AVAYA

Avaya Solution & Interoperability Test Lab

Application Notes for Integrated Research PROGNOSIS IP Telephony Manager with Avaya Communication Manager - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Integrated Research PROGNOSIS IP Telephony Manager to interoperate with Avaya Communication Manager.

PROGNOSIS IP Telephony Manager is a performance management solution for multi-vendor IP telephony solutions. PROGNOSIS IP Telephony Manager provides visibility of Avaya and other vendor's IP Telephony solutions from a single console. Targeted at Managed Service Providers of IP telephony solutions, PROGNOSIS IP Telephony Manager offers a multi-customer, multi-PBX perspective, enabling a significant reduction in complexity when managing multiple IP Telephony vendors.

PROGNOSIS integrates directly to Avaya Communication Manager using Secure Shell (SSH). At the same time, it processes Real-time Transport Control Protocol (RTCP) and Call Detail Recording (CDR) information from Avaya Communication Manager.

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.

JC; Reviewed:
SPOC 6/23/2008
Solution & Interoperability Test Lab Application Notes
©2008 Avaya Inc. All Rights Reserved.
1 of 24
Prognosis95ACM5

1. Introduction

These Application Notes describe the compliance-tested configuration used to validate Integrated Research PROGNOSIS IP Telephony Manager 9.5.1 with Avaya Communication Manager 4.0.1 and 5.0.

The PROGNOSIS IP Telephony Manager is based on the PROGNOSIS product-family architecture for the scalable monitoring of business critical systems. The PROGNOSIS product consists of:

- One or more **PROGNOSIS Monitoring Nodes** (Server Nodes). These are servers used by the PROGNOSIS product to collect, relay and store information collected from the monitored systems. In some cases the monitoring node may actually exist as an agent running on the monitored system but in the case of Avaya Communication Manager, all monitoring nodes are separate servers.

- The **PROGNOSIS GUI** is a Microsoft Windows client program which is used to connect to a PROGNOSIS monitoring node and display the information collected by the monitoring node. The PROGNOSIS GUI may either be installed on a monitoring node or on a separate computer.

The PROGNOSIS IP Telephony Manager product uses three methods to monitor an Avaya Communication Manager system.

- **System Access Terminal (SAT)** - The PROGNOSIS IP Telephony Manager uses a pool of threads to establish SSH connections to the SAT using the IP address of the Avaya Servers. By default, the solution attempts to establish three concurrent SAT connections to an Avaya Communication Manager system. The solution uses the connections to execute SAT commands on the Avaya Server.

- **RTCP Collection** - The PROGNOSIS IP Telephony Manager collects RTCP information sent by Avaya Communication Manager IP Media Processor boards, media gateways and IP Telephones.

- **Call Detail Recording (CDR) Collection** - The PROGNOSIS IP Telephony Manager collects CDR information sent by Avaya Communication Manager.

Figure 1 illustrates the test configuration used to verify Integrated Research PROGNOSIS IP Telephony Manager interoperability with Avaya Communication Manager. It consists of an Avaya Communication Manager system running on a pair of Avaya S8720 Servers with an Avaya G650 Media Gateway and an Avaya G250-BRI Media Gateway as a remote office. A second system runs on an Avaya S8300 Server with an Avaya G700 Media Gateway. Both systems have Avaya IP, digital and analog telephones, and Avaya IP Softphone and Avaya IP Agent users configured for making and receiving calls. IP Trunks connect the two systems together to allow calls between them. Integrated Research PROGNOSIS IP Telephony Manager

was installed on a server running Microsoft Windows Server 2003 Standard Edition with Service Pack 2. Both the Monitoring Node and GUI software are installed on this server. All the systems and telephones are connected using two Avaya C364T-PWR Converged Stackable Switches for network connectivity.
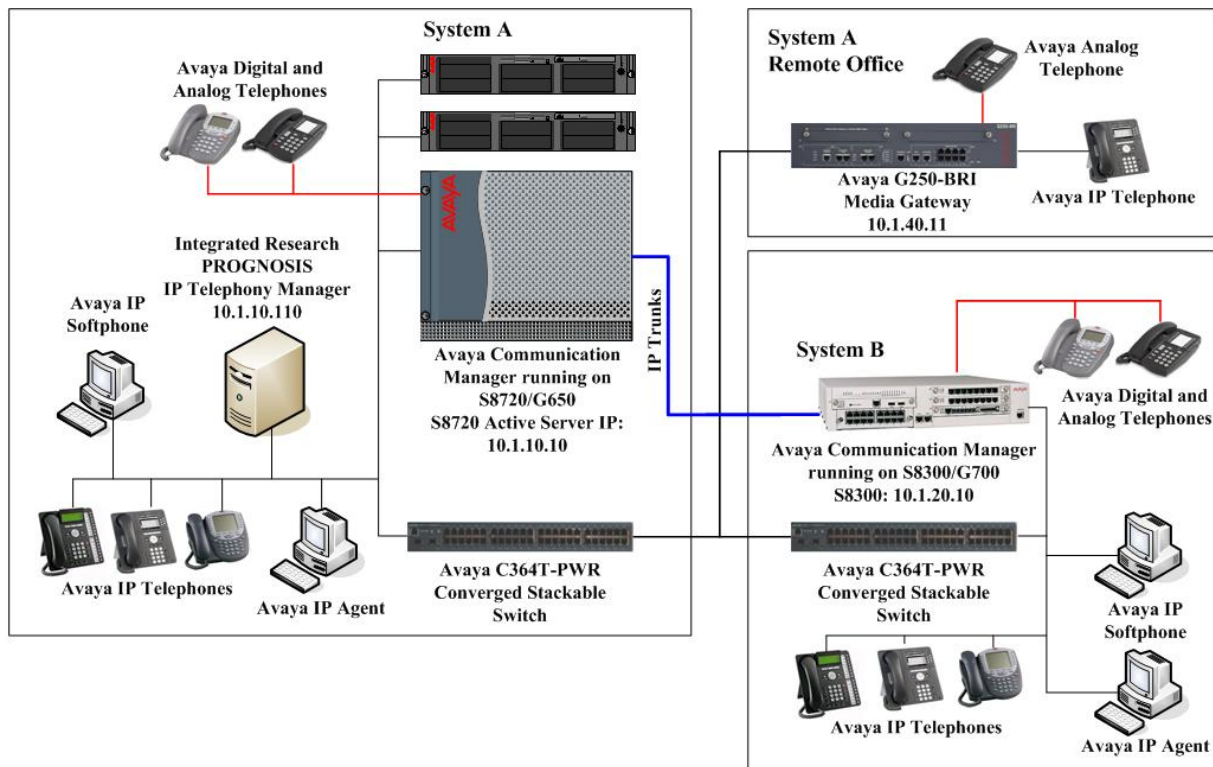

Figure 1: Test Configuration

2. Equipment and Software Validated

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

Equipment	Software
Avaya S8720 Servers	Avaya Communication Manager 4.0.1 (R014x.00.1.731.2) with Service Pack 3 (00.1.731.2-15215) 5.0 (R015x.00.0.825.4) with Service Pack 1 (00.0.825.4-15175)
Avaya G650 Media Gateway • TN2312BP IP Server Interface • TN799DP C-LAN Interface • TN2302AP IP Media Processor	- HW07, FW042 HW01, FW026 HW20, FW117

Solution & Interoperability Test Lab Application Notes
©2008 Avaya Inc. All Rights Reserved.

