



Avaya Solution & Interoperability Test Lab

Application Notes for NetIQ AppManager with Avaya Communication Manager – Issue 1.0

Abstract

These Application Notes describe the steps for configuring NetIQ AppManager with Avaya Communication Manager. NetIQ AppManager for Avaya IP Telephony provides monitoring, management and reporting for Avaya Communication Manager. AppManager performs event monitoring of the call server and gathers call quality data in real-time that can be used to accurately and quickly reflect the end user call experience. AppManager also monitors call activity in order to track call usage and call failures.

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 steps for configuring NetIQ AppManager with Avaya Communication Manager. NetIQ AppManager for Avaya IP Telephony provides monitoring, management and reporting for Avaya Communication Manager. AppManager performs event monitoring of the call server and gathers call quality data in real-time that can be used to accurately and quickly reflect the end user call experience. AppManager also monitors call activity in order to track call usage and call failures.

AppManager includes Knowledge Scripts that create jobs that gather data for call quality and call activity metrics and stores the data in the Avaya CM supplemental database. Each Knowledge Script can be customized to collect data for reporting and send proactive alerts for data in the supplemental database. The following Knowledge Scripts were run during the compliance testing:

- *CallQuery* script monitors call activity via the CDR link
- *CallQuality* and *PhoneQuality* scripts capture call quality metrics received in RTCP packets
- *RetrieveConfigData* script retrieves the phone inventory on Avaya Communication Manager using SNMP. Inventory data may then be used by other Knowledge Scripts that require it.
- *AvayaCM* script to discover Avaya Communication Manager components via SNMP.

To perform the monitoring functions, AppManager uses the following interfaces into the Avaya IP Telephony environment.

- Simple Network Management Protocol (SNMP) – AppManager uses SNMP to collect configuration and status information from Avaya Communication Manager.
- Real-time Transport Control Protocol (RTCP) – AppManager uses RTCP data from Avaya IP Telephones to gather call quality metrics for H.323 IP calls. The call quality metrics include packet loss, latency, and jitter. From these metrics, the MOS (mean opinion score) and the R-Value are computed, which measure overall call quality.
- Call Detail Recording (CDR) – AppManager uses CDR records from Avaya Communication Manager to track call activity.

Figure 1 illustrates the configuration used in these Application Notes. In the sample configuration, two sites, Sites A and B, are connected via an H.323 trunk. AppManager only monitors the VoIP infrastructure at Site A. Site B is present simply to generate inter-site traffic across the H.323 trunk and for access to the PSTN.

Site A has a redundant pair of Avaya S8730 Servers running Avaya Communication Manager with an Avaya G650 Media Gateway. Site A also includes Avaya 4600 and 9600 Series H.323 IP Telephones and an Avaya Digital Telephone. The configuration at Site B is similar to Site A. AppManager connects to each site via the corporate LAN. In this configuration AppManager is running on a Windows 2003 Server. The AppManager installation includes the following core components on the same server:

- **Operator Console** is used to perform AppManager configuration
- **Management Server** manages the data and communicates with agents to start/stop jobs
- **Repository** includes a Microsoft SQL database
- **Agent** is the managed client

