Avaya Solution & Interoperability Test Lab

Application Notes for CTI Data Solutions Proteus Enterprise with Avaya Communication Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps for provisioning CTI Data Solutions Proteus Enterprise to interoperate with Avaya Communication Manager. Proteus Enterprise is a call logging system that records Call Detail Records (CDR) outputted by Avaya Communication Manager over an IP network connection.

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

These Application Notes describe the compliance-tested configuration using CTI Data Solutions Proteus Enterprise 6.1 and Avaya Communication Manager 4.0. This configuration addresses the Call Detail Records (CDR) capability of Avaya Communication Manager.

Proteus Enterprise is a Call Accounting and Billing package that utilizes the CDR Link in Communication Manager. Proteus Enterprise collects, stores, and processes the CDR records to provide usage analysis, call costing and billing capabilities. Survivability mode is supported via secure file transfer protocol (SFTP). When administered with the Survivable CDR feature enabled, the Local Survivable Processor (LSP) saves the CDR information in files that are stored in a special directory on its local hard drive until Proteus Enterprise remotely logs into the LSP via a special login, copies the files to its own storage device, and then goes on to process the CDR data in the same manner that it does normally. Avaya Communication Manager generates CDRs for intra-switch calls, inbound trunk calls and outbound trunk calls. In addition, CDRs are generated for transferred calls and conference calls. Proteus Enterprise creates a custom Avaya Communication Manager configuration file to accurately parse the CDR data. For the compliance testing, a customized format was used with Reliable Session Protocol (RSP) enabled.

An Avaya S8700 Server with an Avaya G650 Media Gateway running Avaya Communication Manager 4.0 was configured as the main server and an Avaya S8300 Server with an Avaya G250 Media Gateway was configured as the LSP.

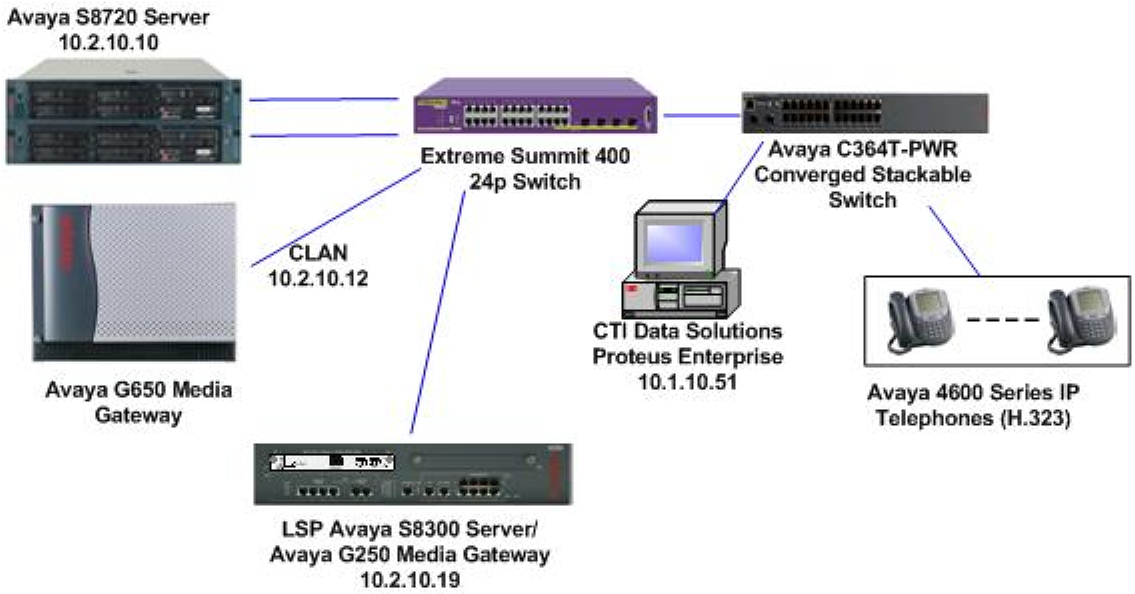


Figure 1: Sample Configuration

2. Equipment and Software Validated

Below is a list of the equipment and software versions used within the compliance-tested network.

Equipment	Software
Avaya S8700 Server running Avaya Communication Manager	4.0.1 (R014x.00.0.731.2)
Avaya G650 Media Gateway IPSI TN2312BP C-LAN TN799DP Medpro TN2302AP	 HW 7, FW 39 HW 1, FW24 HW 20, FW116
Avaya S8300 Server with Avaya G250 Media Gateway (LSP Mode)	4.0.1 (R014x.00.0.731.2)
Extreme Summit 400 24p Switch	Extremeware 7.5e.2.8
Avaya C364T-PWR Converged Stackable Switch	4.3.12
Avaya 4600 Series IP Telephones (H.323) Avaya 9600 Series IP Telephones (H.323)	2.8 1.5
CTI Data Solutions Proteus Enterprise	6.1.01

3. Configure Avaya Communication Manager

This section describes the steps for configuring CDR links, CDR system parameters, and intra-switch CDR extensions on Avaya Communication Manager. The steps are performed through the System Access Terminal (SAT) interface.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>Enter the <b>change node-names ip</b> command. Create a new node name and IP address for Proteus Enterprise. The node name configured below will be used in the ip-services form to specify the remote node of the CDR links.
<pre>
change node-names ip   Page   1 of   2
                                  IP NODE NAMES
    Name   IP Address
AEServer   10.1.10.20
Abacus   10.1.10.31
<b>CDR_Server   10.1.10.51</b>
IPO412a_DC1   10.1.20.10
S8300a_DC1   10.1.30.10
S8500_Val1   10.1.10.14
SEServer   10.1.10.22
</pre></td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td><b>2.</b></td><td>

Enter the **change ip-services** command. On Page 1 of the **ip-services** form, define a primary CDR link by setting the **Service Type** to “CDR1”. A secondary link can be defined by setting Service Type to CDR2. Set **Local Node** to “clanla_DC1” and **Remote Node** to “CDR_Server” as configured in Step 1. The **Local Port** is fixed at “0” and the **Remote Port** may be set to a value between 5000 and 64500, inclusive, but must match the port configured on Proteus Enterprise in Section 4, Step 1.

```
change ip-services                                        Page   1 of   4
                                   IP SERVICES
 Service     Enabled     Local        Local       Remote      Remote
  Type                   Node         Port        Node        Port
SAT            y      clan1a_DC1       5023    any             0
AESVCS         y      clan1a_DC1       8765
CDR1                  clan1a_DC1       0       CDR_Server      9002
```

On Page 3 of the ip-services form enable the RSP for the CDR link by setting **Reliable Protocol** to “**y**”.

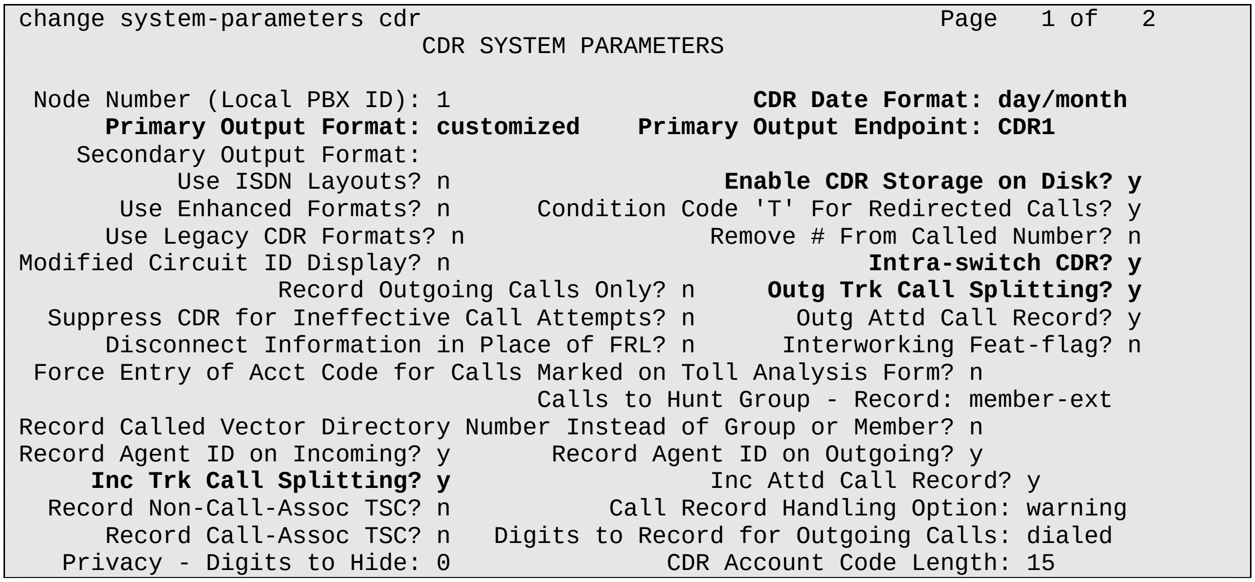
```
change ip-services                                        Page   3 of   4

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

 CDR1            y         30               3           3         30
```

</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>3.</td><td>

Enter the **change system-parameters cdr** command and set the following:

- **CDR Date Format**: set to “day/month”. The date format will be used for the date stamp that begins each new day of call records or in the “customized” CDR output formats (see below).
- **Primary Output Format**: set to “customized” format.
- **Primary Output Endpoint**: set to “CDR1”.
- **Intra-switch CDR**: set to “y” so that CDR records will be generated for calls to/from extensions that are assigned intra-switch CDR (see Step 5).
- **Outg Trk Call Splitting / Inc Trk Call Splitting**: set to “y” if a separate CDR record is desired for any portion of an outgoing/incoming call that is transferred or conferenced.
- **Enable CDR Storage on Disk**: set to “y” to allow CDR’s to be stored on the LSP when in survivable mode.



```
change system-parameters cdr                                    Page   1 of   2
                            CDR SYSTEM PARAMETERS

 Node Number (Local PBX ID): 1                     CDR Date Format: day/month
      Primary Output Format: customized    Primary Output Endpoint: CDR1
    Secondary Output Format:
           Use ISDN Layouts? n                   Enable CDR Storage on Disk? y
       Use Enhanced Formats? n      Condition Code 'T' For Redirected Calls? y
      Use Legacy CDR Formats? n                 Remove # From Called Number? n
Modified Circuit ID Display? n                             Intra-switch CDR? y
                  Record Outgoing Calls Only? n     Outg Trk Call Splitting? y
  Suppress CDR for Ineffective Call Attempts? n       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: member-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? y       Record Agent ID on Outgoing? y
     Inc Trk Call Splitting? y                  Inc Attd Call Record? 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: 15
```

</td></tr>
</table>

Step **Description**

4. If **Primary Output Format** is set to “customized”, then on Page 2 of the system-parameters cdr screen, enter the data items in the order that the information should appear in the customized call records sent over the CDR link. For each field in the CDR record, specify the data item and length as shown below.

```
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: clg-num/in-tac   - 15  31: attd-console     - 2   47:                  -
16: space            - 1   32: space            - 1   48:                  -

                              Record length = 130
```

5. If **Intra-switch CDR** is enabled (Step 3), enter the command **change intra-switch-cdr** and enter the extensions for which intra-switch calls will generate CDR data.

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

                                 Assigned Members:   4    of 5000   administered
   Extension           Extension           Extension           Extension
   10001
   10016
   10018
   10023
```

Note: For ease of implementation, special application **(SA8202) Intra-Switch CDR by COS** is an optional feature that allows customers to enable intra-switch CDR for extensions that are assigned a COS with intra-switch CDR activated. The customer does not have to manually add individual extensions in the **intra-switch-cdr** form. The SA8202 feature also removes the 5000 extension limit for the Avaya S8500 Server, allowing CDR records to be generated for as many extensions as are administered on the switch.

Step **Description**

6. For each trunk group for which CDR records are desired, enter the command **change trunk-group n**, where n is the trunk group number, and set **CDR Reports** to “r”. This will enable the following CDR records to be generated for both incoming and outgoing calls:

- Abandoned calls: The system creates a record with a condition code of "H," indicating the time until the call was abandoned.
- Answered calls: The system creates a record with a condition code of "G," indicating the interval from start of ring to answer.
- Calls to busy stations: The system creates a record with a condition code of "I," indicating a recorded interval of 0.

The example below depicts the trunk group connected to the PSTN in the sample configuration.

```
change trunk-group 19                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 19                   Group Type: isdn          CDR Reports: r
  Group Name: PRI to BT                   COR: 1        TN: 1        TAC: 719
   Direction: two-way        Outgoing Display? n         Carrier Medium: PRI/BRI
 Dial Access? y              Busy Threshold: 255  Night Service:
Queue Length: 0
Service Type: public-ntwrk          Auth Code? n            TestCall ITC: rest
                         Far End Test Line No:
TestCall BCC: 4
```

7. The survivable CDR feature is used to preserve the CDR records associated with calls that occur while a gateway is under the control of an LSP. The following steps are required to allow the calls to be stored on the LSP so they can be then retrieved via SFTP. Enter the **list survivable-processor** command and make a note of the LSP name. In this example it is “lsp_g250”.

```
list survivable-processor


                             SURVIVABLE PROCESSORS
 Name           Type       IP Address     Reg LSP         Translations     Net
                                              Act         Updated          Rgn

 lsp_g250        LSP       10 .2  .10 .19   y   n                           1
```

Step **Description**

8. Enter **change survivable-processor LSP_G250** and set the following parameters.

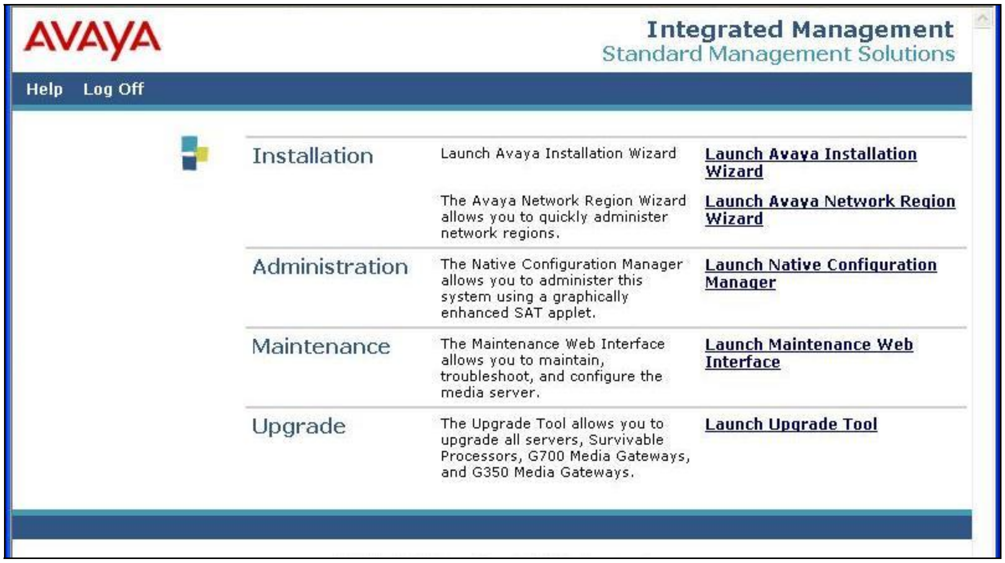
- **Service Type**: set to “CDR1”, which is set as the **Primary Output Endpoint** in Step 3.
- **Enabled**: set to “o” for overwrite.
- **Store to dsk**: set to “y” this allows the CDR’s to be stored to the LSP disk.

