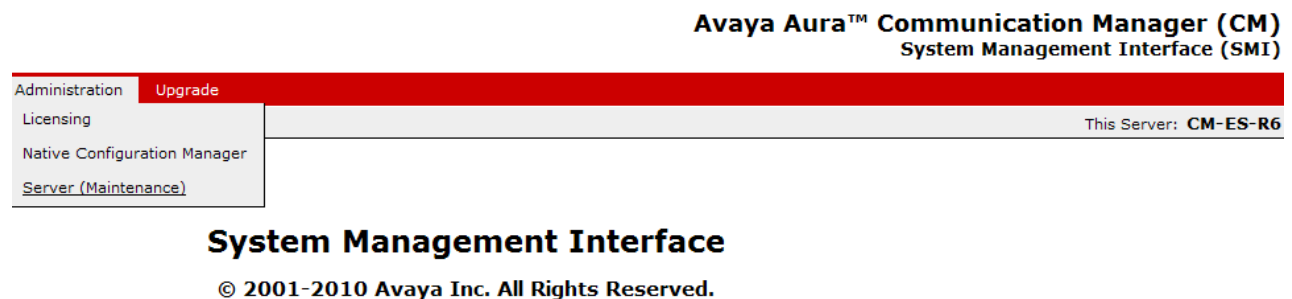
☒ All selected servers at the same time

5. Avaya Aura® Communication Manager

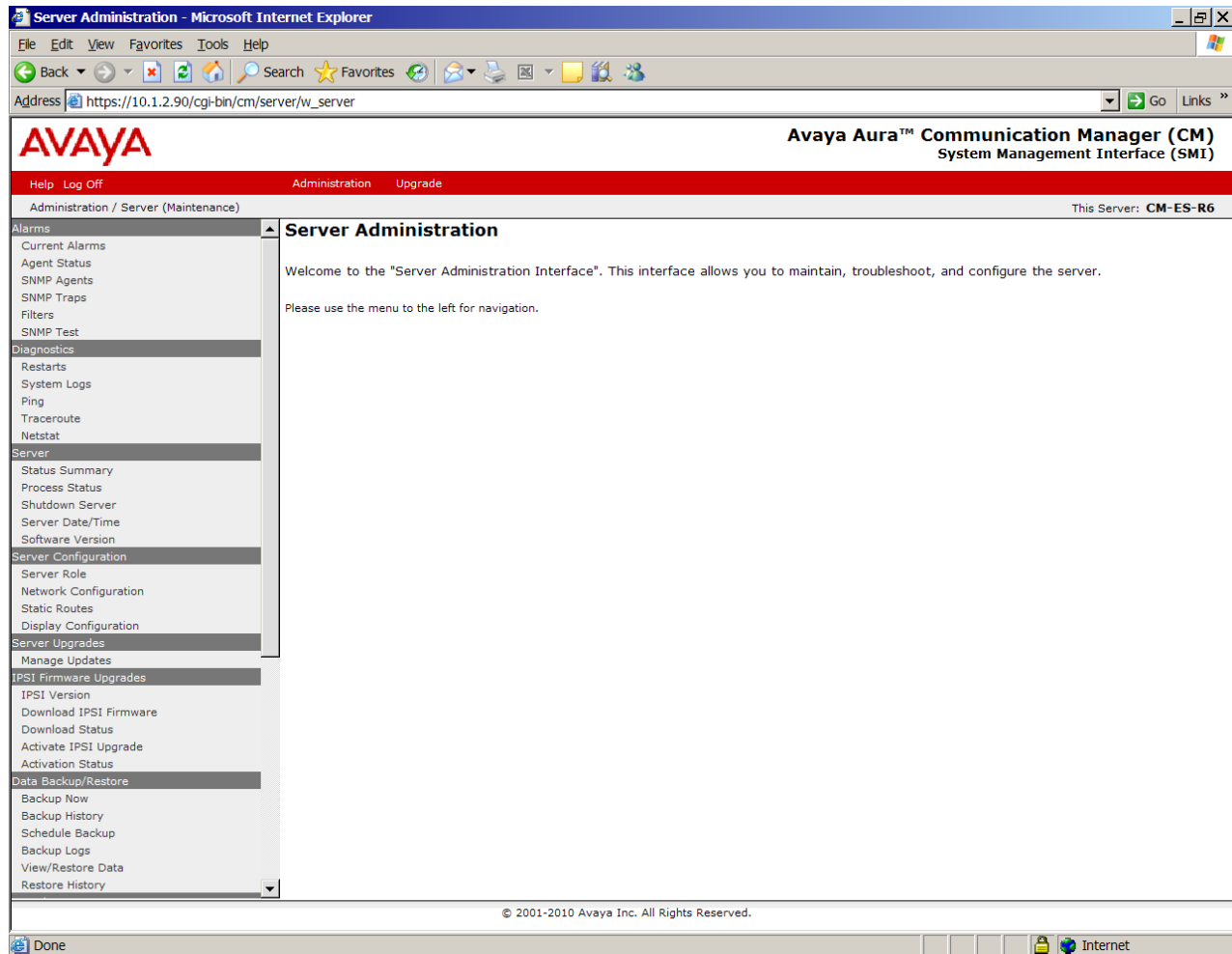
This section illustrates the Communication Manager configuration used in the verification of these Application Notes. The example configuration uses SIP signaling via the “Processor Ethernet” of the Avaya S8800 Servers to Session Manager. In configurations that use an Avaya G650 Media Gateway, it is also possible to use an Avaya C-LAN in an Avaya G650 Media Gateway for SIP signaling to Session Manager. These Application Notes assume that basic Communication Manager administration has already been performed. The Communication Manager configuration shown in this section builds off the Communication Manager configuration previously documented in reference [JRR-VZIPT], with modest changes and additions. Except for the web configuration shown in **Section 4.1**, all remaining configuration is performed via the Communication Manager SAT interface of the Avaya S8800 Server. Screens are abridged for brevity in presentation.

5.1. Processor Ethernet Configuration on S8800 Server

The screens in this section illustrate a previously completed configuration. Consult the product documentation in references [5] and [6] for further procedural guidance. The S8800 Server can be accessed via a web interface in an internet browser. In the sample configuration, enter <http://10.1.2.90> and log in with appropriate credentials (not shown). From the System Management Interface screen, select **Administration → Server (Maintenance)** as shown below.



The resulting **Server Administration** screen is shown below.



Under **Server Configuration**, select **Server Role** to view or configure the server role. In the sample configuration, the Avaya S8800 server is a **main server**, as shown below.

Server Role

This page allows for the specification of the Server's Role.



WARNING:

- Changing the role of this server will **erase any translations** residing on this server and will cause a **Communication Manager reset**. If you wish to preserve existing translations, execute a backup prior to completing this page.
- This server appears to be the **ACTIVE** server. Continuing the process may cause the Standby to become **ACTIVE**. This server will be unavailable for telephony during the configuration process.

Server Settings

This Server is:

- ☒ a main server
- ☐ an enterprise survivable server (ESS)
- ☐ a local survivable server (LSP)

System ID and Module ID:

SID:

MID:

Configure Memory

This Server's Memory Setting:

Large ▼

[Change](#)

[Restart CM](#)

[Help](#)

Under **Server Configuration**, select **Network Configuration** to view the network configuration. The following screen shows the upper portion of the **Network Configuration**.

Network Configuration

This implementation is used to configure the IP related settings for this server. Please note that some changes made on this page may affect settings on other pages under the "Server Configuration" category - please make sure to check all pages for an accurate configuration.



Notes

- The host name and ID of each server in the system must be unique.
- The below fields is used to indicate how each Ethernet port is to be used (functional assignment) and to configure the IP related settings of each port. Ethernet ports may be used for multiple purposes, except for the port assigned to the laptop, which must be dedicated to only that purpose.
- An Ethernet port can be configured without a functional assignment. However, any port intended for use with the Communication Manager application must be assigned the correct functional assignment.
- Physical connections to the Ethernet ports must match settings provided below. Please keep in mind that the labels on the physical ports may be shifted by 1, e.g.: eth0 could be labeled 1, eth1 could be labeled 2, etc.
- Note that any configuration data obtained from an external source will be displayed read-only. To change these settings, please navigate to the external tool used to configure those settings.
- A restart of Communication Manager is needed after the server has been successfully configured. Click the **Restart CM** button below to do so. Please note that this should be done after all configuration is completed. Too many restarts may escalate to a full Communication Manager reboot.
- This server appears to be the **ACTIVE** server. Continuing the process may cause the Standby to become **ACTIVE**. This server will be unavailable for telephony during the configuration process.

Host Name:	<input type="text" value="CM-ES-R6"/>
DNS Domain:	<input type="text"/>
Search Domain List:	<input type="text" value="cm-es-r6"/> (comma separated)
Primary DNS:	<input type="text" value="192.168.1.200"/>
Secondary DNS:	<input type="text"/>
Tertiary DNS:	<input type="text"/>
Server ID:	<input type="text" value="1"/> (Range 1 to 256)

Scrolling down, the following screen shows the lower portion of the **Network Configuration**. Note that the **IPv4 Address** of the server is "10.1.2.90", and that the **Functional Assignment** drop-down has assigned the **Corporate LAN/Processor Ethernet/Control Network** to the same "eth0" interface.

Server ID:	<input type="text" value="1"/> (Range 1 to 256)												
Default Gateway:	<table><tr><td>IPv4</td><td><input type="text" value="10.1.2.1"/></td></tr><tr><td>IPv6</td><td><input type="text"/></td></tr></table>	IPv4	<input type="text" value="10.1.2.1"/>	IPv6	<input type="text"/>								
IPv4	<input type="text" value="10.1.2.1"/>												
IPv6	<input type="text"/>												
eth0:	<table><tr><td>IPv4 Address</td><td>Mask</td><td>IPv6 Address</td><td>Prefix</td></tr><tr><td>IP Configuration:</td><td><input type="text" value="10.1.2.90"/></td><td><input type="text" value="/ 255.255.255.0"/></td><td><input type="text"/></td></tr><tr><td>Functional Assignment:</td><td colspan="3"><input type="text" value="Corporate LAN/Processor Ethernet/Control Network"/></td></tr></table>	IPv4 Address	Mask	IPv6 Address	Prefix	IP Configuration:	<input type="text" value="10.1.2.90"/>	<input type="text" value="/ 255.255.255.0"/>	<input type="text"/>	Functional Assignment:	<input type="text" value="Corporate LAN/Processor Ethernet/Control Network"/>		
IPv4 Address	Mask	IPv6 Address	Prefix										
IP Configuration:	<input type="text" value="10.1.2.90"/>	<input type="text" value="/ 255.255.255.0"/>	<input type="text"/>										
Functional Assignment:	<input type="text" value="Corporate LAN/Processor Ethernet/Control Network"/>												

[Change](#)[Restart CM](#)[Help](#)

5.2. Verify Licensed Features

The Communication Manager license file controls customer capabilities. Contact an authorized Avaya representative for assistance if a required feature needs to be enabled.

On **Page 2** of the **display system-parameters customer-options** form, verify that the **Maximum Administered SIP Trunks** is sufficient for the combination of trunks to the Verizon Business IP Trunk Service and any other SIP applications. Each call from the Verizon Business IP Trunk Service to a non-SIP endpoint on Communication Manager uses one SIP trunk for the duration of the call. Each call from Verizon Business IP Trunk Service to a SIP endpoint uses two SIP trunks for the duration of the call. Of course, a call from the Verizon Business IP Trunk Service that is delivered from Session Manager to Voice Portal, and remains in Voice Portal for self-service, does not consume a Communication Manager SIP trunk.

display system-parameters customer-options		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		12000	100
Maximum Concurrently Registered IP Stations:		18000	3
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	0
Maximum Video Capable IP Softphones:		18000	0
Maximum Administered SIP Trunks:		24000	146
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

On **Page 3** of the **System-Parameters Customer-Options** form, verify that **ARS** 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)? n		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? n		DCS Call Coverage? y	
ASAI Link Plus Capabilities? n		DCS with Rerouting? y	
Async. Transfer Mode (ATM) PNC? n		Digital Loss Plan Modification? y	
Async. Transfer Mode (ATM) Trunking? n		DS1 MSP? y	
ATM WAN Spare Processor? n		DS1 Echo Cancellation? y	
ATMS? y			
Attendant Vectoring? y			

On **Page 4** of the **System-Parameters Customer-Options** form, verify that **IP Trunks**, **IP Stations**, and **ISDN-PRI** features are enabled. If the use of SIP REFER messaging generated by Communication Manager will be required, verify that the **ISDN/SIP Network Call Redirection** feature is enabled. In these Application Notes, Voice Portal will generate SIP REFER messages for inbound calls from Verizon IP Trunk that are transferred to Communication Manager, but Communication Manager will not generate SIP REFER messages in vector processing.

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			

On **Page 5** of the **System-Parameters Customer-Options** form, verify that the **Private Networking** and **Processor Ethernet** features are enabled if these features will be used, as is the case in the sample configuration.