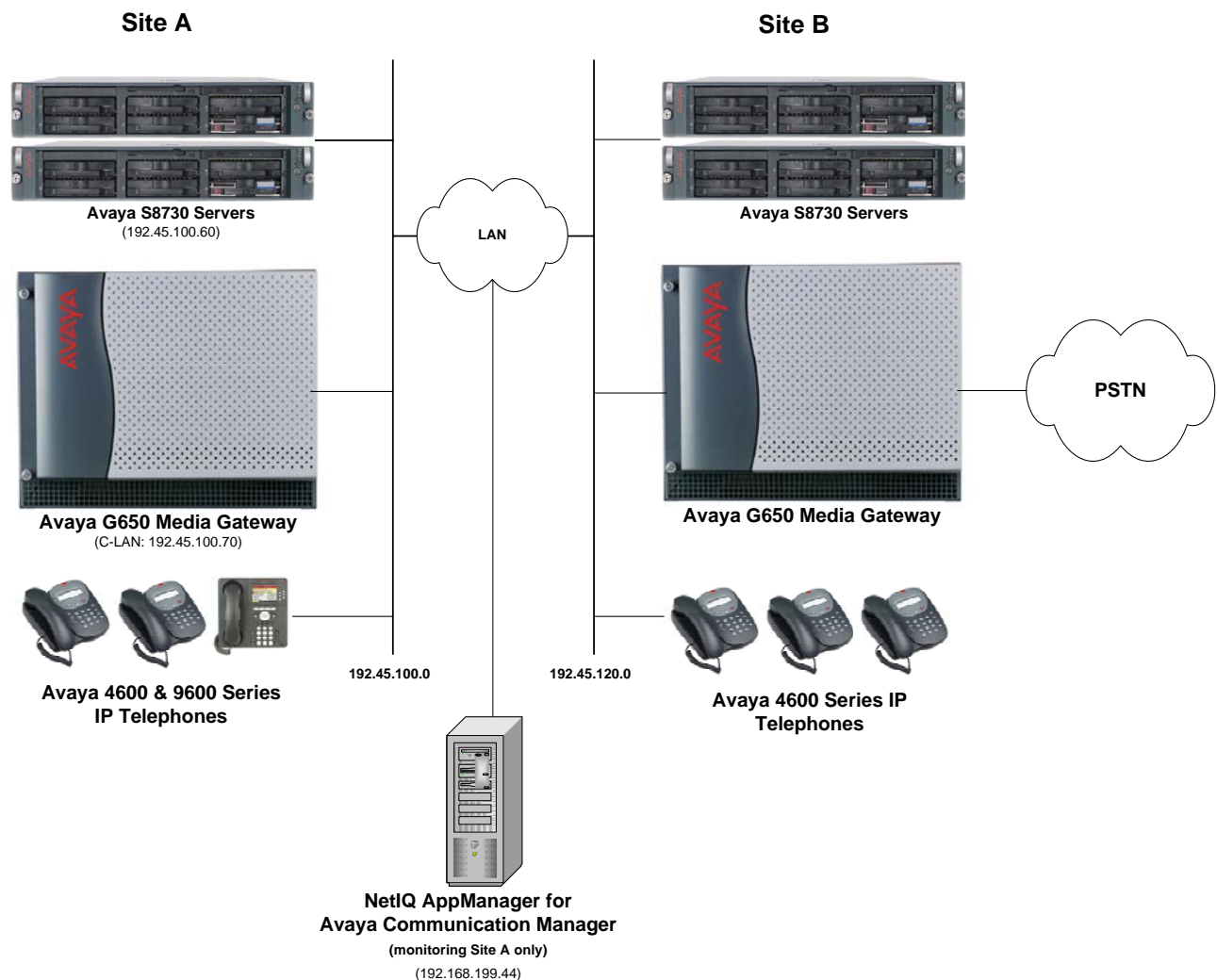


Figure 1: NetIQ AppManager with Avaya Communication Manager

2. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8730 Servers	Avaya Communication Manager 5.1.1 R015x.01.1.415.1 with Service Pack 1 (Patch 16402)
Avaya G650 Media Gateway <ul style="list-style-type: none">TN799DP C-LANTN2302AP Media Processor	HW01 FW026 HW11 FW118
Avaya 4600 Series IP Telephones (H.323)	2.8.3
Avaya 9600 Series IP Telephones (H.323) running Avaya one-X Deskphone Edition	S2.0
Avaya 6400 Series Digital Telephones	-
NetIQ AppManager for Avaya Communication Manager running on Windows 2003 Server SP2	7.3.16.0
Other NetIQ AppManager Core Components running on Windows 2003 Server SP2: <ul style="list-style-type: none">Operator ConsoleManagement ServerAgent	7.0 (Build 7.0.315.0)

3. Configure Avaya Communication Manager

This section describes the Avaya Communication Manager configuration at Site A required to interoperate with AppManager. In the test configuration, AppManager did not monitor Site B so no configuration of Avaya Communication Manager at that site is required. This section is divided into three sub-sections describing the three interfaces used by AppManager to gather data on the VoIP infrastructure. **Section 3.1** describes the SNMP configuration, **Section 3.2** describes the RTCP configuration, and **Section 3.3** describes the CDR configuration.

The configuration of Avaya Communication Manager in **Section 3.1** was performed using the Web interface. The configuration described in **Sections 3.2** and **3.3** was performed using the System Access Terminal (SAT). After the completion of the configuration, perform a **save translation** command to make the changes permanent.

3.1. SNMP

To access the Avaya Communication Manager Web interface, enter the IP address of the Avaya Server into a web browser. Login using appropriate credentials. The following page will appear. Click on **Launch Maintenance Web Interface**.

