



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for CVT Periscope 3L Call Reporting with Avaya Communication Manager - Issue 1.0

### Abstract

These Application Notes describe the configuration steps required for CVT Periscope 3L Call Reporting to interoperate with Avaya Communication Manager.

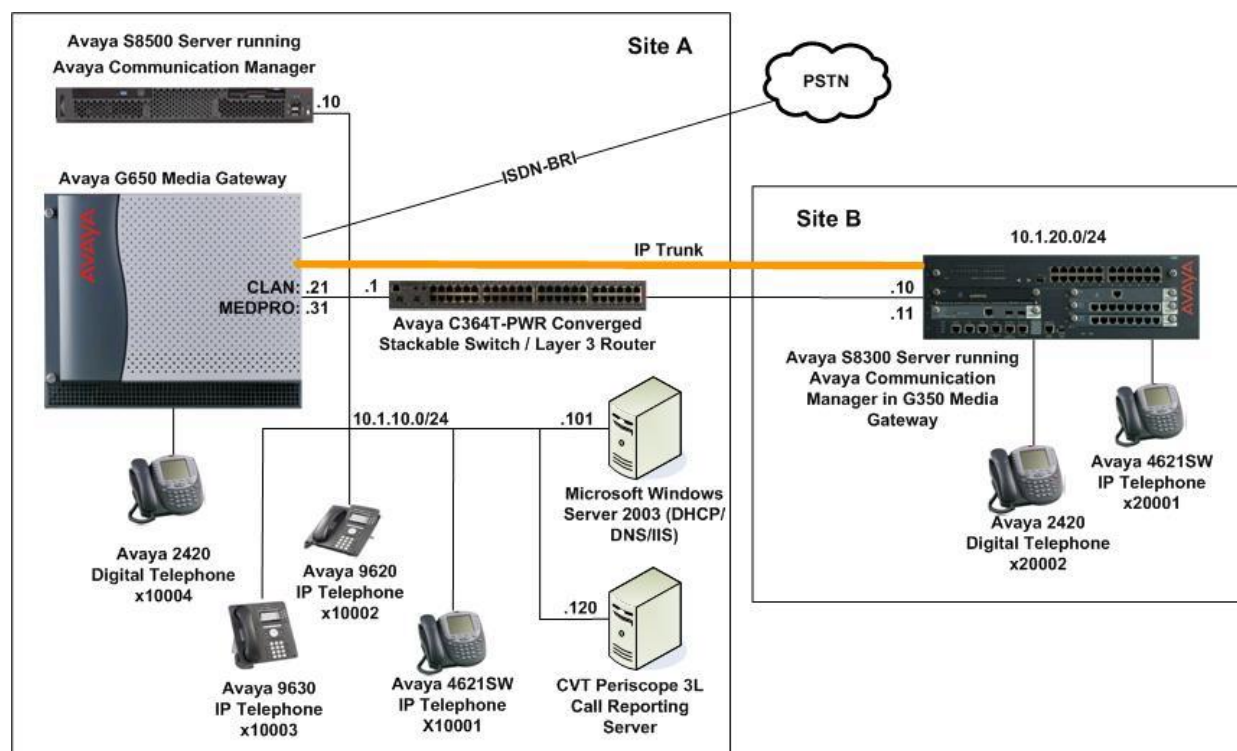
CVT Periscope 3L is a web based reporting tool for the collation, analysis and reporting on call records generated by the Avaya Communication Manager. CVT Periscope 3L interoperates with Avaya Communication Manager over a Call Detail Recording (CDR) link using a Transmission Control Protocol (TCP) socket connection. Call records can be generated for various types of calls and CVT Periscope 3L collects and processes the call records. Feature and serviceability tests were conducted to assess the reliability of the solution.

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

# 1. Introduction

The objective of this interoperability compliance testing is to verify that CVT Periscope 3L Call Reporting Version 3.0 can interoperate with Avaya Communication Manager 4.0.1. CVT Periscope 3L is a web based reporting tool for the collation, analysis and reporting on call records generated by the Avaya Communication Manager. The interface to Avaya Communication Manager is through a TCP socket connection. CVT Periscope 3L can collect CDR records from multiple Avaya Communication Managers. The CDR collection was verified for two Avaya Communication Managers during the compliance testing.

