

Avaya Solution & Interoperability Test Lab

Application Notes for Resource Software International Call Management Software with Avaya Communication Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the Resource Software International (RSI) Call Management Software (CMS) call accounting software to successfully interoperate with Avaya Communication Manager.

RSI CMS is a call accounting software that interoperates with Avaya Communication Manager over the Avaya Reliable Session Protocol (RSP). Call records can be generated for various types of calls. RSI CMS collects, and processes the call records. The serviceability, Local Survivable Process (LSP) mode, and performance tests were conducted to assess the reliability of the solution.

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

1. Introduction

The overall objective of this interoperability compliance testing is to verify that the RSI CMS call accounting software can interoperate with Avaya Communication Manager 5.1.2. RSI CMS connects to Avaya Communication Manager over the local or wide area network using a CDR link running on RSP. Avaya Communication Manager is configured to send CDR records to RSI CMS using a specific TCP/IP port. The serviceability, LSP mode, and performance tests were conducted to assess the reliability of the solution.

1.1. Interoperability Compliance Testing

The compliance test included feature, serviceability, performance, and LSP testing. The feature testing evaluated the ability of the CMS to collect and process CDR records for various types of calls. The unformatted format was utilized during the compliance test. The serviceability test introduced failure scenarios to see if the CMS can resume CDR collection after recovery. The performance test utilized bulk call volumes to generate a substantial amount of CDR records. The Avaya LSP solution was tested by removing the CLAN board in the Avaya G650 Media Gateway.

1.2. Support

Technical support for CMS can be obtained by contacting RSI via http://www.telecost.com/services.htm or by calling (905)576-4575.

2. Reference Configuration

Figure 1 illustrates a sample configuration that was used for the compliance test. The configuration consists of three Avaya Servers running Avaya Communication Manager. Site A is comprised of Avaya Communication Manager running on Avaya S8720 Servers with an Avaya G650 Media Gateway. Site B is comprised of Avaya Communication Manager running on an Avaya S8300 Server residing in an Avaya G700 Media Gateway. Each Avaya Communication Manager is connected to an IP network comprised of an Extreme Networks Summit 48 layer 3 switch. RSI CMS is running on a Windows 2003 Server was connected to the layer 3 switch, and has a RSP session established to each Avaya Communication Manager to collect CDR records. Each system has trunks and phones to generate calls. Avaya 4600 Series IP Telephones, Avaya 6400D Series Digital Telephones, and Avaya IP agent are registered to both Avaya S8720 and S8300 Servers. In addition, there is an H.323 IP trunk established between the two media servers.

Site C is comprised of an Avaya S8300 Server with an Avaya G350 Media Gateway, which has connections to an Avaya 4600 Series IP Telephone and an Avaya 6400D Series Digital Telephone. The Avaya S8300 Server, installed with a Local Survivable Processor (LSP) license, is setup as a LSP to Site A.

