Avaya Solution & Interoperability Test Lab

Application Notes for Pan Cyber Dialguard with Avaya Communication Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Pan Cyber Dialguard to interoperate with Avaya Communication Manager.

Pan Cyber Dialguard is Windows-based call accounting software designed for single and multi-site enterprises. Pan Cyber Dialguard 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 Pan Cyber Dialguard collects and processes the call records.

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 objective of this interoperability compliance testing is to verify that Pan Cyber Dialguard 2.0 can interoperate with Avaya Communication Manager 4.0.1. The interface to Avaya Communication Manager is through a Transmission Control Protocol (TCP) socket connection. Pan Cyber Dialguard can collect Call Detail Recording (CDR) records from multiple Avaya Communication Manager systems. However, for this compliance testing, the CDR collection was verified for one Avaya Communication Manager system.

Figure 1 illustrates the network configuration used to verify the Pan Cyber Dialguard solution. Site A is comprised of an Avaya S8500 Server and an Avaya 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. Pan Cyber Dialguard is installed on a PC running Microsoft Windows XP Professional with Service Pack 2. Site B is comprised of an Avaya S8300 Server with an Avaya G250 Media Gateway, and has connections to two Avaya 9600 Series IP Telephones. 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.

Note that only the Avaya S8500 Server in Site A is configured to send CDR records to Pan Cyber Dialguard. Site B is used only to generate IP trunk calls to Site A.

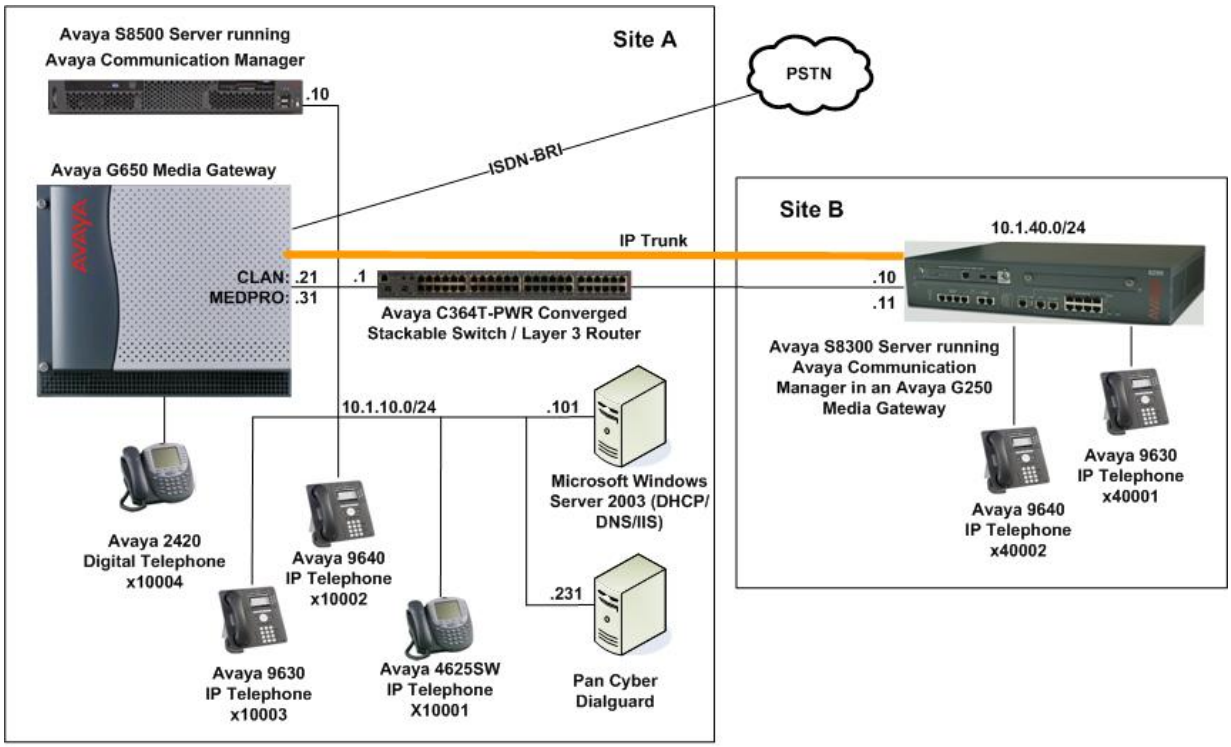


Figure 1: Test Configuration

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 G250 Media Gateway	26.33.0
Avaya 4625SW IP Telephone	2.8.3 (H.323)
Avaya 9630 IP Telephones	1.5 (H.323)
Avaya 9640 IP Telephones	1.5 (H.323)
Avaya 2420 Digital Telephone	-
Avaya C364T-PWR Converged Stackable Switch	4.5.18
Pan Cyber Dialguard	2.0

3. Avaya Communication Manager

This section provides the procedures for configuring 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 Avaya S8XXX servers unless otherwise noted. An Avaya Communication Manager is configured to generate and send the CDR records to the IP address of the Pan Cyber Dialguard server over a TCP socket connection. For this configuration, the CDR link is configured to originate from the Avaya S8500 Server (i.e., with node-name – “procr”) and terminates at the Pan Cyber Dialguard server. The highlights in the following screens indicate the parameter values used during the compliance test.