**Figure 1** illustrates the network configuration used to verify the CVT Periscope 3L solution. Site A is comprised of an Avaya S8500 Server and a G650 Media Gateway, and has connections to the following: Avaya 4600 and 9600 Series IP Telephones, Avaya 2400 Series Digital Telephones, and an ISDN-BRI trunk to the PSTN. CVT Periscope 3L is installed on a server running Microsoft Windows Server 2003 with Service Pack 1. Site B is comprised of an Avaya S8300 Server with a G350 Media Gateway, and has connections to an Avaya 4600 Series IP Telephone and an Avaya 2400 Series Digital Telephone. The Avaya C364T-PWR Converged Stackable Switch provides Ethernet connectivity to the servers and IP telephones and Layer 3 IP routing between the two sites. An IP trunk is configured between Site A and B for the users to call between the two sites.



**Figure 1: Test configuration**

## 2. Equipment and Software Validated

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

Equipment	Software
Avaya S8500 Server	Avaya Communication Manager 4.0.1 (R014x.00.1.731.2)
Avaya G650 Media Gateway - TN2312BP IP Server Interface - TN799DP C-LAN Interface - TN2302AP IP Media Processor - TN2602AP IP Media Processor	- HW07, FW40 HW01, FW24 HW20, FW117 HW02, FW31
Avaya S8300 Server	Avaya Communication Manager 4.0.1 (R014x.00.1.731.2)
Avaya G350 Media Gateway	26.33.0
Avaya 4600 Series IP Telephones - 4621SW	2.8 (H.323)
Avaya 9600 Series IP Telephones - 9620 - 9630	1.5 (H.323) 1.5 (H.323)
Avaya 2400 Series Digital Telephone	-
Avaya C364T-PWR Converged Stackable Switch	4.5.14
CVT Periscope 3L Call Reporting	3.0

## 3. Configure Avaya Communication Manager

This section provides the procedures for configuring Call Detail Recording (CDR) 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 S8500 Server. All steps are the same for the other S8XXX servers unless otherwise noted. An Avaya Communication Manager is configured to generate and send the CDR records to the IP address of the CVT Periscope 3L server over a TCP socket connection. For this configuration, the CDR links are configured to originate from the IP addresses of the Avaya S8500 and S8300 Servers (i.e. with node-name – “procr”) and terminates at the IP address of the CVT Periscope server. The highlights in the following screens indicate the parameter values used during the compliance test.