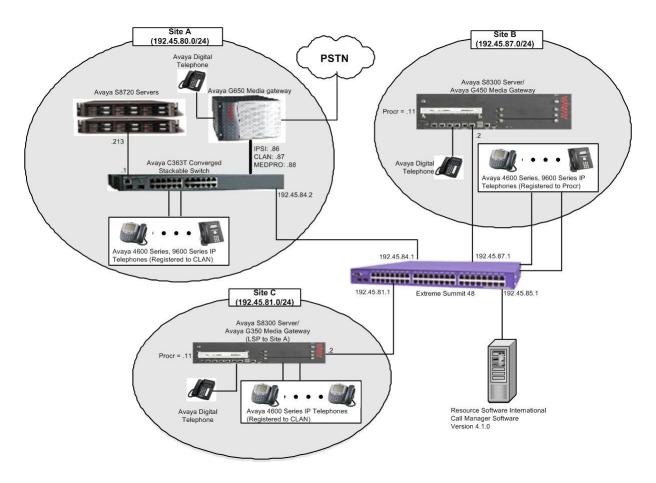


Figure 1. Test configuration of RSI CMS with Avaya Communication Manager

3. Equipment and Software Validated

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

	Equipment	Software					
Avaya S8720 Se	rvers	Avaya Communication Manager 5.1.2					
-		(R015x.01.2.416.4)					
Avaya G650 Me	dia Gateway						
	TN2312BP IPSI	HW11 FW030					
	TN799DP CLAN	HW20 FW017					
	TN2302AP MEDPRO	HW01 FW108					
Avaya S8300 Se	rver	Avaya Communication Manager 5.1.2					
-		(R015x.01.2.416.4)					
Avaya G700 Me	dia Gateway	28.17					
Avaya S8300 Se	rver (with LSP License)	Avaya Communication Manager 5.1.2					
		(R015x.01.2.416.4)					
Avaya G350 Me	dia Gateway	26.31					
Avaya 4600 Seri	es IP Telephone						
	4620SW	2.9					
	4625SW	2.9					
Avaya 9600 Seri	es IP Telephone						
	9630	2.0					
	9650	2.0					
Avaya 64xx Seri	es Digital Telephones						
	6408D+	-					
	6402D	-					
Analog Telephor	ne						
Avaya C363T C	onverged Stackable Switch (Layer 3)	4.5.14					
Extreme Summit	t 48 Switch (Layer 3)	4.1.21					
RSI CMS on Wi	ndows XP with Service Pack 3	4.1.0					

4. Configure Avaya Communication Manager

This section provides procedures for configuring the CDR feature in Avaya Communication Manager. All configuration changes in Avaya Communication Manager are performed through the System Access Terminal (SAT). These steps describe the procedure used for the Avaya S8720 Server. All steps are the same for the other Avaya Servers unless otherwise noted. Avaya Communication Manager will be configured to generate CDR records and send CDR records to the IP address of RSI CMS, using RSP over TCP/IP. For the Avaya S8720 Server, the CDR link originates at the IP address of the CLAN board, and terminates at the CMS. For the Avaya S8300 Server, the CDR link originates at the IP address of the local server (with node-name – "procr") and terminates at the CMS. The highlights in the following screens indicate the parameter values used during the compliance test.

Enter the **change node-names ip** command to create a new node name, for example, **RSI-CDR**. This node name is associated with the IP Address of the CMS. The IP address of S8300 is added in the IP NODE NAMES form for the LSP test. The CLAN entry on this form was previously administered.

change node-names	ip			Page	1 of	1
	IP NO	DDE NAMES				
Name	IP Address	Name	IP	Addres	s	
RSI-CDR	192.45.85.51			•		
CLAN	192.45 .80 .87					
MEDPRO	192.45 .80 .88					
S8300	192.45 .81 .11					
default	0 .0 .0 .0					
procr	192.45 .80 .214				•	

Enter the **change ip-services** command to define the CDR link to use RSP over TCP/IP. The following information should be provided:

- Service Type: CDR1 [If needed, a secondary link can be defined by setting Service Type to CDR2.]
- Local Node: CLAN [For Avaya S8720 Server, the Local Node is set to the node name of the CLAN board. If Avaya S8300 Server was utilized, set the Local Node to **procr**.]
- Local Port: 0 [The Local Port is fixed to 0.]
- Remote Node: **RSI-CDR** [The Remote Node is set to the node name defined previously.]
- Remote Port: **9000** [The Remote Port may be set to a value between 5000 and 64500 inclusive and must match the port configured in the CMS.]

change ip-s	change ip-services							
			IP SERVICE	IS				
Service	Enabled	Local	Local	Remote	Remote			
Type		Node	Port	Node	Port			
CDR1	Cl	LAN	0	RSI-CDR	9000			

On **Page 3**, enable the Reliable Session Protocol (RSP) for the CDR link by setting the Reliable Protocol field to **y**.