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

On **Page 6** of the **System-Parameters Customer-Options** form, verify that any required call center features are enabled. In the sample configuration, **Vectoring** and **Expert Agent Selection** are used.

display system-parameters customer-options		Page 6 of 11
CALL CENTER OPTIONAL FEATURES		
Call Center Release: 5.0		
<div> <div> ACD? y BCMS (Basic)? y BCMS/VuStats Service Level? n BSR Local Treatment for IP & ISDN? n Business Advocate? n Call Work Codes? n DTMF Feedback Signals For VRU? n Dynamic Advocate? n Expert Agent Selection (EAS)? y EAS-PHD? y Forced ACD Calls? n Least Occupied Agent? n Lookahead Interflow (LAI)? n Multiple Call Handling (On Request)? n Multiple Call Handling (Forced)? n PASTE (Display PBX Data on Phone)? n </div> <div> Reason Codes? n Service Level Maximizer? n Service Observing (Basic)? y Service Observing (Remote/By FAC)? n Service Observing (VDNs)? n Timed ACW? n Vectoring (Basic)? y Vectoring (Prompting)? y Vectoring (G3V4 Enhanced)? y Vectoring (3.0 Enhanced)? y Vectoring (ANI/II-Digits Routing)? y Vectoring (G3V4 Advanced Routing)? y Vectoring (CINFO)? n Vectoring (Best Service Routing)? y Vectoring (Holidays)? n Vectoring (Variables)? y </div> </div>		

5.3. Dial Plan

In the sample configuration, the Avaya CPE environment uses five digit local extensions, such as 3xxxx and 4xxxx. Trunk Access Codes (TAC) are 3 digits in length and begin with 1. The Feature Access Code (FAC) to access ARS is the single digit 9. The Feature Access Code (FAC) to access AAR is the single digit 8. The dial plan illustrated here is not intended to be prescriptive; any valid dial plan may be used. The dial plan is modified with the **change dialplan analysis** command as shown below.

change dialplan analysis			DIAL PLAN ANALYSIS TABLE						Page	1 of	12
			Location: all			Percent Full: 2					
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type			
0	3	fac									
1	3	dac									
2	5	ext									
3	5	ext									
4	4	ext									
5	5	ext									
6	3	fac									
60	5	ext									
7	5	ext									
8	1	fac									
9	1	fac									
*	2	fac									
#	2	fac									

5.4. Node Names

Node names are mappings of names to IP Addresses that can be used in various screens. The following abridged “change node-names ip” output shows relevant node-names in the sample configuration. As shown in bold, the node name for Session Manager is “SM1” with IP Address 10.1.2.70. The node name and IP Address (10.1.2.90) for the Processor Ethernet “procr” appears automatically due to the web configuration in **Section 4.1**.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
SM1	10.1.2.70	
procr	10.1.2.90	

5.5. IP Interface for procr

The “add ip-interface procr” or “change ip-interface procr” command can be used to configure the Processor Ethernet (PE) parameters. The following screen shows the parameters used in the sample configuration. While the focus here is the use of the PE for SIP Trunk Signaling, observe that the Processor Ethernet will also be used for registrations from H.323 IP Telephones and H.248 gateways in the sample configuration.

change ip-interface procr		Page 1 of 2
IP INTERFACES		
Type: PROCR		Target socket load: 1700
Enable Interface? y	Allow H.323 Endpoints? y	
Network Region: 1	Allow H.248 Gateways? y	
	Gatekeeper Priority: 5	
IPV4 PARAMETERS		
Node Name: procr	IP Address: 10.1.2.90	
Subnet Mask: /24		

5.6. Network Regions for Gateway, Telephones

Network regions provide a means to logically group resources. In the shared Communication Manager configuration used for the testing, the Avaya G450 Media Gateway is in region 1. To provide testing flexibility, network region 4 was associated with other components used specifically for the Verizon testing.

Non-IP telephones (e.g., analog, digital) derive network region and location configuration from the Avaya gateway to which the device is connected. The following display command shows that media gateway 1 is an Avaya G450 Media Gateway configured for network region 1. It can also be observed that the “Controller IP Address” is the Avaya S8800 processor Ethernet (10.1.2.90), and that the gateway IP Address is 10.1.2.95. These fields are not configured in this screen, but rather simply display the current information for the gateway.

```
change media-gateway 1                                     Page 1 of 2
                                     MEDIA GATEWAY 1

Type: g450
Name: G450 Evolution Srvr
Serial No: 08IS43202588
Encrypt Link? y      Enable CF? n
Network Region: 1    Location: 1
                        Site Data:

Recovery Rule: none

Registered? y
FW Version/HW Vintage: 30 .13 .2 /1
MGP IPv4 Address: 10.1.2.95
MGP IPv6 Address:
Controller IP Address: 10.1.2.90
MAC Address: 00:1b:4f:03:57:b0
```

The following screen shows **Page 2** for media gateway 1. The gateway has an **MM712** media module supporting Avaya digital phones in slot **v3**, an **MM714** supporting analog devices in slot **v5**, and the capability to provide announcements and music on hold via “gateway-announcements” in logical slot **v9**.

```
change media-gateway 1                                     Page 2 of 2
                                     MEDIA GATEWAY 1

Type: g450

Slot  Module Type      Name      DSP Type  FW/HW version
V1:                                     MP80      45    3
V2:
V3:  MM712             DCP MM
V4:
V5:  MM714             ANA MM
V6:
V7:
V8:                                     Max Survivable IP Ext: 8
V9:  gateway-announcements ANN VMM
```

IP telephones can be assigned a network region based on an IP address mapping. The following screen illustrates a subset of the IP network map configuration used to verify these Application Notes. If the IP address of a registering IP Telephone does not appear in the ip-network-map, the phone is assigned the network region of the “gatekeeper” (e.g., CLAN or PE) to which it registers. When the IP address of a registering IP telephone is in the ip-network-map, the phone is assigned the network region assigned by the form shown below. For example, the IP address 65.206.67.11 would be mapped to network region 4, based on the bold configuration below. In production environments, different sites will typically be on different networks, and ranges of IP Addresses assigned by the DHCP scope serving the site can be entered as one entry in the network map, to assign all telephones in a range to a specific network region.

change ip-network-map

Page 1 of 63

IP ADDRESS MAPPING

IP Address	Subnet Bits	Network Region	VLAN	Emergency Location	Ext
FROM: 10.1.2.0	/24	1	n		
TO: 10.1.2.255					
FROM: 65.206.67.0	/24	4	n		
TO: 65.206.67.255					

The following screen shows IP Network Region 4 configuration. In the shared test environment, network region 4 is used to allow unique behaviors for the Verizon test environment. In this example, codec set 4 will be used for calls within region 4. The shared Avaya Interoperability Test Lab environment uses the domain “avaya.com” (i.e., for network region 1 including the region of the processor ethernet “procr”). However, to illustrate the more typical case where the Communication Manager domain matches the enterprise CPE domain known to Verizon, the **Authoritative Domain** in the following screen is “adevc.avaya.globalipcom.com”, the domain known to Verizon, as shown in **Figure 1**. Even with this configuration, note that the domain in the PAI header sent by Communication Manager to Session Manager will contain “avaya.com”, the domain of the near-end of the Avaya signaling group. Session Manager will adapt “avaya.com” to “adevc.avaya.globalipcom.com” in the PAI header.

```

change ip-network-region 4                                     Page 1 of 20
                                IP NETWORK REGION
    Region: 4
    Location:                Authoritative Domain: adevc.avaya.globalipcom.com
        Name: Verizon testing
MEDIA PARAMETERS                                           Intra-region IP-IP Direct Audio: yes
    Codec Set: 4                                           Inter-region IP-IP Direct Audio: yes
    UDP Port Min: 2048                                     IP Audio Hairpinning? y
    UDP Port Max: 3029
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

```

The following screen shows the inter-network region connection configuration for region 4. The first bold row shows that network region 4 is directly connected to network region 1, and that codec set 4 will also be used for any connections between region 4 and region 1. For configurations where multiple remote gateways are used, each gateway will typically be configured for a different region, and this screen can be used to specify unique codec or call admission control parameters for the pairs of regions. If a different codec should be used for inter-region connectivity than for intra-region connectivity, a different codec set can be entered in the **codec set** column for the appropriate row in the screen shown below. Once submitted, the configuration becomes symmetric, meaning that network region 1, **Page 4**, will also show codec set 4 for region 4 to region 1 connectivity.

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

The following screen shows IP Network Region 1 configuration. In this example, codec set 1 will be used for calls within region 1 due to the **Codec Set** parameter on **Page 1**, but codec set 4 will be used for connections between region 1 and region 4 as noted previously. In the shared test environment, network region 1 was in place prior to adding the Verizon test environment and already used **Authoritative Domain** “avaya.com”. Where necessary, Session Manager or the Acme Packet Net-Net SBC will adapt the domain.

change ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1		
Location: Authoritative Domain: avaya.com		
Name: HQ CM and SIP Phones		
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes
Codec Set: 1		Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048		IP Audio Hairpinning? y
UDP Port Max: 65535		
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		

The following screen shows the inter-network region connection configuration for region 1. The bold row shows that network region 1 is directly connected to network region 4, and that codec set 4 will be used for any connections between region 4 and region 1.

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	2	y	NoLimit							n			t
3	3	y	NoLimit							n			t
4	4	y	NoLimit							n			t

5.7. IP Codec Sets

The following screen shows the configuration for codec set 4, the codec set configured to be used for calls within region 4 and for calls between region 1 and region 4. In general, an IP codec set is a list of allowable codecs in priority order. Using the example configuration shown below, all calls with the PSTN via the SIP trunks would prefer to use **G.729A**, but also be capable of using **G.711MU**. Any calls using this same codec set that are between devices capable of the **G.722-64K** codec (e.g., Avaya 9600-Series IP Telephone) can use G.722. The specification of G.722 as the first choice is not required. That is, G.722 may be omitted from the codec set.

change ip-codec-set 4					Page	1	of	2
IP Codec Set								
Codec Set: 4								
Audio		Silence	Frames	Packet				
Codec		Suppression	Per Pkt	Size (ms)				
1:	G.722-64K		2	20				
2:	G.729A	n	2	20				
3:	G.711MU	n	2	20				
4:								
5:								
6:								
7:								

On **Page 2** of the form:

- Configure the **Fax Mode** field to **off**. Verizon does not support T.38 fax on the production circuit used for testing.
- Configure the **Fax Redundancy** field to **0**.

change ip-codec-set 4			Page 2 of 2
IP Codec Set			
Allow Direct-IP Multimedia? n			
	Mode	Redundancy	
FAX	off	0	
Modem	off	0	
TDD/TTY	US	3	
Clear-channel	n	0	

The following screen shows the configuration for codec set 1. The configuration for codec set 1 prefers **G.711MU** but also allows **G.729A**. Codec set 1 is used for Modular Messaging and other local Avaya CPE connections within region 1.

change ip-codec-set 1			Page 1 of 2
IP Codec Set			
Codec Set: 1			
Audio	Silence	Frames	Packet
Codec	Suppression	Per Pkt	Size(ms)
1: G.711MU	n	2	20
2: G.729A	n	2	20
3:			
4:			
5:			
6:			
7:			

5.8. SIP Signaling Groups

This section illustrates the configuration of the SIP Signaling Groups. Each signaling group has a **Group Type** of “sip”, a **Near-end Node Name** of “procr”, and a **Far-end Node Name** of “SM1”. In the example screens, the **Transport Method** for all signaling groups is “tcp”. In production, TLS transport between Communication Manager and Session Manager can be used. The **Enable Layer 3 Test** field is enabled on each of the signaling groups to allow Communication Manager to maintain the signaling group using the SIP OPTIONS method. Fields that are not referenced in the text below can be left at default values, including **DTMF over IP** set to “rtp-payload”, which corresponds to RFC 2833.

The following screen shows signaling group 67. Signaling group 67 will be used for processing incoming PSTN calls from Verizon IP Trunk Service via Session Manager. This includes any Verizon IP Trunk calls that are directed by Session Manager directly to Communication Manager, as well as any Verizon IP Trunk calls that are initially directed to Voice Portal, and then transferred by Voice Portal using SIP REFER to Communication Manager. To enable calls transferred from Voice Portal to Communication Manager using SIP REFER to use signaling group 67, the Session Manager Dial Pattern configuration covering the transferred-to Communication Manager extensions must send calls from the Acme Packet SBC originating “location” to the SIP Entity corresponding to signaling group 67, as shown in **Section 6.8.2**. The **Far-end Network Region** is configured to region “4”. Port “5062” has been configured as both the **Near-end Listen Port** and **Far-end Listen Port**. Session Manager will be configured to direct calls arriving from the PSTN with specific Verizon IP Trunk DID numbers to a route policy that uses a SIP entity link to Communication Manager specifying port “5062”. The use of different ports is one means to allow Communication Manager to distinguish different types of calls arriving from the same Session Manager. In the sample configuration, the **Peer Detection Enabled** field was set to “n”. Other parameters may be left at default values.

change signaling-group 67		Page 1 of 1
SIGNALING GROUP		
Group Number: 67	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? n	Peer Server: Others	
Near-end Node Name: procr	Far-end Node Name: SM1	
Near-end Listen Port: 5062	Far-end Listen Port: 5062	
	Far-end Network Region: 4	
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
	Initial IP-IP Direct Media? n	
H.323 Station Outgoing Direct Media? n	Alternate Route Timer(sec): 6	

The following screen shows signaling group 60, the signaling group to Session Manager that was in place prior to adding the Verizon configuration to the shared Avaya Solutions and Interoperability Test Lab configuration. This signaling group reflects configuration not specifically related to Verizon trunking. For example, calls using Avaya SIP Telephones and calls routed to other Avaya applications, such as Modular Messaging, use this signaling group. Calls involving Voice Portal, Session Manager and Communication Manager that do not involve Verizon may also use signaling group 60. For example, if Voice Portal transfers a non-Verizon call to a Communication Manager user, the call can use trunk group 60. Moreover, if Voice Portal uses the “bridged transfer” option to bridge an inbound PSTN call from Verizon to Communication Manager (i.e., rather than the “blind transfer” or “consultative transfer” options), trunk group 60 will be used. A Voice Portal bridged transfer “bridges” the inbound Verizon call to the Communication Manager leg of the call within Voice Portal (i.e., Voice Portal uses INVITE, and does not use SIP REFER to perform the transfer).