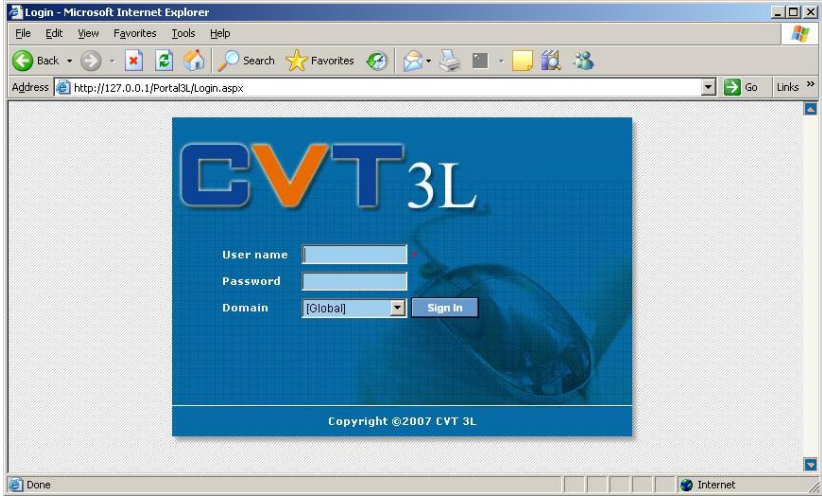
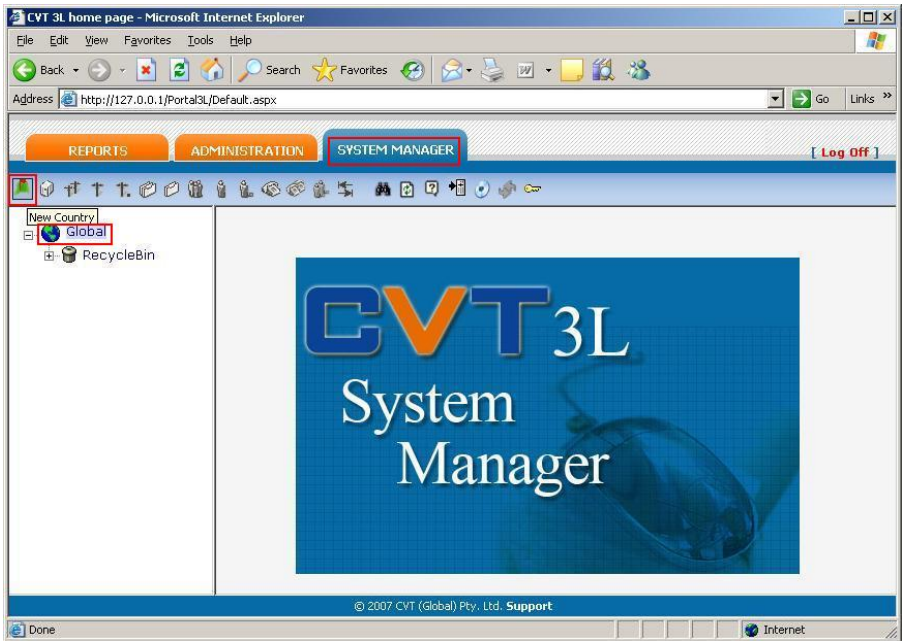
Step	Description																																				
1.	<p>Use the <b>change node-names ip</b> command to add a new node name for the CVT Periscope 3L server.</p> <div><div>change node-names ip</div><div>Page1 of 1</div></div> <table><tr><th colspan="2">IP NODE NAMES</th></tr><tr><th>Name</th><th>IP Address</th></tr><tr><td>default</td><td>0.0.0.0</td></tr><tr><td>procr</td><td>10.1.10.10</td></tr><tr><td>Periscope</td><td>10.1.10.120</td></tr></table>	IP NODE NAMES		Name	IP Address	default	0.0.0.0	procr	10.1.10.10	Periscope	10.1.10.120																										
IP NODE NAMES																																					
Name	IP Address																																				
default	0.0.0.0																																				
procr	10.1.10.10																																				
Periscope	10.1.10.120																																				
2.	<p>Use the <b>change ip-services</b> command to define the CDR link. To define a primary CDR link, the following information should be provided:</p> <ul style="list-style-type: none"><li>• <b>Service Type: CDR1</b> [If needed, a secondary link can be defined by setting Service Type to CDR2.]</li><li>• <b>Local Node: procr</b></li><li>• <b>Local Port: 0</b> [The Local Port is fixed to 0 because Avaya Communication Manager initiates the CDR link.]</li><li>• <b>Remote Node: Periscope</b> [The Remote Node is set to the node name previously defined in Step 1.]</li><li>• <b>Remote Port: 9000</b> [The Remote Port may be set to a value between 5000 and 64500 inclusive, and must match the port configured in CVT Periscope 3L server in Section 4 Step 5.]</li></ul> <div><div>change ip-services</div><div>Page1 of 4</div></div> <table><tr><th colspan="6">IP SERVICES</th></tr><tr><th>Service Type</th><th>Enabled</th><th>Local Node</th><th>Local Port</th><th>Remote Node</th><th>Remote Port</th></tr><tr><td>CDR1</td><td></td><td>procr</td><td>0</td><td>Periscope</td><td>9000</td></tr></table> <p>On Page 3 of the IP SERVICES form, disable the Reliable Session Protocol (RSP) for the CDR link by setting the <b>Reliable Protocol</b> field to <b>n</b>.</p> <div><div>change ip-services</div><div>Page3 of 4</div></div> <table><tr><th colspan="6">SESSION LAYER TIMERS</th></tr><tr><th>Service Type</th><th>Reliable Protocol</th><th>Packet Resp Timer</th><th>Session Connect Message Cntr</th><th>SPDU Cntr</th><th>Connectivity Timer</th></tr><tr><td>CDR1</td><td>n</td><td>30</td><td>3</td><td>3</td><td>60</td></tr></table>	IP SERVICES						Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port	CDR1		procr	0	Periscope	9000	SESSION LAYER TIMERS						Service Type	Reliable Protocol	Packet Resp Timer	Session Connect Message Cntr	SPDU Cntr	Connectivity Timer	CDR1	n	30	3	3	60
IP SERVICES																																					
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port																																
CDR1		procr	0	Periscope	9000																																
SESSION LAYER TIMERS																																					
Service Type	Reliable Protocol	Packet Resp Timer	Session Connect Message Cntr	SPDU Cntr	Connectivity Timer																																
CDR1	n	30	3	3	60																																