```
change survivable-processor LSP_G250                            Page   2 of   3
                   SURVIVABLE PROCESSOR - IP-SERVICES
 Service     Enabled Store   Local             Local    Remote            Remote
  Type               to dsk  Node              Port     Node              Port
  AESVCS       i       n     clan_01a10        8765
  CDR1         o       y
```

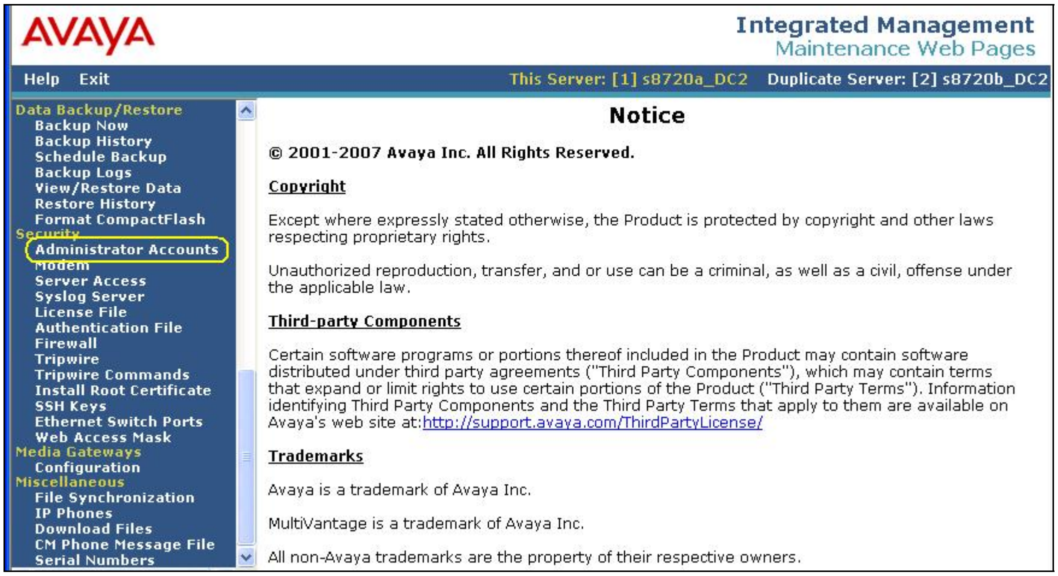
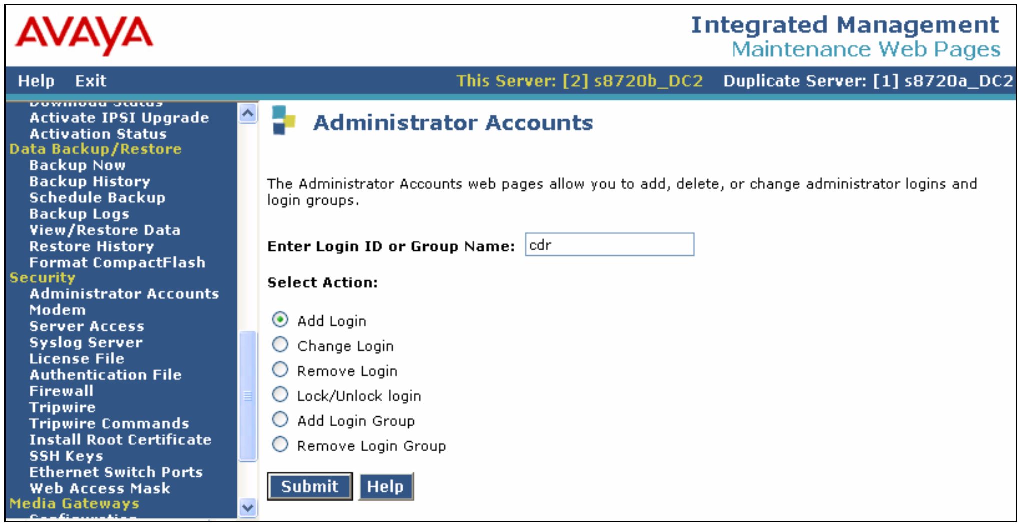
9. Use either of these following commands to save the translations to the LSP:

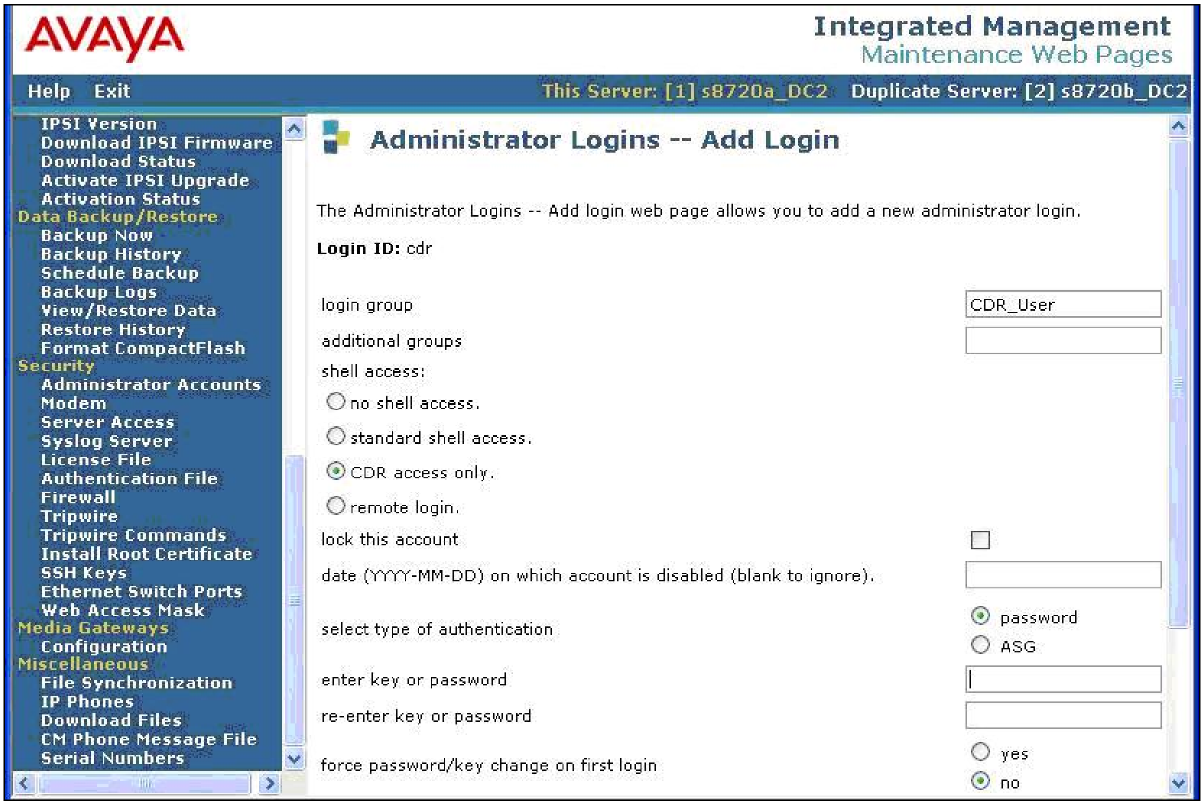
- The **save trans lsp** command locally saves the translations, and performs a filesync operation to all registered LSPs.
- The **save trans lsp n** command, where n is the IP address of a specific LSP, locally saves the translations, and performs a filesync operation to the specified LSP.

10. Access the Main (Avaya S8720 Server) Avaya Communication Manager administration web interface by entering *http://<ip-addr>/* as the URL in an Internet browser, where *<ip-addr>* is the IP address of Avaya Communication Manager. Log in with the appropriate credentials to Avaya Communication Manager, and click **Launch Maintenance Web Interface**.



Installation	Launch Avaya Installation Wizard	Launch Avaya Installation Wizard
	The Avaya Network Region Wizard allows you to quickly administer network regions.	Launch Avaya Network Region Wizard
Administration	The Native Configuration Manager allows you to administer this system using a graphically enhanced SAT applet.	Launch Native Configuration Manager
Maintenance	The Maintenance Web Interface allows you to maintain, troubleshoot, and configure the media server.	Launch Maintenance Web Interface
Upgrade	The Upgrade Tool allows you to upgrade all servers, Survivable Processors, G700 Media Gateways, and G350 Media Gateways.	Launch Upgrade Tool

Step	Description
11.	In the Security section, click **Administrator Accounts**.  AVAYA Integrated Management Maintenance Web Pages Help Exit This Server: [1] s8720a_DC2 Duplicate Server: [2] s8720b_DC2 Data Backup/Restore Backup Now Backup History Schedule Backup Backup Logs View/Restore Data Restore History Format CompactFlash Security Administrator Accounts Modem Server Access Syslog Server License File Authentication File Firewall Tripwire Tripwire Commands Install Root Certificate SSH Keys Ethernet Switch Ports Web Access Mask Media Gateways Configuration Miscellaneous File Synchronization IP Phones Download Files CM Phone Message File Serial Numbers **Notice** © 2001-2007 Avaya Inc. All Rights Reserved. **Copyright** Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law. **Third-party Components** Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at:http://support.avaya.com/ThirdPartyLicense/ **Trademarks** Avaya is a trademark of Avaya Inc. MultiVantage is a trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.
12.	In the **Enter Login or Group Name** field enter a name (see Section 4.2, Step 5) that will used by Proteus Enterprise to login Select the **Add Login** radio button and click **Submit**.  AVAYA Integrated Management Maintenance Web Pages Help Exit This Server: [2] s8720b_DC2 Duplicate Server: [1] s8720a_DC2 Download Status Activate IPSI Upgrade Activation Status Data Backup/Restore Backup Now Backup History Schedule Backup Backup Logs View/Restore Data Restore History Format CompactFlash Security Administrator Accounts Modem Server Access Syslog Server License File Authentication File Firewall Tripwire Tripwire Commands Install Root Certificate SSH Keys Ethernet Switch Ports Web Access Mask Media Gateways Configuration **Administrator Accounts** The Administrator Accounts web pages allow you to add, delete, or change administrator logins and login groups. **Enter Login ID or Group Name:** cdr **Select Action:** ● Add Login ○ Change Login ○ Remove Login ○ Lock/Unlock login ○ Add Login Group ○ Remove Login Group Submit Help

