Avaya Solution & Interoperability Test Lab

Application Notes for PAETEC Communications PINNACLE Communication Management Suite with Avaya Communication Manager – Issue 1.0

Abstract

These Application Notes describe the configuration procedures required for PAETEC Communications PINNACLE Communication Management Suite to successfully interoperate with Avaya Communication Manager to collect call detail records (CDR) using Avaya Reliable Session Protocol (RSP) over TCP/IP. PAETEC Communications PINNACLE Communication Management Suite is a software application toolset with applications for managing costs, billing, invoicing, service requests, trouble tickets, inventory, infrastructure and switch provisioning. This particular solution focused only on the ability of PINNACLE to process call detail records for call usage analysis and call accounting.

The general test approach was to perform a set of call scenarios that would generate varied data in the call detail records and verify that PINNACLE properly parsed and displayed the record fields. The call scenarios included inbound trunk calls, outbound trunk calls and intra-switch calls. Basic serviceability and performance testing was also 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

These Application Notes describes a compliance-tested call detail recording (CDR) solution comprised of Avaya Communication Manager and PAETEC Communications PINNACLE Communication Management Suite. PAETEC Communications PINNACLE Communication Management Suite is a software application toolset with applications for managing costs, billing, invoicing, service requests, trouble tickets, inventory, infrastructure and switch provisioning. This particular solution focused only on the ability of PINNACLE to process call detail records for call usage analysis and call accounting.

Avaya Communication Manager sends call detail records via the Avaya Reliable Session Protocol (RSP). RSP provides a transport mechanism for reliable delivery of CDR records over TCP/IP. PINNACLE does not terminate the RSP protocol. Instead, it relies on a third party buffering device to do this function that sits logically in the path between Avaya Communication Manager and PINNACLE. The device collects and stores the CDR records from Avaya Communication Manager and then periodically transfers the records via FTP to a network FTP server. PINNACLE then periodically processes the file on the FTP server via a mapped network drive or mounted file system. PAETEC Communications resells the Omnitronix Data-Link DL-150 for use as a buffering device. This same device was used in the compliance test.

Avaya Communication Manager can generate call detail records for intra-switch calls, inbound trunk calls and outbound trunk calls. In addition, split records can be generated for transferred calls and conference calls. PINNACLE supports multiple CDR formats. The expanded format was used for the compliance test.

PINNACLE is comprised of three primary components; the database server which stores the data and contains much of the code in stored procedures, the client application which provides the user interface for configuration and initial set-up, and the web client that provides a full featured user interface for extracting data and creating reports. Typically in a large enterprise, these three components would run on separate machines. For the purposes of the compliance test, the database server and client application were run on the same Windows PC. The web client was run on a separate PC.

Figure 1 illustrates the network configuration that was used for the compliance test. The configuration consists of two Media Servers. The first is an Avaya S8300 Media Server running Avaya Communication Manager residing in an Avaya G700 Media Gateway. There are Avaya 6400D Series Digital Telephones and a PSTN PRI trunk connected to the Media Gateway. There are Avaya 4600 Series IP Telephones registered to the Media Server.

The second Media Server is an Avaya S8500 Media Server running Avaya Communication Manager with an Avaya G650 Media Gateway. There are Avaya 4600 Series IP Telephones registered to the Media Server.

All network components are connected to an IP network comprised of an Extreme Networks Alpine 3804 switch and Avaya C363T-PWR Converged Stackable Switch. A Windows 2000 PC

is connected to the network that hosts PAETEC Communications PINNACLE Communication Management Suite database server and client application. This PC also hosts a FTP server. A second PC running Windows 2000 is connected to the network to host the PINNACLE web client. An Omnitronix Data-Link DL-150 is connected to the network. A RSP session is established from Avaya Communication Manager running on the Avaya S8300 Media Server to this device to collect CDR records. In addition, a H.323 IP trunk is established between the two Avaya Media Servers so calls can be placed from one to the other.

Note: CDR data is collected only from one server, the Avaya S8300 Media Server. The Avaya S8500 Media Server and Avaya G650 Media Gateway only appear in the test configuration to generate IP trunk calls to and from the Avaya S8300 Media Server.

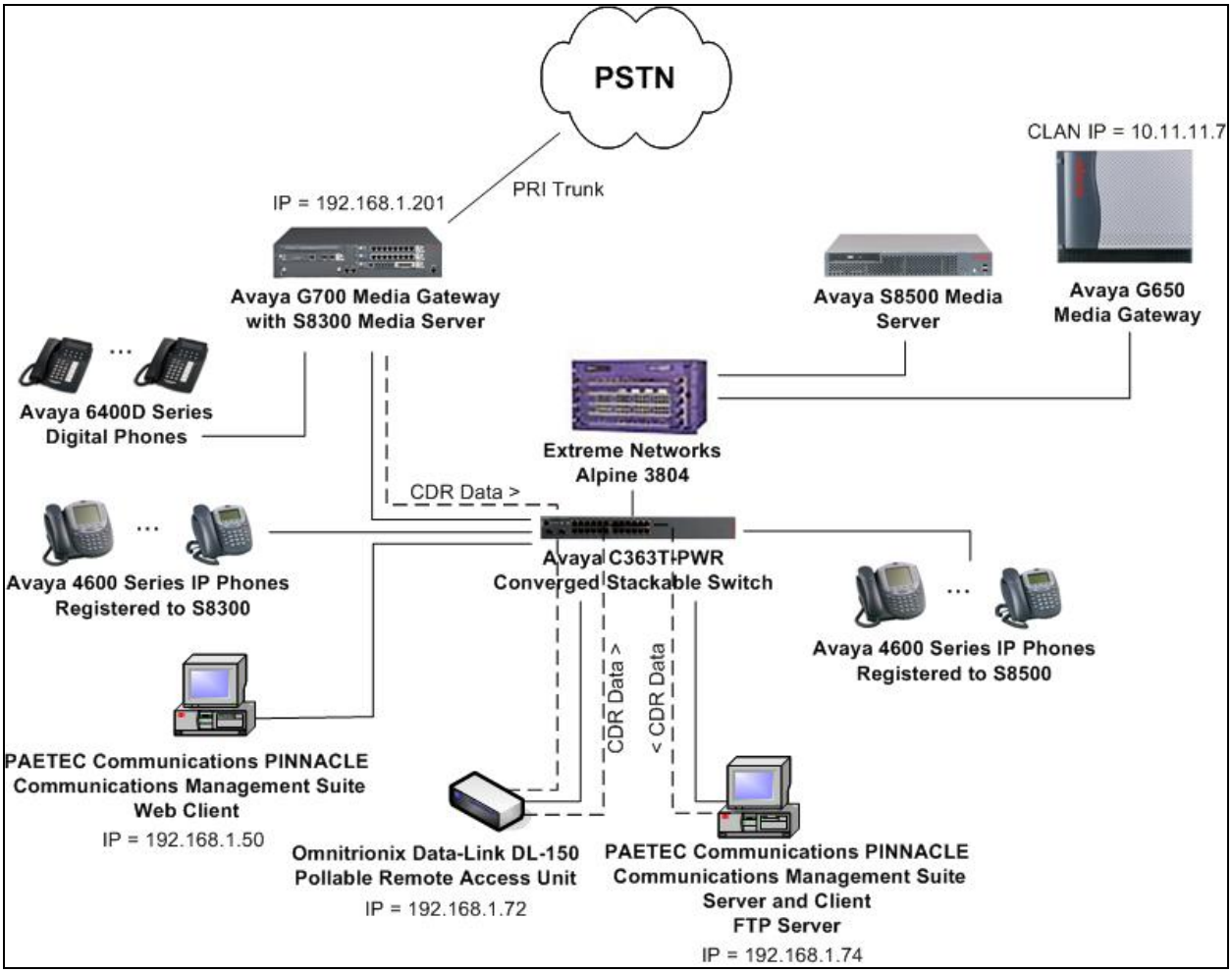


Figure 1: Test Configuration for Collecting CDR Data from a Single Server

2. Equipment and Software Validated

The following equipment and software/firmware were used for the test configuration provided.

Equipment	Software/Firmware
Avaya S8300 Media Server	Communication Manager 3.0.1 (R013x.00.1.346.0)
Avaya G700 Media Gateway (Media Gateway Processor)	24.21.1
Avaya S8500 Media Server	Communication Manager 3.0.1 (R013x.00.1.346.0)
Avaya G650 Media Gateway	-
TN2312BP IP Server Interface (IPSI)	HW 03 FW 22
TN799DP C-LAN Interface (C-LAN)	HW 01 FW 16
TN2302AP IP Media Processor (MEDPRO)	HW 20 FW 108
Avaya 4600 Series IP Telephones	2.3 (4610SW H.323) 2.3 (4620SW H.323) 2.5 (4625SW H.323)
Avaya 6400D Series Digital Telephones	-
Avaya C363T-PWR Converged Stackable Switch	4.5.14
Extreme Networks Alpine 3804	7.2.0 Build 25
PAETEC Communications PINNACLE Communication Management Suite (database server, and client application components)	5.4.2 (running on Windows 2000 Professional SP4)
PAETEC Communications PINNACLE Communication Management Suite (web client component)	5.4.2 (running on Windows 2000 Professional SP4)
Omnitronix Data-Link DL-150 Pollable Remote Access Unit	1.06

3. Configure Avaya Communication Manager

This section describes the procedure for configuring call detail recording on Avaya Communication Manager. These steps are performed through the System Access Terminal (SAT). These steps describe the procedure used for the Avaya S8300 Media Server. All steps are the same for the other media servers unless otherwise noted. Avaya Communication Manager will be configured to generate CDR records using RSP over TCP/IP to the IP address of the Omnitronix Data-Link DL-150. For the Avaya S8300 Media Server, the RSP link originates at the IP address of the local media server. For other Avaya Media Servers, the RSP link originates at the IP address of the C-LAN board.