Step	Description
3.	<p>Enter the <b>change system-parameters cdr</b> command 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.</p> <ul style="list-style-type: none"> <li>• <b>CDR Date Format: month/day</b></li> <li>• <b>Primary Output Format: unformatted</b></li> <li>• <b>Primary Output Endpoint: CDR1</b></li> </ul> <p>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.</p> <ul style="list-style-type: none"> <li>• <b>Use Legacy CDR Formats? n</b> [Specify the use of the new CM 4.0.1 and later formats in the CDR records produced by the system.]</li> <li>• <b>Intra-switch CDR: y</b> [Allows call records for internal calls involving specific stations. Those stations must be specified in the INTRA-SWITCH-CDR form.]</li> <li>• <b>Record Outgoing Calls Only? n</b> [Allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls.]</li> <li>• <b>Outg Trk Call Splitting? y</b> [Allows a separate call record for any portion of an outgoing call that is transferred or conferenced.]</li> <li>• <b>Inc Trk Call Splitting? y</b> [Allows a separate call record for any portion of an incoming call that is transferred or conferenced.]</li> </ul> <div> <div>change system-parameters cdr</div> <div>Page 1 of 1</div> <div>CDR SYSTEM PARAMETERS</div> <div> Node Number (Local PBX ID): 1 <div>CDR Date Format: month/day</div> <div>Primary Output Format: unformatted</div> <div>Primary Output Endpoint: CDR1</div> Secondary Output Format: <div>Use ISDN Layouts? n</div> <div>Enable CDR Storage on Disk? n</div> <div>Use Enhanced Formats? n</div> <div>Condition Code 'T' For Redirected Calls? n</div> <div>Use Legacy CDR Formats? n</div> <div>Remove # From Called Number? n</div> Modified Circuit ID Display? y <div>Intra-switch CDR? y</div> <div>Record Outgoing Calls Only? n</div> <div>Outg Trk Call Splitting? y</div> <div>Suppress CDR for Ineffective Call Attempts? y</div> <div>Outg Attd Call Record? y</div> <div>Disconnect Information in Place of FRL? n</div> <div>Interworking Feat-flag? n</div> Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n <div>Calls to Hunt Group - Record: group-ext</div> Record Called Vector Directory Number Instead of Group or Member? n Record Agent ID on Incoming? n <div>Record Agent ID on Outgoing? y</div> <div>Inc Trk Call Splitting? y</div> <div>Inc Attd Call Record? n</div> Record Non-Call-Assoc TSC? n <div>Call Record Handling Option: warning</div> Record Call-Assoc TSC? n <div>Digits to Record for Outgoing Calls: dialed</div> Privacy - Digits to Hide: 0 <div>CDR Account Code Length: 5</div> </div> </div> <p>If the <b>Intra-switch CDR</b> field is set to <b>y</b> on Page 1 of the CDR SYSTEM PARAMETERS form, then use the <b>change intra-switch-cdr</b> command to define the extensions that will be subjected to call detail records. In the <b>Assigned Members</b> field, enter the specific extensions whose usage will be tracked with the CDR records.</p>