• TN2602AP IP Media Processor • TN2214CP Digital Line • TN2793B Analog Line	HW02, FW034 HW08, FW015 000013
Avaya G250-BRI Media Gateway	26.39.0 (for 4.0.1) 27.27.0 (for 5.0)
Avaya S8300 Server	Avaya Communication Manager 4.0.1 (R014x.00.1.731.2) with Service Pack 3 (00.1.731.2-15215) 5.0 (R015x.00.0.825.4) with Service Pack 1 (00.0.825.4-15175)
Avaya G700 Media Gateway • MM760AP VOIP Media Module • MM712AP DCP Media Module • MM714AP Analog Media Module	26.39.0 (for 4.0.1) 27.29.0 (for 5.0) HW01, FW075 HW04, FW009 HW42, FW089
Avaya 4600 Series IP telephones	2.8.3 (H.323)
Avaya 9600 Series IP telephones	1.5 (H.323)
Avaya 1600 Series IP telephones	1.0.1 (H.323)
Avaya 6200 Series analog telephones	-
Avaya 2400 Series digital telephones	-
Avaya IP Softphone	6.0 Service Pack 2
Avaya IP Agent	7.0.23.116
Avaya C364T-PWR Converged Stackable Switches	4.5.18
Integrated Research PROGNOSIS IP Telephony Manager	9.5.1 Patch 2
Microsoft Windows Server 2003 Standard Edition	Service Pack 2

3. Configure Avaya Communication Manager

This section describes the steps needed to configure Avaya Communication Manager to interoperate with Integrated Research PROGNOSIS IP Telephony Manager. This section describes the steps to create a login account and a SAT User Profile for PROGNOSIS to access Avaya Communication Manager and the steps to enable RTCP and CDR reporting. The steps are repeated for each Avaya Communication Manager system.
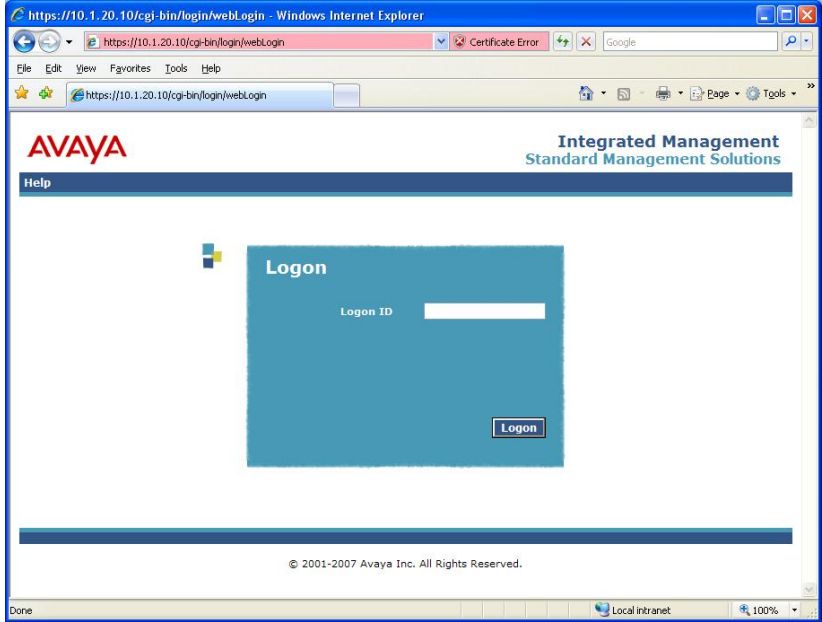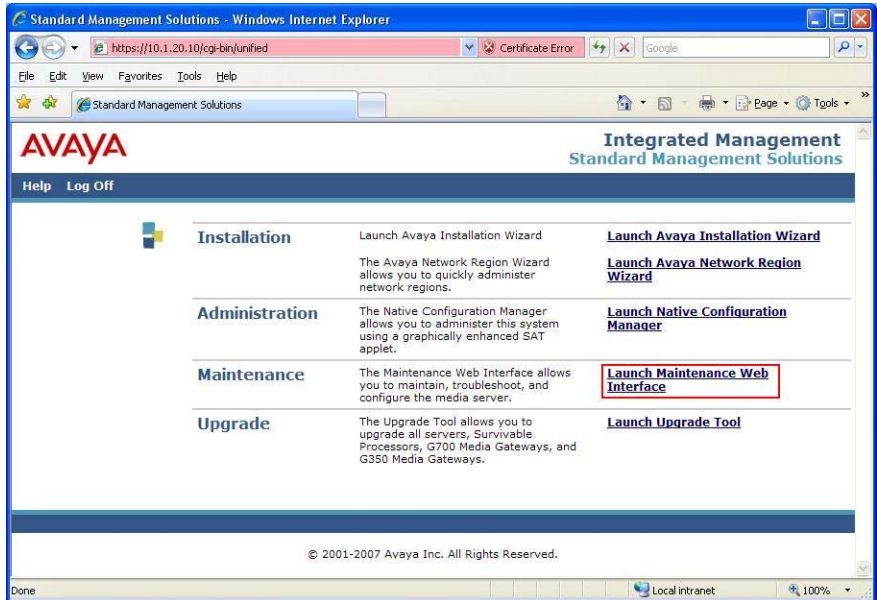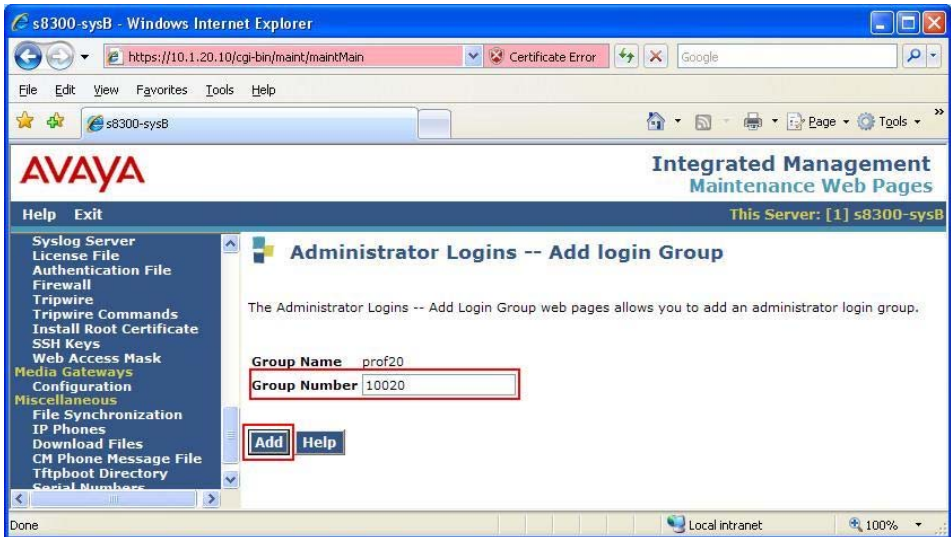
3.1. Configure SAT User Profile

A SAT User Profile specifies which SAT screens may be accessed by the user assigned the profile and the type of access to each screen. As PROGNOSIS IP Telephony Manager does not modify any system configuration, create a SAT User Profile with limited permissions to assign to the PROGNOSIS login account.