As with signaling group 67, the **Near-end Node Name** is “procr” and the **Far-end Node Name** is “SM1”, the node name of the Session Manager. Unlike the signaling groups used for the Verizon signaling, the **Far-end Network Region** is “1”. The **Peer Detection Enabled** field is set to “y” and a peer Session Manager has been previously detected. The **Far-end Domain** is set to “avaya.com” matching the configuration in place prior to adding the Verizon SIP Trunking configuration.

change signaling-group 60		Page 1 of 1
SIGNALING GROUP		
Group Number: 60	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: SM1	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
Far-end Network Region: 1		
Far-end Domain: avaya.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 10	

5.9. SIP Trunk Groups

This section illustrates the configuration of the SIP Trunks Groups corresponding to the SIP signaling groups from the previous section.

The following shows **Page 1** for trunk group 67, which will be used for incoming calls from Verizon. The **Number of Members** field defines how many simultaneous calls are permitted for the trunk group. The **Service Type** field should be set to “public-ntwrk” for the trunks that will handle calls with Verizon. Although not strictly necessary, the **Direction** has been configured to “incoming” to emphasize that trunk group 67 is used for incoming calls only in the sample configuration.

change trunk-group 67		Page 1 of 21	
TRUNK GROUP			
Group Number: 67	Group Type: sip	CDR Reports: y	
Group Name: From-SM-Acme-VZ	COR: 1	TN: 1	TAC: 167
Direction: incoming	Outgoing Display? n		
Dial Access? n	Night Service:		
Service Type: public-ntwrk	Auth Code? n		
		Signaling Group: 67	
		Number of Members: 6	

The following shows **Page 2** for trunk group 67. All parameters shown are default values, except for the **Preferred Minimum Session Refresh Interval**, which has been changed from the default 600 to 900. Although not strictly necessary, some SIP products prefer a higher session refresh interval than the Communication Manager default value, which can result in unnecessary SIP messages to re-establish a higher refresh interval for each call.

change trunk-group 67		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto		Redirect On OPTIM Failure: 5000	
SCCAN? n	Digital Loss Group: 18		
Preferred Minimum Session Refresh Interval(sec): 900			
Delay Call Setup When Accessed Via IGAR? n			

The following shows **Page 3** for trunk group 67. All parameters except those in bold are default values. Optionally, replacement text strings can be configured using the “system-parameters features” screen, such that incoming “private” (anonymous) or “restricted” calls can display an Avaya-configured text string on called party telephones.

change trunk-group 67		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: public	UI Treatment: service-provider	
	Replace Restricted Numbers? y	Replace Unavailable Numbers? y
Show ANSWERED BY on Display? y		

The following shows **Page 4** for trunk group 67. The **PROTOCOL VARIATIONS** page is one reason why it can be advantageous to configure incoming calls from Verizon to arrive on specific signaling groups and trunk groups. The bold fields have non-default values. The **Convert 180 to 183 for Early Media** field is new in Communication Manager Release 6. Verizon recommends that inbound calls to the enterprise result in a 183 with SDP rather than a 180 with SDP, and setting this field to “y” for the trunk group handling inbound calls from Verizon produces this result. Note that Voice Portal also sends 183 with SDP for inbound Verizon calls directed from Session Manager to Voice Portal for self-service. Although not strictly necessary, the **Telephone Event Payload Type** has been set to 101 to match Verizon configuration. Setting the **Network Call Redirection** flag to “y” enables advanced services associated with the use of the REFER message, while also implicitly enabling Communication Manager to signal “send-only” media conditions for calls placed on hold at the enterprise site. If neither REFER signaling nor “send-only” media signaling is required, this field may be left at the default “n” value. In the testing associated with these Application Notes, the **Network Call Redirection** flag was set to “n”. Voice Portal will send SIP REFER messages to transfer inbound calls from Verizon to Communication Manager, but Communication Manager will not use SIP REFER in vector processing in the sample configuration.

The Verizon IP Trunk Service does not support the History-Info header. As described further in [JRR-VZIPT], Communication Manager can be used to generate Diversion header, or the Session Manager Verizon adapter may be used to convert History Into header to Diversion Header.

change trunk-group 67	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n Prepend '+' to Calling Number? n Send Transferring Party Information? n Network Call Redirection? n Send Diversion Header? y Support Request History? n Telephone Event Payload Type: 101 Convert 180 to 183 for Early Media? y Always Use re-INVITE for Display Updates? n Enable Q-SIP? n	

The following shows **Page 1** for trunk group 60, the bi-directional “tie” trunk group to Session Manager that existed before adding the Verizon SIP Trunk configuration to the shared Avaya Solutions and Interoperability Test Lab network. Recall that this trunk is used for communication with other Avaya applications, such as Modular Messaging and internal calls with Voice Portal, and does not reflect any unique Verizon configuration.

change trunk-group 60	Page 1 of 21	
TRUNK GROUP		
Group Number: 60	Group Type: sip	CDR Reports: y
Group Name: SM1	COR: 1	TN: 1 TAC: 160
Direction: two-way	Outgoing Display? n	
Dial Access? n	Night Service:	
Queue Length: 0		
Service Type: tie	Auth Code? n	
	Signaling Group: 60	
	Number of Members: 100	

The following shows **Page 3** for trunk group 60. Note that unlike the trunks associated with Verizon calls that use “public” numbering, this tie trunk group uses a “private” **Numbering Format**.

change trunk-group 60		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: private		
UI Treatment: service-provider		
Replace Restricted Numbers? n		
Replace Unavailable Numbers? n		
Modify Tandem Calling Number: no		
Show ANSWERED BY on Display? y		

The following shows **Page 4** for trunk group 60. Note that unlike the trunks associated with Verizon calls that have non-default “protocol variations”, this trunk group maintains all default values. **Support Request History** must remain set to the default “y” to support proper subscriber mailbox identification by Modular Messaging.

change trunk-group 60		Page 4 of 21
PROTOCOL VARIATIONS		
Mark Users as Phone? n		
Prepend '+' to Calling Number? n		
Send Transferring Party Information? n		
Network Call Redirection? n		
Send Diversion Header? n		
Support Request History? y		
Telephone Event Payload Type:		
Convert 180 to 183 for Early Media? n		
Always Use re-INVITE for Display Updates? n		
Enable Q-SIP? n		

5.10. Basic Contact Center Configuration

This section describes the basic commands used to configure Vector Directory Numbers (VDNs) and corresponding vectors, announcements, skills, and agents used to verify call flows. These Application Notes provide rudimentary contact center configuration to illustrate and test the processing of Verizon IP Trunk calls transferred by Voice Portal to a Communication Manager VDN. In general, call centers will use more complex vector functionality tailored to individual needs.

This section provides an example configuration of a VDN and corresponding vector that will be used to verify Voice Portal blind transfer, consult transfer, and bridged transfer to a VDN. In this case, Voice Portal will not canvas Communication Manager for agent availability prior to transferring the call to the VDN. The inbound Verizon IP Trunk call is transferred to VDN 36880 shown in the following screen.

```

display vdn 36880                                     Page 1 of 3
                                         VECTOR DIRECTORY NUMBER

      Extension: 36880
      Name*: Route-To-Skill-80
      Destination: Vector Number 80
      Attendant Vectoring? n
      Meet-me Conferencing? n
      Allow VDN Override? n
      COR: 1
      TN*: 1
  
```

VDN 36880 is associated with vector number 80, which is shown below. Vector 80 plays an announcement (step 02). In the sample configuration, the “announcement” with extension 31881 was a brief announcement (“e.g., thank you for choosing Avaya”) that enabled Communication Manager to answer the call. For an inbound call from Verizon to Voice Portal that is subsequently transferred by Voice Portal to this VDN/vector using SIP REFER, answering the call via the announcement step in the vector serves to complete the REFER call processing, allowing the Acme Packet Net-Net SBC to provide new SDP attributes to Verizon on the public side of the SBC. Without this announcement step, pre-answer media treatments from Communication Manager, such as ring back while an agent is ringing, may not be heard by the PSTN caller. Next, the “queue-to skill 80” (step 03) is used. If an agent in skill 80 is available, the call will ring the agent, and the caller will hear ring back until the agent answers. If an agent in skill 80 is not available at the time the call is queued to skill 80, the announcement with extension 31880 (step 04) will be heard. In this simple vector configuration, this announcement is a recurring announcement that will repeat until an agent becomes available.

```

display vector 80                                     Page 1 of 6
                                         CALL VECTOR

      Number: 80                                     Name: Route-skill-80
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
02 announcement 31881
03 queue-to skill 80 pri m
04 announcement 31880
05 stop
06
  
```


The following screens illustrate the hunt group / skill configuration for hunt-group / skill 80. On **Page 1**, observe the bold parameters.

change hunt-group 80		Page 1 of 4
HUNT GROUP		
Group Number: 80		ACD? y
Group Name: ACD-Hunt-80		Queue? y
Group Extension: 36680		Vector? y
Group Type: ucd-mia		
TN: 1		
COR: 1		MM Early Answer? n
Security Code:		Local Agent Preference? n
ISDN/SIP Caller Display:		

On **Page 2**, observe the bold parameters.

change hunt-group 80		Page 2 of 4
HUNT GROUP		
Skill? y	Expected Call Handling Time (sec): 180	
AAS? n		
Measured: none		

The following screens illustrate the announcement extensions used in the call vector steps. All announcements use the G450 Media Gateway.

Recall that announcement 31881 was used to answer a call in the call vector to complete SIP REFER call processing, prior to queuing the call to a skill.

display announcement 31881		Page 1 of 1
ANNOUNCEMENTS/AUDIO SOURCES		
Extension: 31881		COR: 1
Annc Name: Call-entering-queue-annc		TN: 1
Annc Type: integrated		Queue? y
Group/Board: 001V9		
Protected? n		Rate: 64

Recall that announcement 31880 was used as a repeating announcement heard by a caller while a call was in queue to a skill (i.e., call arrives to a vector and no agent was immediately available).

display announcement 31880		Page 1 of 1
ANNOUNCEMENTS/AUDIO SOURCES		
Extension: 31880		COR: 1
Annc Name: Recurring-in-Queue-80-annc		TN: 1
Annc Type: integ-rep		Queue? y
Group/Board: 001V9		
Protected? n		Rate: 64

The following screen illustrates an example agent login-ID. This agent will staff skill 80.

```

change agent-loginID 46880                                     Page 1 of 3
                                AGENT LOGINID

Login ID: 46880                                           AAS? n
Name: Joey Skillful                                     AUDIX? n
TN: 1                                                    LWC Reception: spe
COR: 1                                                    LWC Log External Calls? n
Coverage Path:                                           AUDIX Name for Messaging:
Security Code:                                           LoginID for ISDN/SIP Display? n
                                                         Password: 1234
                                                         Password (enter again): 1234
                                                         Auto Answer: station
                                                         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: :

```

The following screen illustrates **Page 2** for the example agent login-ID. Observe Skill Number (SN) 80 is used.

```

change agent-loginID 46880                                     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      SN  RL SL      SN  RL SL
1: 80      1    16:          31:          46:
2:          17:          32:          47:
3:          18:          33:          48:
4:          19:          34:

```

After logging in agent-loginID 46880 from the telephone with station user extension 30002, the “list agent-loginID” command can be used to verify the status.

```

list agent-loginID

                                AGENT LOGINID
Login ID      Name      Extension      Dir Agt  AAS/AUD      COR Ag Pr
SO
      Skill/Lv Skill/Lv Skill/Lv Skill/Lv Skill/Lv Skill/Lv Skill/Lv
Skill/Lv

46880      Joey Skillful 30002
           80/01      /      /      /      /      /      /      /

```

5.11. Public Numbering

The “change public-unknown-numbering” command may be used to define the format of numbers sent to Verizon in SIP headers such as the “From” and “PAI” headers.