Step	Description
13.	In the **login group** field, enter “CDR_User”, leave the additional groups field blank. Click on the **CDR access only** radio button. Click on the **password** radio button and enter the desired password twice. This password will be used by Proteus Enterprise to access the survivable CDR file on the LSP. All other remaining fields can be left with their default values. Click the **Add** button at the bottom of the page (not shown). The account details created on the Main Avaya Communication Manage will be propagated to the LSP. 

Administrator Logins -- Add Login

The Administrator Logins -- Add login web page allows you to add a new administrator login.

Login ID: cdr

login group: CDR_User

additional groups:

shell access:

○ no shell access.

○ standard shell access.

● CDR access only.

○ remote login.

lock this account □

date (YYYY-MM-DD) on which account is disabled (blank to ignore).

select type of authentication ● password ○ ASG

enter key or password

re-enter key or password

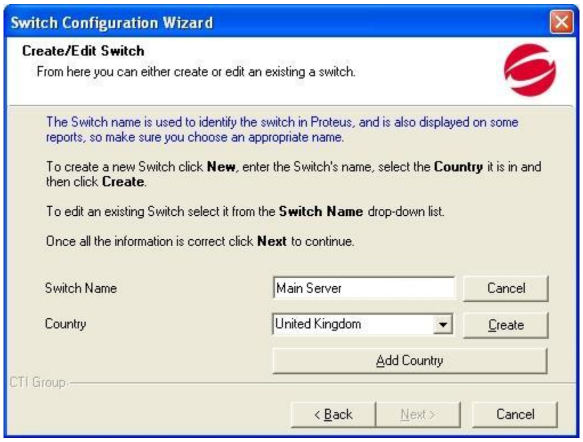
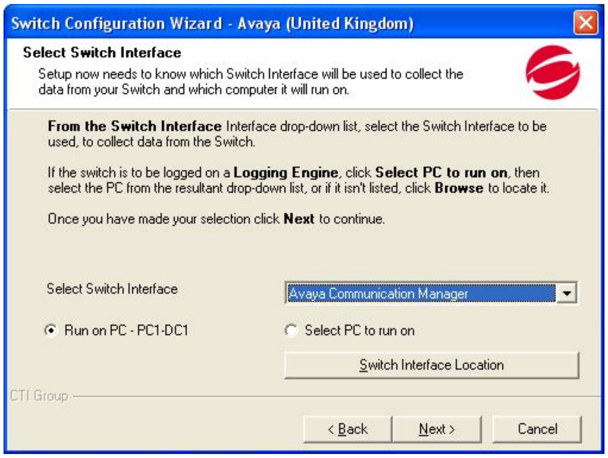
force password/key change on first login ○ yes ● no

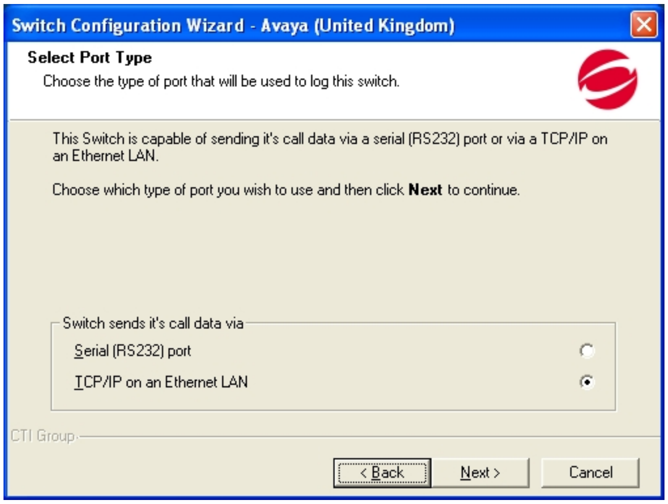
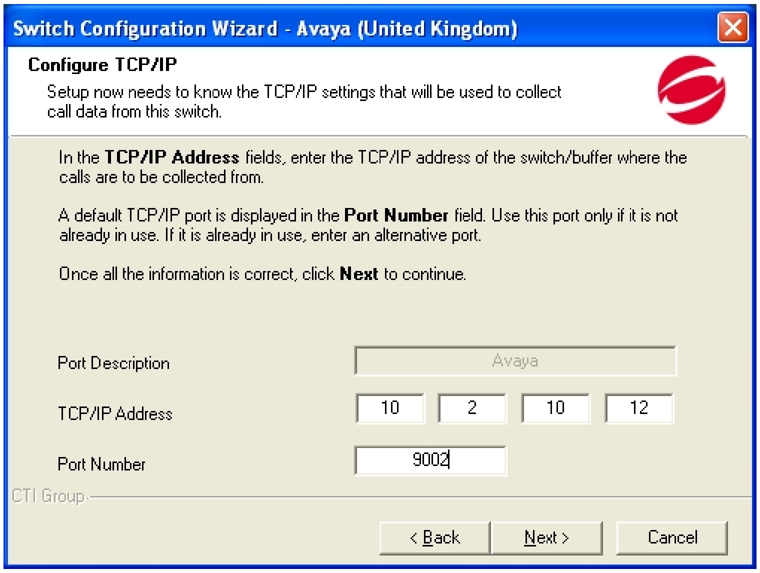
4. Configure CTI Data Solutions Proteus Enterprise

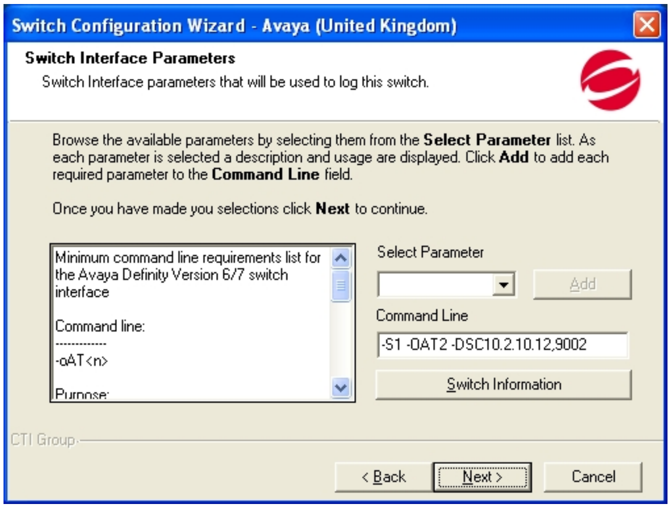
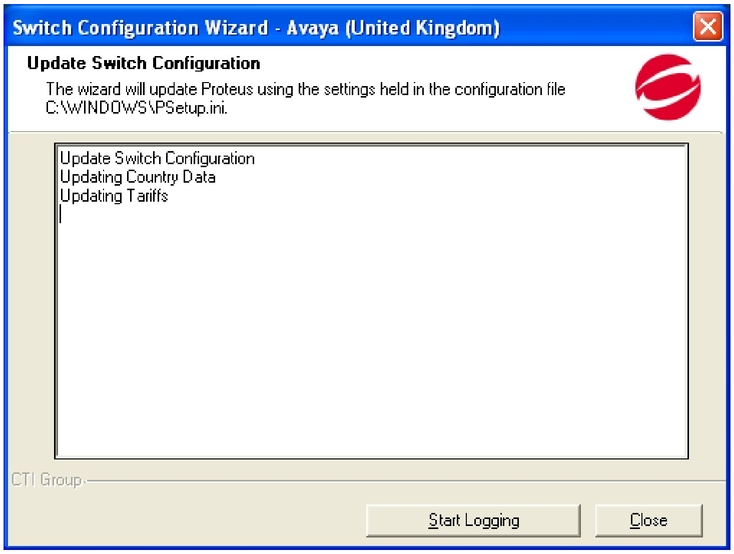
The configuration information provided in this section describes the steps required to set up Proteus Enterprise to collect CDR records generated by Avaya Communication Manager over a TCP/IP link.

4.1. Configure Proteus Enterprise to Suport Avaya Communication Manager Configured as the Main Server

The configuration of the Proteus Enterprise application is done via the Switch Configuration Wizard as part of the Proteus Enterprise installation process. Only the screens relevant for the configuration between Proteus Enterprise and Avaya Communication Manager are shown in the following steps.

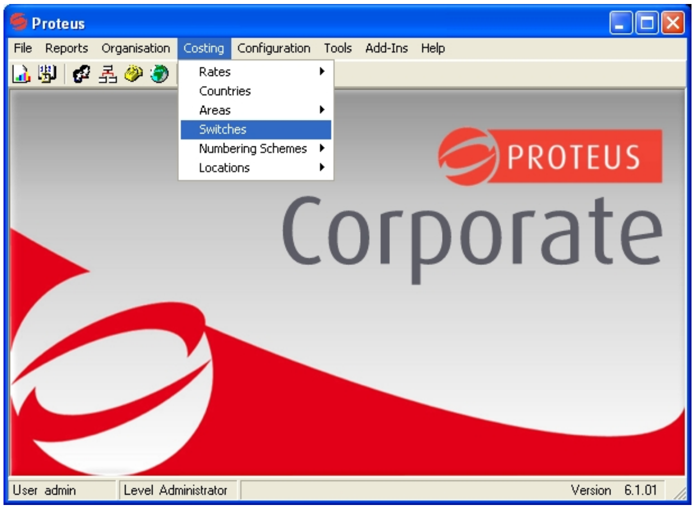
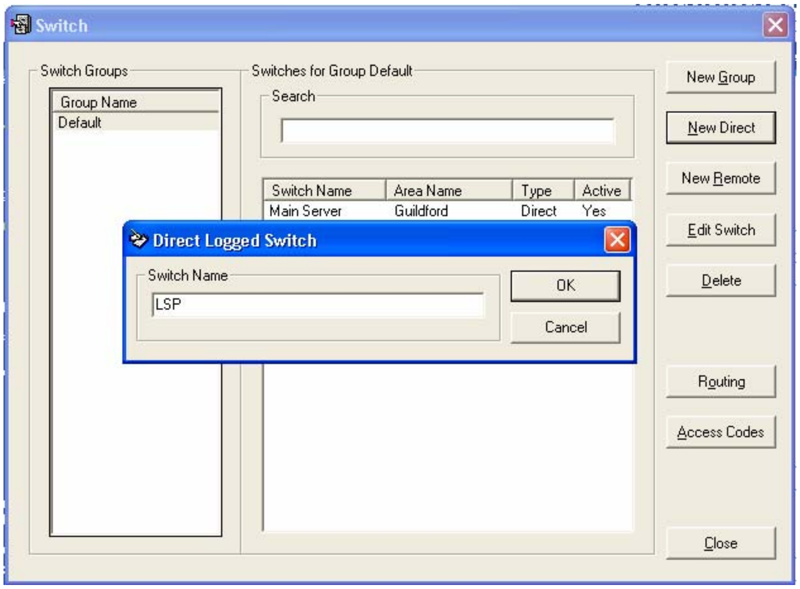
Step	Description
1.	In the Create/Edit Switch screen enter a descriptive name in the **Switch Name** field. From the **Country** drop down menu, select the country and the click the **Create** button.  Switch Configuration Wizard **Create/Edit Switch** From here you can either create or edit an existing a switch. The Switch name is used to identify the switch in Proteus, and is also displayed on some reports, so make sure you choose an appropriate name. To create a new Switch click **New**, enter the Switch's name, select the **Country** it is in and then click **Create**. To edit an existing Switch select it from the **Switch Name** drop-down list. Once all the information is correct click **Next** to continue. Switch Name: Main Server Country: United Kingdom Cancel Create Add Country CTI Group < Back Next > Cancel
2.	In the Select Switch Interface screen, select Avaya Communication Manager from the **Select Switch Interface** drop down menu. Click **Next >** to continue.  Switch Configuration Wizard - Avaya (United Kingdom) **Select Switch Interface** Setup now needs to know which Switch Interface will be used to collect the data from your Switch and which computer it will run on. **From the Switch Interface** Interface drop-down list, select the Switch Interface to be used, to collect data from the Switch. If the switch is to be logged on a **Logging Engine**, click **Select PC to run on**, then select the PC from the resultant drop-down list, or if it isn't listed, click **Browse** to locate it. Once you have made your selection click **Next** to continue. Select Switch Interface: Avaya Communication Manager ● Run on PC - PC1-DC1 ○ Select PC to run on Switch Interface Location CTI Group < Back Next > Cancel

Step	Description