Step	Description
1.	Enter the **add user-profile** *n* command, where *n* is the next unused profile number. Enter a descriptive name for **User Profile Name** and enable all categories by setting the **Enbl** field to **y**. In this configuration, the user profile 20 is created.

```
add user-profile 20                                              Page   1 of  41
                             USER PROFILE 20

User Profile Name: Prognosis

       This Profile is Disabled? n                 Shell Access? n
Facility Test Call Notification? n    Acknowledgement Required? n
     Grant Un-owned Permissions? n               Extended Profile? n

            Name         Cat Enbl          Name                Cat Enbl
                Adjuncts A   y      Routing and Dial Plan J      y
             Call Center B   y                     Security K      y
                Features C   y                      Servers L      y
                Hardware D   y                     Stations M      y
             Hospitality E   y      System Parameters N      y
                      IP F   y                 Translations O      y
             Maintenance G   y                     Trunking P      y
Measurements and Performance H   y                       Usage Q      y
           Remote Access I   y                 User Access R      y
```

Step	Description
2.	On Pages 2 to 41 of the USER PROFILE forms, set the permissions of all objects to **rm** (read and maintenance). This can be accomplished by typing **rm** into the field **Set All Permissions To**. Submit the form to create the user profile.

```
add user-profile 20                                              Page   2 of  41
                             USER PROFILE 20
 Set Permissions For Category:    To:          Set All Permissions To: rm

                    Name          Cat  Perm
                aar analysis J   rm
          aar digit-conversion J   rm
            aar route-chosen J   rm
abbreviated-dialing 7103-buttons C   rm
    abbreviated-dialing enhanced C   rm
       abbreviated-dialing group C   rm
    abbreviated-dialing personal C   rm
     abbreviated-dialing system C   rm
              aca-parameters P   rm
             access-endpoints P   rm
              adjunct-names A   rm
       administered-connections C   rm
            aesvcs cti-link A   rm
            aesvcs interface A   rm
```

3.2. Configure Login Group
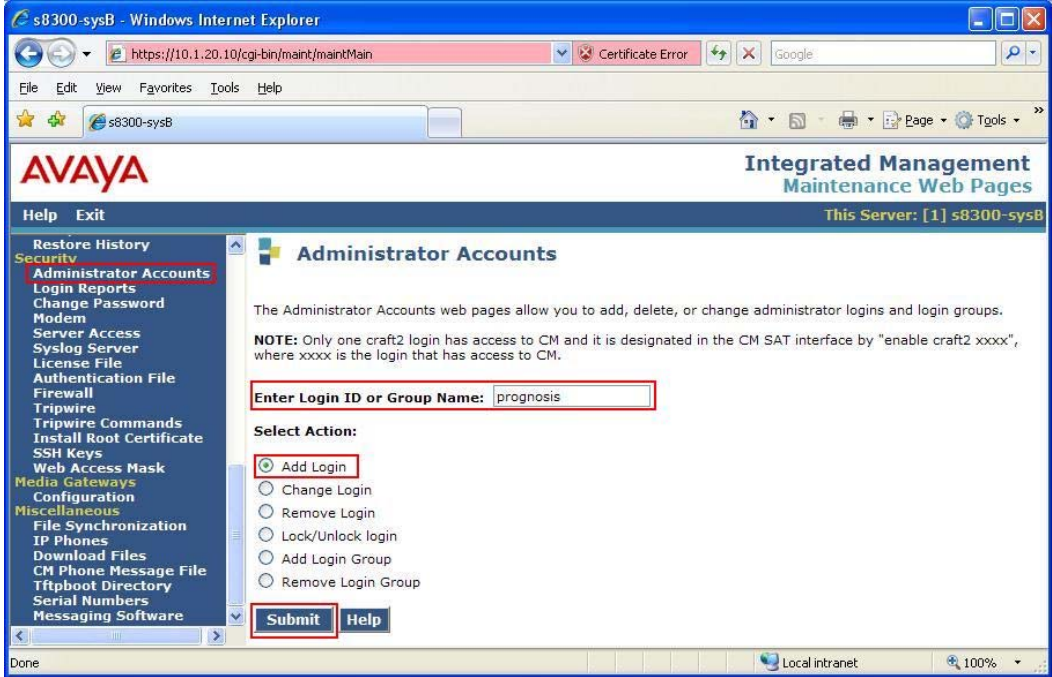
Create a Login Group in the range 10,020 - 10,069 to correspond to the SAT User Profile created in **Section 3.1**.

Step	Description
1.	Using a web browser, enter https://<IP address of Avaya Server> to connect to the Avaya Server being configured and log in using appropriate credentials.
2.	Click **Launch Maintenance Web Interface**. This will open up the **Maintenance Web Pages** in a new window that will allow the user to complete the configuration process.

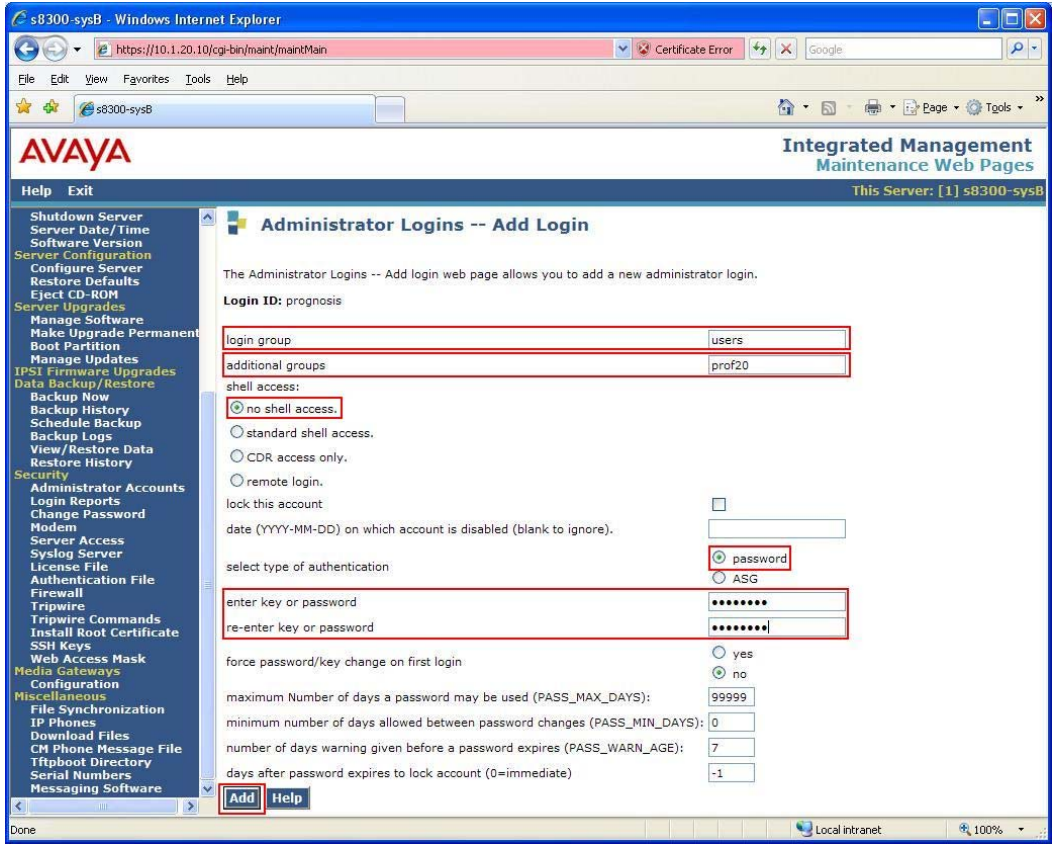| Step	Description
3.	From the navigation panel on the left side, click **Administrator Accounts**. For the field **Enter Login ID or Group Name**, Avaya recommends the group name be in the form prof<nn> where nn is the group number. In this configuration, the group **prof20** is created to correspond to the user profile 20. Select **Add Login Group** and click **Submit**.
4.	For the Group Number field, enter the value **10020**, which is obtained by adding the Access Mask Base (default value of 10000) to the user profile number. Click **Add**. This completes the creation of the login group.