In the first bolded row shown in the example abridged output below, a specific Communication Manager extension (x30002) is mapped to a Verizon DID number (732-945-0288), when the call uses trunk group 67. In the other bolded rows shown in the example abridged output below, entries are made for the specific Communication Manager Vector Directory Numbers (VDN) illustrated in the prior section. In the course of the testing, this configuration was varied, with different Verizon numbers associated with various Communication Manager extensions and functions.

change public-unknown-numbering 5					Page	1 of	2
NUMBERING - PUBLIC/UNKNOWN FORMAT							
Ext	Ext	Trk	CPN	Total			
Len	Code	Grp (s)	Prefix	CPN			
				Len			
5	3	60		5	Total Administered: 3		
5	556			5	Maximum Entries: 9999		
5	30002	67	7329450288	10			
5	36880	67	7329450288	10			

5.12. Incoming Call Handling Treatment for Incoming Calls

In general, the “incoming call handling treatment” for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. For incoming Verizon calls that are delivered by Session Manager to Communication Manager rather than Voice Portal, if the number sent by Verizon is unchanged by Session Manager, then the number can be mapped to an extension using the incoming call handling treatment of the receiving trunk group. As an example, the following screen illustrates a conversion of number 732-945-0285 to extension 30002.

change inc-call-handling-trmt trunk-group 67					Page	1 of	30
INCOMING CALL HANDLING TREATMENT							
Service/	Number	Number	Del	Insert			
Feature	Len	Digits					
public-ntwrk	10	7329450285	all	30002			

For calls that are transferred by Voice Portal to Communication Manager using SIP REFER, the incoming call handling table can be used to manipulate the number in the INVITE message sent by the Acme Packet SBC. In the sample configuration, no such configuration was necessary. For example, for a transfer by Voice Portal to VDN 36880, Voice Portal included 36880 in the Refer-To header. The Acme Packet SBC extracted 36880 from the Refer-To header, and sent 36880 in the INVITE towards Session Manager and Communication Manager.

5.13. Uniform Dial Plan (UDP) Configuration

Although not specifically related to Verizon, this section shows the UDP configuration, with the bold row showing the calls of the form 33xxx will be routed via AAR. The bold row corresponding to pattern “44xxx” allows calls dialed by Communication Manager users to be routed via AAR to the Voice Portal self-service applications.

change uniform-dialplan 3						Page	1	of	2
UNIFORM DIAL PLAN TABLE									
						Percent Full: 0			
Matching Pattern	Len	Del	Insert Digits	Net	Node Conv Num				
31	5	0		aar	n				
3100	5	0		aar	n				
33	5	0		aar	n				
3400	5	0		aar	n				
44	5	0		aar	n				

5.14. Route Pattern for Internal Calls via Avaya Aura® Session Manager

Although not specifically related to Verizon, this section shows an example AAR routing to trunk group 60 to Session Manager. If a Communication Manager user dials a Voice Portal application (e.g., 44000), the call will use this route pattern. As shown in reference [JRR-VZIPT], calls to Modular Messaging also use this route pattern. Route pattern 60 contains trunk group 60, the “private” tie trunk group to Session Manager.

change route-pattern 60														Page	1	of	3					
Pattern Number: 60														Pattern Name: SM FS								
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:	60	0					0	n user														
2:								n user														
3:								n user														
4:								n user														
5:								n user														
6:								n user														
BCC VALUE														TSC	CA-TSC	ITC BCIE Service/Feature PARM				No.	Numbering	LAR
0	1	2	M	4	W	Request								Dgts	Format							
														Subaddress								
1:	y	y	y	y	y	n	n	rest								none						
2:	y	y	y	y	y	n	n	rest								none						
3:	y	y	y	y	y	n	n	rest								none						
4:	y	y	y	y	y	n	n	rest								none						
5:	y	y	y	y	y	n	n	rest								none						
6:	v	v	v	v	v	n	n	rest								none						

5.15. Private Numbering

Although not specifically related to Verizon, this section shows the private numbering configuration associated with the calls using trunk group 60. The bold rows configure any five digit number beginning with 3 or 4 (i.e., 3xxxx, 4xxxx) that uses trunk group 60 to retain the original 5 digit number (i.e., no digit manipulation is specified, and the **Total Len** is 5).

change private-numbering 0					Page 1 of 2	
NUMBERING - PRIVATE FORMAT						
Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len		
5	2			5	Total Administered: 5	
5	3	60		5	Maximum Entries: 540	
5	4	60		5		
5	5			5		

5.16. Avaya Aura® Communication Manager Stations

In the sample configuration, five digit station extensions were used with the format 3xxxx. The following abbreviated screen shows an example extension for an Avaya H.323 IP telephone. As documented in reference [JRR-VZIPT], coverage path 60 is assigned to give this user coverage to Modular Messaging.

change station 30002		Page	1 of 5
		STATION	
Extension: 30002	Lock Messages? n	BCC: 0	
Type: 9620	Security Code: *	TN: 1	
Port: S00038	Coverage Path 1: 60	COR: 1	
Name: Joey Votto	Coverage Path 2:	COS: 1	
	Hunt-to Station:		

On **Page 2**, the **MWI Served User Type** is set to “sip-adjunct” for the SIP integration to Modular Messaging.

change station 30002		Page 2 of 5
STATION		
FEATURE OPTIONS		
LWC Reception: spe	Auto Select Any Idle Appearance? n	
LWC Activation? y	Coverage Msg Retrieval? y	
LWC Log External Calls? n	Auto Answer:	
none		
CDR Privacy? n	Data Restriction? n	
Redirect Notification? y	Idle Appearance Preference? n	
Per Button Ring Control? n	Bridged Idle Line Preference? n	
Bridged Call Alerting? n	Restrict Last Appearance? y	
Active Station Ringing: single		
	EMU Login Allowed? n	
H.320 Conversion? n	Per Station CPN - Send Calling Number?	
Service Link Mode: as-needed	EC500 State: enabled	
Multimedia Mode: enhanced	Audible Message Waiting? n	
MWI Served User Type: sip-adjunct	Display Client Redirection? n	
	Select Last Used Appearance? n	
	Coverage After Forwarding? s	
	Multimedia Early Answer? n	
	Direct IP-IP Audio Connections? y	

5.17. Coverage Path

This section illustrates an example coverage path for a station with a mailbox on Modular Messaging. Hunt group 60, the hunt group to Modular Messaging, is **Point1** in coverage path 60. See reference [JRR-VZIPT] for additional information on coverage to Modular Messaging.

change coverage path 60		Page 1 of 1
COVERAGE PATH		
Coverage Path Number: 60		
Cvg Enabled for VDN Route-To Party? y	Hunt after Coverage? n	
Next Path Number:	Linkage	
COVERAGE CRITERIA		
Station/Group Status	Inside Call	Outside Call
Active?	n	n
Busy?	y	y
Don't Answer?	y	y
All?	n	n
DND/SAC/Goto Cover?	y	y
Holiday Coverage?	n	n
Number of Rings: 2		
COVERAGE POINTS		
Terminate to Coverage Pts. with Bridged Appearances? n		
Point1: h60	Rng:	Point2:
Point3:		Point4:
Point5:		Point6:

5.18. Saving Avaya Aura® Communication Manager Configuration Changes


The command “save translation all” can be used to save the configuration.


6. Avaya Aura® Session Manager Configuration

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

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

Session Manager is managed via System Manager. Using a web browser, access “https://<ip-addr of System Manager>/SMGR”. In the **Log On** screen, enter appropriate **Username** and **Password** and press the **Log On** button (not shown).

ess  https://10.1.2.60/SMGR/

 Avaya Aura™ System Manager 6.0




Home / Log On


Log On

Username :

Password :

Once logged in, a **Home Screen** is displayed. An abridged **Home Screen** is shown below.

Address  https://10.1.2.60/SMGR/   Go



Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at April 29, 2010 5:07 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

▶ Elements

▶ Events

▶ Groups & Roles

Licenses

▶ Routing

▶ Security

▶ System Manager Data

▶ Users

Help

Home Screen

Sub Pages

Action	Description	Help
Elements	This section provides various functionality related to elements. Some functionality is implemented by SMGR generic services and some are provided by product specific element managers.	Help for RTS
Events	Event Management section of the System Manager Console. This part of SMGR lets you view and administer logs and alarms related to the individual domains of SMGR.	Help to manage events like logs and alarms
Groups & Roles	Groups and Roles administration section of System Manager Console. This part of SMGR lets you create and manage groups , roles and permissions.	Help to manage groups and roles
Licenses	Licence Administration section of the system Manager Console. This part of SMGR lets you view and administer licenses.	Help to administer

For readers familiar with prior releases of Session Manager, the configurable items under **Routing** in Release 6 were located under a heading called **Network Routing Policy** in prior releases. Select **Routing**. The screen shown below shows the various sub-headings.

▶ Elements
▶ Events
▶ Groups & Roles
Licenses
▼ Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults
▶ Security
▶ System Manager Data
▶ Users

When Routing is selected, the right side outlines a series of steps. The sub-sections that follow are in the same order as the steps outlined under **Introduction to Network Routing Policy (NRP)** in the abridged screen shown below.

Introduction to Network Routing Policy

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.

The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).

Step 2: Create "Locations"

Step 3: Create "Adaptations"

Step 4: Create "SIP Entities"

- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"

Step 5: Create the "Entity Links"

- Between Session Managers
- Between Session Managers and "other SIP Entities"

Scroll down to review additional steps if desired as shown below. In these Application Notes, all steps are illustrated with the exception of **Step 9**, since “Regular Expressions” were not used.

Step 6: Create "Time Ranges"

- Align with the tariff information received from the Service Providers

Step 7: Create "Routing Policies"

- Assign the appropriate "Routing Destination" and "Time Of Day"

(Time Of Day = assign the appropriate "Time Range" and define the "Ranking")

Step 8: Create "Dial Patterns"

- Assign the appropriate "Locations" and "Routing Policies" to the "Dial Patterns"

Step 9: Create "Regular Expressions"

- Assign the appropriate "Routing Policies" to the "Regular Expressions"

Each "Routing Policy" defines the "Routing Destination" (which is a "SIP Entity") as well as the "Time of Day" and its associated "Ranking".

6.1. Domains

To view or change SIP domains, select **Routing → Domains**. Click on the checkbox next to the name of the SIP domain and **Edit** to edit an existing domain, or the **New** button to add a domain. Click the **Commit** button after changes are completed. The following screen shows a list of configured SIP domains. The Session Manager used in the verification of these Application Notes was shared among many Avaya interoperability test efforts. The domain “avaya.com” was already being used for communication among a number of Avaya systems and applications. The domain “avaya.com” is not known to the Verizon production service.

Domain Management

EditNewDuplicateDeleteMore Actions ▾

5 Items | RefreshFilter: Enable

<input type="checkbox"/>	Name	Type	Default	Notes
<input type="checkbox"/>	adevc.avaya.globalipcom.com	sip	<input type="checkbox"/>	CPE domain for Verizon Trunk Test
<input type="checkbox"/>	avaya.com	sip	<input type="checkbox"/>	
<input type="checkbox"/>	avocs.contoso.com	sip	<input type="checkbox"/>	Microsoft OCS Test Environment
<input type="checkbox"/>	contosomed1.avocs.contoso.com	sip	<input type="checkbox"/>	Mediation server inserts this
<input type="checkbox"/>	pcelban0001.avayalincroft.globalipcom.com	sip	<input type="checkbox"/>	Verizon network domain for IP Trunk

Select : All, None

The domain “adevc.avaya.globalipcom.com” is the domain known to Verizon as the enterprise SIP domain. In the sample configuration, Verizon included this domain as the host portion of the To header in the SIP INVITE for inbound IP Trunk calls. Verizon set the host port of the Request-URI header with the outside (public) IP Address of the SBC (1.1.1.2).

Home / Routing / Domains

▸ Elements▸ Events▸ Groups & RolesLicenses▾ RoutingDomainsLocationsAdaptations

Domain Management

CommitCancel

1 Item | RefreshFilter: Enable

Name	Type	Default	Notes
* <input type="text" value="adevc.avaya.globalipcom.com"/>	<input type="text" value="sip"/>	<input type="checkbox"/>	<input type="text" value="CPE domain for Verizon Trunk Test"/>

6.2. Locations

To view or change locations, select **Routing → Locations**. The following screen shows an abridged list of configured locations. Click on the checkbox corresponding to the name of a location and **Edit** to edit an existing location, or the **New** button to add a location. Click the **Commit** button after changes are completed. Assigning unique locations can allow Session Manager to perform location-based routing, bandwidth management, and call admission control.

Location

EditNewDuplicateDeleteMore Actions ▼Commit

13 Items | RefreshFilter: Enable

<input type="checkbox"/>	Name	Notes
<input type="checkbox"/>	AC-BR2	Branch 2 for AudioCodes MP-118
<input type="checkbox"/>	Acme1	Net-Net SD1 Inside
<input type="checkbox"/>	Acme2	Net-Net SD2 Inside
<input type="checkbox"/>	adevc	Inside network used for VZ test
<input type="checkbox"/>	Aura-SBC	Location for Avaya Aura SBC
<input type="checkbox"/>	BaskingRidge HQ	Fred's ACM & ASM's

The following screen shows the **Location Details** for the location named “Acme1”, corresponding to the Acme Packet Net-Net SBC relevant to these Application Notes. Later, the location with name “Acme1” will be assigned to the corresponding SIP Entity. The IP Address 65.206.67.1 of the inside (private) interface of “Acme1” is entered in the **IP Address Pattern** field.