Step	Description
1.	Use the **change node-names ip** command to create a new node name with the IP address of the Omnitronix Data-Link DL-150. The example below shows a node name of *BufferDevice* was created for the Omnitronix Data-Link DL-150. The IP address is set to *192.168.1.72* as shown in **Figure 1**. This will be the far-end of the RSP link and will be used in Step 3. `change node-names ip` Page 1 of 1 IP NODE NAMES Name / IP Address / Name / IP Address **BufferDevice 192.168.1 .72** Wireless-S8500 10 .11 .11 .7 default 0 .0 .0 .0 procr 192.168.1 .201
2.	Next, the node name of the near end of the RSP link must be determined. This information will be used in Step 3. If the Avaya S8300 Media Server is used, the near end of the RSP link is the Media Server node name and is pre-defined as *procr*. If any other Media Server is used, the near end of the RSP link is the C-LAN board. To locate the node name of the C-LAN, use the **list ip-interface all** command. If multiple C-LANs are displayed, locate the C-LAN in the list that will be used for the RSP connection. Note the name in the **Node Name / IP-Address** field.
3.	Use the **change ip-services** command to define the CDR link to use RSP over TCP/IP. To define a primary CDR link, set the **Service Type** to *CDR1*. A secondary link can be defined by setting **Service Type** to *CDR2*. If using the Avaya S8300 Media Server, the **Local Node** is set to *procr* which is the node name of the local processor. If using another Avaya Media Server, the node name is set to the node name of the C-LAN board. The **Local Port** number is fixed to *0*. The **Remote Node** is set to the node name that was created in Step 1 for the Omnitronix Data-Link DL-150. The **Remote Port** may be set to a value between 5000 and 64500 inclusive and must match the port configured in the Omnitronix Data-Link DL-150. See Section 4 Step 5. The example below shows the values used in the compliance test using an Avaya S8300 Media Server. `change ip-services` Page 1 of 3 IP SERVICES Service Type / Enabled / Local Node / Local Port / Remote Node / Remote Port **CDR1 procr 0 BufferDevice 9000**

Step	Description
4.	On Page 3 of the **change ip-services** command, enable the RSP for the CDR link by setting **Reliable Protocol** to *y*. Default values can be used for the other fields.

```
change ip-services                                          Page   3 of   3

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

 CDR1             y         30                3          3         60
```

Step	Description
5.	Use 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 example below shows the values used in the compliance test. **CDR Date format:** *month/day* **Primary Output Format:** *expanded* **Primary Output Endpoint:** *CDR1* **Use ISDN Layouts?** *n* **Use Enhanced Formats?** *n* **Modified Circuit ID Display?** *n* 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. • **Record Outgoing Calls Only?** *n* [Allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls.] • **Suppress CDR for Ineffective Call Attempts?** *y* [Prevents calls that are blocked from appearing in the CDR record.] • **Intra-switch CDR?** *y* [Allows call records for internal calls involving specific stations.] • **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):                        CDR Date Format: month/day
      Primary Output Format: expanded      Primary Output Endpoint: CDR1
    Secondary Output Format:
          Use ISDN Layouts? n
       Use Enhanced Formats? n      Condition Code 'T' For Redirected Calls? n
Modified Circuit ID Display? n                   Remove # From Called Number? n
                  Record Outgoing Calls Only? n            Intra-switch CDR? y
  Suppress CDR for Ineffective Call Attempts? y     Outg Trk Call Splitting? y
      Disconnect Information in Place of FRL? n       Outg Attd Call Record? y
                                                    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

     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: 5
```

Step	Description

6.	If **Intra-switch CDR** is set to *y*, use the **change intra-switch-cdr** command to define the extensions that will be subject to call detail records. In the **Assigned Members** field, enter a specific extension whose usage will be tracked with a CDR record. Add an entry for each additional extension of interest.
	
	`change intra-switch-cdr` Page 1 of 2
	`INTRA-SWITCH CDR`
	
	`Assigned Members: 4 of 1000 administered`
	`1: 3000 19: 37: 55: 73: 91:`
	`2: 3001 20: 38: 56: 74: 92:`
	`3: 3010 21: 39: 57: 75: 93:`
	`4: 3011 22: 40: 58: 76: 94:`
	`5: 23: 41: 59: 77: 95:`
	`6: 24: 42: 60: 78: 96:`
	`7: 25: 43: 61: 79: 97:`
	`8: 26: 44: 62: 80: 98:`
	`9: 27: 45: 63: 81: 99:`
	`10: 28: 46: 64: 82: 100:`
	`11: 29: 47: 65: 83: 101:`
	`12: 30: 48: 66: 84: 102:`
	`13: 31: 49: 67: 85: 103:`
	`14: 32: 50: 68: 86: 104:`
	`15: 33: 51: 69: 87: 105:`
	`16: 34: 52: 70: 88: 106:`
	`17: 35: 53: 71: 89: 107:`
	`18: 36: 54: 72: 90: 108:`

7.	For each trunk group for which CDR records are desired, verify that CDR reporting is enabled. To do this, 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 3` Page 1 of 19
	`TRUNK GROUP`
	
	`Group Number: 3 Group Type: isdn` **`CDR Reports: y`**
	`Group Name: PSTN PRI 2 COR: 1 TN: 1 TAC: 103`
	`Direction: two-way Outgoing Display? n 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? n Out? n`
	`Answer Supervision Timeout: 0`

4. Configure Omnitronix Data-Link DL-150

This section describes the configuration of the Omnitronix Data-Link DL-150 Pollable Remote Access Unit.

Step	Description
1.	To configure the Omnitronix Data-Link DL-150, connect port 2 of the device to the serial port of a PC. Port 2 is used for administration. From the PC, launch a terminal emulator application such as HyperTerminal. Configure the terminal emulator to use the serial port connected to the device with the following parameters: 19200 bits/sec, 8 data bits, no parity, 1 stop bit, and Xon/Xoff flow control. Initiate a serial connection from the PC to the device. No prompt is provided by the device. Type **status** on the blank display to view current settings and to verify communication.

```
status
Data-Link DL150 1.06 STD       Unit Serial #  : 540001450
Unit ID : Data-Link

Date    : MON 02/20/06         % Full alarm   : OFF
Time    : 09:00:37             No Data Alarm 1: OFF
Memory  : 32768K               No Data Alarm 2: OFF
% Full  : 01%                  Release mode   : LINE
Modem   : Yes                  Duplex         : FULL
Network : Yes                  Password       : OFF
IP Add  : 192.168.1.72         Compress       : OFF
MAC Add : 00:10:A3:01:3D:48
--------------------------------------------------------------------------
               Port 1    Port 2    Port 3    Port 4
Baud Rate      19200     19200     19200     19200
Parity, etc.   8N1       8N1       8N1       8N1
File Records   00000003  00000000  00000000  00000000
File Bytes     00000207  00000000  00000000  00000000
File % Full    00%       00%       00%       00%
ASCII/Binary   ASCII     ASCII     ASCII     ASCII
Handshake      XON/XOFF  XON/XOFF  XON/XOFF  XON/XOFF
File Wrap      OFF       OFF       OFF       OFF
Alarm Filter   OFF       OFF       OFF       OFF
COMPLETE
```

Step	Description
2.	To access the main setup menu, type **setup**. The first step is to set the network settings including the initial IP address. To adjust these settings, choose the menu option for **Network Settings** by typing an *a* next to the **Enter your Selection** prompt. Do not follow menu option selections with a carriage return. **setup** Data-Link DL150 - Main Setup Menu A) **Network Settings** B) Serial Settings C) Modem Settings D) User Profile Settings E) Alarm/Filter Definitions F) Action Definitions G) General Settings H) Alarm Log Settings I) Audit Log Settings Enter your Selection: **a**

Step	Description
3.	The **Network Settings** menu is displayed with the current values of the settings for options **A - F**. Enter the appropriate values for options **A – C**. Default values will be used for options **D** and **E**. To change a value, enter the menu option next to the **Enter your Selection** prompt. When prompted, enter the new value for the selected parameter. Do not follow the entry with a carriage return. Option **F** will be addressed in the next step. The example below shows the values used by the compliance test. The **IP Address** parameter represents the IP address of the device and is set to *192.168.1.72* as shown in **Figure 1**. The **IP Address** value must match the IP address of the node name of the Omnitronix Data-Link DL-150 configured on Avaya Communication Manager in Section 3 Step 2. The network where the device is connected determines the values of the **Subnet Mask** and **Router Address**. For the compliance test, these values were *255.255.255.0* and *192.168.1.1* respectively. Data-Link DL150 - Network Settings A) **IP Address** **[192.168.1.72]** B) **Subnet Mask** **[255.255.255.0]** C) **Router Address** **[192.168.1.1]** D) Telnet Duplex [FULL] E) Inactivity Timeout [0] F) IP Record Collection Settings [AVAYA DEFINITY RELIABLE PROTOCOL] G) SNMP Settings H) FTP Settings I) PPP Settings J) E-mail Settings K) Real-Time Socket Settings L) SNMP Trap Capture Settings M) IP Address Restrictions Note: Changes to IP Address, Subnet Mask, or Router Address will not take effect until any open Telnet command processor sessions are ended. Enter your Selection:

Step	Description
4.	Next, verify the **IP Record Collection Settings.** The example below shows the correct setting of *AVAYA DEFINITY RELIABLE PROTOCOL*. However, if this parameter is set to any other value or to verify the settings related to this IP Record Collection method, select menu option **F**. Do not follow the entry with a carriage return.

```
Data-Link DL150 - Network Settings
A) IP Address                          [192.168.1.72]
B) Subnet Mask                         [255.255.255.0]
C) Router Address                      [192.168.1.1]
D) Telnet Duplex                       [FULL]
E) Inactivity Timeout                  [0]
F) IP Record Collection Settings       [AVAYA DEFINITY RELIABLE PROTOCOL]
G) SNMP Settings
H) FTP Settings
I) PPP Settings
J) E-mail Settings
K) Real-Time Socket Settings
L) SNMP Trap Capture Settings
M) IP Address Restrictions
   Note: Changes to IP Address, Subnet Mask, or Router
         Address will not take effect until any open
         Telnet command processor sessions are ended.