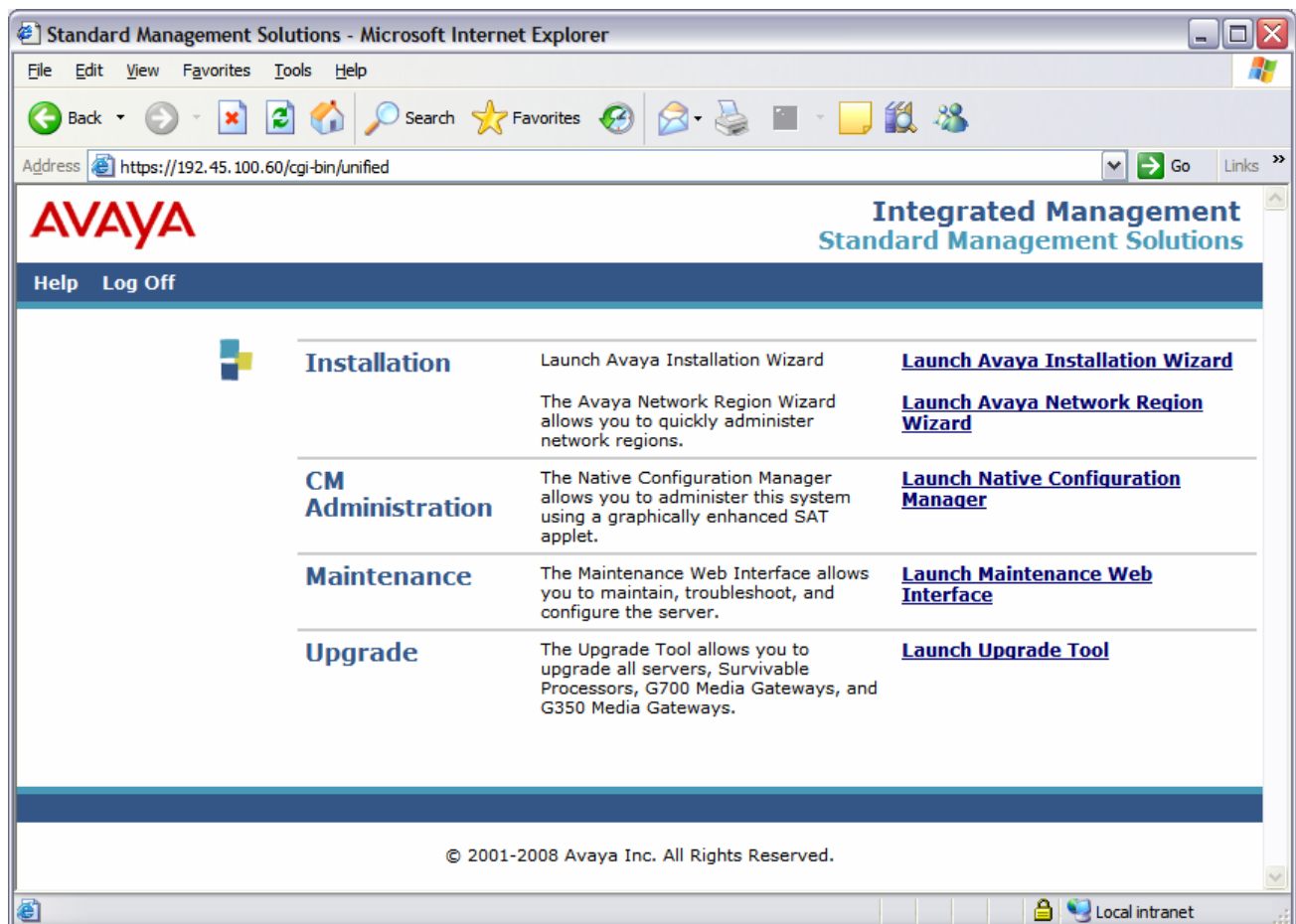


Figure 2: Avaya Communication Manager Web Interface – Initial Webpage

Navigate to **Alarms→SNMP Agents** in the left pane. Under **IP Addresses for SNMP Access**, select *Any IP address*. Under **SNMP Users / Communities**, select *Enable SNMP Version 1* and enter *public* for the **Community Name (read-only)** field. Repeat this for SNMP Version 2c. Click **Submit** at the bottom of the web page (not shown in the figure).

AVAYA Integrated Management Maintenance Web Pages

Help Exit This Server: [1] devcon31srv1 Duplicate Server: [2] devcon31srv2

Alarms
 Current Alarms
 Agent Status
 SNMP Agents
 SNMP Traps
 Filters
 SNMP Test

Diagnostics
 Restarts
 System Logs
 Temperature/Voltage
 Ping
 Traceroute
 Netstat
 Modem Test
 Network Time Sync
 Raid Status

Server
 Status Summary
 Process Status
 Interchange Servers
 Busy-out Server
 Release Server
 Shutdown Server
 Server Date/Time
 Software Version

Server Configuration
 Configure Server
 Restore Defaults
 Eject CD-ROM

Server Upgrades
 Pre Upgrade Step
 Manage Software
 Make Upgrade Permanent
 Boot Partition
 Manage Updates
 BIOS Upgrade

IPSI Firmware Upgrades
 IPSI Version
 Download IPSI Firmware
 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
 Login Account Policy
 Login Reports
 Modem
 Server Access
 Syslog Server

SNMP Agents

The SNMP Agents Web page allows modification of SNMP properties. SNMP allows the active server to monitor the SNMP port for incoming requests and commands (gets and sets).