Location Details

General

* Name:

Notes:

Managed Bandwidth: Kbit/sec ▼

* Average Bandwidth per Call: Kbit/sec ▼

Location Pattern

1 Item | Refresh

Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* <input type="text" value="65.206.67.1"/>	<input type="text"/>

The following screen shows the **Location Details** for the location named “BaskingRidge HQ”. The SIP Entities and associated IP Addresses for this location correspond to the shared components of the Avaya Interoperability Lab test environment, such as Communication Manager Release 6 and Session Manager Release 6.

Location Details

CommitCancel

General

* Name:

BaskingRidge HQ

Notes:

CME, CS1K R5 & R7, AAC R6, CM I

Managed Bandwidth:

Kbit/sec

* Average Bandwidth per Call:

80

Kbit/sec

Location Pattern

AddRemove

5 ItemsRefreshFilter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.7.7.*	
<input type="checkbox"/>	* 10.32.1.*	
<input type="checkbox"/>	* 10.32.2.*	
<input type="checkbox"/>	* 172.28.43.*	
<input type="checkbox"/>	* 10.1.2.*	

The following screen shows the **Location Details** for the location named “VoicePortal”. The IP Address Pattern contains the IP Address 65.206.67.87 of the Voice Portal single server system used in the sample configuration.

Location Details

CommitCancel

General

*

Name:

VoicePortal

Notes:

Verizon Testing

Managed Bandwidth:

Kbit/sec

*

Average Bandwidth per Call:

80

Kbit/sec

Location Pattern

AddRemove

1 Item | RefreshFilter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 65.206.67.87	

Select : All, None

6.3. Adaptations

To view or change adaptations, select **Routing → Adaptations**. Click on the checkbox corresponding to the name of an adaptation and **Edit** to edit an existing adaptation, or the **New** button to add an adaptation. Click the **Commit** button after changes are completed.

The following screen shows a portion of the list of adaptations in the sample configuration.

Adaptations				
<div>EditNewDuplicateDeleteMore Actions ▼Commit</div>				
14 Items Refresh			Filter: Enable	
<input type="checkbox"/>	Name	Module name	Egress URI Parameters	Notes
<input type="checkbox"/>	Avaya-R6.0	DigitConversionAdapter odstd=avaya.com osrcd=avaya.com		Avaya.com for shared SIL ntwk
<input type="checkbox"/>	Cisco-UCM6	CiscoAdapter avaya.com		
<input type="checkbox"/>	Cisco-UCM7	CiscoAdapter avaya.com		
<input type="checkbox"/>	CiscoUCME	CiscoAdapter avaya.com		
<input type="checkbox"/>	CM-ES Inbound	DigitConversionAdapter odstd=avaya.com osrcd=avaya.com		
<input type="checkbox"/>	CM-ES-VZ Inbound	DigitConversionAdapter odstd=avaya.com		

6.3.1. Adaptation for Avaya Aura® Session Manager to Avaya Voice Portal

The adapter named “Voice-Portal” shown below will later be assigned to the SIP Entity for Voice Portal. This adaptation uses the “DigitConversionAdapter” and specifies the “odstd=avaya.com” parameter to adapt the domain in the Request URI to the domain expected by Voice Portal in the sample configuration. For example, for inbound calls from Verizon to the Avaya CPE, the Request-URI header sent to Voice Portal will contain “avaya.com” as expected by Voice Portal. However, this is not sufficient. Voice Portal 5.1 also expects the To header to contain the configured domain. Since Session Manager 6.0 does not adapt the To header, the Acme Packet Net-Net SBC is used to adapt the To header to “avaya.com” as detailed in **Section 7**.

In the example screen shown below, the Verizon IP Trunk DID number 732-945-0288 is adapted to the number 44000. In the sample configuration, Voice Portal will match 44000 to a Voice Portal application.

Adaptation Details

CommitCancel

General

* Adaptation name:Voice-Portal

Module name:DigitConversionAdapter

Module parameter:odstd=avaya.com

Egress URI Parameters:

Notes:Voice Portal Adapter

Digit Conversion for Incoming Calls to SM

AddRemove

0 Items RefreshFilter: Enable

	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
--	------------------	-----	-----	---------------	---------------	-------------------	-------

Digit Conversion for Outgoing Calls from SM

AddRemove

3 Items RefreshFilter: Enable

	Matching Pattern	Min	Max	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 7329450288	* 10	* 10	* 10	44000	both	VP Test App IP Trunk
<input type="checkbox"/>	* 8668510107	* 10	* 10	* 10	44000	both	VP Test App IPTF
<input type="checkbox"/>	* 8668518119	* 10	* 10	* 10	44000	both	VP Test App IP-IVR

6.3.2. Adaptation for Avaya Aura® Session Manager to Acme Packet Net-Net SBC

The adapter assigned to the SIP Entity to the Acme Packet SBC is the same as the one used in reference [JRR-VZIPT]. This adapter is named “History_Diversion_IPT” and uses the Session Manager “VerizonAdapter”. The adapter is configured to apply two parameters:

- “osrcd=adevc.avaya.globalipcom.com”. This configuration enables the source domain to be overwritten with “adevc.avaya.globalipcom.com”. For example, for inbound IP Trunk

calls from Verizon, the PAI header sent to Verizon in the 200 OK will contain “adevc.avaya.globalipcom.com”. Depending on the enterprise domain configuration, it may not be necessary for Session Manager to adapt the domain in this fashion. In the sample configuration, where “avaya.com” was already in use in a shared Avaya environment, it was appropriate for Session Manager to adapt the domain from “avaya.com” to “adevc.avaya.globalipcom.com” where the latter is the CPE domain known to Verizon.

- “odstd=pcelban0001.avayalincroft.globalipcom.com” This configuration enables the destination domain to be overwritten with “pcelban0001.avayalincroft.globalipcom.com”, the Verizon IP Trunk service domain used in the sample configuration.

The following screen shows the partial list of adaptations, including the History_Diversion_IPT parameters. For the inbound calls from Verizon to Voice Portal that are the focus of these Application Notes, no conversion of digits is required by this adapter.

Adaptations

Edit
New
Duplicate
Delete
More Actions
Commit

16 Items Refresh
Filter: Ena

<input type="checkbox"/>	Name	Module name	Egress URI Parameters	Notes
<input type="checkbox"/>	Avaya-R6.0	DigitConversionAdapter odstd=avaya.com osrcd=avaya.com		
<input type="checkbox"/>	Cisco-UCM6	CiscoAdapter avaya.com		
<input type="checkbox"/>	Cisco-UCM7	CiscoAdapter avaya.com		
<input type="checkbox"/>	CiscoUCME	CiscoAdapter iosrcd=avaya.com odstd=192.45.131.1		
<input type="checkbox"/>	CM-ES Inbound	DigitConversionAdapter odstd=avaya.com osrcd=avaya.com		
<input type="checkbox"/>	CM-ES-VZ Inbound	DigitConversionAdapter odstd=avaya.com		Avaya.com for shared S ntwk
<input type="checkbox"/>	Digit_Conversion_VZ	DigitConversionAdapter osrcd=adevc.avaya.globalipcom.com odstd=pcelban0001.avayalincroft.globalipcom.com		Verizon DID to CM Extn map, param above shou on VZ-adapter
<input type="checkbox"/>	History_Diversion_IPT	VerizonAdapter osrcd=adevc.avaya.globalipcom.com odstd=pcelban0001.avayalincroft.globalipcom.com		
<input type="checkbox"/>	MM Normalized	DigitConversionAdapter avaya.com		
<input type="checkbox"/>	MS_OCS_Domain_Adaptor	DigitConversionAdapter 135.8.19.139		IP Address of MS OCS Mediation Server
<input type="checkbox"/>	OITTAdapter	DigitConversionAdapter 135.8.19.109		
<input type="checkbox"/>	S87x0-CM521-VZ Inbound	DigitConversionAdapter iodstd=avaya.com		try not to put avaya.com far-end domain CM sig
<input type="checkbox"/>	ToJuniper	DigitConversionAdapter		
<input type="checkbox"/>	To-Surv-CM	DigitConversionAdapter avaya.com		
<input type="checkbox"/>	Voice-Portal	DigitConversionAdapter odstd=avaya.com		Voice Portal Adapter

6.3.3. Adaptation for Avaya Aura® Session Manager to Avaya Aura® Communication Manager

The adapter described here is also common to reference [JRR-VZIPT]. This adapter is necessary only if certain calls from Verizon will be routed by Session Manager directly to Communication Manager, rather than first routing to Voice Portal for self-service.

The adapter named “CM-ES-VZ Inbound” shown below will later be assigned to the SIP Entity linking Session Manager to Communication Manager for calls involving Verizon. This adaptation uses the “DigitConversionAdapter” and specifies the “odstd=avaya.com” parameter to adapt the domain to the domain expected by Communication Manager in the sample configuration. More specifically, this configuration enables the destination domain to be overwritten with “avaya.com” for calls that egress to a SIP entity using this adapter. For example, for inbound IP Trunk calls from Verizon directly to Communication Manager, the Request-URI header sent to Communication Manager will contain “avaya.com” as expected by Communication Manager in the shared Avaya Interoperability Lab configuration. Depending on the Communication Manager configuration, it may not be necessary for Session Manager to adapt the domain in this fashion.

Adaptation Details

CommitCancel

General

* Adaptation name:CM-ES-VZ Inbound

Module name:DigitConversionAdapter

Module parameter:odstd=avaya.com

Egress URI Parameters:

Notes:Avaya.com for shared SIL ntwk

In the testing associated with these Application Notes, it is not necessary for this adapter to perform digit conversion. If desired, consult [JRR-VZIPT] for examples of digit conversion for inbound Verizon IP Trunk calls routed by Session Manager to Communication Manager, rather than to Voice Portal.

6.4. SIP Entities

To view or change SIP entities, select **Routing → SIP Entities**. Click the checkbox corresponding to the name of an entity and **Edit** to edit an existing entity, or the **New** button to add an entity. Click the **Commit** button after changes are completed.

Compared with the configuration documented in reference [JRR-VZIPT], the only new SIP Entity is for Voice Portal. Other SIP Entities are illustrated below for completeness.

6.4.1. SIP Entity for Avaya Voice Portal

The SIP Entity named “VoicePortal” is shown below. The **FQDN or IP Address** is set to “65.206.67.87”, the IP Address of the single server Voice Portal used in the sample configuration. If necessary, see reference [ICR] for an example using a common FQDN to distribute calls among several VoicePortal servers. The **Type** of entity is “Voice Portal”. The **Location** is set to “VoicePortal”, the location configured in Section 6.2. The **Adaptation** is set to “Voice-Portal”, the adaptation configured in Section 6.3. Default parameters can be retained in other fields or modified to suit as desired.

SIP Entity Details

General

* Name:	<input type="text" value="VoicePortal"/>
* FQDN or IP Address:	<input type="text" value="65.206.67.87"/>
Type:	<input type="text" value="Voice Portal"/>
Notes:	<input type="text" value="Verizon Testing"/>
Adaptation:	<input type="text" value="Voice-Portal"/>
Location:	<input type="text" value="VoicePortal"/>
Time Zone:	<input type="text" value="America/New_York"/>
Override Port & Transport with DNS SRV:	<input type="checkbox"/>
* SIP Timer B/F (in seconds):	<input type="text" value="4"/>
Credential name:	<input type="text"/>
Call Detail Recording:	<input type="text" value="none"/>

SIP Link Monitoring

SIP Link Monitoring:

6.4.2. SIP Entity for Acme Packet Net-Net SBC

The following screen shows the **SIP Entity Details** corresponding to “Acme1”. The **FQDN or IP Address** field is configured with the Acme Packet Net-Net SBC inside IP Address (65.206.67.1). “Other” is selected from the **Type** drop-down menu for SBC SIP Entities. This Acme Packet Net-Net SBC has been assigned to **Location** “Acme1”, shown in **Section 6.2**, and the “History_Diversion_IPT” adapter shown in **Section 6.3** is applied. Other parameters can retain default values.

SIP Entity Details

[Commit](#)[Cancel](#)

General

* Name:	<input type="text" value="Acme1"/>
* FQDN or IP Address:	<input type="text" value="65.206.67.1"/>
Type:	<input type="text" value="Other"/>
Notes:	<input type="text" value="Inside IP Acme1"/>
Adaptation:	<input type="text" value="History_Diversion_IPT"/>
Location:	<input type="text" value="Acme1"/>
Time Zone:	<input type="text" value="America/New_York"/>
Override Port & Transport with DNS SRV:	<input type="checkbox"/>
* SIP Timer B/F (in seconds):	<input type="text" value="4"/>
Credential name:	<input type="text"/>
Call Detail Recording:	<input type="text" value="none"/>

6.4.3. SIP Entity for Avaya Aura® Session Manager

The following screen shows the upper portion of the **SIP Entity Details** corresponding to “SM1”. The **FQDN or IP Address** field for “SM1” is the Session Manager Security Module IP Address (10.1.2.70), which is used for SIP signaling with other networked SIP entities. The **Type** for this SIP entity is “Session Manager”. Select an appropriate location for the Session Manager from the **Location** drop-down menu. In the shared test environment, the Session Manager used location “BaskingRidge HQ”. The default **SIP Link Monitoring** parameters may be used. If desired, these timers may be customized for each entity.