Enter your Selection: f
```

Step	Description

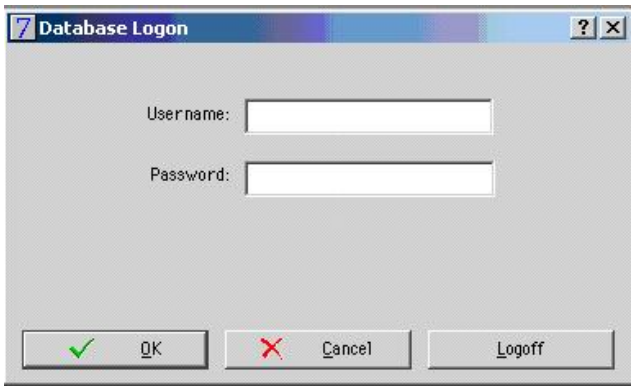
5.	The **IP Record Collection Setup** menu is displayed. To change the IP Record Collection method, select option **A**. This will display a new collection method with a new list of parameters specific to that collection method. Selecting option **A** again will select the next collection method in the list. Repeatedly selecting option **A** will cycle through the complete list of collection methods. Stop cycling through the choices when the **IP Record Collection** field is set to *AVAYA DEFINITY RELIABLE PROTOCOL.*
	
	To change any other parameter value, enter the menu option next to the **Enter your Selection** prompt. When prompted, enter the new value for the selected parameter. Do not follow the entry with a carriage return.
	
	The example below shows the values used for the compliance test. The CDR records will be stored in a file called *FILE1* and will use port *9000*. This port number must match the port number used in defining the CDR IP service on Avaya Communication Manager in Section 3 Step 2. Default values can be used for the other options.
	
	Enter a carriage return to return to the previous menu.
	
	`Data-Link DL150 - IP Record Collection (IPRC) Setup`
	`A) IP Record Collection [AVAYA DEFINITY RELIABLE PROTOCOL]`
	`B) Store Collected Data In [FILE1]`
	`C) Data Alarm/Filter Enable [OFF]`
	`D) Target Name []`
	`E) Port [9000]`
	`F) Time Stamping [OFF]`
	
	`Enter your Selection:`

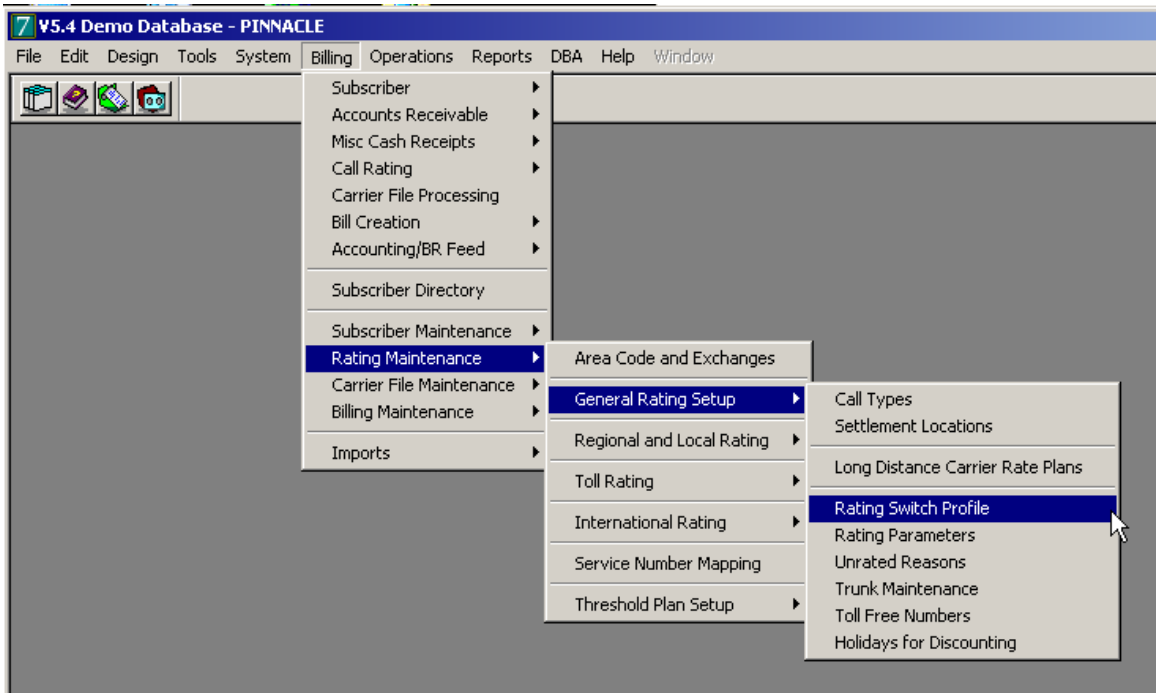
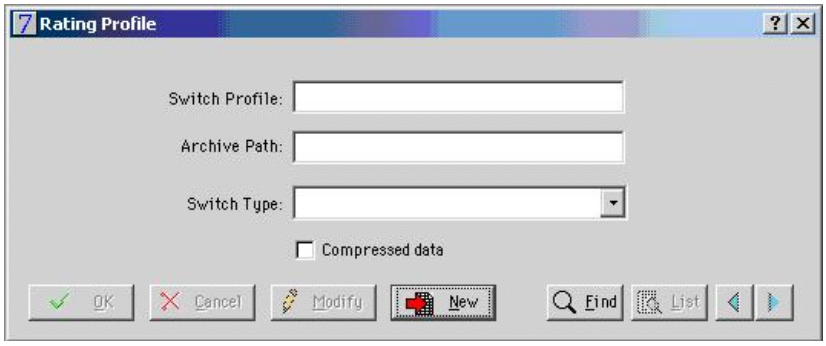
6.	The **Network Settings** menu is displayed again. Next, set the **FTP Settings**. Select menu option **H**.
	
	`Data-Link DL150 - Network Settings`
	`A) IP Address [192.168.1.72]`
	`B) Subnet Mask [255.255.255.0]`
	`C) Router Address [192.168.1.1]`
	`D) Telnet Duplex [FULL]`
	`E) Inactivity Timeout [0]`
	`F) IP Record Collection Settings [AVAYA DEFINITY RELIABLE PROTOCOL]`
	`G) SNMP Settings`
	`H) **FTP Settings**`
	`I) PPP Settings`
	`J) E-mail Settings`
	`K) Real-Time Socket Settings`
	`L) SNMP Trap Capture Settings`
	`M) IP Address Restrictions`
	`Note: Changes to IP Address, Subnet Mask, or Router`
	`Address will not take effect until any open`
	`Telnet command processor sessions are ended.`
	
	`Enter your Selection: **h**`

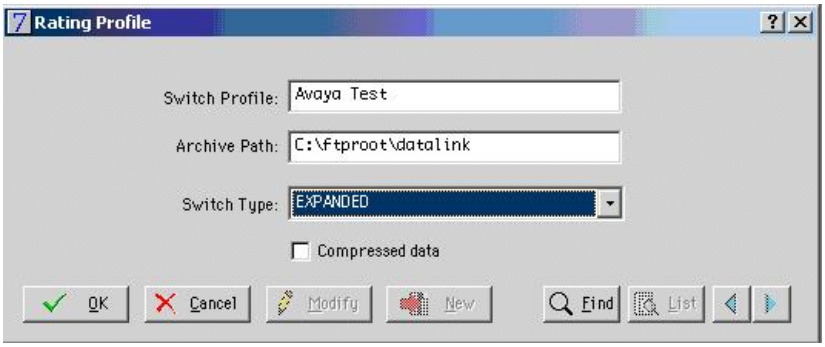
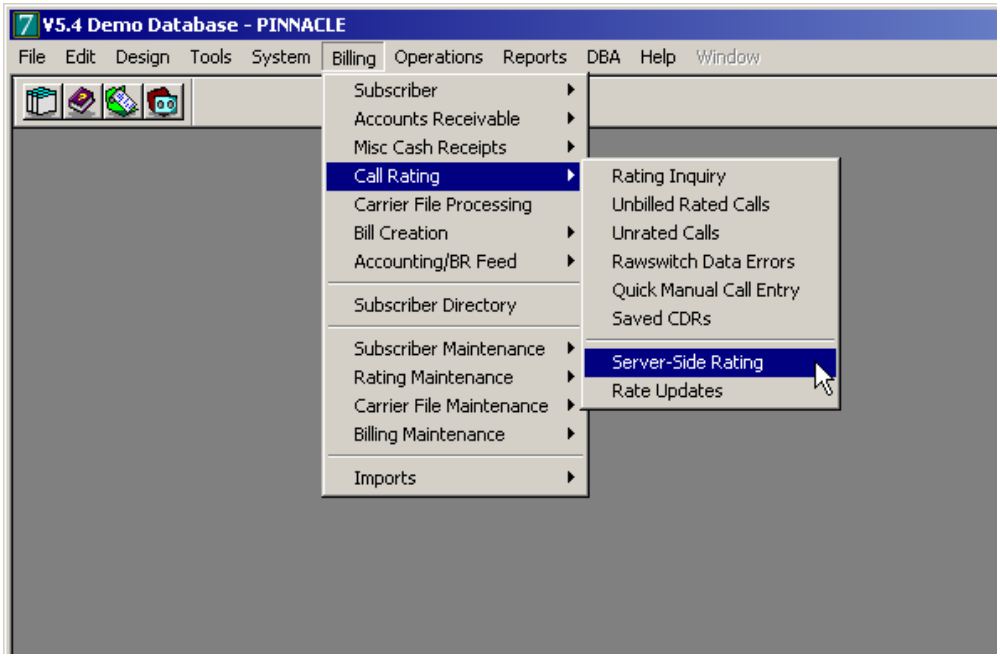
Step	Description