3.	In the Select Port Type screen, select the **TCP/IP on an Ethernet LAN** radio button. Click **Next >**.  Switch Configuration Wizard - Avaya (United Kingdom) **Select Port Type** Choose the type of port that will be used to log this switch. This Switch is capable of sending it's call data via a serial (RS232) port or via a TCP/IP on an Ethernet LAN. Choose which type of port you wish to use and then click **Next** to continue. Switch sends it's call data via Serial (RS232) port ○ TCP/IP on an Ethernet LAN ●
4.	Enter the CLAN IP address and Port configured in Section 3, Steps 1 and 2. In the **TCP/IP Address** and **Port Number** fields. Click **Next >**.  Switch Configuration Wizard - Avaya (United Kingdom) **Configure TCP/IP** Setup now needs to know the TCP/IP settings that will be used to collect call data from this switch. In the **TCP/IP Address** fields, enter the TCP/IP address of the switch/buffer where the calls are to be collected from. A default TCP/IP port is displayed in the **Port Number** field. Use this port only if it is not already in use. If it is already in use, enter an alternative port. Once all the information is correct, click **Next** to continue. Port Description: Avaya TCP/IP Address: 10 2 10 12 Port Number: 9002

Step	Description
5.	In the **Command Line** field, enter the following parameters as shown below. - **"-S1"** - Enables listening mode for the port being monitored. - **"-0AT2"** – Logs custom CDR format defined in Section 3, Step 4. - **"-DSC10.2.10.12,9002"** – Enables RSP logging. In order to log CDR's using RSP the CLAN IP address and Port number configured in Section 3, Steps 1 and 2 is needed. Click **Next >**.  Switch Configuration Wizard - Avaya (United Kingdom) **Switch Interface Parameters** Switch Interface parameters that will be used to log this switch. Browse the available parameters by selecting them from the **Select Parameter** list. As each parameter is selected a description and usage are displayed. Click **Add** to add each required parameter to the **Command Line** field. Once you have made you selections click **Next** to continue. Minimum command line requirements list for the Avaya Definity Version 6/7 switch interface Command line: ------------- -oAT<n> Purpose: Select Parameter Command Line -S1 -0AT2 -DSC10.2.10.12,9002 Add Switch Information CTI Group < Back Next > Cancel
6.	Click **Start Logging**. The following four programs will be launched: Costing Engine, Switch Interface, Report Scheduler and Real Time Monitor. Shown in the verification Steps 2 , 3 and 4.  Switch Configuration Wizard - Avaya (United Kingdom) **Update Switch Configuration** The wizard will update Proteus using the settings held in the configuration file C:\WINDOWS\PSetup.ini. Update Switch Configuration Updating Country Data Updating Tariffs

4.2. Configure Proteus Enterprise to Suport Avaya Communication Manager Configured as the LSP Server

Survivable CDR data files can be retrieved by Proteus Enterprise from Avaya Communication Manager running in LSP mode using SFTP.

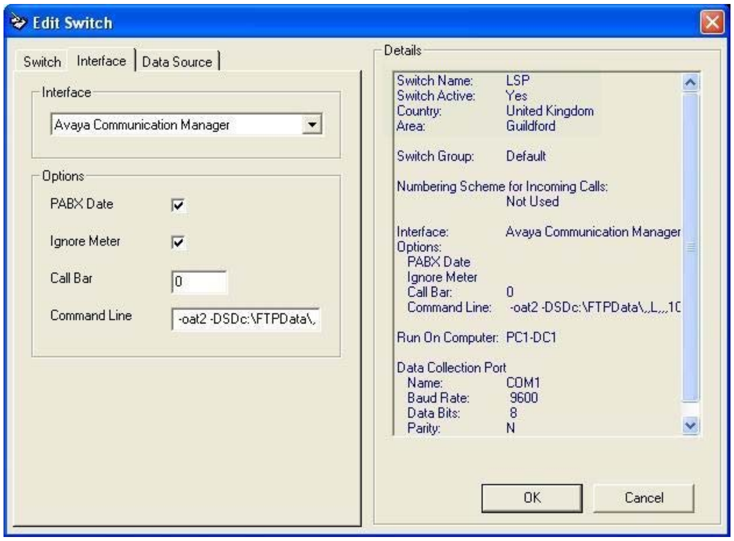
Step	Description
1.	Click on **Start → Programs → CTI Group → Proteus Corporate → Proteus.** Enter the appreciate username and password. From the toolbar, select **Costing → Switches**.  Proteus File Reports Organisation Costing Configuration Tools Add-Ins Help Rates Countries Areas Switches Numbering Schemes Locations PROTEUS Corporate User admin Level Administrator Version 6.1.01
2.	In the Switch screen, click the **New Direct** button. In the Direct Logged Switch dialog box enter the name of the LSP Server and click **OK**.  Switch Switch Groups Group Name Default Switches for Group Default Search New Group New Direct New Remote Edit Switch Delete Routing Access Codes Close Direct Logged Switch OK Cancel Switch Name | Area Name | Type | Active Main Server | Guildford | Direct | Yes Switch Name: LSP

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td><b>3.</b></td><td>