SIP Entity Details

General

* Name:	<input type="text" value="SM1"/>
* FQDN or IP Address:	<input type="text" value="10.1.2.70"/>
Type:	<input type="text" value="Session Manager"/>
Notes:	<input type="text"/>
Location:	<input type="text" value="BaskingRidge HQ"/>
Outbound Proxy:	<input type="text"/>
Time Zone:	<input type="text" value="America/New_York"/>
Credential name:	<input type="text"/>

SIP Link Monitoring

SIP Link Monitoring:

Scrolling down, the following screen shows the middle portion of the **SIP Entity Details**, a listing of the **Entity Links** previously configured for “SM1”. Use the **Next** button to reveal additional links (not shown). The links relevant to these Application Notes are described in the following section.

Entity Links

Add Remove

34 Items Refresh							Filter: Enable
<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	
<input type="checkbox"/>	SM1	TCP	* 5060	AACR6	* 5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM1	TCP	* 5060	Acme1	* 5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM1	TCP	* 5060	Acme2	* 5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM1	TCP	* 5060	AG2330	* 5080	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM1	TCP	* 5060	AuraSBC	* 5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM1	TCP	* 5060	CallCenter	* 5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM1	TCP	* 5060	Cisco-UCM6	* 5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM1	TCP	* 5060	Cisco-UCM7	* 5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM1	TCP	* 5060	CiscoUCME	* 5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM1	UDP	* 5060	CiscoUCME	* 5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM1	TCP	* 5060	CM Evolution Server	* 5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM1	TCP	* 5062	CM-Evolution-procr-5062	* 5062	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM1	TCP	* 5060	CS1K R5.5	* 5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM1	TCP	* 5060	CS1K R7	* 5060	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	SM1	TCP	* 5060	Denver Nortel CS1000e	* 5060	<input checked="" type="checkbox"/>	

Select : All, None
< Previous Page 1 of 3 Next >

Scrolling down, the following screen shows the lower portion of the **SIP Entity Details**, a listing of the configured ports for “SM1”. In the sample configuration, TCP port 5060 was already in place for the shared test environment, using **Default Domain** “avaya.com”. To enable calls with Verizon to be distinguished from other types of SIP calls using the same Session Manager, TCP port 5062 was added, with **Default Domain** “adevc.avaya.globalipcom.com”. Click the **Add** button to configure a new port. TCP is used in the sample configuration for improved visibility during testing.

Port

Add Remove

5 Items Refresh					Filter: Enable
<input type="checkbox"/>	Port	Protocol	Default Domain	Notes	
<input type="checkbox"/>	5060	TCP	avaya.com		
<input type="checkbox"/>	5060	UDP	avaya.com		
<input type="checkbox"/>	5061	TLS	avaya.com		
<input type="checkbox"/>	5062	TCP	adevc.avaya.globalipcom.com	Verizon testing CPE-domain	
<input type="checkbox"/>	5070	TCP	avocs.contoso.com		

6.4.4. SIP Entity for Avaya Aura® Communication Manager (Not Specific to Verizon)

The following screen shows a portion of the **SIP Entity Details** corresponding to an Communication Manager SIP Entity named “CM Evolution Server”. This is the SIP Entity that was already in place in the shared Avaya Interoperability Test Lab environment, prior to adding the Verizon IP Trunk configuration. The **FQDN or IP Address** field contains the IP Address of the “processor ethernet” (10.1.2.90). In systems with Avaya G650 Media Gateways containing C-LAN cards, C-LAN cards may also be used as SIP entities, instead of, or in addition to, the “processor ethernet”. “CM” is selected from the **Type** drop-down menu. In the shared test environment, the **Adaptation** “CM-ES Inbound” and **Location** “BaskingRidge HQ” had already been assigned to the Communication Manager SIP entity. Reference [JRR-VZIPT] can be consulted for additional details.

SIP Entity Details

[Commit](#)[Cancel](#)

General

* **Name:**

* **FQDN or IP Address:**

Type:

Notes:

Adaptation:

Location:

Time Zone:

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording:

6.4.5. SIP Entity for Avaya Aura® Communication Manager (Specific to Verizon)

The following screen shows the **SIP Entity Details** for an entity named “CM-Evolution-procr-5062”. This entity uses the same **FQDN or IP Address** (10.1.2.90) as the prior entity with name “CM Evolution Server”; both correspond to the S8800 Processor Ethernet. Later, a unique port, 5062, will be used for the Entity Link to “CM-Evolution-procr-5062”. Using a different port is one approach that will allow Communication Manager to distinguish traffic originally from Verizon from other SIP traffic arriving from the same IP Address of Session Manager, such as SIP traffic generated by Avaya SIP Telephones or Avaya Modular Messaging. The adapter “CM-ES-VZ Inbound” is applied to this SIP entity. Recall that this adapter can be used to adapt the domain as well as map Verizon numbers to the corresponding Communication Manager extensions. If desired, a location can be assigned if location-based routing criteria will be used.

Depending on Session Manager configuration, calls that are transferred by Voice Portal to a Communication Manager extension may use this SIP Entity. For example, using the sample configuration, if a call to a Verizon IP Trunk DID number is routed by Session Manager to Voice Portal, and the Voice Portal application requests a blind transfer to a Communication Manager extension, the transferred call will use this SIP Entity and its corresponding Communication Manager signaling group (e.g., 67) and trunk group (e.g., 67). When the Acme Packet SBC receives the REFER triggered by the Voice Portal blind transfer, the SBC will send an INVITE to Session Manager, and Session Manager will choose this SIP Entity to route the transferred call.

SIP Entity Details

Commit Cancel

General

* Name: CM-Evolution-procr-5062

* FQDN or IP Address: 10.1.2.90

Type: CM

Notes: CM-ES procr IP, different port

Adaptation: CM-ES-VZ Inbound

Location:

Time Zone: America/New_York

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.5. Entity Links

To view or change Entity Links, select **Routing** → **Entity Links**. Click on the checkbox corresponding to the name of a link and **Edit** to edit an existing link, or the **New** button to add a link. Click the **Commit** button after changes are completed.

Compared with the configuration documented in reference [JRR-VZIPT], the only new Entity Link is for Voice Portal. Other Entity Links are illustrated below for completeness.

Note – In the Entity Link configurations below (and in the Communication Manager SIP trunk configuration), TCP was selected as the transport protocol for the Avaya CPE in the sample configuration. TCP was used to facilitate trace analysis during network verification. The use of TLS protocol is recommended by Avaya in customer deployments.

6.5.1. Entity Link for Avaya Aura® Session Manager and Avaya Voice Portal

Compared with the configuration documented in reference [JRR-VZIPT], the entity link shown below is the only addition. The Entity Link named “VoicePortal” represents the link between Session Manager and Voice Portal using the TCP protocol and port 5060.

Entity Links

Commit

Cancel

1 Item Refresh		Filter: Enable						
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes	
* VoicePortal	* SM1	TCP	* 5060	* VoicePortal	* 5060	<input checked="" type="checkbox"/>	Verizon Testing	

6.5.2. Entity Link for Avaya Aura® Session Manager and Acme Packet Net-Net SBC

The following screen shows the entity link named “Acme1” linking Session Manager with the Acme Packet Net-Net SBC, using TCP and port 5060.

Entity Links

Commit

Cancel

1 Item Refresh		Filter: Enable						
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes	
* Acme1	* SM1	TCP	* 5060	* Acme1	* 5060	<input checked="" type="checkbox"/>		

6.5.3. Entity Links for Avaya Aura® Session Manager to Avaya Aura® Communication Manager

As in [JRR-VZIPT], two SIP Entity Links, using different TCP ports, link the same SM1 with Communication Manager. For one link, named “CM Evolution Server”, both entities use port

5060. For the other, named “CM-ES-VZ-5062”, both entities use port 5062. The link named “CM Evolution Server” shown below links Session Manager “SM1” with the Communication Manager processor ethernet. This link existed in the shared configuration prior to adding the Verizon-related configuration. This link, using port 5060, can carry traffic between Session Manager and Communication Manager that is not necessarily related to calls with Verizon, such as traffic related to SIP Telephones registered to Session Manager, or traffic related to Modular Messaging, which has SIP integration to Session Manager.

Entity Links

1 Item Refresh		Filter: Enable					
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* CM Evolution Server	* SM1	TCP	* 5060	* CM Evolution Server	* 5060	<input checked="" type="checkbox"/>	

The link named “CM-ES-VZ-5062” shown below also links Session Manager “SM1” with the Communication Manager processor ethernet. However, this link uses port 5062 for both entities in the link. This link was created to allow Communication Manager to distinguish calls from Verizon from other calls that arrive from the same Session Manager. Other methods of distinguishing traffic could be used, if desired.

Entity Links

1 Item Refresh		Filter: Enable					
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* CM-ES-VZ-5062	* SM1	TCP	* 5062	* CM-Evolution-procr-5062	* 5062	<input checked="" type="checkbox"/>	Same IP, diff port

6.6. Time Ranges

To view or change Time Ranges, select **Routing → Time Ranges**. The Routing Policies shown subsequently will use the “24/7” range since time-based routing was not the focus of these Application Notes. Click the **Commit** button after changes are completed.

Time Ranges

[Edit](#) [New](#) [Duplicate](#) [Delete](#) [More Actions ▾](#) [Commit](#)

3 Items 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"/>	<input type="text" value="00:00"/>	<input type="text" value="23:59"/>	<input type="text" value="Time Range 24/7"/>
<input type="checkbox"/>	Anytime	<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"/>	<input type="text" value="00:00"/>	<input type="text" value="23:59"/>	<input type="text" value=""/>
<input type="checkbox"/>	Off-Hours	<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"/>	<input type="text" value="18:00"/>	<input type="text" value="23:59"/>	<input type="text" value="for testing"/>
Select : All , None											

6.7. Routing Policies

To view or change routing policies, select **Routing → Policies**. Click on the checkbox corresponding to the name of a policy and **Edit** to edit an existing policy, or **New** to add a policy. Click the **Commit** button after changes are completed.

Compared with the configuration documented in reference [JRR-VZIPT], the only new routing policy is for Voice Portal. Other routing policies are illustrated below for completeness.

6.7.1. Routing Policy for Avaya Voice Portal

The following screen shows the **Routing Policy Details** for the policy named “To-Voice-Portal”. Note that the SIP Entity as Destination contains the SIP Entity “VoicePortal” configured in **Section 6.4.1**.

Routing Policy Details

CommitCancel

General

* Name: To-Voice-Portal

Disabled: ☐

Notes: Verizon testing

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
VoicePortal	65.206.67.87	Voice Portal	Verizon Testing

Time of Day

AddRemoveView Gaps/Overlaps

1 Item RefreshFilter: 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

6.7.2. Verizon-Specific Routing Policy for Avaya Aura® Communication Manager

The following screen shows the **Routing Policy Details** for the policy named “CM-ES-R6-VZ-Inbound”. This is the routing policy that directs calls to the Verizon-specific SIP entity, using a unique port 5062. Later, dial patterns will be defined for calls to be sent to this routing policy. The dial patterns to be sent to this routing policy will include calls transferred out of Voice Portal using REFER.

Routing Policy Details

[Commit](#) [Cancel](#)

General

* **Name:**

Disabled: ☐

Notes:

SIP Entity as Destination

[Select](#)

Name	FQDN or IP Address	Type	Notes
CM-Evolution-procr-5062	10.1.2.90	CM	CM-ES procr IP, different port

Time of Day

[Add](#)

[Remove](#)

[View Gaps/Overlaps](#)

1 Item | [Refresh](#)

Filter: [Enable](#)

<input type="checkbox"/>	Ranking	1 ▲	Name	2 ▲	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

6.7.3. General Routing Policy for Avaya Aura® Communication Manager

The following screen shows the **Routing Policy Details** for the policy named “To CM-ES R6”. This is the routing policy that was in place prior to adding the Verizon-specific configuration. This routing policy will be associated with dial patterns for calls that are not necessarily related to Verizon, such as calls from Modular Messaging to Communication Manager. In the sample configuration, this policy may also be used for Verizon calls transferred out of Voice Portal using the “bridged transfer” method, since such a “transfer” is really a bridged call that remains in Voice Portal and does not result in a REFER being sent to the SBC.

Routing Policy Details

[Commit](#) [Cancel](#)

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

[Select](#)

Name	FQDN or IP Address	Type	Notes
CM Evolution Server	10.1.2.90	CM	

Time of Day

[Add](#)

[Remove](#)

[View Gaps/Overlaps](#)

1 Item Refresh											Filter: Enable			
<input type="checkbox"/>	Ranking	1 ▲	Name	2 ▲	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

6.8. Dial Patterns

To view or change dial patterns, select **Routing → Dial Patterns**. Click on the checkbox corresponding to the name of a pattern and **Edit** to edit an existing pattern, or **New** to add a pattern. Click the **Commit** button after changes are completed.

Once Dial Patterns are configured that associate dialed numbers with routing policies, a return to the routing policy screen will list the Dial Patterns associated with the policy.