7.	The **FTP Settings** menu is displayed. The example below shows the values used for the compliance test. The **FTP Server Address** is the IP address of the FTP server in the network. In the case of the compliance test, this is the same host machine running PINNACLE. The **Username**, **Password**, and **Account** fields correspond to a user account established on the FTP server configured for the purpose of transferring the CDR files. Once the values are properly set, enter a carriage return to return to the previous menu. Enter two more carriage returns to exit the **setup** command and return to the command level. Data-Link DL150 - FTP Settings A) FTP AutoDelete for GETs [OFF] B) FTP Push Enable [ON] C) **FTP Server Address** **[192.168.1.74]** D) **Username** **[datalink]** E) **Password** **[datalink]** F) **Account** **[datalink]** G) Directory [] H) Minutes Between Push Attempts [10] I) Select Files to Push J) Remote File Names K) Allow FTP User Bump by New User [OFF] L) Encrypted FTP Setup [OFF] Enter your Selection:

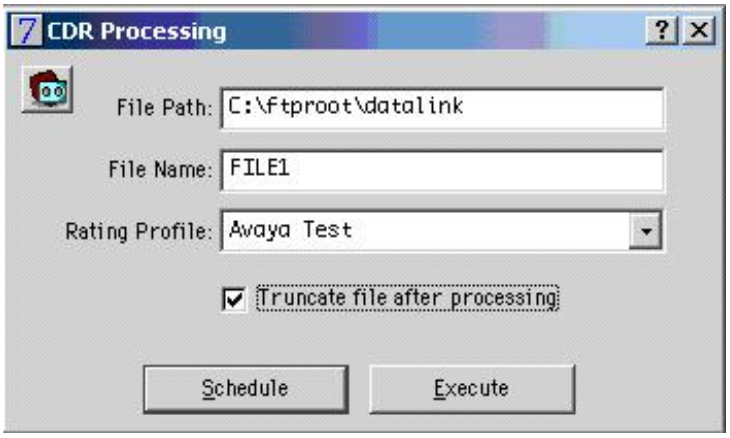
5. Configure PAETEC Communications PINNACLE Communication Management Suite

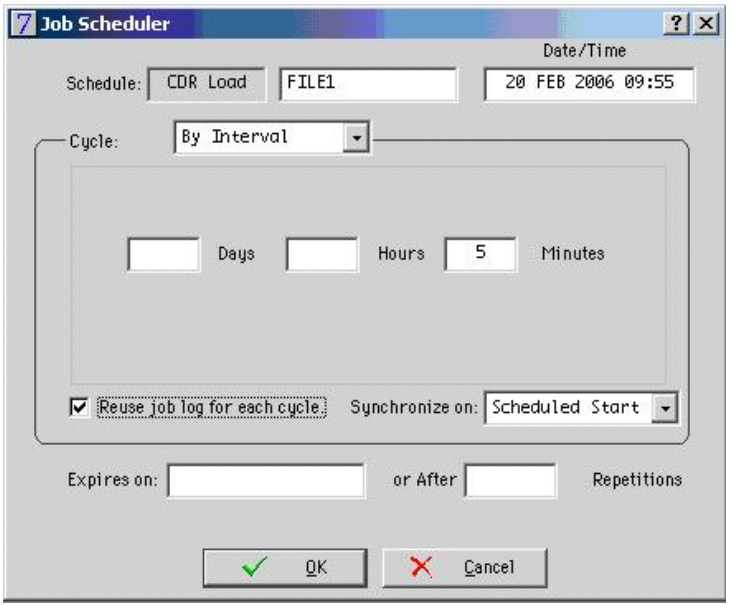
This section describes the configuration of PINNACLE. The usernames and passwords used in the following procedures were created during the initial installation. For installation procedures, please refer to reference [3]. All configuration of PINNACLE is performed through the PINNACLE client application.

Step	Description
1.	Launch the PINNACLE client from the Windows start menu by navigating to **Start → Programs → Pinnacle → PINNACLE v5.4.2**
2.	The application opens with a **Database Logon** window. Enter a valid **Username** and **Password**. Select **OK** to continue. 

Step	Description
3.	The PINNACLE client main window appears. The next step is to create a switch profile for the Avaya Media Server running Avaya Communication Manager that will be sending the CDR records. From the menu at the top of the window, navigate to **Billing → Rating Maintenance → General Rating Setup → Rating Switch Profile**. 
4.	The **Rating Profile** window appears. Select **New**. 

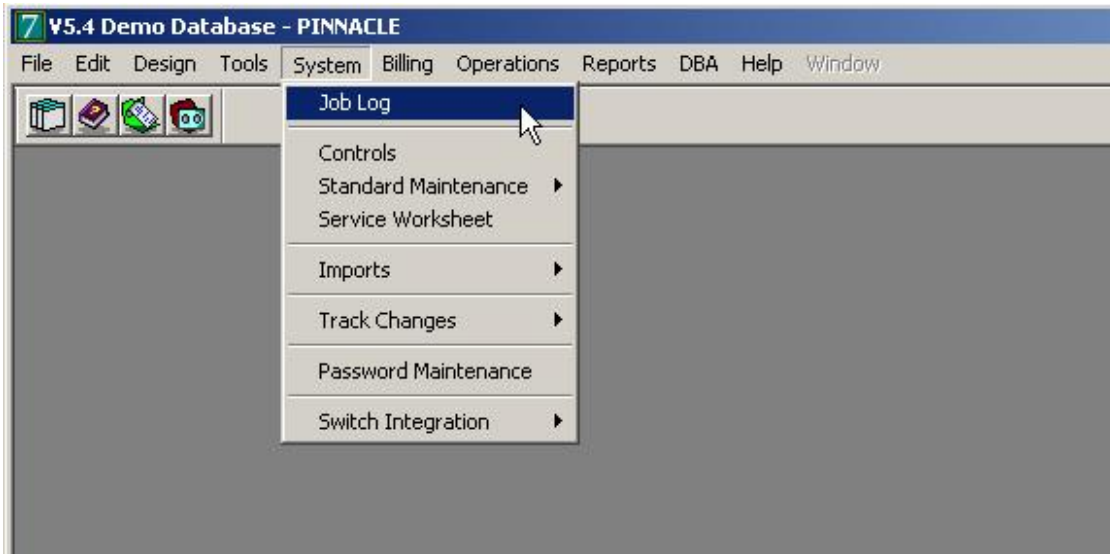
Step	Description
5.	Enter a descriptive name in the **Switch Profile** field. Set the **Archive Path** to any path that will be used to archive copies of the text files containing CDR records. Set the **Switch Type** to the desired CDR format. The example below shows the profile used for compliance testing. The **Switch Profile** was set to *Avaya Test*. Archive files were kept in the same directory where new record files are received on the FTP server. The CDR format used was *EXPANDED*. Select **OK** to continue. 
6.	Next, PINNACLE needs to be configured with information on where to locate the CDR records for this profile. To set these parameters, navigate to **Billing →Call Rating → Server-Side Rating** from the menu bar. 

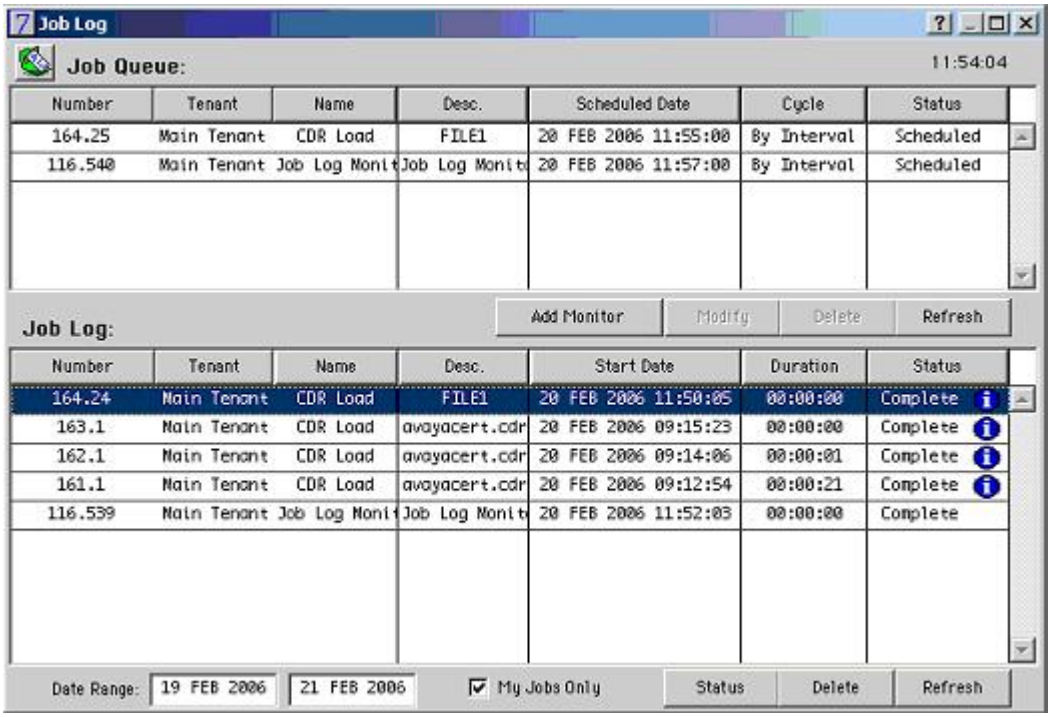