3.3. Configure Login

Create a login account for PROGNOSIS to access the SAT.

Step	Description
1.	From the navigation panel on the left side, click **Administrator Accounts**. For the field **Enter Login ID or Group Name**, enter the login to be created. In this configuration, the login **prognosis** is created. Select **Add Login** and click **Submit**.

Step	Description
2.	On the Administrator Logins -- Add Login page, configure the login as follows: • **login group**: **users** [Limits the permissions of the login] • **additional groups**: **prof20** [Enter the login group created in **Section 3.2**.] • **shell access: no shell access** [Shell access not required.] • **select type of authentication: password** [Uses a password for authentication.] • **enter key or password / re-enter key or password** [Define the password] Click **Add** to continue. This completes the configuration of the login.

3.4. Configure RTCP Monitoring

To allow PROGNOSIS IP Telephony Manager to monitor the quality of IP calls, configure Avaya Communication Manager to send RTCP reporting to the IP address of the PROGNOSIS server.

Step	Description
| 1. | Enter the **change system-parameters ip-options** command. In the **RTCP MONITOR SERVER** section, set **Default Server IP Address** to the IP address of the PROGNOSIS IP Telephony Manager server. Set **Default Server Port** to *5005* and **Default RTCP Report Period (secs)** to *5*.<br><br>```
change system-parameters ip-options                          Page   1 of   3
                       IP-OPTIONS SYSTEM PARAMETERS

 IP MEDIA PACKET PERFORMANCE THRESHOLDS
    Roundtrip Propagation Delay (ms)    High: 800      Low: 400
                     Packet Loss (%)    High: 40       Low: 15
                    Ping Test Interval (sec): 20
     Number of Pings Per Measurement Interval: 10

 RTCP MONITOR SERVER
         Default Server IP Address: 10 .1   .10 .110
                Default Server Port: 5005
  Default RTCP Report Period(secs): 5

AUTOMATIC TRACE ROUTE ON
           Link Failure? y

 H.248 MEDIA GATEWAY                  H.323 IP ENDPOINT
  Link Loss Delay Timer (min): 5     Link Loss Delay Timer (min): 5
                                     Primary Search Time (sec): 75
                                 Periodic Registration Timer (min): 20
``` |
| 2. | Enter the **change ip-network-region *n*** command, where *n* is IP network region number to be monitored. Set **RTCP Reporting Enabled** to *y* and **Use Default Server Parameters** to *y*.<br><br>Note: Only one RTCP MONITOR SERVER can be configured per IP network region.<br><br>```
change ip-network-region 1                                    Page   1 of  19
                           IP NETWORK REGION
   Region: 1
Location: 1       Authoritative Domain:
    Name: Local
MEDIA PARAMETERS                    Intra-region IP-IP Direct Audio: yes
     Codec Set: 1                   Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                        IP Audio Hairpinning? y
   UDP Port Max: 65535
DIFFSERV/TOS PARAMETERS                    RTCP Reporting Enabled? y
 Call Control PHB Value: 46       RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46        Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5    AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                              RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
``` |

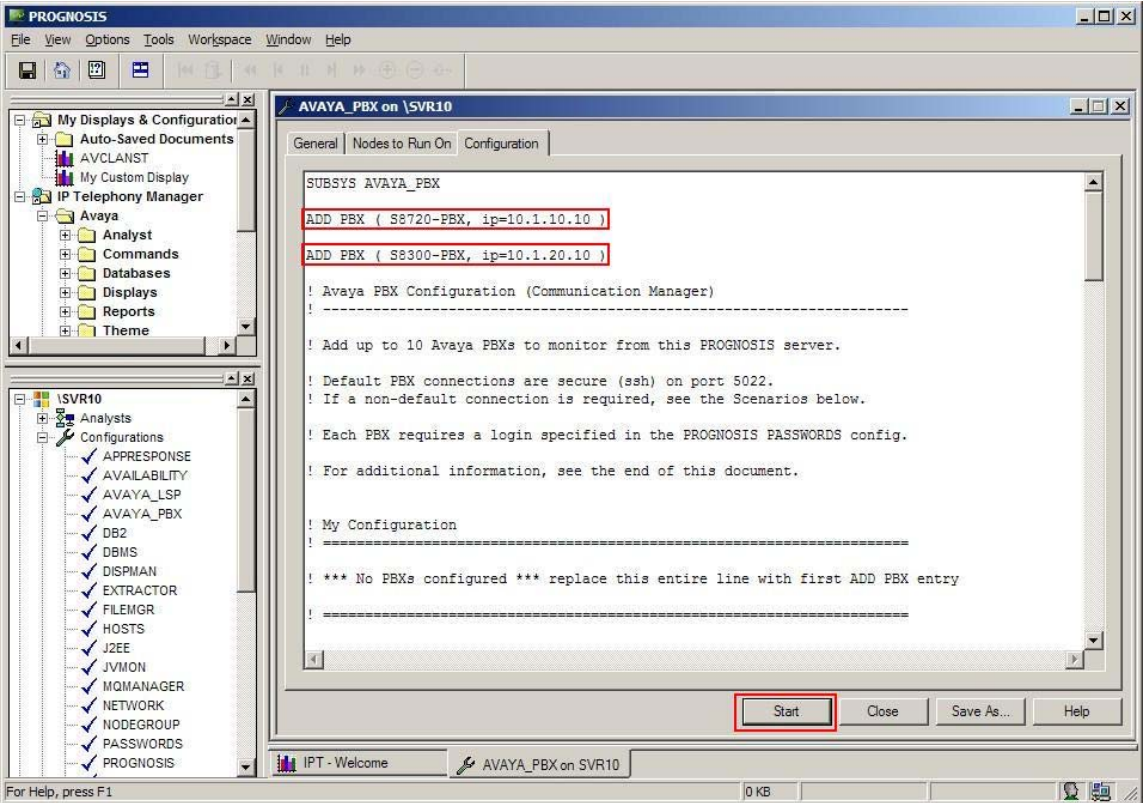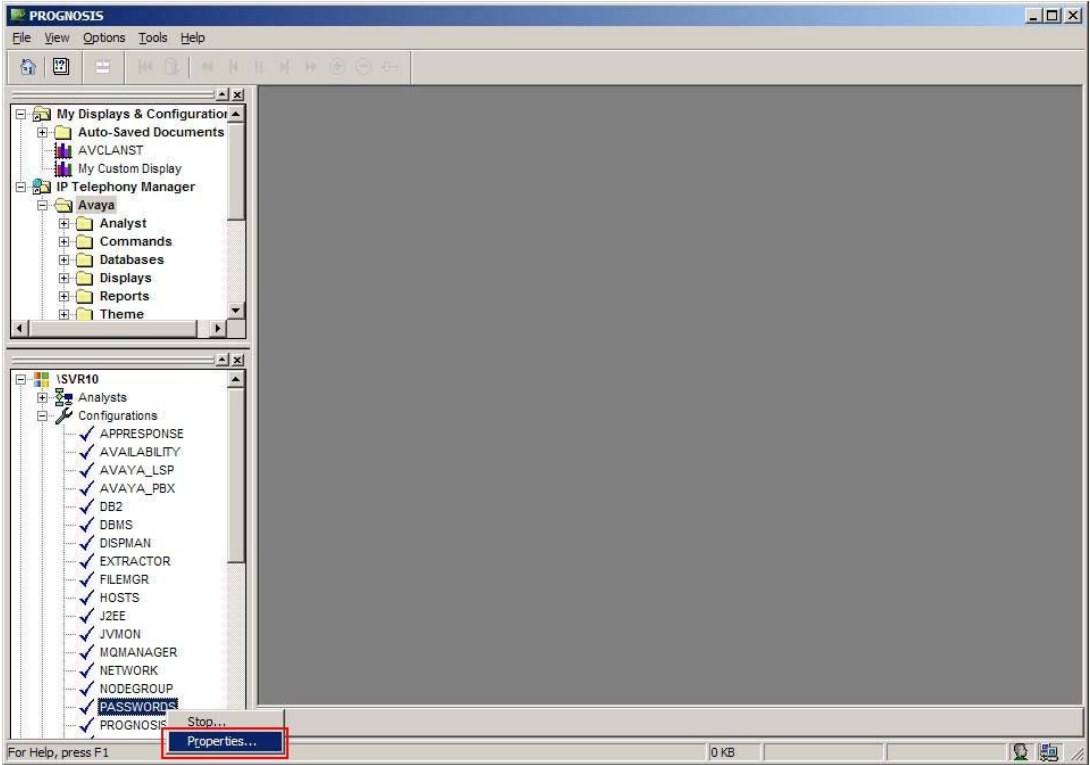| Step	Description
3.	Repeat **Step 2** for all IP network regions that are required to be monitored.