change ip-se	rvices				Page 3 of	4
Service Type	Reliable Protocol	SESSION Packet Resp Timer	LAYER TIMERS Session Connect Message Cntr	SPDU Cntr	Connectivity Timer	
CDR1	У	30	3	3	60	

Enter the **change system-parameters cdr** command from the SAT to set the parameters for the type of calls to track and the format of the CDR data. The example below shows the settings used during the compliance test. Provide the following information:

- CDR Date Format: month/day
- Primary Output Format: unformatted

• Primary Output Endpoint: CDR1

The remaining parameters define the type of calls that will be recorded and what data will be included in the record. See reference [2] for a full explanation of each field. The test configuration used some of the more common fields described below.

- Enable CDR Storage on Disk?: y [Enable the Survivable CDR feature. Default is n.]
- Use Legacy CDR Formats?: **n** [Allows CDR formats to use 5.x CDR formats. If the field is set to y, then CDR formats utilize the 3.x CDR formats.]
- Intra-switch CDR: y [Allows call records for internal calls involving specific stations. Those stations must be specified in the INTRA-SWITCH CDR form.]
- Record Outgoing Calls Only?: **n** [Allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls.]
- Outg Trk Call Splitting?: y [Allows a separate call record for any portion of an outgoing call that is transferred or conferenced.]
- Inc Trk Call Splitting?: y [Allows a separate call record for any portion of an incoming call that is transferred or conferenced.]

```
change system-parameters cdr
                                                                              Page 1 of 1
                                  CDR SYSTEM PARAMETERS
 Node Number (Local PBX ID): 1
                                                              CDR Date Format: month/day
      Primary Output Format: unformatted Primary Output Endpoint: CDR1
    Secondary Output Format:
       Use ISDN Layouts? n
Use Enhanced Formats? n

Use Legacy CDR Formats? n

Condition Code 'T' For Redirected Calls? y

Remove # From Called Number? n
                                              Remove # From Called Number? n
  Dedified Circuit ID Display? n

Record Outgoing Calls Only? n

Suppress CDR for Ineffective Call Attempts? y
Disconnect Information in Place of FRL? y

Intra-switch CDR? y

Outg Trk Call Splitting? y

Outg Attd Call Record? n

Interworking Feat-flag? n
Modified Circuit ID Display? n
 Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
                                      Calls to Hunt Group - Record: member-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? n Record Agent ID on Outgoing? n
  Inc Trk Call Splitting? y
Record Non-Call-Assoc TSC? n
                                                Call Record Handling Option: warning
      Record Call-Assoc TSC? n Digits to Record for Outgoing Calls: dialed
   Privacy - Digits to Hide: 0
                                                     CDR Account Code Length: 6
```

If the Intra-switch CDR field is set to y on Page 1 of the system-parameters cdr form, then enter the **change intra-switch-cdr** command to define the extensions that will be subject to call detail records. In the Assigned Members field, enter the specific extensions whose usage will be tracked.

Note: To simplify the process of adding multiple extensions in the Extension field, the Intraswitch CDR by COS feature may be utilized in the SPECIAL APPLICATIONS form under the system-parameters section. To utilize this feature, contact an authorized Avaya account representative to obtain the license.

```
change intra-switch-cdr

INTRA-SWITCH CDR

Assigned Members: 5 of 5000 administered

Extension Extension Extension

22001
22002
22003
22007
22009
26001
26007
```