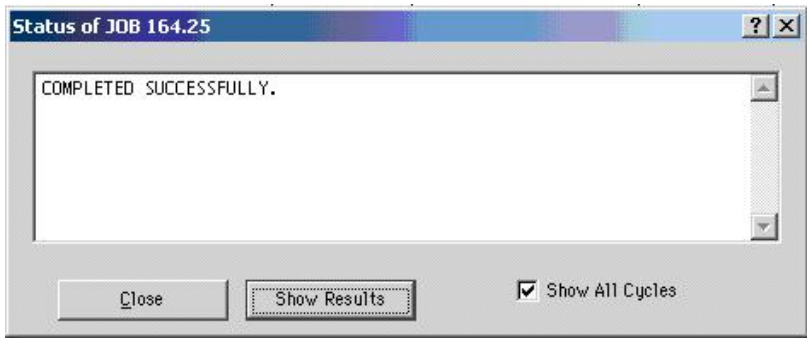
Step	Description
7.	The **CDR Processing** window appears. In the **File Path** field, enter the location where the FTP server will store the incoming files containing CDR data. In the **File Name** field, enter the name of the file containing the CDR data. This must match the same value configured on the Omnitronix DL-150 shown in Section 4 Step 5. Enter the profile name in the **Rating Profile** field of the profile created in Step 5 of this section. Lastly, click the check box next to the **Truncate file after processing** field. The example below shows the values used in the compliance test. Select **Schedule** to continue. 

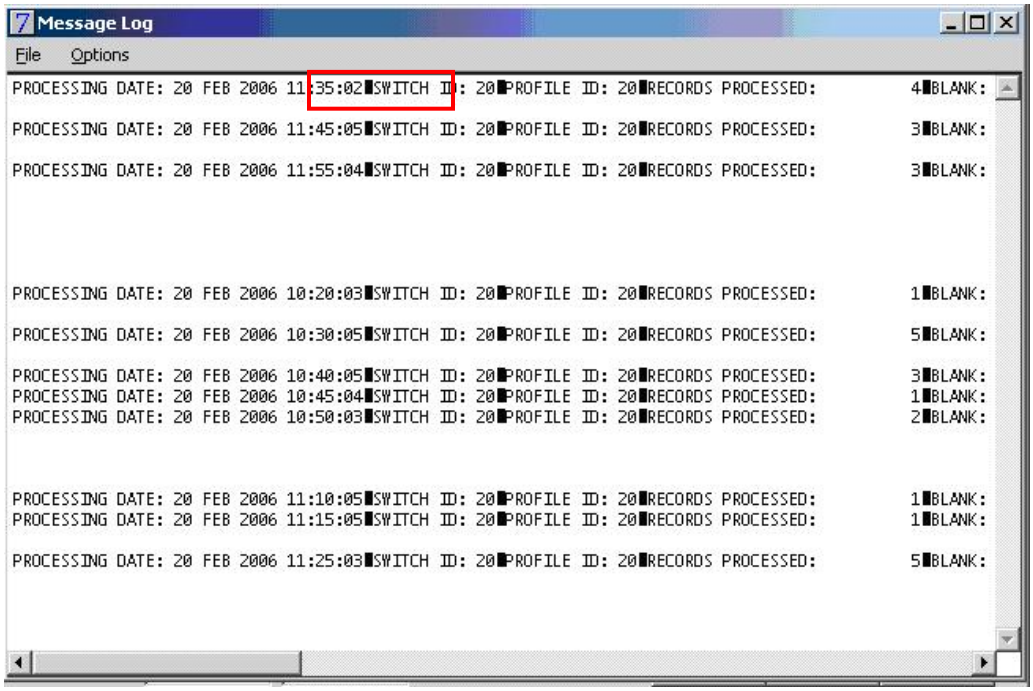
Step	Description
8.	Lastly, the **Job Scheduler** window appears. The parameters on this window determine how often PINNACLE processes the CDR files collected by the FTP Server. The example below shows typical values that were used for the compliance test. The **Cycle** field was set to *By Interval*. The interval was set to *5* minutes. Click the check box next to **Reuse job log for each cycle**. Otherwise, a new job log file is created for each processing cycle of the CDR data. Default values were used for the other fields. Select the **OK** button to complete the configuration. 

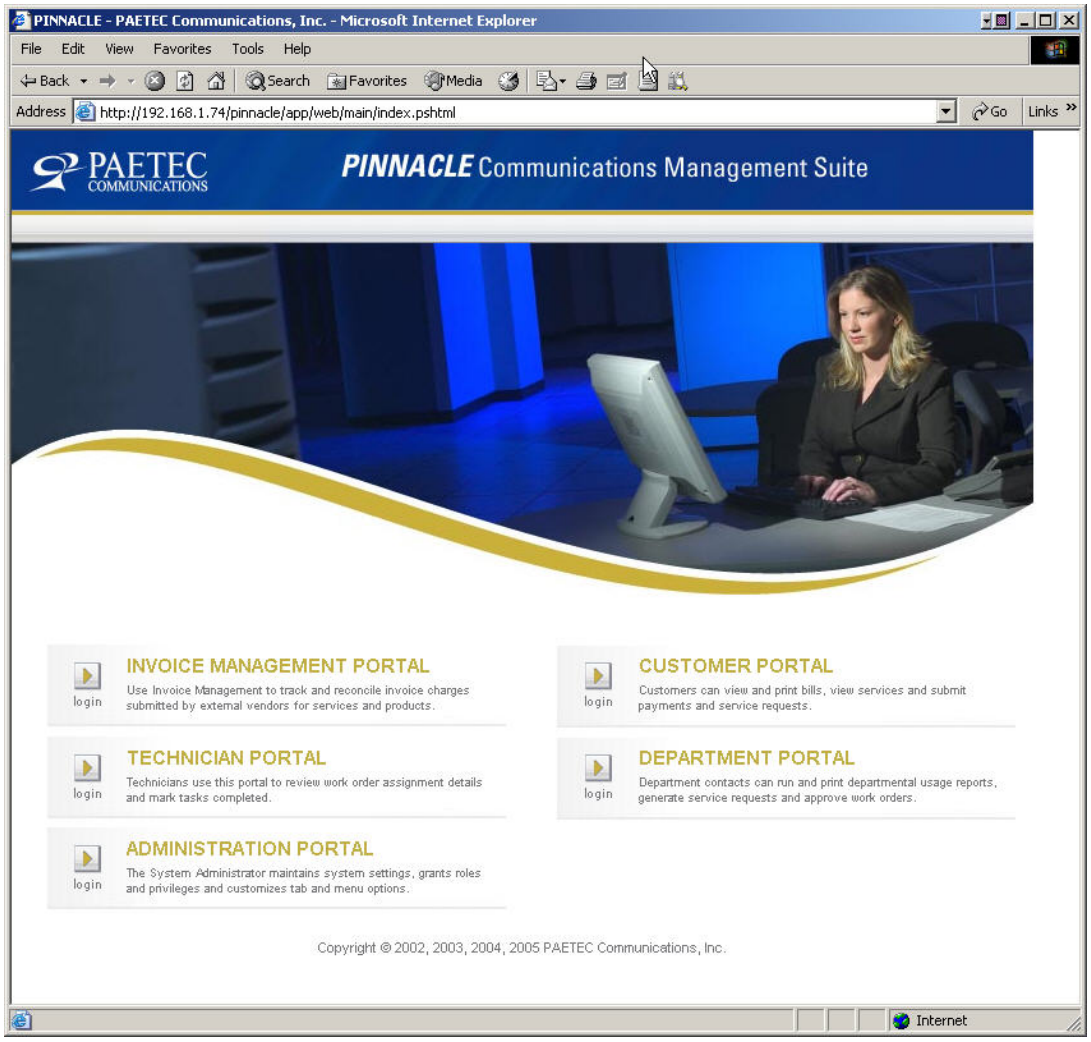
6. Using PAETEC Communications PINNACLE Communication Management Suite to View Call Reports

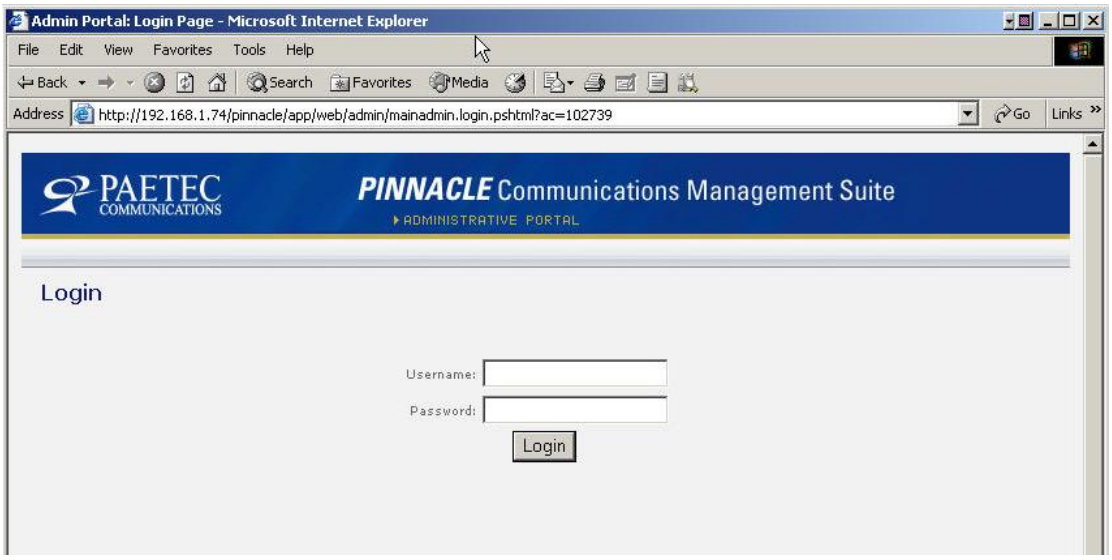
This section describes using the PINNACLE web client for viewing call summary reports of the CDR data collected from Avaya Communication Manager. The report shown in the following procedure does not display the call charges. To calculate the call charge, significantly more configuration is required including defining subscribers, carriers, local dialing areas, mapping extensions to DID numbers, rate plans, etc. These items are out of the scope of these Application Notes. For a detailed description of how to set-up the rating structure for an enterprise, please refer to reference [4] and [5].

Step	Description
1.	The PINNACLE web client is used to run the desired report. However, before the report can be run, the Switch ID must be known. This is an internal value that is assigned by the database to each switch it is managing. This value can be determined by examining the Message Log using the PINNACLE client. From the PINNACLE client main window, navigate to **System→ Job Log**. 

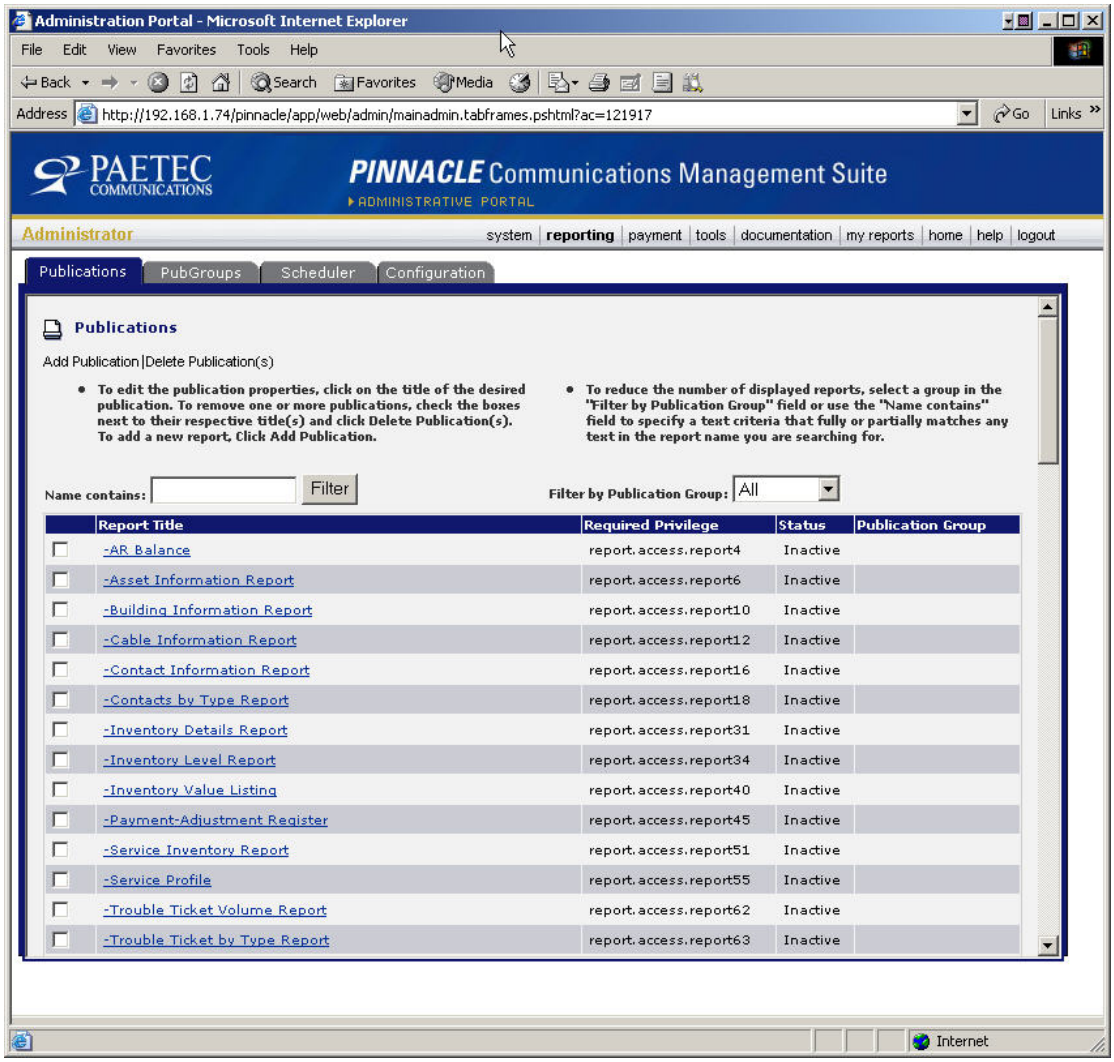
Step	Description