3.5. Configure CDR Monitoring

To allow PROGNOSIS IP Telephony Manager to monitor the CDR information, configure Avaya Communication Manager to send CDR information to the IP address of the PROGNOSIS server.
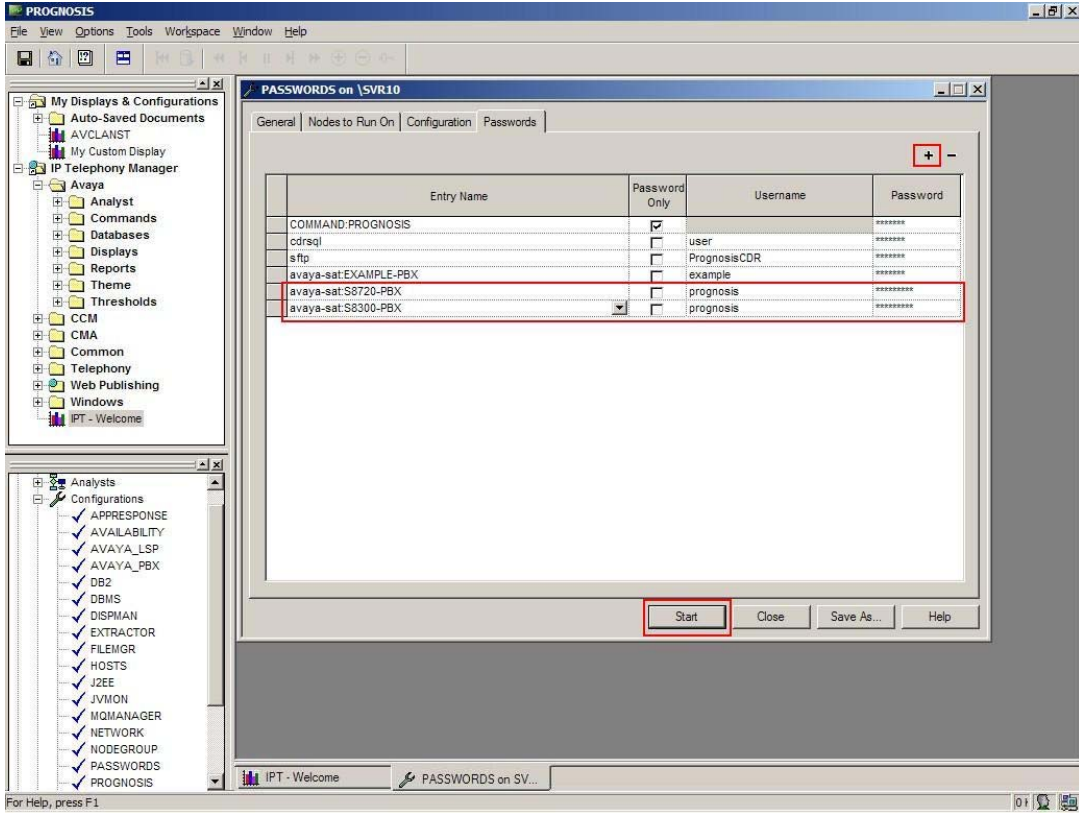
Step	Description
1.	Enter the **change node-names ip** command to add a new node name for the PROGNOSIS server. Note also the node name **clan1** that was added for one of the CLAN boards, which will be used by Avaya Communication Manager to send out the CDR information. ``` change node-names ip Page 1 of 2 IP NODE NAMES Name IP Address clan1 10.1.10.21 clan2 10.1.10.22 default 0.0.0.0 medpro1 10.1.10.31 medpro2 10.1.10.32 procr 10.1.10.9 val1 10.1.10.41 prognosis 10.1.10.110 ```
2.	Enter 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: clan1** [Avaya Communication Manager will use this CLAN to send out the CDR] **Local Port: 0** [The Local Port is fixed to 0 because Avaya Communication Manager initiates the CDR link.] **Remote Node: prognosis** [The Remote Node is set to the node name previously defined in Step 1.] **Remote Port: 50000** [The Remote Port may be set to a value between 5000 and 64500 inclusive. The default port for PROGNOSIS server is 50000. Note that PROGNOSIS server uses the same port number for every S8XXX Server.] ``` change ip-services Page 1 of 4 IP SERVICES Service Enabled Local Local Remote Remote Type Node Port Node Port CDR1 clan1 0 prognosis 50000 ```