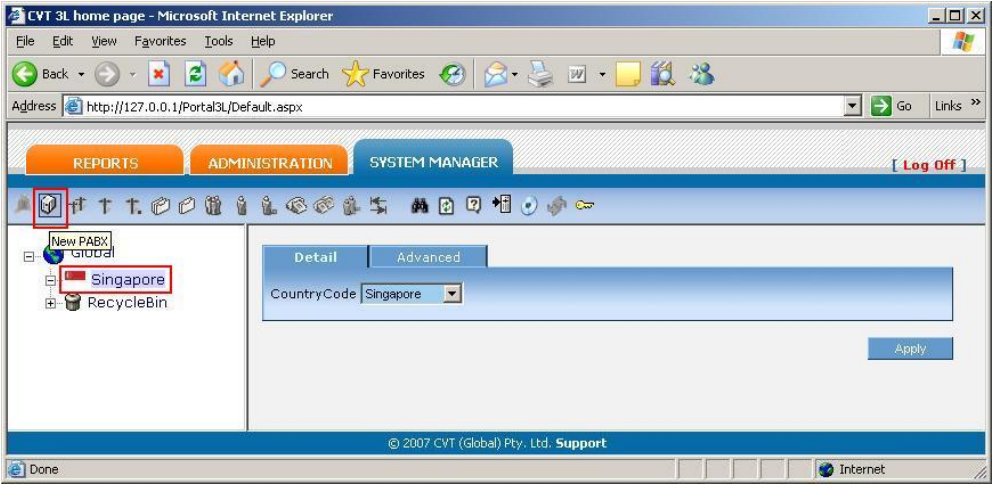
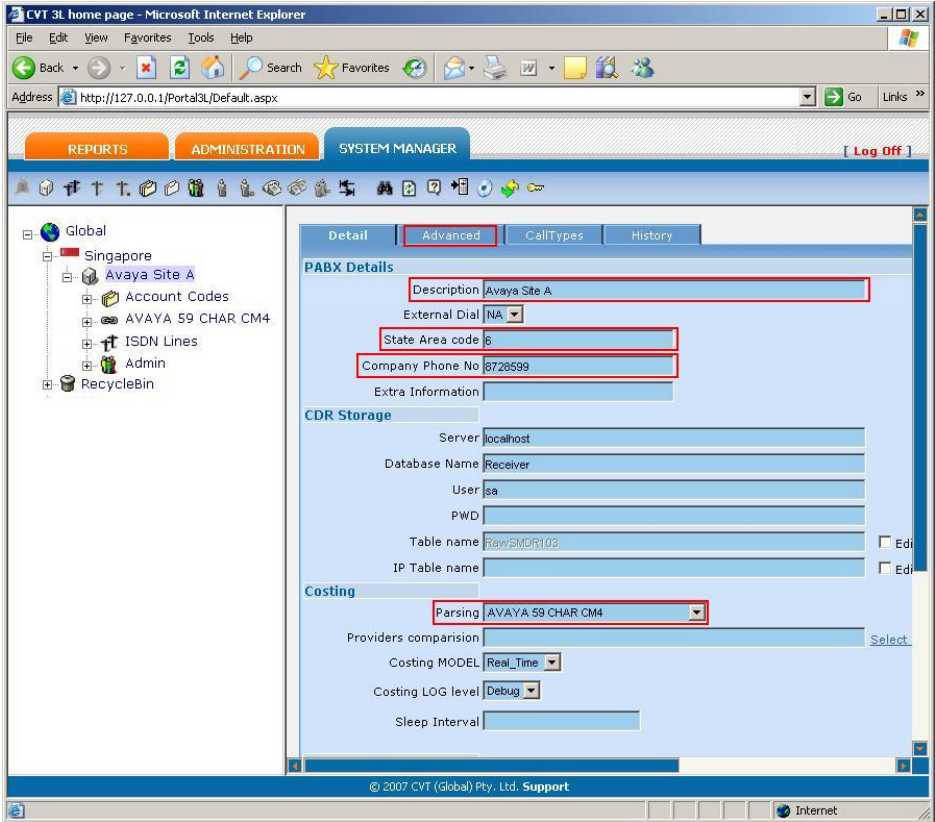
Step	Description
	<div>change intra-switch-cdr<div>Page1 of 3</div><div>INTRA-SWITCH CDR</div><div>Assigned Members: 4 of 5000 administered</div><div>ExtensionExtensionExtensionExtension</div><div>10001</div><div>10002</div><div>10003</div><div>10004</div></div>
4.	<div>For each trunk group for which CDR records are desired, verify that CDR reporting is enabled. Use the <b>change trunk-group <i>n</i></b> command, where <i>n</i> is the trunk group number, to verify that the CDR Reports field is set to <b>y</b>. This applies to all types of trunk groups.</div>
	<div>change trunk-group 2<div>Page1 of 21</div><div>TRUNK GROUP</div><div>Group Number: 2Group Type: isdnCDR Reports: y</div><div>Group Name: Singtel BRI Line 2COR: 95TN: 1TAC: 702</div><div>Direction: two-wayOutgoing Display? nCarrier Medium: PRI/BRI</div><div>Dial Access? yBusy Threshold: 255Night Service: 10004</div><div>Queue Length: 0</div><div>Service Type: public-ntwrkAuth Code? nTestCall ITC: rest</div><div>Far End Test Line No:</div><div>TestCall BCC: 4</div></div>