For each trunk group for which CDR records are desired, verify that CDR reporting is enabled. Use the **change trunk-group** *n* command, where *n* is the trunk group number, to verify that the CDR Reports field is set to y. This applies to all types of trunk groups.

```
TRUNK GROUP

Group Number: 80 Group Type: isdn CDR Reports: y
Group Name: OUTSIDE CALL COR: 1 TN: 1 TAC: 103
Direction: two-way Outgoing Display? y Carrier Medium: PRI/BRI
Dial Access? y Busy Threshold: 255 Night Service:
Queue Length: 0
Service Type: tie Auth Code? n TestCall ITC: rest
Far End Test Line No:

TestCall BCC: 4
TRUNK PARAMETERS
Codeset to Send Display: 6 Codeset to Send National IEs: 6
Max Message Size to Send: 260 Charge Advice: none
Supplementary Service Protocol: a Digit Handling (in/out): enbloc/enbloc

Trunk Hunt: cyclical
Digital Loss Group: 13
Incoming Calling Number - Delete: Insert: Format:
Bit Rate: 1200 Synchronization: async Duplex: full
Disconnect Supervision - In? y Out? y
Answer Supervision Timeout: 0
```

5. Configure the Avaya LSP Solution

This section describes how to configure the main Avaya Communication Manager and a LSP licensed Avaya Communication Manager to perform an Avaya LSP CDR solution. This section also includes the verification steps.

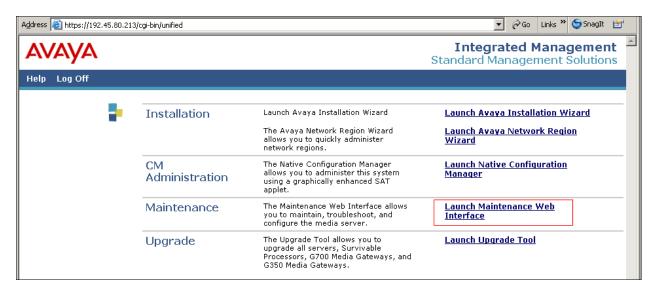
5.1. Configure the S8720 Server with G650 Media Gateway for the Avaya LSP Solution

This section describes how to configure the S8720 Server with a G650 Media Gateway for the Avaya LSP CDR Solution. The following steps must be performed:

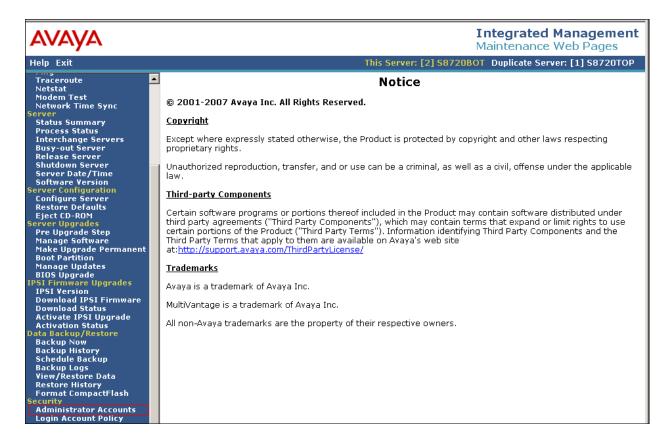
- Create member credentials (username/password) for a sftp account
- Change "survivable-processor <assigned Survivable Processor node-name>" form
- Save the translation for LSP

5.1.1. CDR credentials for sftp

To create credentials, enter <a href="https://<IP address of Avaya S8720 Server">https://<IP address of Avaya S8720 Server in the URL, and log in with the appropriate credentials for accessing the Integrated Management Standard Management Solutions pages. Select the Launch Maintenance Web Interface link.

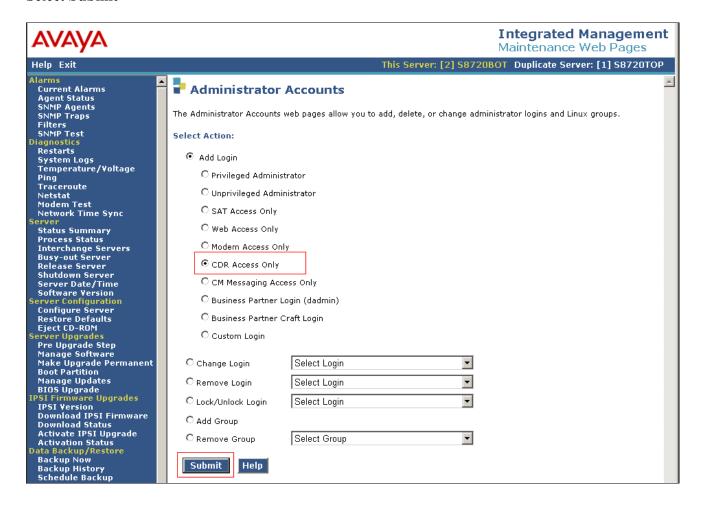


Select the **Administrator Accounts** link under the Security section.