2.	When the **Job Log** window appears, select the **Refresh** button to update the entries in the table with the latest data. In the **Job Log** list in the lower half of the window, find the entry associated with the job processing CDR records for the switch in question. Do this by locating the CDR file name specified in Section 0 Step 7 in the **Desc** column. For the compliance test, the default CDR file name *FILE1* was used. In the example below, this entry is highlighted in the list. Double-click on this entry to open the **Message Log**. 
3.	A status window appears. Select **Show Results** to continue. 

Step	Description
4.	The **Message Log** appears. The Switch ID is shown in each entry in the log in the **SWITCH ID** field. The Switch ID is an internal system generated value. In the example below, the **SWITCH ID** is *20*. This is the value that will be needed in subsequent steps to run the reports. 

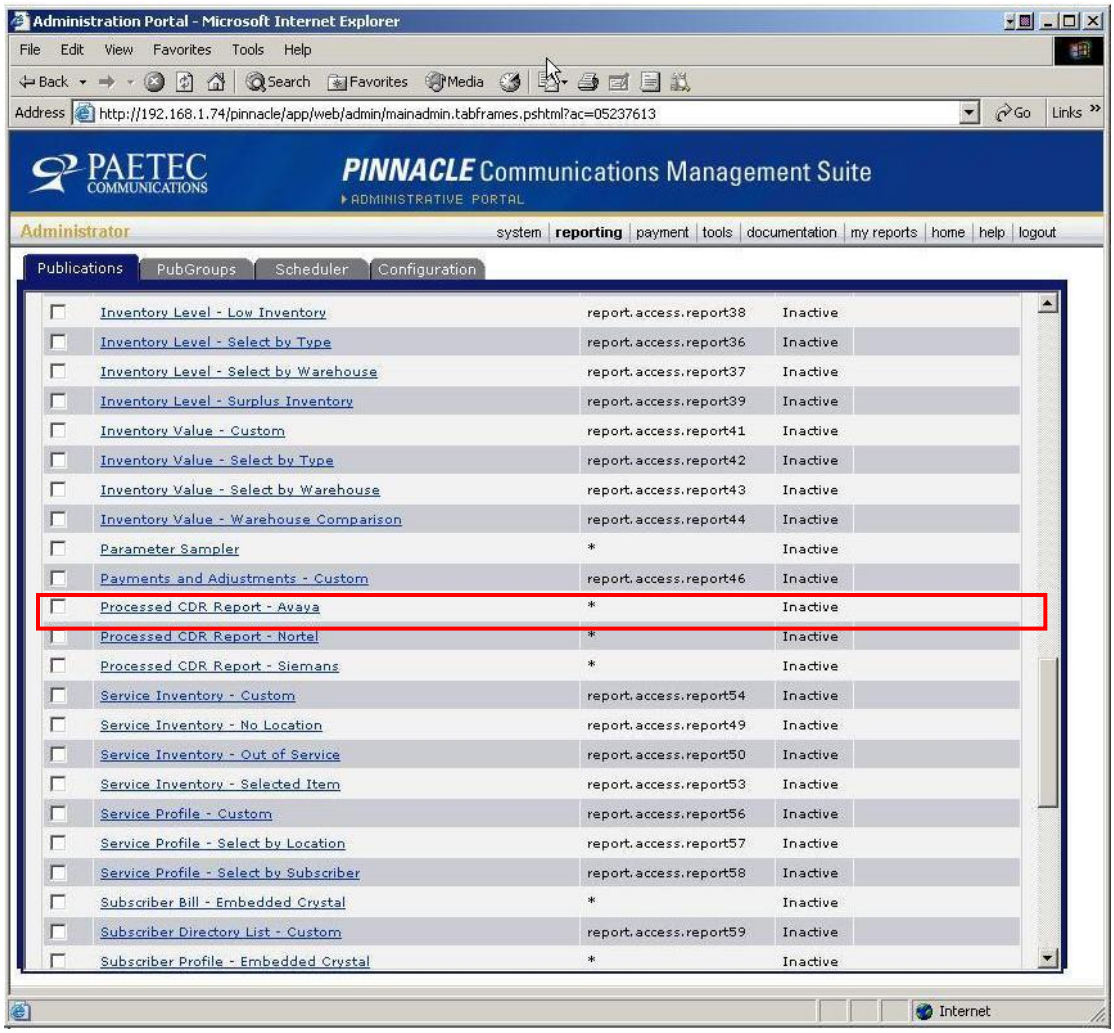
Step	Description
5.	To run the report, use the PINNACLE web client. Open a web browser and enter the following URL in the **Address** field: http://*ip_address*/pinnacle/app/web/main/index.pshtml where *ip_address* is the IP address of the PINNACLE database server. The example below shows the URL used for the compliance test. The IP address of the PINNACLE database server was *192.168.1.74* as shown in **Figure 1**. Select the **ADMINISTRATION PORTAL** to continue. 

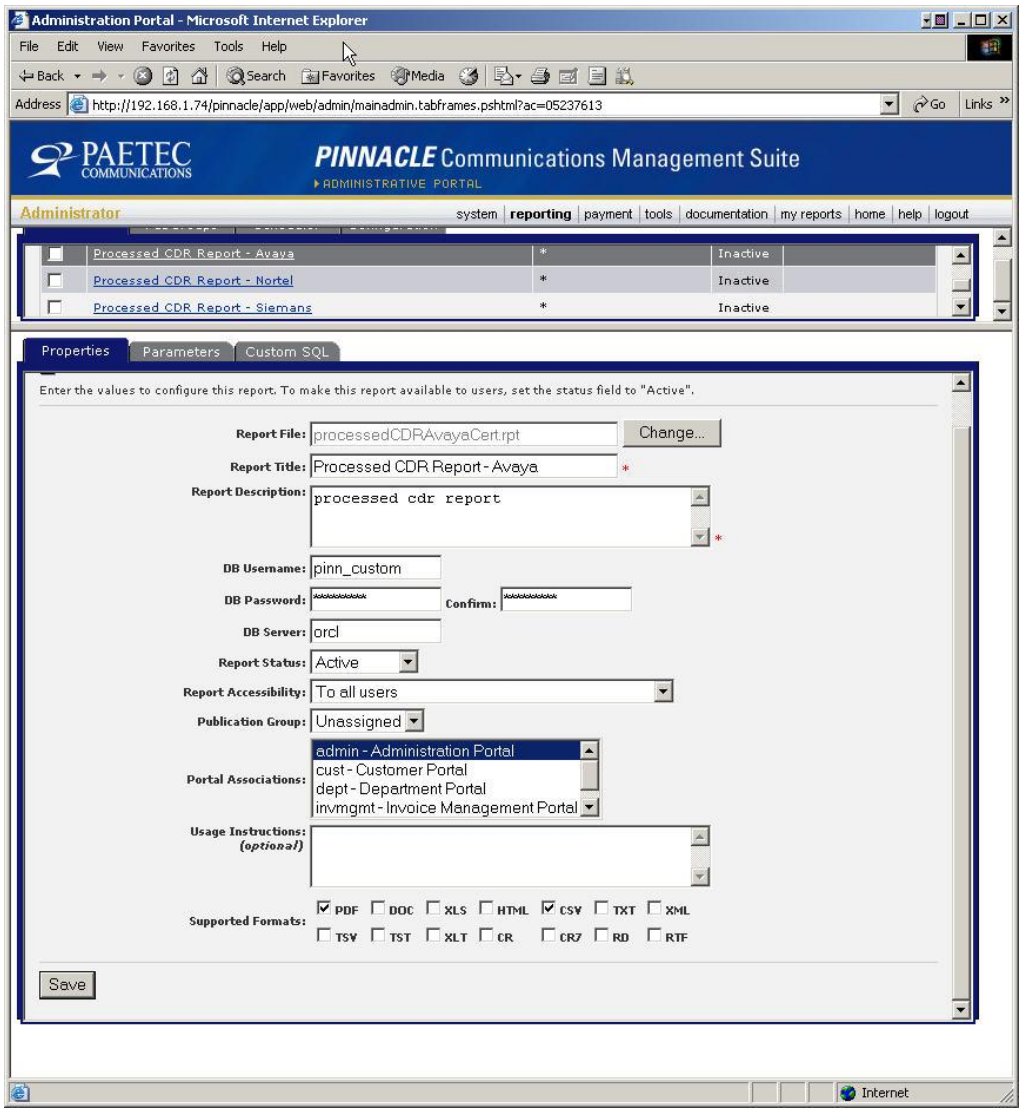
Step	Description
6.	A **Login** page appears. Enter a valid **Username** and **Password**. 
7.	The **Administrator Welcome** page appears. Select the **reporting** option in the menu below the banner to continue. 

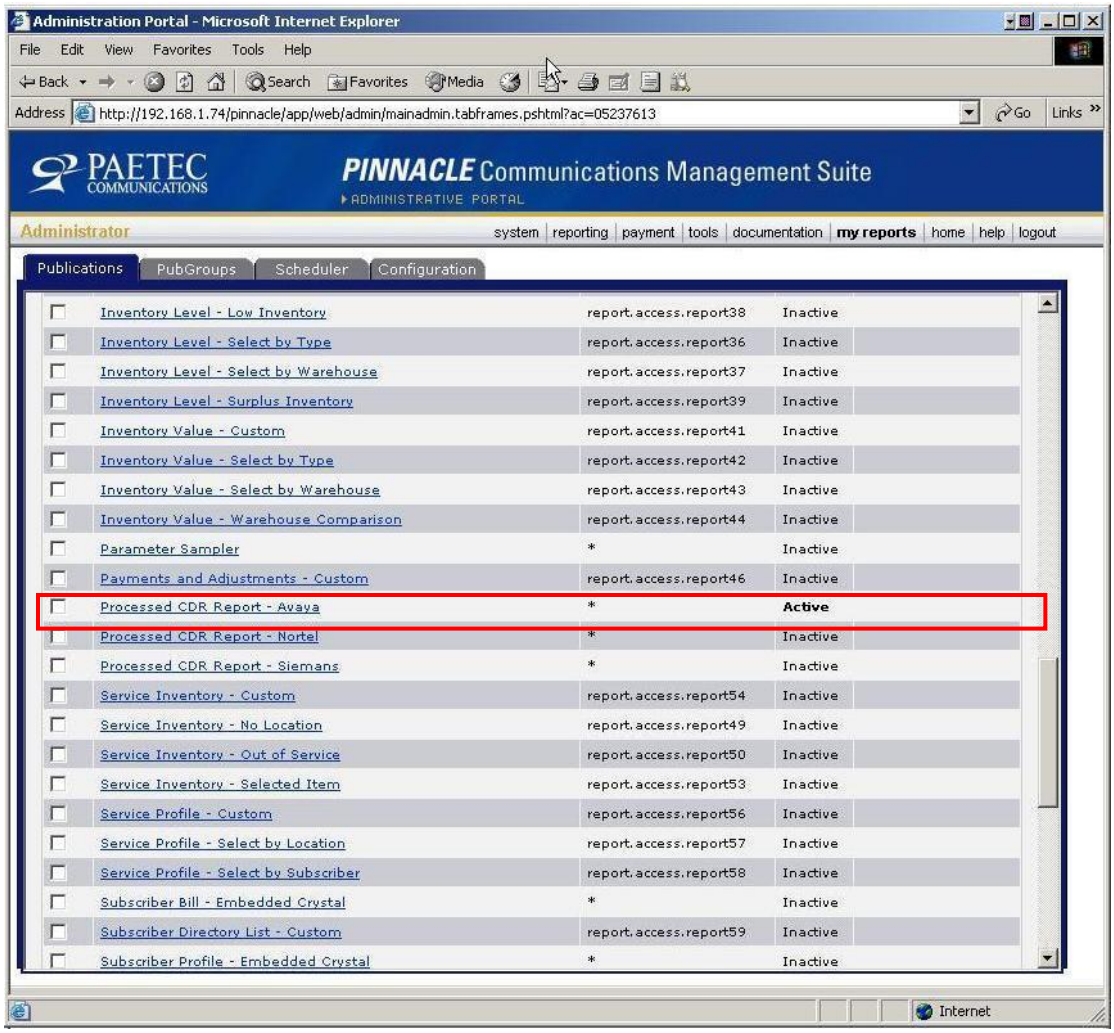
Step	Description
8.	The reporting window opens with the **Publications** tab. This tab displays a list of sample reports that have been customized with customer specific data such as database server name and password as part of the initial installation process. To use any of these reports, the report must first be made active and accessible to the necessary users.

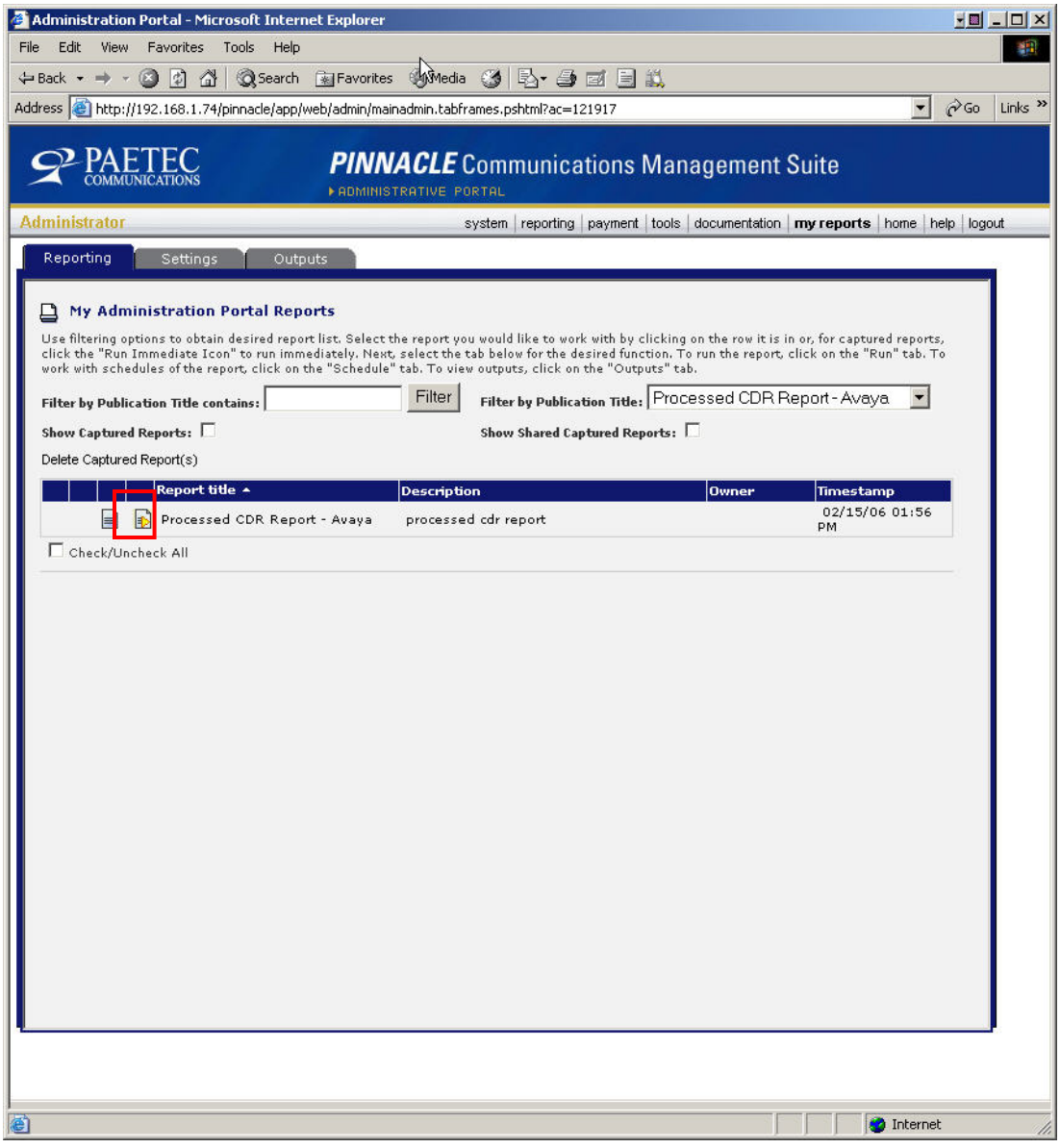


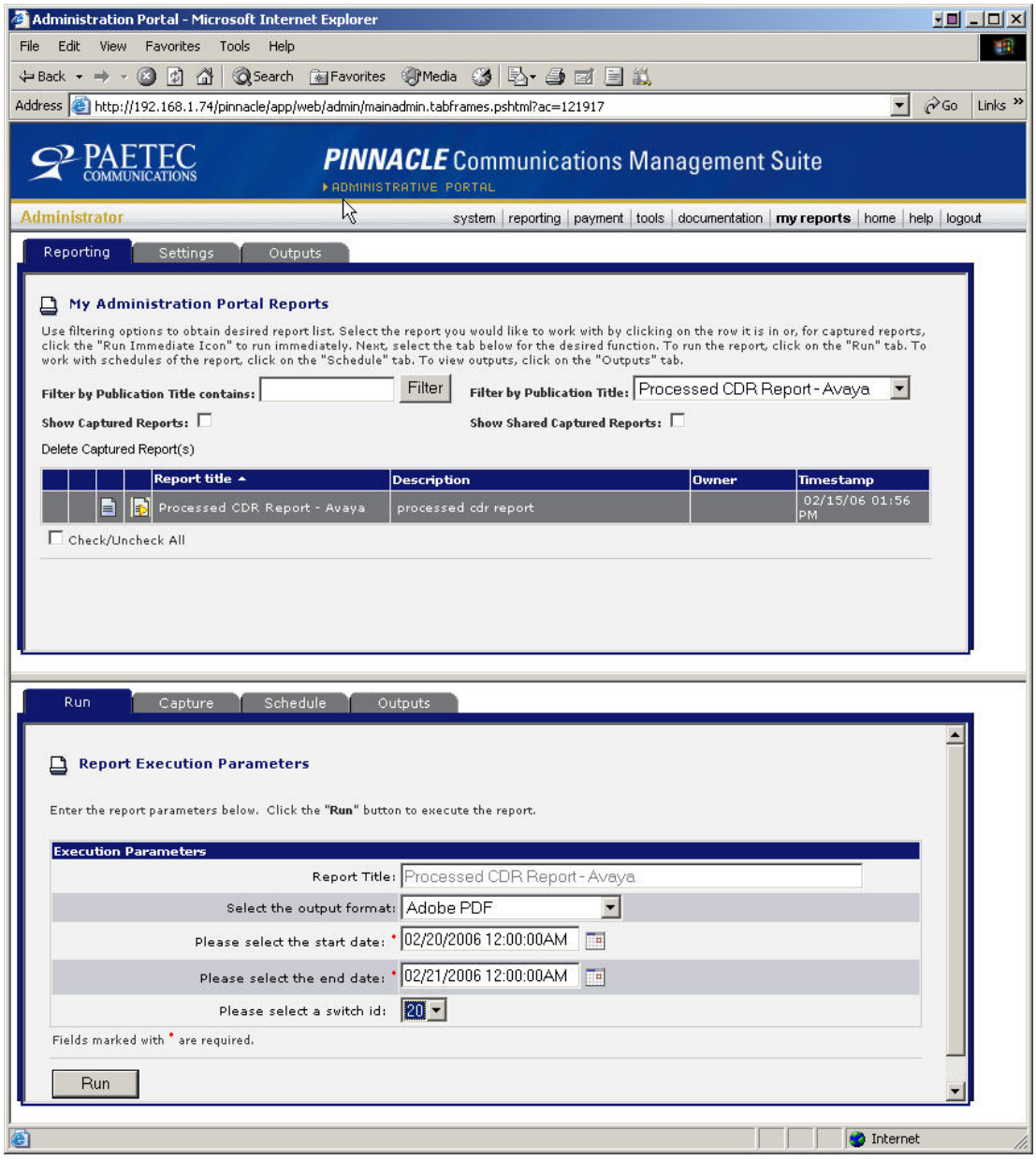
Step	Description
9.	The compliance test used the sample report, *Processed CDR Report – Avaya***,** to view the CDR records processed by PINNACLE. To activate this report, scroll-down the list of reports until it appears in the window. Double-click on this entry in the table. The example below shows this entry highlighted in the table.



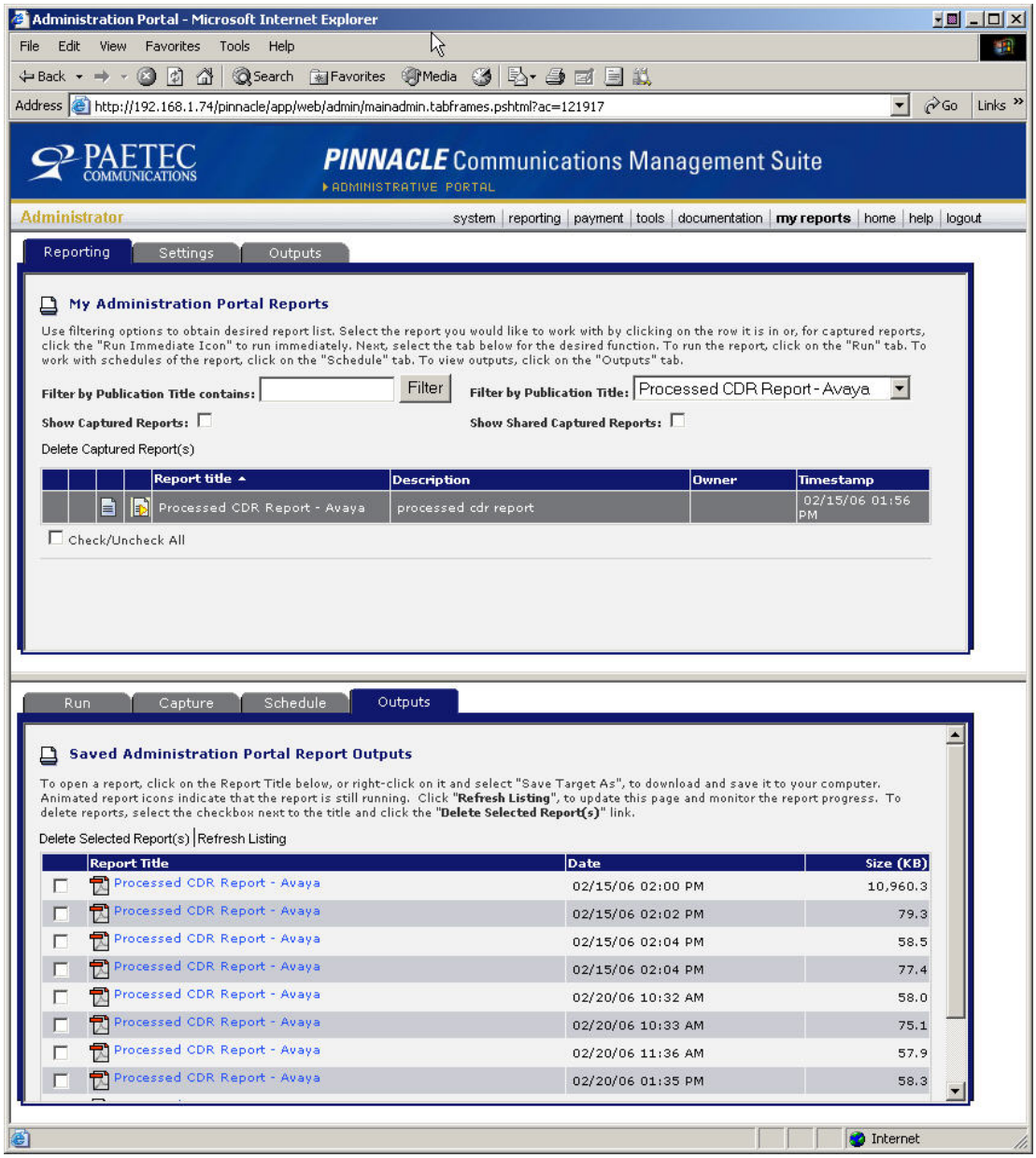
Step	Description