## 4. Configure CVT Periscope 3L Call Reporting

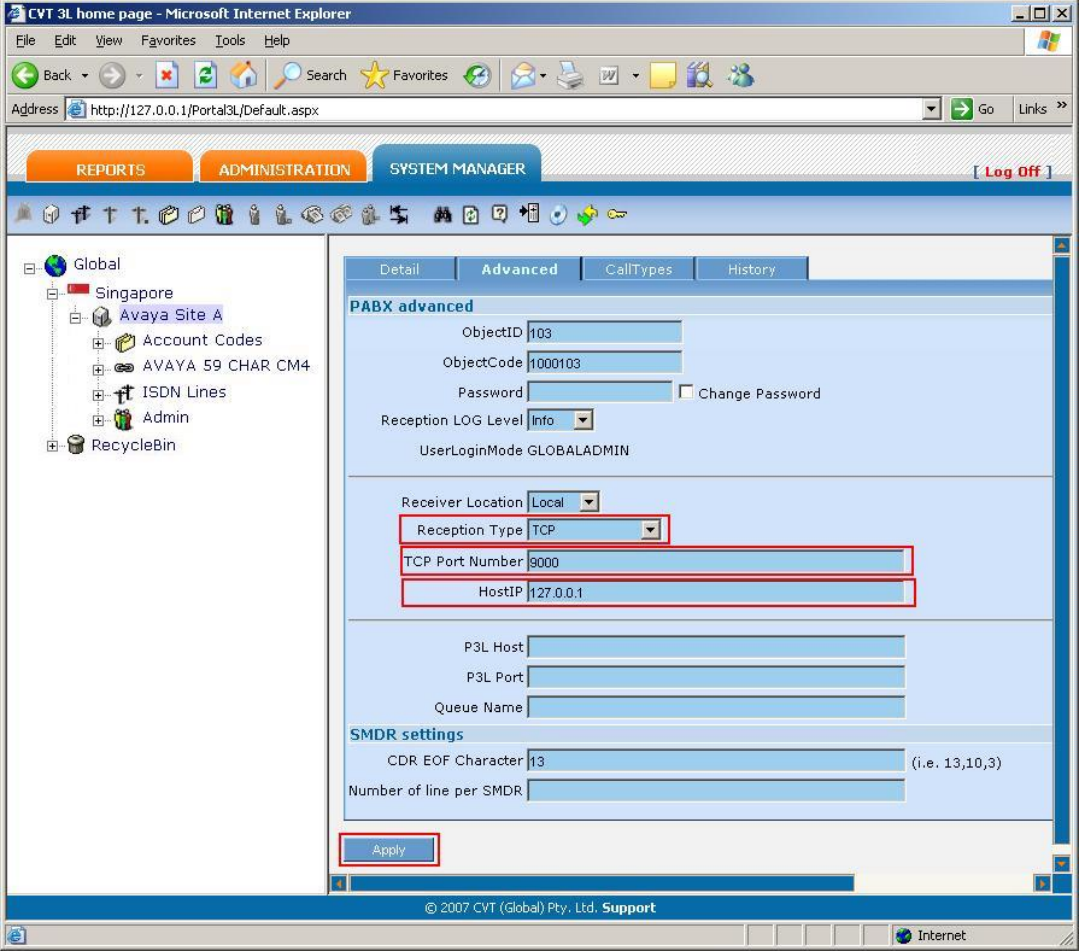
This section describes the configuration of CVT Periscope 3L.