In the Administrator Accounts page, check the CDR Access Only box under the Add Login section.

Select Submit

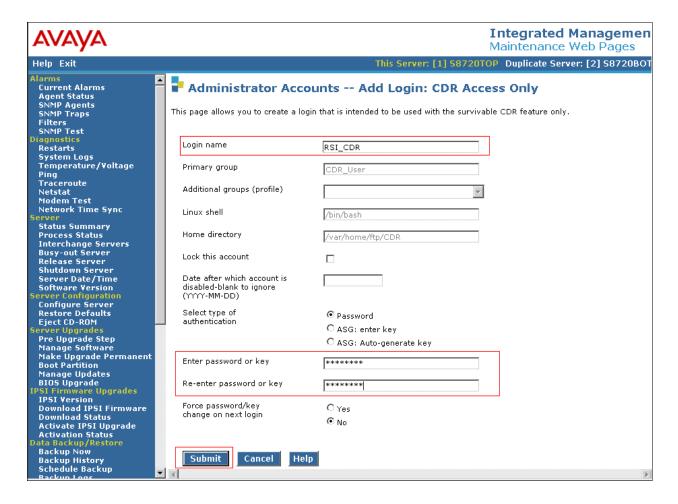


In the Administrator Accounts –Add Login: CDR Access Only page, provide the following information:

- Login name
- Enter password or key
- Re-enter password or key

The above credentials will be utilized to access the LSP licensed Avaya Communication Manager.

Click on Submit



5.1.2. Survivable-Processor Form

Enter the **change survivable-processor S8300** command, where **S8300** is an LSP licensed Avaya S8300 Server, configured in **Section 3**. Make sure that the Enabled field is set to **o** (overwrite), and the Store to dsk field is to **y**.

change sur	vivable-p	rocessor	S8300			Page	2 of	3	
SURVIVABLE PROCESSOR - IP-SERVICES									
Service	Enabled	Store	Local	Local	Remote		Remo	ote	
Type		to dsk	Node	Port	Node		Port	5	
CDR1	0	У							

After Section 4.1.1 and 4.1.2 are completed, run either the save translation all or save translation lsp command from Avaya S8720 Server, so that the translation in Avaya S8720 Server will be pushed to the LSP licensed Avaya S8300 Server.

To confirm whether the translation is pushed to the LSP licensed Avaya Communication Manager, execute the **list survivable-processor** command on both Avaya Communication Managers (S8720 and S8300), and check the last Translations Updated field, and they should match. The following shows a sample screen, resulted from performing the above command.

list surviv	vable-processor	•		
Name	Туре	SURVIVABLE PROCESSORS IP Address Reg LSP Act	Translations Updated	Net Rgn
S8300	LSP	192.45 .81 .11 y n	22:00 4/1/2009	1

5.2. Verification from the Avaya S8300 Server for the Avaya LSP Solution

This section describes how to verify the Avaya LSP CDR solution from the Avaya S8300 Server. Enter the **display ip-services** command. Notice that the Local Node field is changed to **procr**.

display	ip-services				Page	1 of	4	
			IP SERVICES					
Service	Enabled	Local	Local	Remote	Remote			
Type		Node	Port	Node	Port			
CDR1	pi	rocr	0	RSI-CDR	9000			

Enter the **display survivable-processor S8300** command, and verify that the survivable-processor S8300 form in Avaya S8720 and S8300 Servers are identical.