6.8.1. Dial Pattern for Calls from Verizon Directly to Avaya Voice Portal

The following screen illustrates an example dial pattern for a Verizon IP Trunk DID number that Session Manager will route to Voice Portal. In this case, the Pattern specifies “7329450288”, a Verizon IP Trunk DID number designated for a Voice Portal self-service application. Under **Originating Locations and Routing Policies**, the **Originating Location Name** is “Acme1”, the name of the location configured in **Section 6.2** and assigned to the Acme Packet Net-Net SIP entity in **Section 6.3**. The **Routing Policy Name** is “To-Voice-Portal”, the name of the routing policy configured in **Section 6.7.1**.

Dial Pattern Details

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

SIP Domain:

Notes:

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"/>	Acme1	Net-Net SD1 Inside	To-Voice-Portal	0	<input type="checkbox"/>	VoicePortal	Verizon testing
Select : All, None							

Similar dial patterns can be defined for each Verizon number. Of course, if numbers are contiguous, one dial pattern can cover multiple numbers.

6.8.2. Dial Pattern for Calls Transferred by Avaya Voice Portal to an Avaya Aura® Communication Manager Extension

The following screen illustrates a dial pattern corresponding to a Communication Manager extension to which Voice Portal can transfer inbound calls from Verizon. In this case, the Pattern specifies “36880”, a Vector Directory Number (VDN). Similar dial patterns can be specified covering other Communication Manager extensions to which Voice Portal can transfer inbound calls from Verizon. Under **Originating Locations and Routing Policies**, the **Originating Location Name** is “Acme1”, the name of the location configured in **Section 6.2** and assigned to the Acme Packet Net-Net SIP entity in **Section 6.3**. The originating location is the SBC because the SBC is configured such that REFER messages generated by Voice Portal cause the SBC to send a new INVITE message to the Refer-To destination of the REFER, which is the target of the transfer (e.g., the VDN). The **Routing Policy Name** is “CM-ES-R6-VZ-Inbound”, the name of the routing policy configured in **Section 6.7.2**. In sum, this dial pattern is used to allow calls originally routed from Verizon directly to Voice Portal to be transferred to Communication Manager extensions using the same signaling group and trunk group (i.e., 67) used for calls routed directly from Verizon to Communication Manager, as in reference [JRR-VZIPT].

Dial Pattern Details

General

* **Pattern:**

* **Min:**

* **Max:**

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

<input type="button" value="Add"/> <input type="button" value="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"/>	Acme1	Net-Net SD1 Inside	CM-ES-R6-VZ-Inbound	0	<input type="checkbox"/>	CM-Evolution-procr-5062	Inbound VZ to unique CM port

6.8.3. Dial Patterns for Calls from Verizon Directly to Avaya Aura® Communication Manager

Consult reference [JRR-VZIPT] for example dial patterns for any inbound Verizon calls that Session Manager should route directly to Communication Manager, rather than first routing to Voice Portal for a self-service opportunity.

7. Acme Packet Net-Net Session Border Controller

The Acme Packet Net-Net SBC configuration used in the verification of these Application Notes is the same as the configuration previously documented in [JRR-VZIPT], except as noted in this section. Reference [JRR-VZIPT] documents a similar configuration where the Acme Packet SBC communicates with the same Verizon IP Trunk Service on the public side of the SBC, and communicates with Session Manager on the private side of the SBC (i.e., as a hub for SIP communication with Communication Manager and Modular Messaging). In reference [JRR-VZIPT], Voice Portal was not present in the configuration. In these Application Notes, Voice Portal is added to the configuration shown in [JRR-VZIPT], and Voice Portal becomes the focus of the testing. Therefore, this section highlights the changes and additions to the Acme Packet SBC configuration required to execute the Voice Portal testing summarized in **Section 9**.

In the sample configuration, an Acme Packet 4250 Net-Net Session Border Controller is used as the edge device between the Avaya CPE and Verizon Business. Using similar configuration, the Acme Packet 3800 or 4500 platforms may be used.

7.1. Session Agent Change for Avaya Aura® Session Manager Release 6

The session agent configured for Session Manager Release 6 in **Section 6.1** of reference [JRR-VZIPT] is re-used in these Application Notes. Since the test objectives for these Application Notes include the testing of Voice Portal REFER-based transfers of Verizon IP Trunk calls to Communication Manager destinations, but do not include REFER-based transfers towards Verizon PSTN destinations, the “refer-call-transfer” parameter for this session agent is changed to “enabled”. The relevant part of the session agent configuration is included below.

```
session-agent
  hostname          10.1.2.70
  ip-address        10.1.2.70
  port              5060
  state             enabled
  app-protocol      SIP
  transport-method  StaticTCP
  realm-id          INSIDE
  description       Session-Manager-R6
  allow-next-hop-ip enabled
  loose-routing     enabled
  send-media-session enabled
  ping-method       OPTIONS;hops=0
  ping-interval     60
  ping-send-mode    keep-alive
  options           trans-timeouts=1
  refer-call-transfer enabled
  reuse-connections TCP
  tcp-keepalive     enabled
```

7.2. SIP Manipulation For To Header Towards Avaya Voice Portal

As noted in **Section 1.3**, Voice Portal 5.1 requires that the host portion of the To header match the configured domain in Voice Portal. Since Session Manager 6.0 can not adapt the domain in the To header, the SBC is used to ensure that the domain in the To header matches the “avaya.com” domain shown in Voice Portal in **Section 4.2**.

The following header-rule is added to the SIP “out-manipulationid” applied to the “inside” realm towards Session Manager. The new-value in the element-rule is set to “avaya.com”, as shown in bold below. In this case, “avaya.com” replaces any value in the host portion of the To header.

header-rule

name	Inbound_To
header-name	To
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	
match-value	
new-value	
element-rule	
name	To
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	avaya.com

7.3. SIP Manipulation to Preserve User-to-User Information for REFER-based Transfers to Avaya Aura® Communication Manager

If User-to-User Information should be passed from Voice Portal to Communication Manager for REFER-based transfers (e.g., blind transfer, and consultative transfer using REFER), the following header-rules can be added to the configuration.

The following header rule should be added to the SIP “in-manipulationid” applied to the “inside” realm towards Session Manager. The approach is to store the contents of any “User-to-User” portion of the Refer-To header of a REFER message from Voice Portal after the literal text “UI”. Later, the SIP “out-manipulationid” will key off the literal text UI so that the SBC can

include the user to user information in the INVITE message generated when the refer-call-transfer option is enabled.

header-rule

name	requi
header-name	Refer-To
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	REFER
match-value	
new-value	
element-rule	
name	getUII
parameter-name	User-to-User
type	uri-header
action	store
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	
element-rule	
name	appenduriuser
parameter-name	
type	uri-user
action	replace
match-val-type	any
comparison-type	boolean
match-value	\$requi.\$getUII
new-value	\$ORIGINAL+UII+\$requi.\$getUII.\$0

The following header rules should be added to the SIP “out-manipulationid” applied to the “inside” realm towards Session Manager. The header rules named “get_UII”, “get_UII_To”, and “get_UII_Route” restore the original URI sans the literal text “UII” and any user to user information. By specifying the match-value “(.*)(UII)(.*)”, the original URI is located in “\$1”, the information before the literal text “UII”, when UII is present. The actual user to user information is in “\$3” after the literal text “UII”.

header-rule

name	get_UII
header-name	Request-URI
action	manipulate
comparison-type	case-sensitive
msg-type	request
methods	INVITE

```

match-value
new-value
element-rule
    name                store_UII
    parameter-name
    type                uri-user
    action              store
    match-val-type      any
    comparison-type     case-sensitive
    match-value         (.*)(UII)(.*)
    new-value
element-rule
    name                get_UII
    parameter-name
    type                uri-user
    action              find-replace-all
    match-val-type      any
    comparison-type     case-sensitive
    match-value         (.*)(UII)(.*)
    new-value           $get_UII.$store_UII.$1

```

```

header-rule
    name                get_UII_To
    header-name         To
    action              manipulate
    comparison-type     case-sensitive
    msg-type            request
    methods             INVITE
    match-value
    new-value
element-rule
    name                store_UII
    parameter-name
    type                uri-user
    action              store
    match-val-type      any
    comparison-type     case-sensitive
    match-value         (.*)(UII)(.*)
    new-value
element-rule
    name                get_UII
    parameter-name
    type                uri-user
    action              find-replace-all
    match-val-type      any

```

comparison-type	case-sensitive
match-value	(.*)(UII)(.*)
new-value	\$get_UII_To.\$store_UII.\$1

header-rule

name	get_UII_Route
header-name	Route
action	manipulate
comparison-type	case-sensitive
msg-type	any
methods	INVITE
match-value	
new-value	
element-rule	
name	store_UII
parameter-name	
type	uri-user
action	store
match-val-type	any
comparison-type	case-sensitive
match-value	(.*)(UII)(.*)
new-value	
element-rule	
name	get_UII
parameter-name	
type	uri-user
action	find-replace-all
match-val-type	any
comparison-type	case-sensitive
match-value	(.*)(UII)(.*)
new-value	\$get_UII_Route.\$store_UII.\$1

The following header rule inserts the User-to-User header into the INVITE message when UII is present. The “\$3” represents the actual user to user information.

header-rule

name	add_UII
header-name	User-to-User
action	add
comparison-type	boolean
msg-type	request
methods	INVITE
match-value	\$get_UII.\$store_UII
new-value	\$get_UII.\$store_UII.\$3

8. Verizon Business IP Trunk Configuration

Information regarding Verizon Business IP Trunk service offer can be found at <http://www.verizonbusiness.com/us/products/voip/trunking/> or by contacting a Verizon Business sales representative.

The sample configuration described in these Application Notes was located in the Avaya Solutions and Interoperability Lab. The Verizon Business IP trunk service was accessed via a Verizon Private IP (PIP) T1 connection. Verizon Business provided all of the necessary service provisioning.

8.1. Fully Qualified Domain Name (FQDN)s

The following Fully Qualified Domain Names (FQDN) were provided by Verizon for the sample configuration.

CPE (Avaya)	Verizon Network
<i>adevc.avaya.globalipcom.com</i>	<i>pcelban0001.avayalincroft.globalipcom.com</i>

8.2. Service Access information

The following service access information (FQDN, IP addressing, ports, Verizon DID numbers) was provided by Verizon for the sample configuration. The bold number with the “*” is the number illustrated in the sample configuration in these Application Notes. Other numbers can be configured similarly.

CPE (Avaya)	Verizon Network
<i>adevc.avaya.globalipcom.com</i> <i>UDP port 5060</i>	<i>172.30.209.21</i> <i>UDP Port 5071</i>

IP Trunk DID Numbers
732-945-0285 → 732-945-0287
732-945-0288*
732-945-0228 → 732-945-0229
732-945-0231 → 732-945-0244

9. General Test Approach and Test Results

The test environment consisted of:

- A simulated enterprise site with Voice Portal, Communication Manager, Session Manager, Avaya phones, and an Acme Packet Net-Net SBC.
- The production Verizon Business IP Trunk service, to which the simulated enterprise site was connected.

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

- Inbound Verizon IP Trunk calls to Voice Portal applications.
- Caller interaction with Voice Portal applications, including caller DTMF input.
- Voice Portal applications transferring of inbound calls to Communication Manager skills / agents using blind transfer, consult transfer, and bridged transfer.
- Transfer of User-to-User Information from Voice Portal to Communication Manager as part of transfer scenarios
- Call and two-way talk path establishment between callers and Communication Manager agents following transfers from Voice Portal.

The above test objectives were verified successfully. Any limitations are noted in **Section 1.3**.

10. Verification Steps

10.1. Verification Tests

The following steps may be used to verify the configuration:

1. Place an inbound Verizon IP Trunk call to an Voice Portal application, and verify that two-way talk path exists. Interact with the Voice Portal prompts and verify that the call remains stable for several minutes and can be disconnected properly.
2. Place an inbound Verizon IP Trunk call to an Voice Portal application that can transfer an inbound call to a Communication Manager skill, and select the appropriate prompt(s) to request a transfer to an agent. Verify that the transfer completes successfully. Verify that when no agent in the skill is available, the caller hears appropriate wait treatment (e.g., an announcement). Verify that when an agent in the skill becomes available, the call is successfully routed to the agent and two-way talk path exists between the caller and the agent.

10.2. Avaya Aura® System Manager and Avaya Aura® Session Manager Verifications

This section contains verification steps that may be performed using System Manager for Session Manager.

10.2.1. Verify SIP Entity Link Status

Log in to System Manager. Expand **Elements** → **Session Manager** → **System Status** → **SIP Entity Monitoring**, as shown below.

▼ Session Manager
Dashboard
Session Manager
Administration
Communication Profile
Editor
▶ Network Configuration
▶ Device and Location
Configuration
▶ Application Configuration
▼ System Status
System State
Administration
SIP Entity Monitoring

From the list of monitored entities, select an entity of interest, such as “Acme1”. Under normal operating conditions, the **Link Status** should be “Up” as shown in the example screen below.

All Entity Links to SIP Entity: Acme1							
Refresh		Summary View					
1 Item				Filter: Enable			
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
<input type="checkbox"/> Show	SM1	65.206.67.1	5060	TCP	Up	200 OK	Up

Return to the list of monitored entities, and select another entity of interest, such as “VoicePortal”. Under normal operating conditions, the **Link Status** should be “Up” as shown in the example screen below. In this case, “Show” under Details was selected to view additional information.