Step	Description
1.	Use the **change node-names ip** command to add a new node name for the Pan Cyber Dialguard server.

```
change node-names ip                                          Page   1 of   1
                                   IP NODE NAMES
    Name                IP Address
default               0.0.0.0
procr                 10.1.10.10
Dialguard             10.1.10.231
```

2. Use the **change ip-services** command to define the CDR link. To define a primary CDR link, 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: procr**
- **Local Port: 0** [The Local Port is fixed to 0 because Avaya Communication Manager initiates the CDR link.]
- **Remote Node: Dialguard** [The Remote Node is set to the node name previously defined in **Step 1**.]
- **Remote Port: 5025** [The Remote Port may be set to a value between 5000 and 64500 inclusive, and must match the port configured in Pan Cyber Dialguard server in **Section 4**.]

```
change ip-services                                            Page   1 of   4

                                   IP SERVICES
 Service      Enabled      Local        Local        Remote       Remote
  Type                     Node         Port         Node         Port
CDR1                    procr            0        Dialguard       5025
```

On Page 3 of the IP SERVICES form, disable the Reliable Session Protocol (RSP) for the CDR link by setting the **Reliable Protocol** field to **n**.

```
change ip-services                                            Page   3 of   4

                              SESSION LAYER TIMERS
  Service      Reliable  Packet Resp   Session Connect  SPDU  Connectivity
   Type        Protocol     Timer       Message Cntr    Cntr     Timer

 CDR1            n         30                3           3         60
```

Step	Description
3.	Enter the **change system-parameters cdr** command to set the parameters for the type of calls to track and the format of the CDR data. The following settings are used during the compliance test. • **CDR Date Format**: **month/day** • **Primary Output Format**: **customized** • **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. • **Use Legacy CDR Formats? n** [Specify the use of the new Avaya Communication Manager 4.0.1 and later formats in the CDR records produced by the system.] • **Intra-switch CDR: y** [Allows call records for internal calls involving specific stations. Those stations must be specified in the INTRA-SWITCH-CDR form in **Step 4**.] • **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   2
                            CDR SYSTEM PARAMETERS

 Node Number (Local PBX ID): 1                      CDR Date Format: month/day
      Primary Output Format: customized     Primary Output Endpoint: CDR1
    Secondary Output Format:
           Use ISDN Layouts? n                   Enable CDR Storage on Disk? n
       Use Enhanced Formats? n      Condition Code 'T' For Redirected Calls? n
      Use Legacy CDR Formats? n                 Remove # From Called Number? n
Modified Circuit ID Display? y                              Intra-switch CDR? y
                   Record Outgoing Calls Only? n      Outg Trk Call Splitting? y
  Suppress CDR for Ineffective Call Attempts? y       Outg Attd Call Record? y
      Disconnect Information in Place of FRL? n      Interworking Feat-flag? n
 Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
                                    Calls to Hunt Group - Record: group-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? n       Record Agent ID on Outgoing? y
     Inc Trk Call Splitting? y                  Inc Attd Call Record? n
  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: 5
```

Step	Description
	On Page 2 of the CDR SYSTEM PARAMETERS form, define the customized CDR format as shown.

```
change system-parameters cdr                                          Page   2 of   2
                              CDR SYSTEM PARAMETERS

     Data Item - Length          Data Item - Length          Data Item - Length
 1: date              - 6   17: in-trk-code      - 4   33: vdn               - 5
 2: space             - 1   18: space            - 1   34: return            - 1
 3: time              - 4   19: auth-code        - 7   35: line-feed         - 1
 4: space             - 1   20: space            - 1   36:                    -
 5: sec-dur           - 5   21: in-crt-id        - 3   37:                    -
 6: space             - 1   22: space            - 1   38:                    -
 7: cond-code         - 1   23: out-crt-id       - 3   39:                    -
 8: space             - 1   24: space            - 1   40:                    -
 9: code-dial         - 4   25: isdn-cc          - 11  41:                    -
10: space             - 1   26: space            - 1   42:                    -
11: code-used         - 4   27: ppm              - 5   43:                    -
12: space             - 1   28: space            - 1   44:                    -
13: dialed-num        - 18  29: acct-code        - 15  45:                    -
14: space             - 1   30: space            - 1   46:                    -
15: calling-num       - 15  31: attd-console     - 2   47:                    -
16: space             - 1   32: space            - 1   48:                    -

                                 Record length = 130
```

4.	If the **Intra-switch CDR** field is set to **y** on Page 1 of the CDR SYSTEM PARAMETERS form, then use the **change intra-switch-cdr** command to define the extensions for which intra-switch call detail records will be generated. In the **Extension** field, enter the specific extensions whose usage will be tracked with the CDR records.