display s	urvivable-	processo	r S8300			Page	2	of	3	
SURVIVABLE PROCESSOR - IP-SERVICES										
Service	Enabled	Store	Local	Local	Remote			Remo	te	
Type		to dsk	Node	Port	Node			Port		
CDR1	0	У								

5.3. Verification from the Avaya Media Gateway for the Avaya LSP Solution

This section describes how to verify the Avaya LSP CDR solution from the Avaya G350 Media Gateway. Telnet into the media gateway, and run the **show mgc** command. As the following screen showed, the active controller has changed from 192.45.80.87 (prior to LSP) to 192.45.81.11 (post LSP).

6. Configure Resource Software International Call Management Software

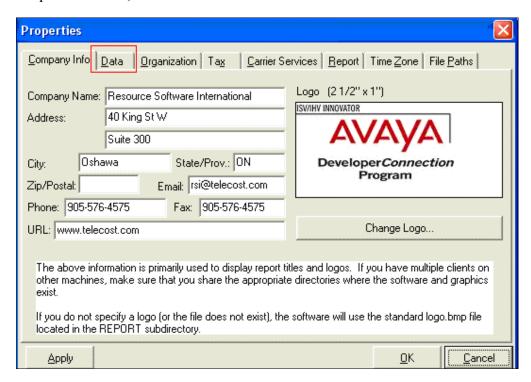
This section describes the operation of RSI CMS. The CMS connects to Avaya Communication Manager via RSP over the TCP/IP port. CDR data is sent from Avaya Communication Manager (CLAN port) into the CMS where the raw data is transformed into call records, which are then immediately available for reporting. RSI installs, configures, and customizes the CMS application for their end customers. The following sections, Section 5.1 and 5.2, describe how to configure the CDR format and RSP, respectively.

6.1. Configure the CDR format

Navigate to **All Programs** → **RSI** → **CMS**, and launch the CMS icon. From the SHADOW Voice and Data Management [cms] screen, navigate to **File** → **Properties**.

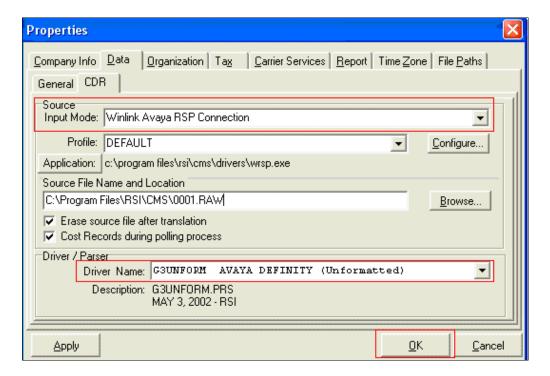


From the Properties screen, click the **Data** tab.



Using the drop-down menu, select the Winlink Avaya RSP Connection for the Source Input Mode field and G3UNFORM AVAYA DEFINITY (Unformatted) for the Driver Name field.

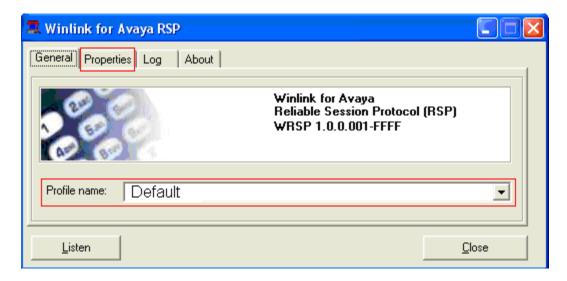
Click the **OK** button to save.