Step	Description
1.	<p>Using the web browser on the CVT Periscope 3L server, browse to the URL <code>http://&lt;ip-address&gt;/Portal3L/Login.aspx</code> to log in to the CVT Periscope 3L web-based administration, where <code>&lt;ip-address&gt;</code> is the location of the CVT Periscope 3L server. Enter the <b>User Name</b> and <b>Password</b> provided by CVT and click <b>Sign In</b>.</p> 
2.	<p>Click on the <b>SYSTEM MANAGER</b> tab and then on <b>Global</b> in the left window. Click on the <b>New Country</b> button and enter the country name to create a new country object.</p> 



Step	Description
3.	<p>Click on the country object created in Step 2 in the left window and click the <b>New PABX</b> button to add an entry for the Avaya Communication Manager in Site A.</p> 
4.	<p>Enter a descriptive name for <b>Description</b>. Enter the appropriate values for <b>State Area code</b> and <b>Company Phone No.</b> Select <b>AVAYA 59 CHAR CM4</b> for the field <b>Parsing</b>. Click on the <b>Advanced</b> tab to continue.</p> 



Step	Description
5.	<p>In the PABX <b>Advanced</b> tab, specify the parameters for the CVT Periscope 3L Receiver. Select <b>TCP</b> for <b>Reception Type</b> and <b>127.0.0.1</b> for <b>HostIP</b>, which says that the Periscope Host machine is located on this server. The <b>TCP Port Number</b> must match the value of the <b>Remote Port</b> field administered on the Avaya Communication Manager in Section 3 Step 2. Click <b>Apply</b>.</p> 
6.	<p>Repeat Steps 3 to 5 to add a second entry for the Avaya Communication Manager in Site B. Note that the <b>TCP Port Number</b> must be different for the second Avaya Communication Manager.</p>

## 5. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing. The feature testing evaluated the ability of CVT Periscope 3L to collect and process CDR records for various types of calls. The serviceability test introduced failure scenarios to see if CVT Periscope 3L can resume CDR collection after failure recovery.

## 5.1. General Test Approach

The general test approach was to manually place intra-switch calls, inter-switch calls, inbound and outbound PSTN trunk calls to and from telephones on the Avaya Communication Managers, and verify that CVT Periscope 3L collects the CDR records and reports the correct attributes of the call. For serviceability testing, the CDR links on Avaya Communication Managers were disabled and re-enabled and the Avaya SXXX servers were also rebooted.

## 5.2. Test Results

All feature tests passed. CVT Periscope 3L successfully captured and processed call records from Avaya Communication Manager. CVT Periscope 3L also successfully processed the CDR data, and produced call accounting reports. The types of calls generated during the compliance test include intra-switch calls, inbound/outbound PSTN trunk calls, inbound/outbound inter-switch IP trunk calls, transferred calls and conferenced calls.

For serviceability testing, the following observations were made.

- CVT Periscope 3L does not use the Avaya Reliable Session Protocol (RSP). As such, CDR records are lost when the CVT Periscope 3L is disconnected from the LAN or when rebooted.