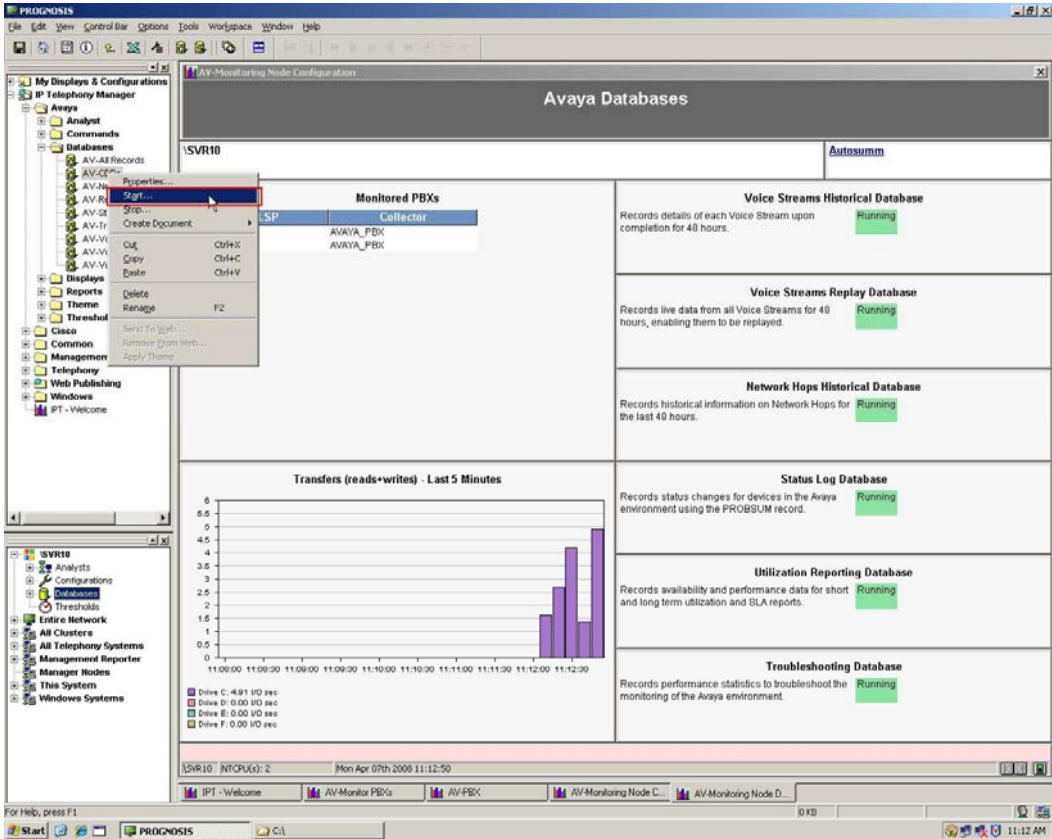| Step	Description
	On Page 3 of the IP SERVICES form, disable the Reliable Session Protocol (RSP) for the CDR link by setting the **Reliable Protocol** field to **n**.

```
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 were used during the compliance test.

- **CDR Date Format**: **month/day**
- **Primary Output Format**: **unformatted**
- **Primary Output Endpoint**: **CDR1**

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

- **Use Legacy CDR Formats? y** [Specify the use of the Avaya Communication Manager 3.x ("legacy") 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.]
- **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? n** [Do not allow a separate call record for any portion of an incoming call that is transferred or conferenced.]

Step	Description
|  | ```
change system-parameters cdr                                Page   1 of   1
                          CDR SYSTEM PARAMETERS

  Node Number (Local PBX ID):                     CDR Date Format: month/day
       Primary Output Format: unformatted    Primary Output Endpoint: CDR1
     Secondary Output Format:             Secondary Output Endpoint:
            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? y              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? 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: member-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? 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: 15
``` |
| 4. | If the **Intra-switch CDR** field is set to **y** on Page 1 of the CDR SYSTEM PARAMETERS form, then enter the **change intra-switch-cdr** command to define the extensions that will be subjected to call detail recording. In the **Assigned Members** 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:  8    of 5000   administered
   Extension         Extension          Extension          Extension
   10001
   10002
   10003
   10004
   10005
   10006
   10007
   10008
``` |
| 5. | For each trunk group for which CDR records are desired, verify that CDR reporting is enabled. Enter the **change trunk-group _n_** command, where _n_ is the trunk group number, to verify that the **CDR Reports** field is set to **y**. Repeat for all trunk groups to be reported. |

Step	Description
| | ```
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 Integrated Research PROGNOSIS IP Telephony Manager

This section describes the configuration of Integrated Research PROGNOSIS IP Telephony Manager required to interoperate with Avaya Communication Manager.

Step	Description
1.	On the Integrated Research PROGNOSIS IP Telephony Manager server, click **Start > All Programs > PROGNOSIS IP Telephony Manager > PROGNOSIS GUI** to start the PROGNOSIS GUI application. Enter a valid Windows user account and password to log in.
2.	To configure the Avaya Communication Manager systems to be monitored, expand **Configurations** of the Monitoring Node, right-click on **AVAYA_PBX** and select **Properties**.

Step	Description
3.	In the **Configurations** tab, add an entry for each Avaya Communication Manager system to be managed. The template to add a system is provided in the PROGNOSIS GUI application. In this sample configuration, the following entries are added for the two Avaya Communication Manager systems with the names **S8720-PBX** and **S8300-PBX** and with the IP addresses of the Avaya Servers 10.1.10.10 and 10.1.20.10 respectively. The PROGNOSIS Monitoring Node will use SSH to connect to port 5022 of the Avaya Servers by default. ADD PBX (\S8720-PBX, ip=10.1.10.10) ADD PBX (\S8300-PBX, ip=10.1.20.10) Click **Start** to proceed.

JC; Reviewed:
SPOC 6/23/2008
Solution & Interoperability Test Lab Application Notes
©2008 Avaya Inc. All Rights Reserved.
15 of 24
Prognosis95ACM5

Step	Description
4.	To configure the SAT login account and password, expand **Configurations** of the Monitoring Node, right-click on **PASSWORDS** and select **Properties**.

Step	Description
5.	Click the + **'plus'** button to add a new password entry for each of the configured system in **Step 3**. The **Entry Name** must be of the form avaya-sat:<pbx-name>. For the system with the name **S8720-PBX**, enter **avaya-sat:S8720-PBX** for **Entry Name**, uncheck **Password Only**, and enter the login account created in **Section 3.3** for **Username** and **Password**. Repeat to add another entry for the second system **S8300-PBX**. Click **Start** to proceed.

Solution & Interoperability Test Lab Application Notes
©2008 Avaya Inc. All Rights Reserved.

Step	Description
6.	By default, the CDR database used for the collection of CDR information is not started. To start the database, expand **IP Telephony Manager > Avaya > Databases** of the Monitoring Node, right-click on **AV-CDRs** and click **Start**. This completes the configuration for PROGNOSIS IP Telephony Manager.

5. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing evaluated the ability of the PROGNOSIS IP Telephony Manager to correctly retrieve the configuration, performance, alarms and errors from an Avaya Communication Manager system. In addition, the ability of PROGNOSIS IP Telephony Manager to receive and process both RTCP and CDR information from Avaya Communication Manager was also validated.

The serviceability testing introduced failure scenarios to see if PROGNOSIS IP Telephony Manager is able to resume service after failure recovery and Avaya Server interchange.

5.1. General Test Approach

The general test approach was to use PROGNOSIS GUI to display the configurations of Avaya Communication Manager systems and verify against what is displayed on the SAT interface. The SAT interface is accessed by using either telnet or Secure Shell (SSH) to the Avaya S8720 and S8300 Servers. Calls were placed between various Avaya endpoints and PROGNOSIS GUI was used to display the RTCP and CDR information collected.

For feature testing, PROGNOSIS GUI was used to view the configurations of Avaya Communication Manager such as media gateways, cabinets, port networks, trunk groups, route patterns, CLAN, MEDPRO and DS1 boards, IP network regions, stations, processor occupancy, alarm and error information. Various conditions such as media gateway, port network, trunk group, trunk member and endpoint failures were created to see if PROGNOSIS IP Telephony Manager was able to detect the outage. For the collection of RTCP and CDR information, the endpoints included Avaya IP, digital and analog telephones, and Avaya IP Softphone and IP Agent users. The types of calls made included intra-switch calls, inbound/outbound inter-switch IP trunk calls, transferred calls and conference calls.

For serviceability testing, reboots were applied to the PROGNOSIS IP Telephony Manager Server and Avaya Servers to simulate system unavailability. Interchanging of the Avaya S8720 Servers was also performed during testing.

5.2. Test Results

All test cases passed successfully. Integrated Research PROGNOSIS IP Telephony Manager successfully interoperates with Avaya Communication Manager.

6. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya Communication Manager and Integrated Research PROGNOSIS IP Telephony Manager.

6.1. Verify Avaya Communication Manager

Verify that PROGNOSIS IP Telephony Manager has established three concurrent SSH connections to the SAT by using the **status logins** command.