6.2. Configure the RSP

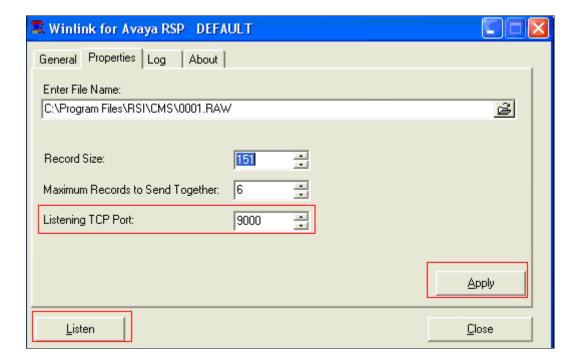
Navigate to **All Programs** → **RSI** → **CMS**, and launch the WRSP icon. Under the General tab, enter a descriptive name for the Profile Name field.

Click on the **Properties** tab.

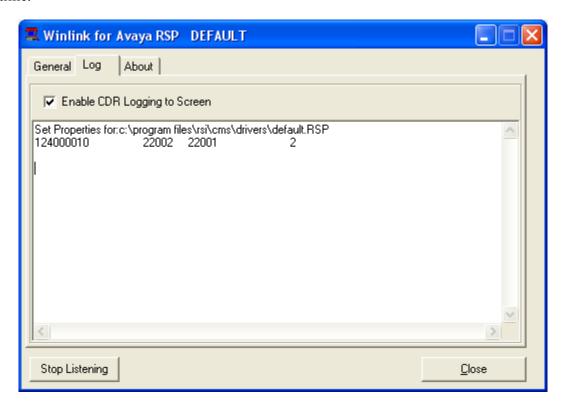


The following screen shows the default RSP port 9000. The Listening TCP Port field can be changed to any value that matches the Avaya Communication Manager. Click **Apply** to save any changes to this screen.

Click the **Listen** button to start the WRSP listening for a RSP connection



Click the checkbox, **Enable CDR Logging to Screen**, in order to view the incoming CDR in real time.



7. General Test Approach

The general test approach was to manually place intra-switch and inter-switch calls, inbound trunk and outbound trunk calls to and from telephones attached to the Avaya Servers, and verified that the CMS collected the CDR records and properly classified and reported the attributes of the call. For serviceability testing, physical and logical links were disabled/reenabled, Avaya Servers were reset and the CMS was restarted. The LSP test was performed from the CMS using the sftp command to Avaya S8300 Server (LSP) to collect the CDR records. For performance testing, a call generator was used to place calls over an extended period of time.

7.1. Test Results

All executed test cases passed. RSI CMS successfully collected the CDR records from Avaya Communication Manager via a RSP connection for all types of calls generated including intraswitch calls, inbound/outbound PSTN trunk calls, inbound/outbound private IP trunk calls, transferred calls, and conference calls. For serviceability testing, RSI CMS was able to resume collection of CDR records after failure recovery including buffered CDR records for calls that were placed during the outages. RSI CMS also successfully collected the CDR records from the Avaya S8300 Server using the sftp command. Performance tests verified that RSI CMS could collect call records during a sustained, high volume of calls.

8. Verification Steps

The following steps may be used to verify the configuration:

- On the SAT of the Avaya S8720 Server, enter the **status cdr-link** command and verify that the CDR link state is up.
- Place a call and verify that RSI CMS received CDR records for the call. Compare the values of the data fields in the CDR record with the expected values, and verify that they match.
- Place internal, inbound trunk, and outbound trunk calls to and from various telephones, generate an appropriate report in RSI CMS, and verify the report's accuracy.

9. Conclusion

These Application Notes describe the procedures for configuring RSI CMS to collect call detail records from Avaya Communication Manager running on Avaya Servers. RSI CMS successfully passed all compliance testing.

10. References

This section references the Avaya and RSI documentation that are relevant to these Application Notes.

The following Avaya product documentation can be found at http://support.avaya.com. [1] *Administrator Guide for Avaya Communication Manager*, Issue 4, January 2008, Document Number 03-300509.

[2] Feature Description and Implementation For Avaya Communication Manager, Issue 6, January 2008, Document Number 555-245-205

©2009 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and TM 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.