```
change intra-switch-cdr                                               Page   1 of   3
                              INTRA-SWITCH CDR

                                   Assigned Members:   4    of 5000   administered
   Extension          Extension          Extension          Extension
   10001
   10002
   10003
   10004
```

5.	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.

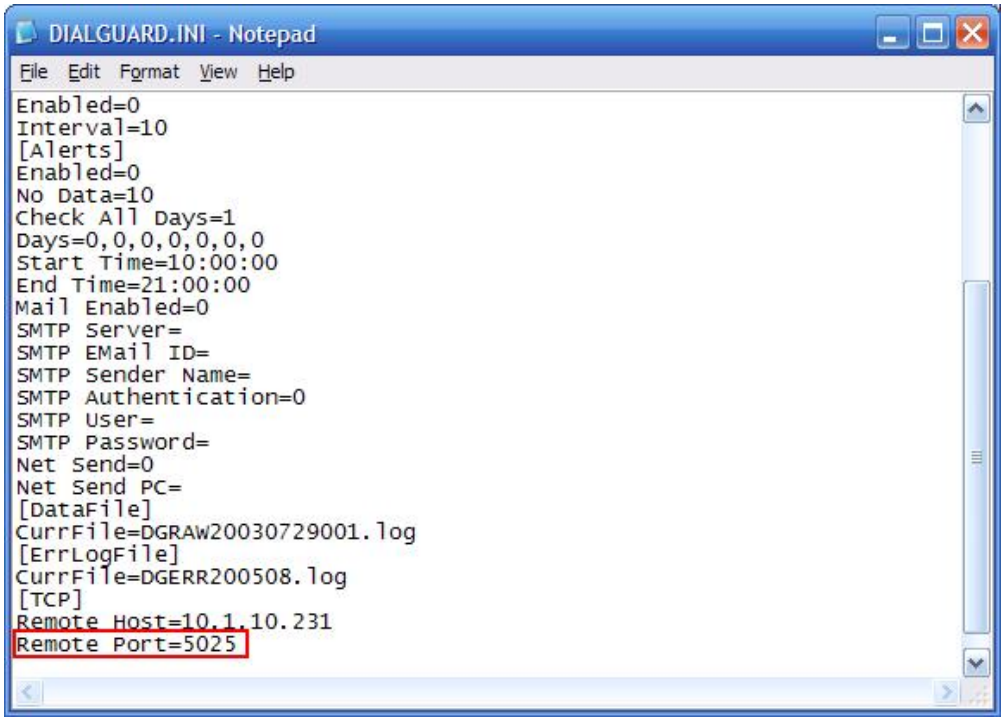
```
change trunk-group 2                                                  Page   1 of  21
                                  TRUNK GROUP