In the Edit Switch screen, click the **Interface** tab. From the **Interface** drop down menu select Avaya Communication Manager. In the **Command Line** field enter the following parameters.

- **“-oat2”** – Logs custom CDR format defined in Section 3, Step 4
- “**-DSD”** – The command to log from a specified directory
- **“c:\FTPData\”** - The directory, for this configuration, where the downloaded CDR files from the LSP Server will be stored.

Click **OK**.



Interface: Avaya Communication Manager

Options
PABX Date ☑
Ignore Meter ☑
Call Bar 0
Command Line -oat2 -DSDc:\FTPData\,

Switch Name: LSP
Switch Active: Yes
Country: United Kingdom
Area: Guildford

Switch Group: Default

Numbering Scheme for Incoming Calls: Not Used

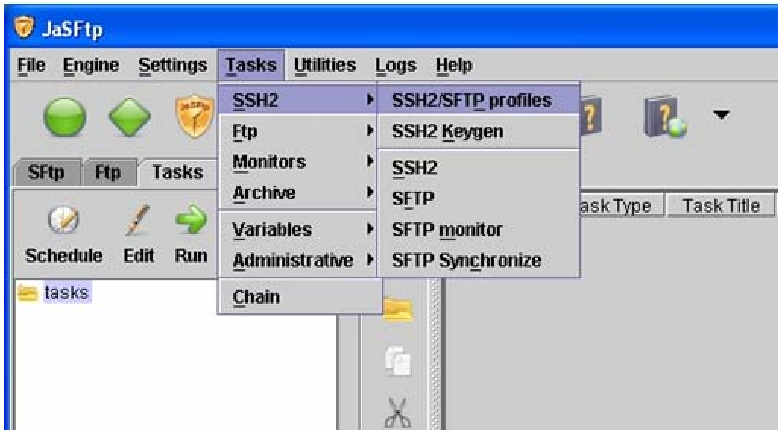
Interface: Avaya Communication Manager
Options:
PABX Date
Ignore Meter
Call Bar: 0
Command Line: -oat2 -DSDc:\FTPData\,,L,,,1C

Run On Computer: PC1-DC1

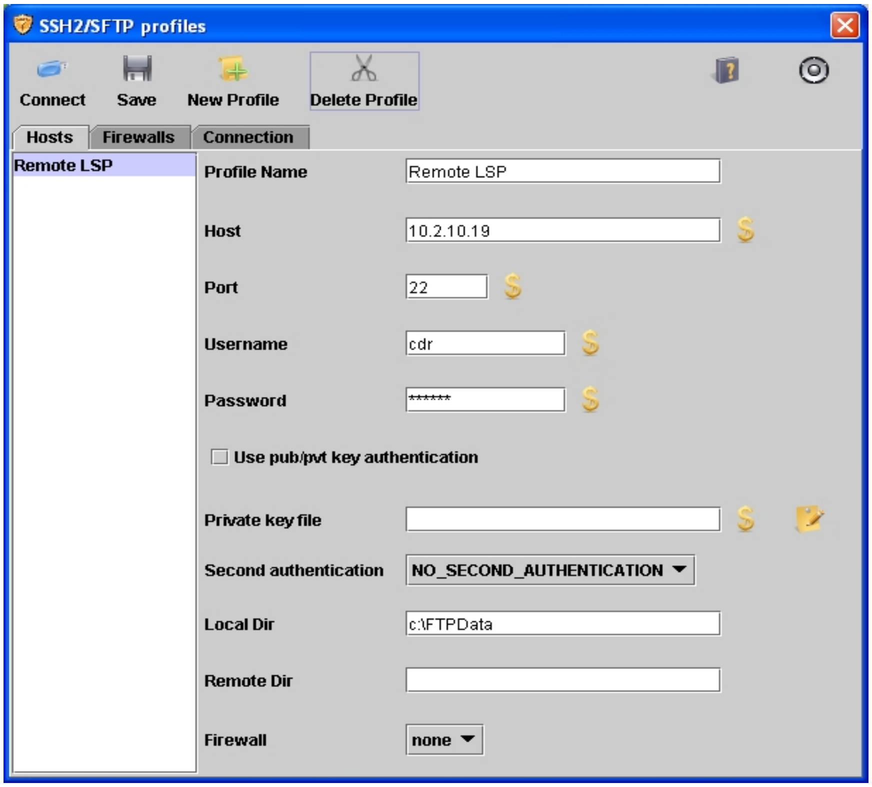
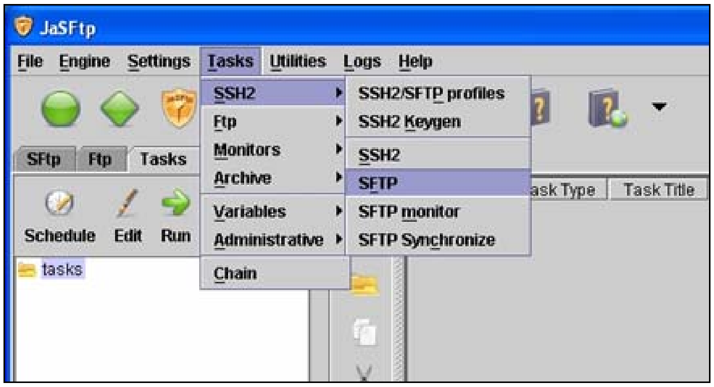
Data Collection Port
Name: COM1
Baud Rate: 9600
Data Bits: 8
Parity: N

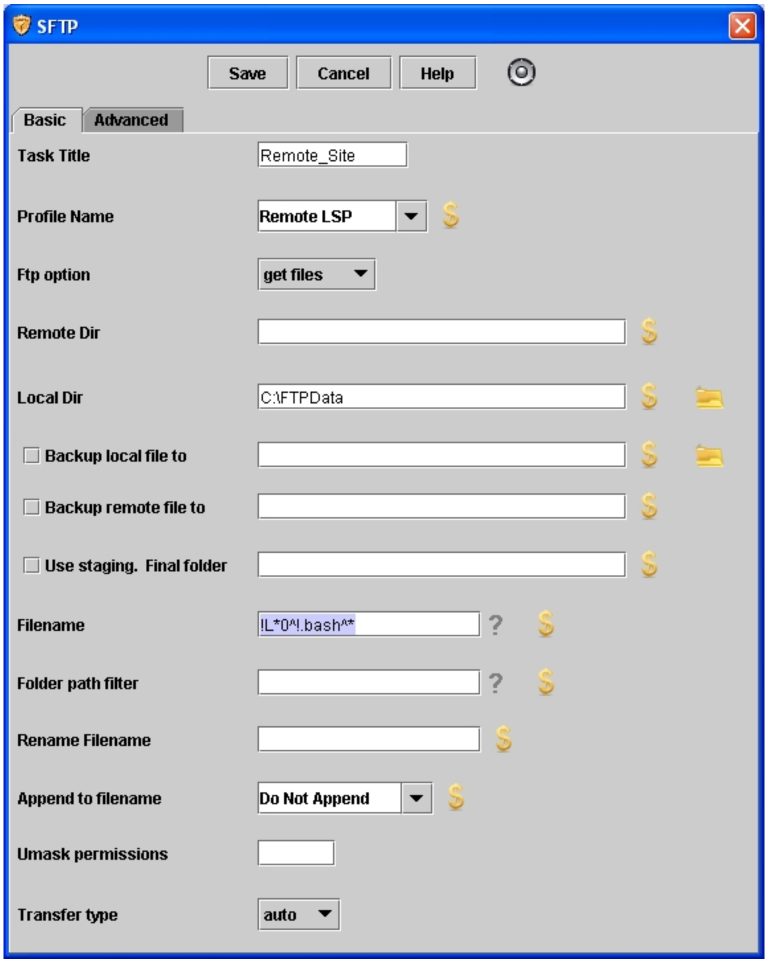
</td></tr>
<tr><td><b>4.</b></td><td>

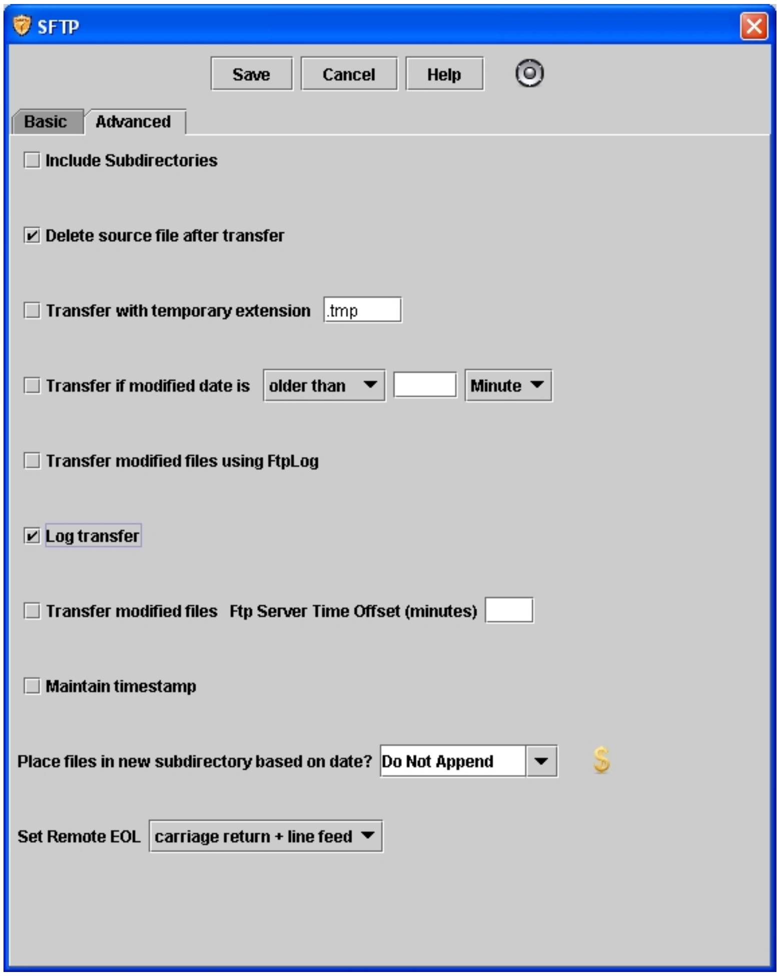
Proteus Enterprise uses a third party automated secure transfer protocol application called JaSFtp7 to retrieve the stored CDR files from the LSP server. Click on **Start → Programs → JaSFtp7 → JaSFtp7**. The first step on the SFTP client is to create a profile by selecting **Tasks → SSH2 → SSH2/SFTPprofiles**.



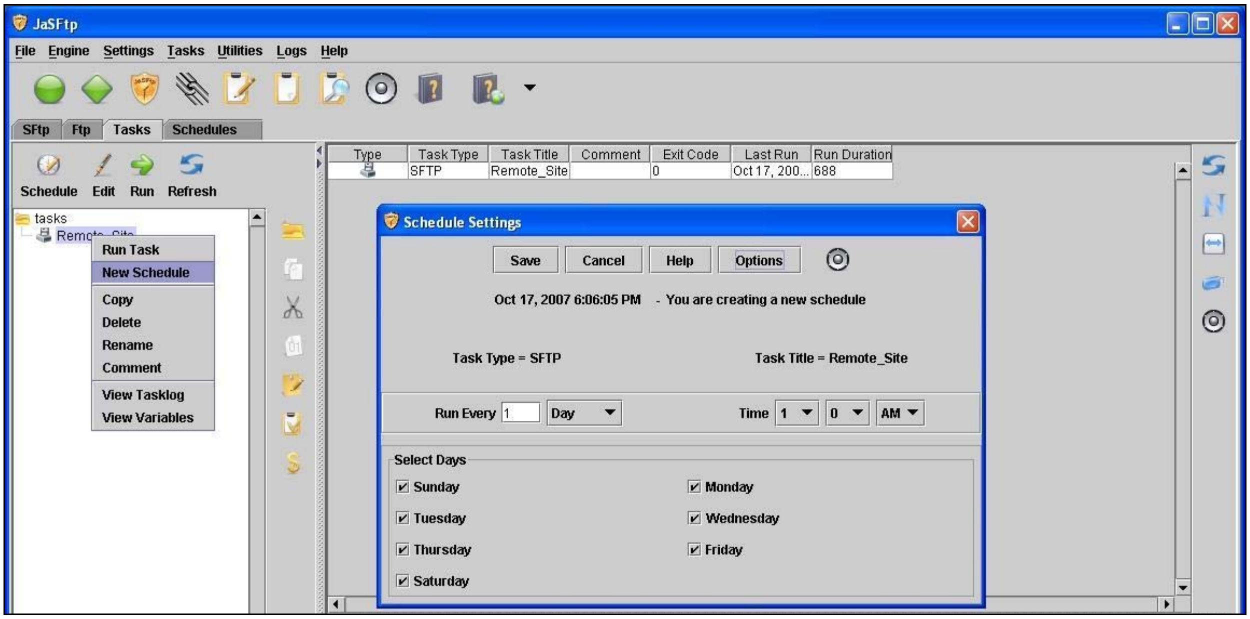
</td></tr>
</table>

Step	Description
5.	Enter a descriptive name in the **Profile Name** field. Enter the IP address of the LSP server in the **Host** field. Enter the username and password configured in Section 3, Step 12, and Step 13. In the **Local Dir** field enter the path as specified in the Proteus Enterprise switch interface command line in Step 3. Click **Save** at the top of the screen.  SSH2/SFTP profiles Connect Save New Profile Delete Profile Hosts Firewalls Connection Remote LSP Profile Name: Remote LSP Host: 10.2.10.19 Port: 22 Username: cdr Password: ****** ☐ Use pub/pvt key authentication Private key file: Second authentication: NO_SECOND_AUTHENTICATION Local Dir: c:\FTPData Remote Dir: Firewall: none
6.	Create a task by selecting **Tasks → SSH2 → SFTP**.  JaSFtp File Engine Settings Tasks Utilities Logs Help SSH2 Ftp Monitors Archive Variables Administrative Chain SSH2/SFTP profiles SSH2 Keygen SSH2 SFTP SFTP monitor SFTP Synchronize SFtp Ftp Tasks Schedule Edit Run tasks ask Type Task Title

Step	Description
7.	Click on the **Basic** tab. Enter an appropriate name in the **Task Title** field. From the drop down menu select the profile name created in Steps 4 and 5 for the **Profile Name** field. In the **Local Dir** field enter the path for the local directory where the files will be stored. In the **Filename** field enter a string to filter out the files needed.  SFTP Save Cancel Help Basic Advanced Task Title: Remote_Site Profile Name: Remote LSP Ftp option: get files Remote Dir: Local Dir: C:\FTPData ☐ Backup local file to ☐ Backup remote file to ☐ Use staging. Final folder Filename: !L*0^!.bash^* Folder path filter: Rename Filename: Append to filename: Do Not Append Umask permissions: Transfer type: auto

Step	Description
8.	Click on the **Advanced** tab and select **Delete source file after transfer**  ☐ Include Subdirectories ☑ Delete source file after transfer ☐ Transfer with temporary extension .tmp ☐ Transfer if modified date is older than Minute ☐ Transfer modified files using FtpLog ☑ Log transfer ☐ Transfer modified files Ftp Server Time Offset (minutes) ☐ Maintain timestamp Place files in new subdirectory based on date? Do Not Append Set Remote EOL carriage return + line feed