10.	After double-clicking the entry, the properties for the selected report appear in the bottom of the window. The example below shows the bottom frame of the window expanded so that all the properties can be viewed at once. To activate the report and make it available to users, make the following changes to the form. Set the **Report Status** field to *Active*. Set the **Report Accessibility** field to *To all users*. In the **Portal Associations** field, highlight the choice of *admin – Administration Portal* in the text box. In the **Supported Formats** field, put a check in the check box next to each format to be enabled. As part of the compliance test, *pdf* and *csv* were selected. Select the default values for all other fields. The **DB Username**, **DB Password** and **DB Server** values were established as part of the initial system installation. Select the **Save** button to submit the changes. 

Step	Description
11.	The window returns to the list of reports. The report, *Processed CDR Report – Avaya*, is now shown as active. To run a report, select the **my reports** option from the tool bar. 

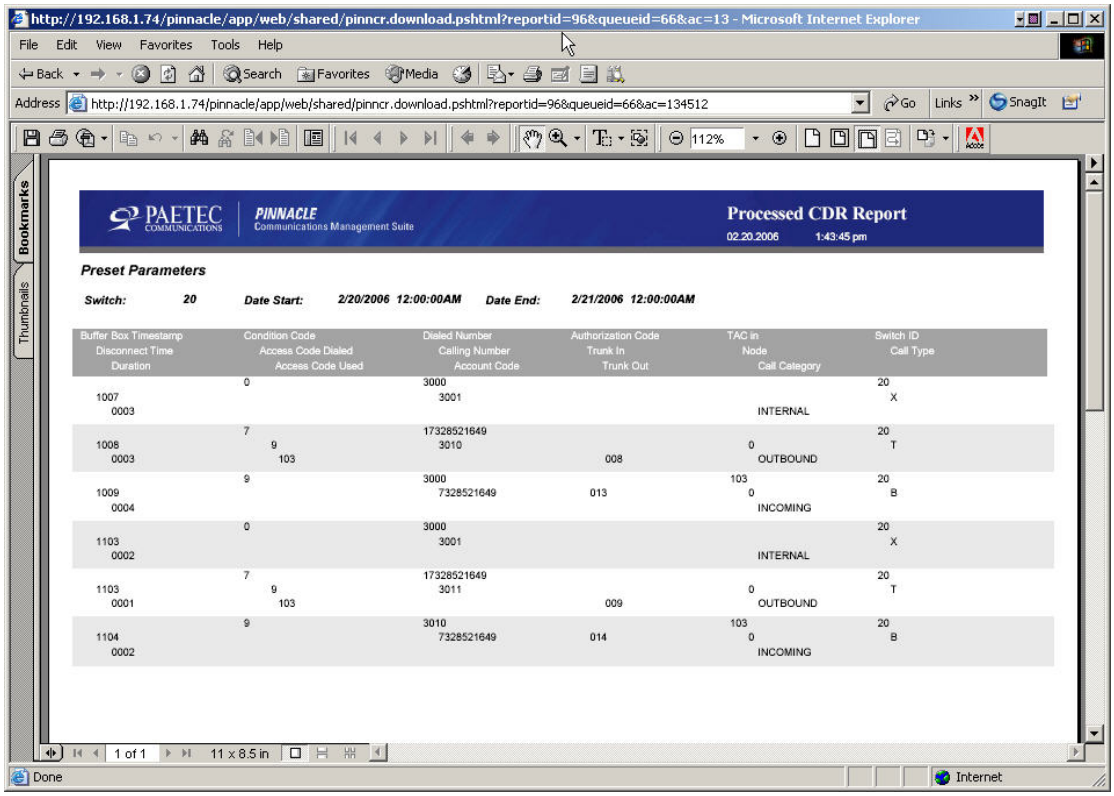
Step	Description
12.	The **my reports** window opens with the **Reporting** tab. In the **Filter by Publication Title** field, select the report, *Processed CDR Report – Avaya*, from the pull-down menu. This limits the reports listed in the window to just this one. This report would not be available in the pull-down prior to performing Step 9. Double-click the report icon containing the yellow arrow to continue. See the example below. 

Step	Description
13.	The window shows the run parameters in the bottom half of the window. Enter the start and end dates for the calls to be included in the report. Enter the **SWITCH ID** obtained in Step 4 of this section. Select the **Run** button to create the report. 

Step	Description
14.	After selecting the **Run** button, the bottom half of the window displays the **Outputs** tab. This shows a list of reports previously run from this login. The actual report output is displayed in a separate window.



Step	Description
15.	Below is an example of the **Report Output** window displaying calls made between 2/20/06 at 12:00:00 AM to 2/21/06 at 12:00:00AM on switch 20.



7. Interoperability Compliance Testing

The interoperability compliance testing included feature, serviceability and performance testing. The feature testing evaluated the ability of PINNACLE to collect and process CDR records for various types of calls. The serviceability testing introduced failure scenarios to verify that PINNACLE can resume CDR collection after failure recovery. The performance testing produced bulk call volumes to generate a substantial amount of CDR records.

7.1. General Test Approach