```
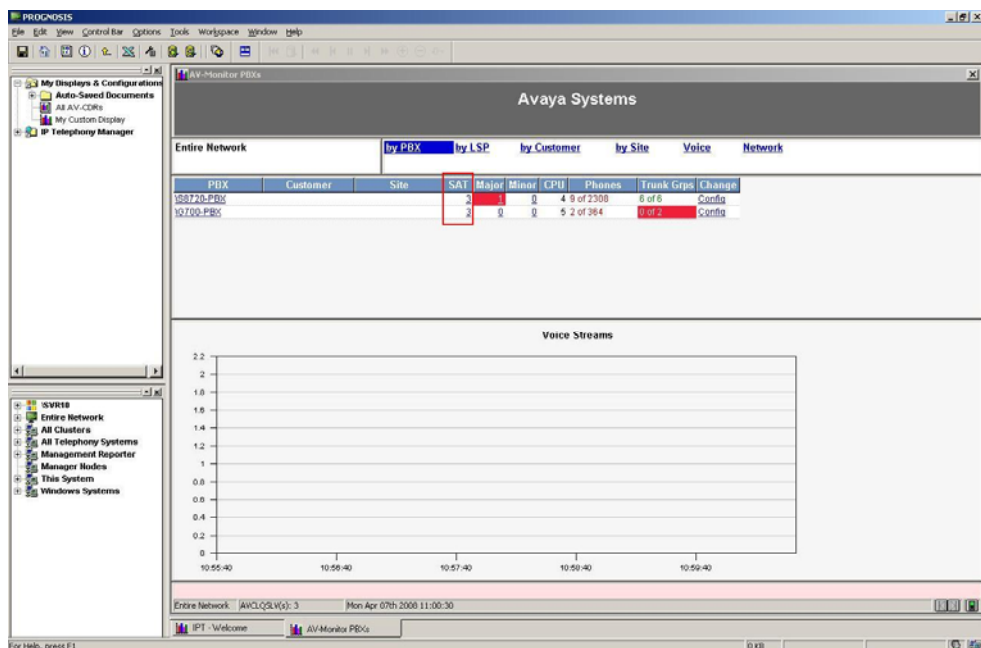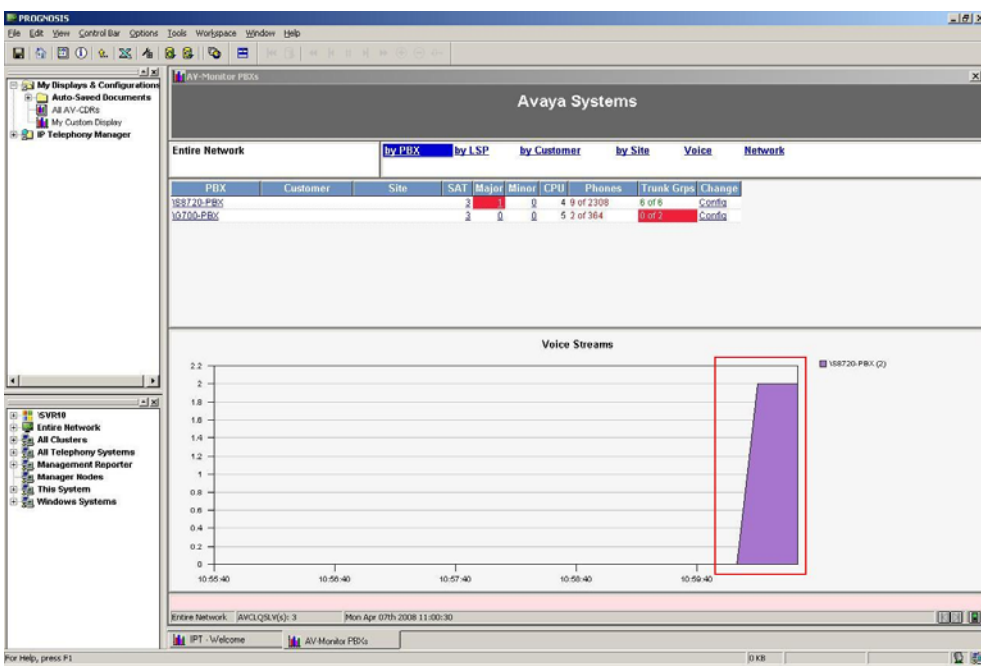status logins
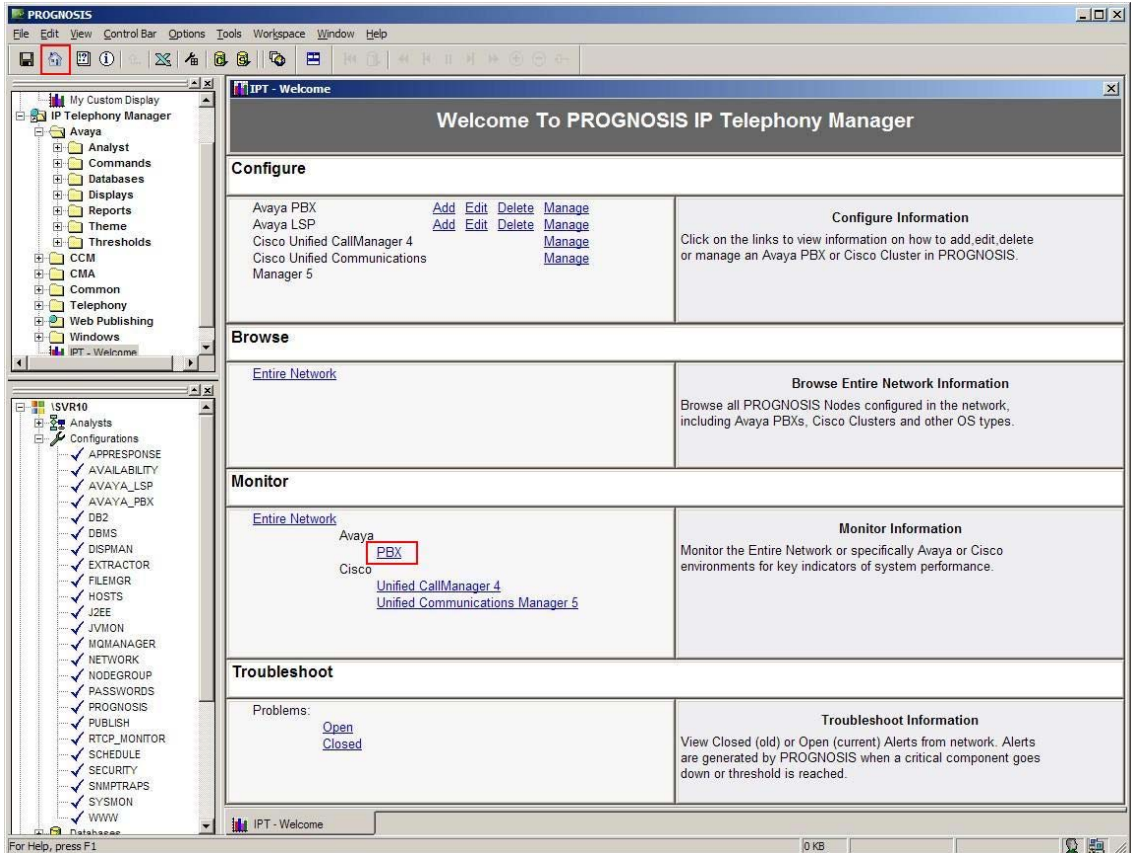
                    COMMUNICATION MANAGER LOGIN INFORMATION