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td><b>9.</b></td><td>In the JaSFtp screen click the <b>Tasks</b> tab. In the left pane under <b>tasks</b>, right click the task title, <b>Remote_Site</b>, created in Step 7 and select <b>New Schedule</b>. In the dialog box select the relevant options appropriate to the environment for the frequency of how often the task will run to retrieve the CDRs from the LSP server. Click <b>Save</b>.



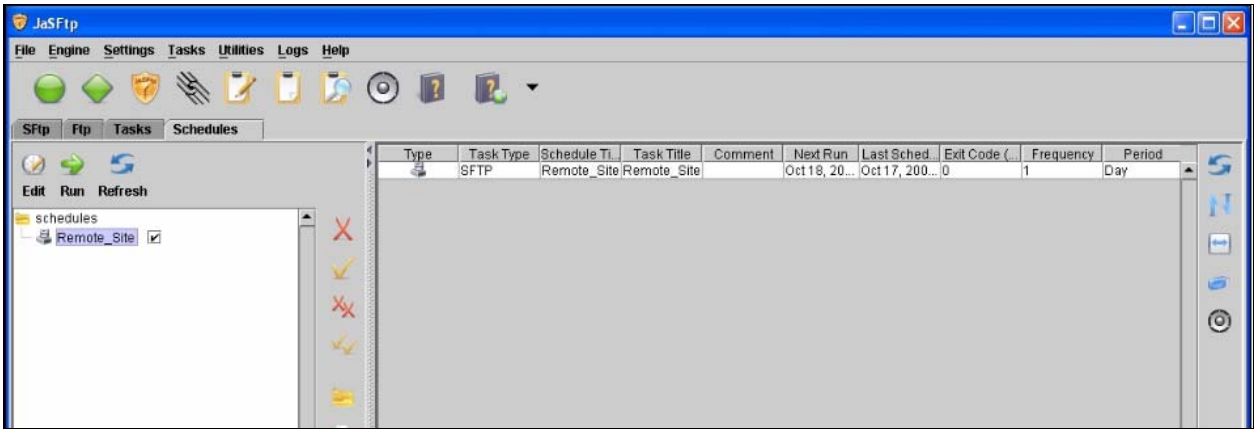
<table>
<tr><th>Type</th><th>Task Type</th><th>Task Title</th><th>Comment</th><th>Exit Code</th><th>Last Run</th><th>Run Duration</th></tr>
<tr><td></td><td>SFTP</td><td>Remote_Site</td><td></td><td>0</td><td>Oct 17, 200...</td><td>688</td></tr>
</table>

Oct 17, 2007 6:06:05 PM - You are creating a new schedule

Task Type = SFTP Task Title = Remote_Site

Run Every 1 Day Time 1 0 AM

Select Days
☑ Sunday ☑ Monday
☑ Tuesday ☑ Wednesday
☑ Thursday ☑ Friday
☑ Saturday
</td></tr>
<tr><td><b>10.</b></td><td>Click on the <b>Schedules</b> tab. In the left pane expand the <b>schedules</b> heading. The tick in the check box next to the Remote_Site task title indicates the task is running.



schedules
Remote_Site ☑

<table>
<tr><th>Type</th><th>Task Type</th><th>Schedule Ti...</th><th>Task Title</th><th>Comment</th><th>Next Run</th><th>Last Sched...</th><th>Exit Code (...</th><th>Frequency</th><th>Period</th></tr>
<tr><td></td><td>SFTP</td><td>Remote_Site</td><td>Remote_Site</td><td></td><td>Oct 18, 20...</td><td>Oct 17, 200...</td><td>0</td><td>1</td><td>Day</td></tr>
</table>
</td></tr>
</table>

5. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing. The feature testing evaluated the ability of Proteus Enterprise to collect and process CDR records for various types of calls. The source and destination of each call was verified on the Proteus Enterprise application. The serviceability testing introduced failure scenarios to see if Proteus Enterprise could resume CDR collection after failure recovery.

5.1. General Test Approach

The general test approach was to verify that Proteus Enterprise collects CDR records, and properly classifies and reports the attributes regarding the following.

- Intra-switch calls
- Inbound trunk calls
- Outbound trunk calls
- Conference calls
- Transfer calls
- Forwarded calls

For serviceability testing, logical links were disabled and re-enabled.

5.2. Test Results

All feature and performance tests passed. Proteus Enterprise successfully captured and processed call records from Avaya Communication Manager. Proteus Enterprise also successfully processed the CDR data, performed call costing, and produced call accounting reports.

Proteus Enterprise successfully collected the CDR records from Avaya Communication Manager for all types of calls generated including intra-switch calls, inbound/outbound PSTN trunk calls, inbound/outbound private IP trunk calls, transferred calls, and conference calls. For serviceability testing, Proteus Enterprise was able to resume collecting CDR records after failure. During the fail over of the Main Avaya Communication Manager to the LSP, CDR records that were created and stored on the LSP were successfully retrieved and processed by Proteus Enterprise during the fail back to the Main Avaya Communication Manager. Proteus Enterprise continued collecting the CDR records from the Main Avaya Communication Manager.

6. Verification Steps

The following steps may be used to verify the configuration.

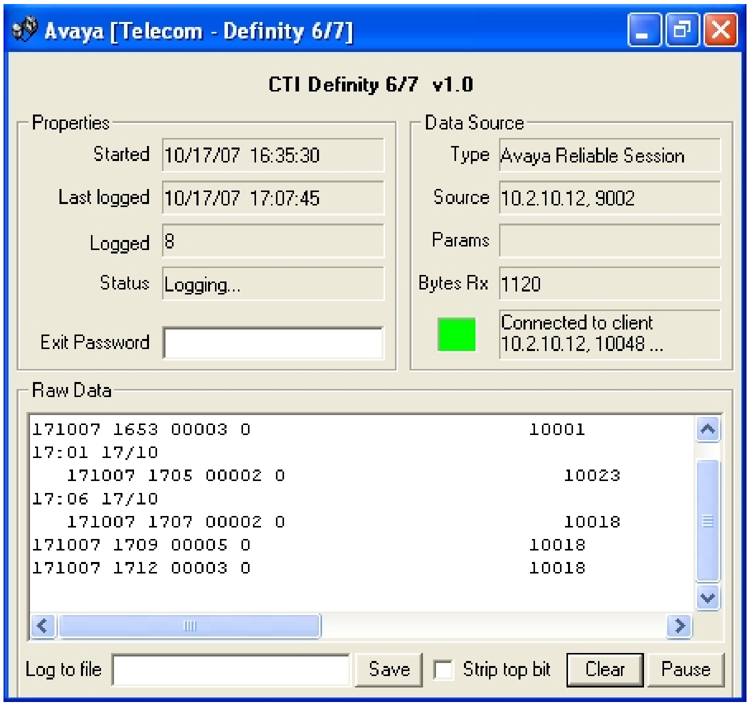
<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>

On the SAT, enter the **status cdr-link** command to verify that the CDR link state is up.

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

       Link State: up                            CDR not administered
Number of Retries:
      Date & Time: 0   /0 /0  0 :0 :0            0   /0 /0  0 :0 :0
  Forward Seq. No: 0                             0
 Backward Seq. No: 0                             0
CDR Buffer % Full:   0.19                          0.00
      Reason Code:
```