The general test approach was to manually place intra-switch calls, inbound trunk and outbound trunk calls to and from telephones attached to the Avaya Media Servers and verify that PINNACLE collects the CDR records and properly classifies and reports the attributes of the call. For serviceability testing, physical and logical links were disabled/re-enabled, media servers were reset and PINNACLE was restarted. For performance testing, a call generator was used to place calls over an extended period of time.

7.2. Test Results

PINNACLE successfully processed 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, PINNACLE was able to resume collecting CDR records after failure recovery including buffered CDR records for calls that were placed during the outages. Performance tests verified that PINNACLE could collect call records during a sustained, high volume of calls.

The following observations were made during the PINNACLE compliance testing.

- The sample report named *Processed CDR Report – Avaya* that was used for the testing required the Switch ID to run the report. This value is not as readily available as the Switch Profile name.
- The sample report named *Processed CDR Report – Avaya* that was used for the testing did not sort the records in time order. The records were sorted based on an internal database identifier.
- A CDR record with condition code of E, which indicated that trunks were not available, was not classified as an unrateable call in the report. However, this call would not have been charged since it also had duration of 0.

8. Verification Steps

The following steps may be used to verify the configuration:

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

9. Support

Technical support for PINNACLE can be obtained from PAETEC Communications via the link at http://www.pinnsoft.com or via email at pinnhelp@paetec.com or by phone at (585) 340-2900.

10. Conclusion

These Application Notes describe the procedures for configuring PAETEC Communications PINNACLE Communication Management Suite to collect call detail records from Avaya Communication Manager running on Avaya Media Servers. PINNACLE successfully passed all compliance testing.

11. Additional References

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

[1] *Feature Description and Implementation For Avaya Communication Manager*, Release 3.0, Issue 3.0, June 2005, Document Number 555-245-205.

[2] *Administrator Guide for Avaya Communication Manager*, Release 3.0, Issue 1.0, June 2005, Document Number 03-300509.

The following PINNACLE product documentation is available from PAETEC Communications. Visit http://www.paetec.com for company and product information.

[3] *PINNACLE System Administation Guide*

[4] *PINNACLE Cost Manager Reference Guide*

[5] *PINNACLE Operations Manager Reference Guide*

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.