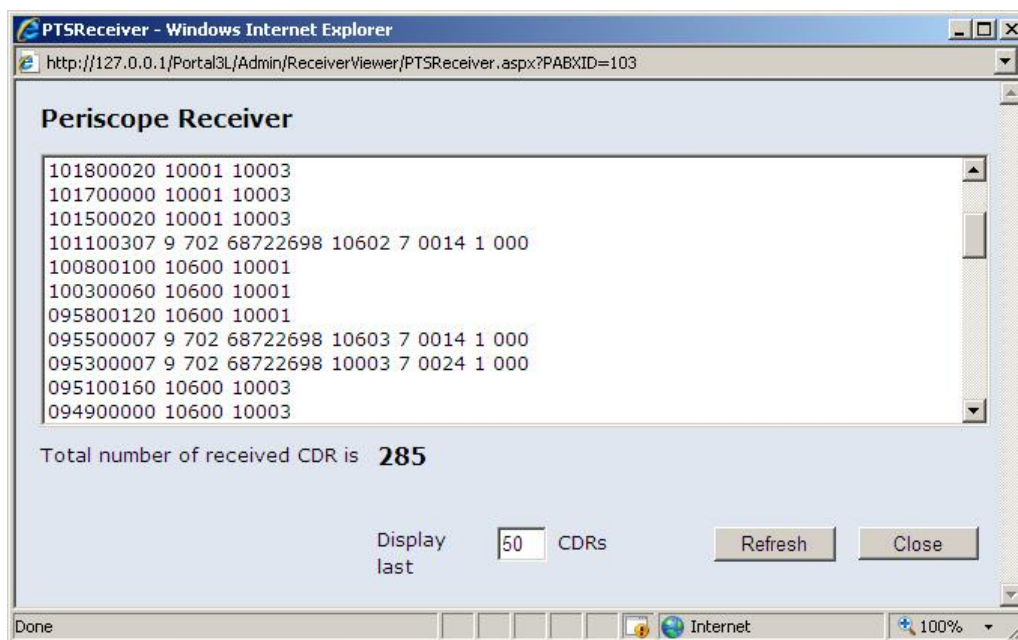
## 6. Verification Steps

The following steps may be used to verify the configuration:

- Use the **ping** utility on the CVT Periscope 3L server to verify the IP connectivity to the Avaya S8XXX Servers.
- On the SAT of each Avaya S8XXX Server, enter the **status cdr-link** command and verify that the Link State shows up.

status cdr-link	
CDR LINK STATUS	
Primary	Secondary
Link State: <b>up</b>	CDR not administered
Date & Time: 2007/8 /20 9 :40:34	0 /0 /0 0 :0 :0
Forward Seq. No: 134	0
Backward Seq. No: 325	0
CDR Buffer % Full: 0.00	0.00
Reason Code: OK	

- Place a call and verify that CVT Periscope 3L receives the CDR record for the call. Compare the values of 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 CVT Periscope 3L and verify the report's accuracy.

## 7. Support

Technical support for CVT Periscope 3L can be obtained by contacting CVT's Support Desk at +61 (2) 94253300, or sending an e-mail to [support@cvt.com.au](mailto:support@cvt.com.au).

## 8. Conclusion

These Application Notes describe the procedures for configuring the CVT Periscope 3L Call Reporting to collect call detail records from Avaya Communication Manager. CVT Periscope 3L successfully passed the compliance testing.

## 9. References

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

The following Avaya product documentation can be found at <http://support.avaya.com>.

[1] *Feature Description and Implementation For Avaya Communication Manager*, Release 4.0, Issue 5, February 2007, Document Number 555-245-205.

[2] *Administrator Guide for Avaya Communication Manager*, Release 4.0, Issue 3, February 2007, Document Number 03-300509.

The following Periscope 3L Call Reporting documentations are provided by CVT.

[3] *CVT Periscope 3L Installation Guide*, Version 3.0.

[4] *CVT Periscope 3L Administration Guide*, Version 3.0.

---

**©2007 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 Developer*Connection* Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).