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: VoicePortal

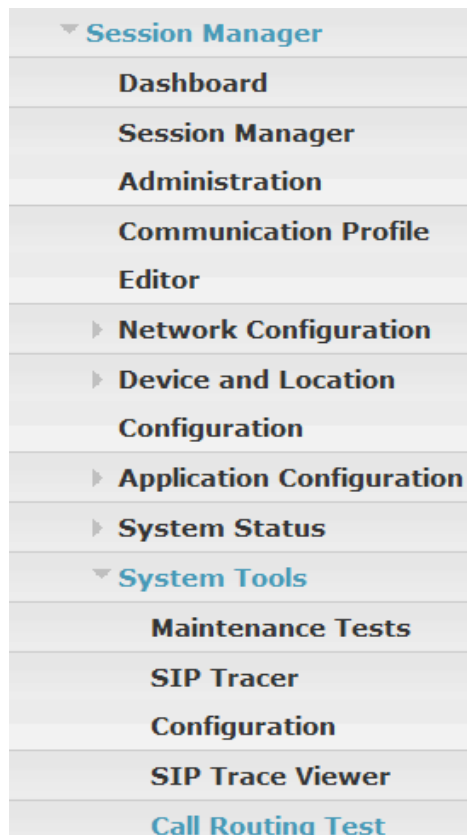
Refresh

Summary View

1 Item							Filter: Enable
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▼ Hide	SM1	65.206.67.87	5060	TCP	Up	200 OK	Up
Time Last Down	Time Last Up	Last Message Sent		Last Response Latency (ms)			
Never	Oct 14, 2010 8:43:26 AM EDT	Oct 14, 2010 2:33:56 PM EDT		15			

10.2.2. 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**, as shown below.



A screen such as the following is displayed.

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"/>	Calling Party Address <input type="text"/>
Calling Party URI <input type="text"/>	Session Manager Listen Port <input type="text" value="5060"/>
Day Of Week <input type="text" value="Monday"/>	Time (UTC) <input type="text" value="16:59"/>
Called Session Manager Instance <input type="text" value="SM1"/>	Transport Protocol <input type="text" value="TCP"/>
<input type="button" value="Execute Test"/>	

Populate the fields for the call parameters of interest and click **Execute Test**. For example, the following shows a call routing test for an inbound Verizon IP Trunk call from the PSTN to Voice Portal via Acme1 (65.206.67.1). Under **Routing Decisions**, observe that the call will route to Voice Portal (65.206.67.87) using the SIP entity named “VoicePortal”. The domain in the Request-URI is converted to “avaya.com”, and the digits are manipulated such that the Verizon IP Trunk DID number (i.e., 732-945-0288) is converted to a number that will trigger a Voice Portal application (i.e., 44000). This adaptation is performed by the adapter assigned to the Voice Portal entity. Scroll down to inspect the details of the **Routing Decision Process** if desired (not shown).

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="7329450288@10.1.2.70"/>	Calling Party Address <input type="text" value="65.206.67.1"/>
Calling Party URI <input type="text" value="anyuser@anyhost.com"/>	Session Manager Listen Port <input type="text" value="5060"/>
Day Of Week <input type="text" value="Monday"/>	Time (UTC) <input type="text" value="14:38"/>
Called Session Manager Instance <input type="text" value="SM1"/>	Transport Protocol <input type="text" value="TCP"/>
<input type="button" value="Execute Test"/>	

Routing Decisions

Route < sip:44000@avaya.com > to SIP Entity VoicePortal (65.206.67.87). Terminating Location is VoicePortal.

The following screen shows another example of a call routing test. In this case, the call routing test shows the results when a call is launched by the Acme Packet Net-Net SBC in response to a REFER from Voice Portal to Communication Manager Vector Directory Number (VDN) 36880. That is, when Voice Portal transfers the Verizon caller to VDN 36880 using REFER, Session Manager will receive an INVITE from the SBC with the number 36880. Session Manager will route this call to the SIP Entity “CM-Evolution-procr-5062” associated with the Verizon-specific trunk group 67 on Communication Manager.

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="36880@10.1.2.70"/>	Calling Party Address <input type="text" value="65.206.67.1"/>
Calling Party URI <input type="text" value="anyuser@anyhost.com"/>	Session Manager Listen Port <input type="text" value="5060"/>
Day Of Week <input type="text" value="Thursday"/>	Time (UTC) <input type="text" value="18:22"/>
Called Session Manager Instance <input type="text" value="SM1"/>	Transport Protocol <input type="text" value="TCP"/>

Routing Decisions

Route < sip:36880@avaya.com > to SIP Entity CM-Evolution-procr-5062 (10.1.2.90). Terminating Location is BaskingRidge HQ.

10.3. Avaya Voice Portal Verifications

From the Voice Portal **Home** screen shown in **Section 4.3**, select **Real-Time Monitoring → System Monitor**. The following screen was captured while Voice Portal was processing a call from the Verizon IP Trunk service. The links such as **MPP1** can be used to access additional information, if desired (not shown).

AVAYA

Wel
Last logged in 11/11/10 at 3:

Voice Portal 5.1 (VoicePortal)

HomeHelp

Expand All | Collapse All

▼ User Management

Roles

Users

Login Options

▼ Real-Time Monitoring

System Monitor

Active Calls

Port Distribution

▼ System Maintenance

Audit Log Viewer

Trace Viewer

Log Viewer

Alarm Manager

▼ System Management

MPP Manager

Software Upgrade

System Backup

▼ System Configuration

Alarm Codes

Alarm/Log Options

Applications

MPP Servers

Report Data

SNMP

Speech Servers

VoIP Connections

VPMS Servers

You are here: [Home](#) > Real-Time Monitoring > System Monitor

System Monitor (11/15/10 10:46:31 AM EST)

This page displays the current state of the local Voice Portal system plus any remote Voice Portal systems that you have configur information about the colored alarm symbols, click Help.

Summary

VoicePortal Details

Last Poll: 11/15/10 10:46:26 AM EST

Server Name	Type	Mode	State	Config	Call Capacity			Active Calls		Calls Today	Alarms
					Current	Licensed	Maximum	In	Out		
VPMS / MPP1	VPMS / MPP	Online	Running	OK	10	10	10	1	0	2	
Summary	VP				10	10	10	1	0	2	

Help

From the Voice Portal **Home** screen shown in **Section 4.3**, select **Real-Time Monitoring** → **Active Calls**. The following screen was captured while Voice Portal was processing an inbound Verizon IP Trunk call. As can be observed, the call was from PSTN caller 908-848-5704 to Verizon IP Trunk number 732-945-0288 (i.e., number received by Voice Portal in the user portion of the To header). The call is being processed by the Application “SampleApp” configured in **Section 4.5**.

Voice Portal 5.1 (VoicePortal) Home ? Help

Expand All | Collapse All

You are here: [Home](#) > Real-Time Monitoring > Active Calls

Active Calls (11/15/10 10:47:28 AM EST)

This page displays the status of all the active calls being handled by the Voice Portal system.

Total Active Calls: 1 Last Poll: 11/15/10 10:47:28 AM EST

Port	Port Group	Protocol	Call Type	MPP Server	Start Time	Calling Number/URI	Called Number/URI	Application	ASR Server
1	SessionManager	SIP_Trunk	Inbound	MPP1	11/15/10 10:45:52 AM EST	tel:9088485704	tel:7329450288	SampleApp	

[Help](#)

From the Voice Portal **Home** screen shown in **Section 4.3**, select **System Management** → **MPP Manager**. In the resultant screen, the state of the MPP server(s) can be verified or managed, as shown below. The following screen was captured while Voice Portal was processing an inbound Verizon IP Trunk call.

AVAYA WELCOME

Last logged in 11/11/10 at 3:30 PM

Voice Portal 5.1 (VoicePortal) Home ? Help

Expand All | Collapse All

You are here: [Home](#) > System Management > MPP Manager

MPP Manager (11/15/10 10:49:20 AM EST)

This page displays the current state of each MPP in the Voice Portal system. To enable the state and mode commands, select one or more MPPs. To enable the mode commands, the selected MPPs must also be stopped.

Last Poll: 11/15/10 10:49:08 AM EST

Server Name	Mode	State	Config	Auto Restart	Restart Schedule	Active Calls		
					Today	Recurring	In	Out
<input type="checkbox"/> MPP1	Online	Running	OK	Yes	No	None	1	0

State Commands

[Start](#) [Stop](#) [Restart](#) [Reboot](#) [Halt](#) [Cancel](#)

Mode Commands

[Offline](#) [Test](#) [Online](#)

Restart/Reboot Options

☐ One server at a time

☒ All selected servers at the same time

[Help](#)

10.4. Troubleshooting Tools

The Communication Manager “list trace vector”, “list trace vdn”, “list trace tac”, and/or “status trunk-group” commands are helpful diagnostic tools to verify correct operation and to troubleshoot problems. MST (Message Sequence Trace) diagnostic traces (performed by Avaya Support) can be helpful in understanding specific interoperability issues.

The logging and reporting functions within the Avaya VPMS web interface may be used to examine the details of Voice Portal calls. In addition, if port monitoring is available, a SIP protocol analyzer such as Wireshark can be used to capture SIP traces at the various interfaces. SIP traces can be instrumental in understanding SIP protocol issues resulting from configuration problems.

11. Conclusion

These Application Notes describe a sample configuration of Avaya Voice Portal with the Verizon Business IP Trunk service. The Verizon Business IP Trunk service allows PSTN calling using SIP trunks. Avaya Voice Portal is a speech-enabled interactive voice response system that allows enterprises to provide multiple self and assisted service resources to their customers in a flexible and customizable manner.

The sample 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 interoperability compliance testing as part of the Avaya DevConnect Service Provider program.

Avaya Voice Portal has not been independently certified by Verizon Business. These Application Notes may be used to facilitate Avaya Voice Portal customer engagements via the Verizon Business field process.

12. References

12.1. Avaya

Avaya product documentation, including the following, is available at <http://support.avaya.com>

- [1] *Planning for Voice Portal*, June 2010
<http://support.avaya.com/css/P8/documents/100089470>
- [2] *Implementing Voice Portal on a single server*, June 2010
<http://support.avaya.com/css/P8/documents/100089465>
- [3] *Implementing Voice Portal on multiple servers*, June 2010
<http://support.avaya.com/css/P8/documents/100089466>
- [4] *Administering Voice Portal*, June 2010
<http://support.avaya.com/css/P8/documents/100089113>
- [5] *Installing and Configuring Avaya Aura™ Communication Manager*, Doc ID 03-603558, Release 6.0 June, 2010 available at <http://support.avaya.com/css/P8/documents/100089133>

- [6] *Administering Avaya Aura™ Communication Manager*, Doc ID 03-300509, Issue 6.0 June 2010 available at <http://support.avaya.com/css/P8/documents/100089333>
- [7] *Administering Avaya Aura™ Session Manager*, Doc ID 03-603324, Release 6.0, June 2010 available at <http://support.avaya.com/css/P8/documents/100082630>
- [8] *Installing and Configuring Avaya Aura™ Session Manager*, Doc ID 03-603473 Release 6.0, June 2010 available at <http://support.avaya.com/css/P8/documents/100089152>
- [9] *Maintaining and Troubleshooting Avaya Aura™ Session Manager*, Doc ID 03-603325, Release 6.0, June 2010 available at <http://support.avaya.com/css/P8/documents/100089154>
- [10] *Administering Avaya Aura™ System Manager*, Document Number 03-603324, Release 5.2, November 2009 available at <http://support.avaya.com/css/P8/documents/100089681>

Avaya Application Notes, including the following, are also available at <http://support.avaya.com>

Application Notes Reference [JRR-VZIPT] documents Verizon IP Trunk Service with Avaya Aura™ Communication Manager Release 6 and Avaya Aura™ Session Manager Release 6. The configuration documented in [JRR-VZIPT] served as the starting point for the configuration in these Application Notes. That is, Avaya Voice Portal was added to the configuration documented in [JRR-VZIPT].

[JRR-VZIPT] Application Notes for Avaya Aura™ Communication Manager 6.0, Avaya Aura™ Session Manager 6.0, and Acme Packet Net-Net with Verizon Business IP Trunk SIP Trunk Service – Issue 1.0

https://devconnect.avaya.com/public/download/dyn/SM6Acme_VzB_IPT.pdf

Application Notes Reference [ICR] documents an Intelligent Customer Routing configuration using Voice Portal.

[ICR] Intelligent Customer Routing with Acme Packet Session Border Controller using Avaya Aura™ Session Manager 6.0, Avaya Aura™ Communication Manager 6.0 and Avaya Voice Portal 5.1 – Issue 1.0

<http://support.avaya.com/css/P8/documents/100113293>

12.2. Acme Packet

Acme Packet Support (login required):

<http://www.acmepacket.com/support.htm>

12.3. Verizon Business

Information in the following Verizon documents was also used for these Application Notes. Contact a Verizon Business Account Representative for additional information.

- *Test Suite for Retail VoIP Interoperability IP Trunking*
- *Retail VoIP Network Interface Specification (for non-registering devices)*

©2010 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.