</td></tr>
<tr><td>2.</td><td>

Place a call and verify that Proteus Enterprise received the CDR record for the call and then processed the call. The following Switch Interface screen is launched after Step 6 in Section 4.1. The Switch Interface screen displays the Proteus Enterprise is connected, monitoring and logging the CDRs from the Main Avaya Communication Manager server.



Avaya [Telecom - Definity 6/7]

CTI Definity 6/7 v1.0

Properties

Started: 10/17/07 16:35:30

Last logged: 10/17/07 17:07:45

Logged: 8

Status: Logging...

Exit Password:

Data Source

Type: Avaya Reliable Session

Source: 10.2.10.12, 9002

Params:

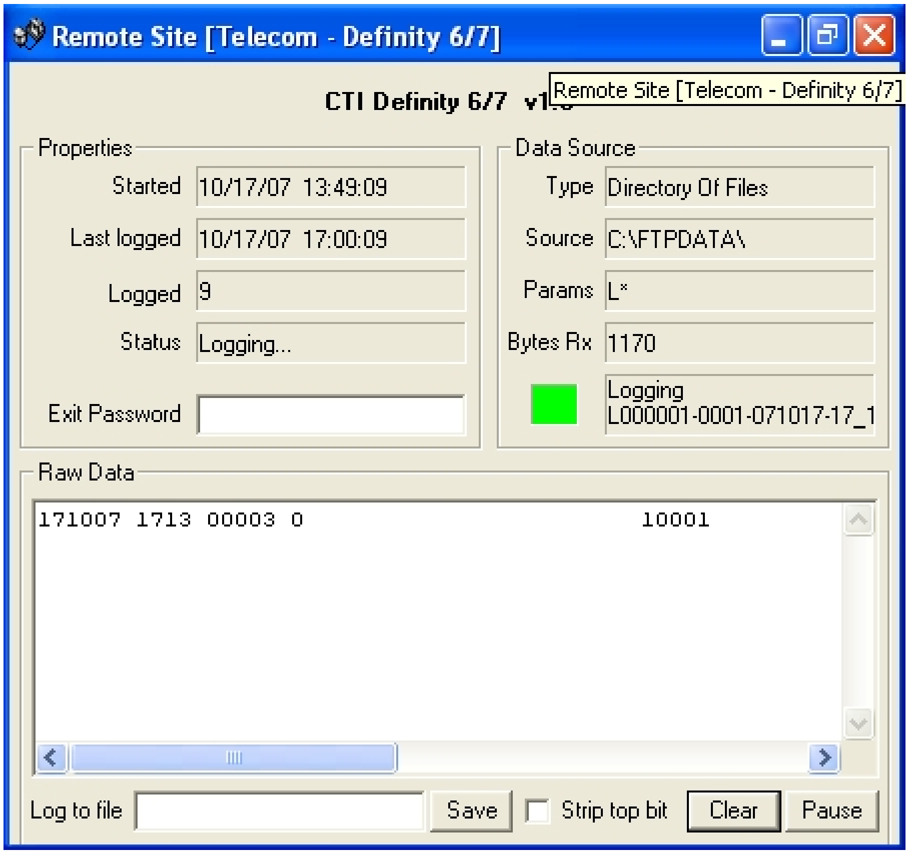
Bytes Rx: 1120

🟩 Connected to client 10.2.10.12, 10048 ...

Raw Data

```
171007 1653 00003 0                          10001
17:01 17/10
   171007 1705 00002 0                          10023
17:06 17/10
   171007 1707 00002 0                          10018
171007 1709 00005 0                          10018
171007 1712 00003 0                          10018
```

</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td><b>3.</b></td><td>The following Switch Interface is also launched after Step 6 in Section 4.1. This Switch Interface screen below displays the Proteus Enterprise is connected, monitoring and logging the LSP Avaya Communication server.


Remote Site [Telecom - Definity 6/7]

CTI Definity 6/7 v1.

Properties

Started 10/17/07 13:49:09

Last logged 10/17/07 17:00:09

Logged 9

Status Logging...

Exit Password

Data Source

Type Directory Of Files

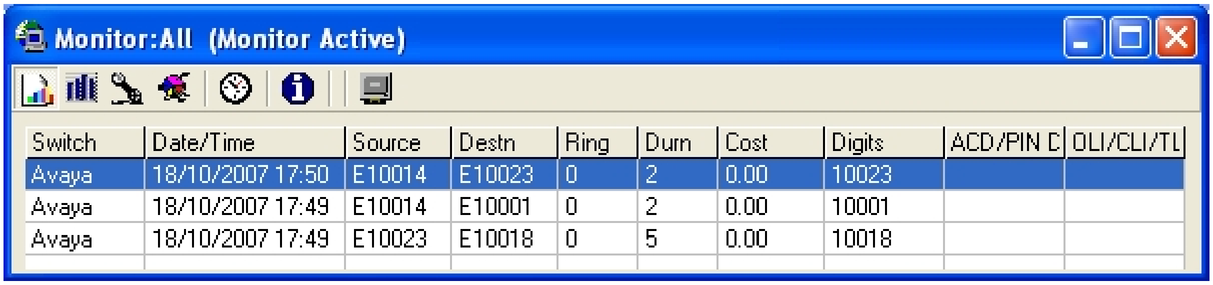
Source C:\FTPDATA\

Params L*

Bytes Rx 1170

🟩 Logging L000001-0001-071017-17_1

Raw Data
<pre>171007 1713 00003 0   10001</pre>

Log to file Save □ Strip top bit Clear Pause
</td></tr>
<tr><td><b>4.</b></td><td>The following Proteus Enterprise Real Time Monitor screen allows you to verify the processed calls.


Monitor:All (Monitor Active)
<table>
<tr><th>Switch</th><th>Date/Time</th><th>Source</th><th>Destn</th><th>Ring</th><th>Durn</th><th>Cost</th><th>Digits</th><th>ACD/PIN C</th><th>OLI/CLI/TL</th></tr>
<tr><td>Avaya</td><td>18/10/2007 17:50</td><td>E10014</td><td>E10023</td><td>0</td><td>2</td><td>0.00</td><td>10023</td><td></td><td></td></tr>
<tr><td>Avaya</td><td>18/10/2007 17:49</td><td>E10014</td><td>E10001</td><td>0</td><td>2</td><td>0.00</td><td>10001</td><td></td><td></td></tr>
<tr><td>Avaya</td><td>18/10/2007 17:49</td><td>E10023</td><td>E10018</td><td>0</td><td>5</td><td>0.00</td><td>10018</td><td></td><td></td></tr>
</table>
</td></tr>
</table>

7. Support

If technical support is required for CTI Data Solutions Proteus Enterprise, contact Technical Support.

WWW: http://support.ctidata.co.uk.

Email: support@ctidata.co.uk

Phone: +44 (0) 84 5123 2761

8. Conclusion

These Application Notes describe the required configuration steps for Proteus Enterprise to collect call detail records from Avaya Communication Manager. Proteus Enterprise 6.1 was successfully compliance tested with Avaya Communication Manager 4.0.1.

9. Additional References

This section references the product documentation that are relevant to these Application Notes.

Avaya product documentation can be found at http://support.avaya.com.

- *Administrator Guide for Avaya Communication Manager (4.0)*, Document ID 03-300509, Issue 3.1, February 2007.

The following documentation is available on request from CTI Data Solutions Ltd.

Proteus Enterprise:

- Proteus Enterprise v6 Installation Guide.doc
- Getting Started with Proteus Enterprise 6

More information is available for Proteus Enterprise at http://www.ctidata.co.uk/Solutions/ProteusEnterprise.aspx

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.