Group Number: 2                     Group Type: isdn          CDR Reports: y
  Group Name: Singtel BRI Line 2          COR: 95       TN: 1        TAC: 702
   Direction: two-way        Outgoing Display? n         Carrier Medium: PRI/BRI
 Dial Access? y              Busy Threshold: 255  Night Service: 10004
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n            TestCall ITC: rest
                          Far End Test Line No:
TestCall BCC: 4
```

4. Configure Pan Cyber Dialguard

This section describes the configuration of Pan Cyber Dialguard.

Step	Description
1.	Pan Cyber Dialguard acts as a TCP server to receive the CDR connection from the Avaya Communication Manager. Edit the file **DIALGUARD.INI** located in the Pan Cyber Dialguard installation directory **C:\Dialguard**. In the **[TCP]** section, the field **Remote Port** sets the TCP port that Pan Cyber Dialguard listens on. In this compliance testing, the TCP port is set to **5025**. Save the file and restart Pan Cyber Dialguard.



5. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing. The feature testing evaluated the ability of Pan Cyber Dialguard to collect and process CDR records for various types of calls. The serviceability test introduced failure scenarios to see if Pan Cyber Dialguard 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 Manager, and verify that Pan Cyber Dialguard collects the CDR records and reports the correct attributes of the call. For serviceability testing, the CDR link on Avaya Communication Manager was disabled and re-enabled and the Avaya S8500 Server was also rebooted.

5.2. Test Results

All feature tests passed. Pan Cyber Dialguard successfully captured and processed call records from Avaya Communication Manager. Pan Cyber Dialguard 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 conference calls.

For serviceability testing, the following observations were made.

- Pan Cyber Dialguard does not use the Avaya RSP. As such, CDR records are lost when the Pan Cyber Dialguard PC is disconnected from the LAN or when rebooted.

6. Verification Steps

The following steps may be used to verify the configuration:

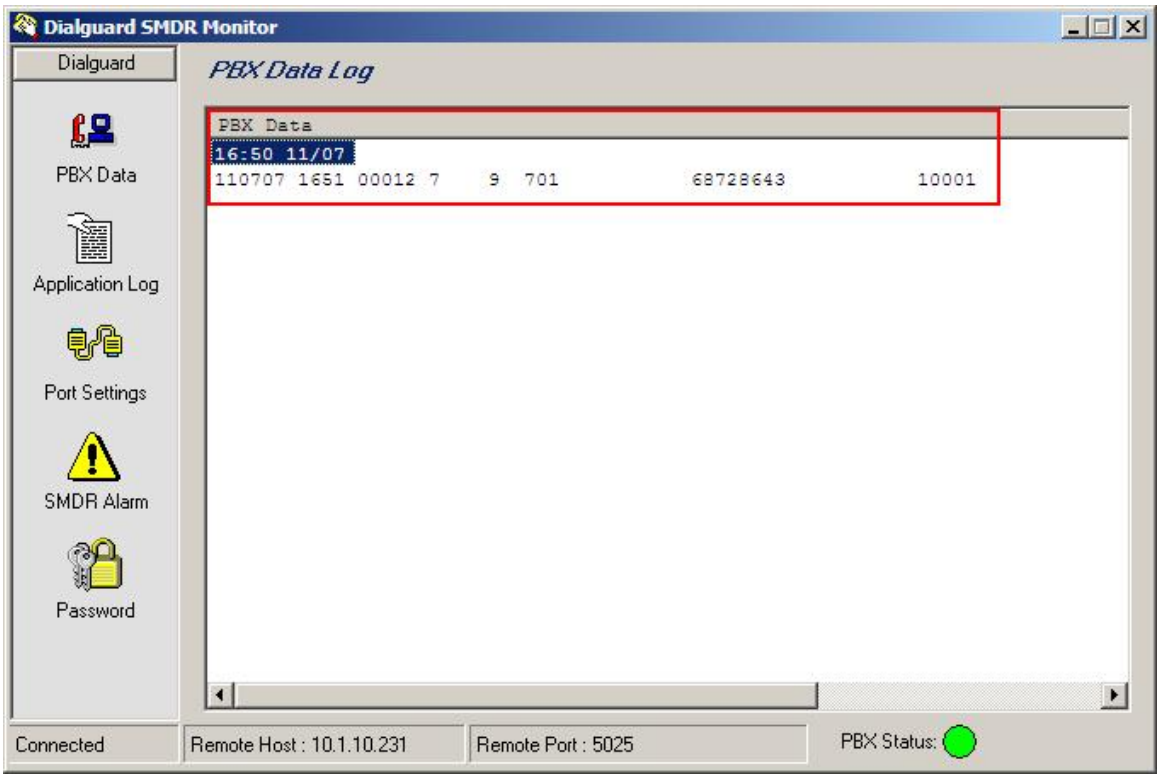
- Use the **ping** utility on the Pan Cyber Dialguard PC to verify the IP connectivity to the Avaya S8500 Server. Note: Use of the ping utility may or may not be reliable depending on how the customer's network is configured to handle ICMP traffic.
- On the SAT of the Avaya S8500 Server, enter the **status cdr-link** command and verify that the **Link State** shows **up**.

```
status cdr-link
                                CDR LINK STATUS
                    Primary                       Secondary

       Link State: up                             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 Pan Cyber Dialguard 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. The screenshot illustrates a call record for a call placed from extension 10001 to an external party at 68728643 lasting for 12 seconds.



- Place internal, inbound trunk, and outbound trunk calls to and from various telephones, generate an appropriate report in Pan Cyber Dialguard and verify the report's accuracy.

7. Support

Technical support for Pan Cyber Dialguard can be obtained by contacting Pan Cyber's Support Desk at +971 6 5572778 and +971 4 3377033 or by sending an e-mail to dialguard@pancyber.com.

8. Conclusion

These Application Notes describe the procedures for configuring Pan Cyber Dialguard to collect call detail records from Avaya Communication Manager. Pan Cyber Dialguard successfully passed the compliance testing.

9. Additional References

This section references the Avaya and Pan Cyber 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.

Product documentation for Pan Cyber Dialguard can be found at:

http://www.pancyber.com/dialguard/dialguard.pdf

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.