Login      Profile    User's Address       Active Command              Session

*dadmin      2         10.1.10.152        stat logins                      1
 prognosi    20        10.1.10.110        list measurements summary        3
 prognosi    20        10.1.10.110        list registered-ip-stations      4
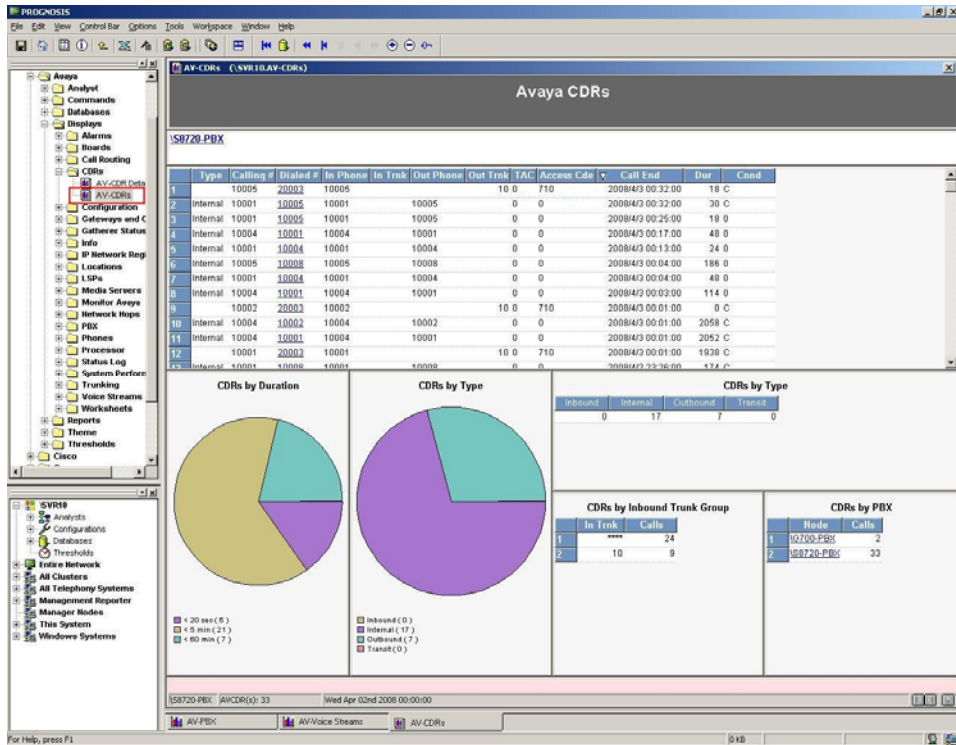 prognosi    20        10.1.10.110        stat trunk 10                    5
```

6.2. Verify Integrated Research PROGNOSIS IP Telephony Manager

The following steps are done using the PROGNOSIS GUI.

Step	Description
1.	After logging into PROGNOSIS GUI, click on the **Home** button on the toolbar to display the **Welcome** screen. In the **Monitor** section, click **Entire Network** > **Avaya** > **PBX** to display the list of Avaya Communication Manager Servers configured in **Section 4**.

JC; Reviewed:
SPOC 6/23/2008

Solution & Interoperability Test Lab Application Notes
©2008 Avaya Inc. All Rights Reserved.

20 of 24
Prognosis95ACM5

Step	Description
2.	In the **Avaya System** page, verify that the **SAT** field for each configured Avaya Communication Manager shows **3** connections.
3.	Make a call between two Avaya IP telephones that belong to an IP Network Region that is being configured to send RTCP information to the PROGNOSIS server. Verify that the **Voice Streams** section shows two active voice streams reflecting the quality of the call.

Solution & Interoperability Test Lab Application Notes

Step	Description
4.	Expand **IP Telephony Manager > Avaya > Displays > CDRs** of the Monitoring Node and double-click **AV-CDRs**. Make an incoming call through a trunk group configured for CDR reporting in **Section 3.5 Step 5**. Answer the call and hang up after about 10 seconds. Verify that a new CDR record is displayed for the call.

7. Support

For technical support on Integrated Research PROGNOSIS IP Telephony Manager, contact the Integrated Research Support Team at:

- Phone: +61 (2) 9966 1066
- Fax: +61 (2) 9921-1042
- Email: support@prognosis.com

8. Conclusion

These Application Notes describe the procedures for configuring the Integrated Research PROGNOSIS IP Telephony Manager 9.5.1 to interoperate with Avaya Communication Manager Release 4.0.1 and 5.0. In the configuration described in these Application Notes, the PROGNOSIS IP Telephony Manager established SSH connections to the SAT to view the configurations of Avaya Communication Manager and to monitor for failures. PROGNOSIS IP Telephony Manager also processed the RTCP information to monitor the quality of IP calls and collected CDR information from the Avaya Communication Manager. During compliance testing, all test cases were completed successfully.

9. Additional References

The following document can be found at http://support.avaya.com:

[1] *Feature Description and Implementation For Avaya Communication Manager*, Release 5.0, Issue 6, January 2008, Document Number 555-245-205.
[2] *Administrator Guide for Avaya Communication Manager*, Release 5.0, Issue 4.0, January 2008, Document Number 03-300509.
[3] *Feature Description and Implementation For Avaya Communication Manager*, Release 4.0, Issue 5, February 2007, Document Number 555-245-205.
[4] *Administrator Guide for Avaya Communication Manager*, Release 4.0, Issue 3, February 2007, Document Number 03-300509.

The following PROGNOSIS documentations are provided by Integrated Research.

[5] *PROGNOSIS IP Telephony Manager 9.5 Installation Guide*
[6] *PROGNOSIS IP Telephony Manager 9.5 User Guide*

©2008 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.

JC; Reviewed:
SPOC 6/23/2008

Solution & Interoperability Test Lab Application Notes
©2008 Avaya Inc. All Rights Reserved.

24 of 24
Prognosis95ACM5