Note: Prior to making any configuration changes the Master Agent should be put in a Down state. The Master Agent Status is shown below for your convenience. Once the configuration has been completed, then the Master Agent should be placed in an Up state. Changes to both the configuration on the SNMP Agents and/or SNMP Traps pages should be completed before Starting the Master Agent. Please use the Agent Status page to Start or Stop the Master Agent.

[View G3-AVAYA-MIB Data](#)
 Master Agent status: Up

IP Addresses for SNMP Access

☐ No Access
☒ Any IP address
☐ Following IP addresses:

IP address1 :
 IP address2 :
 IP address3 :
 IP address4 :
 IP address5 :

SNMP Users / Communities

☒ **Enable SNMP Version 1**
 Community Name (read-only) :
 Community Name (read-write) :

☒ **Enable SNMP Version 2c**
 Community Name (read-only) :
 Community Name (read-write) :

☐ **Enable SNMP Version 3**

Figure 3: SNMP Agents

The Avaya Server firewall must also be configured to allow SNMP traffic. To do this, navigate to **Security**→**Firewall** from the left pane. Locate *snmp* in the **Service** column and then select both the **Input to Server** and **Output from Server** checkboxes. Click **Submit** at the bottom of the webpage (not shown in the figure).

**Integrated Management
Maintenance Web Pages**

[Help](#) [Exit](#)

This Server: [1] devcon31srv1 Duplicate Server: [2] devcon31srv2

Netstat

Modem Test

Network Time Sync

Raid Status

Server

Status Summary

Process Status

Interchange Servers

Busy-out Server

Release Server

Shutdown Server

Server Date/Time

Software Version

Server Configuration

Configure Server

Restore Defaults

Eject CD-ROM

Server Upgrades

Pre Upgrade Step

Manage Software

Make Upgrade Permanent

Boot Partition

Manage Updates

BIOS Upgrade

IPSI Firmware Upgrades

IPSI Version

Download IPSI Firmware

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

Login Account Policy

Login Reports

Modem

Server Access

Syslog Server

License File

Authentication File

Firewall

Tripwire

Tripwire Commands

Install Root Certificate

SSH Keys

Ethernet Switch Ports

Web Access Mask

Firewall

The Firewall Web page lets you enable network services on the corporate LAN interface to the Avaya server. Unselected services are automatically disabled.

WARNING: Some network services are required for proper operation of or access to the server. For additional details, click **Help**.

Please wait...

Input to Server	Output from Server	Service	Port/Protocol
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ftp	21/tcp
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ssh	22/tcp
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	telnet	23/tcp
<input type="checkbox"/>	<input checked="" type="checkbox"/>	domain	53/udp
<input type="checkbox"/>	<input type="checkbox"/>	bootps	67/udp
<input type="checkbox"/>	<input type="checkbox"/>	bootpc	68/udp
<input type="checkbox"/>	<input type="checkbox"/>	tftp	69/udp
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	http	80/tcp
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ntp	123/udp
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	snmp	161/udp
<input type="checkbox"/>	<input type="checkbox"/>	snmptrap	162/udp
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	https	443/tcp
<input type="checkbox"/>	<input checked="" type="checkbox"/>	syslog	514/udp
<input type="checkbox"/>	<input type="checkbox"/>	ldap	389/tcp
<input type="checkbox"/>	<input type="checkbox"/>	ldaps	636/tcp
<input type="checkbox"/>	<input type="checkbox"/>	radius	1812/udp
<input type="checkbox"/>	<input type="checkbox"/>	securID	5500/udp
<input type="checkbox"/>	<input type="checkbox"/>	safeword	5030/tcp

Figure 4: Firewall

Lastly, the SNMP agent must be started. Navigate to **Alarms→Agent Status**. If the **Master Agent status** is *Down*, then click the **Start Agent** button. If the **Master Agent status** is *Up*, then the agent must be stopped and restarted.

AVAYA Integrated Management Maintenance Web Pages

Help Exit This Server: [1] devcon31srv1 Duplicate Server: [2] devcon31srv2

Alarms

- Current Alarms
- Agent Status
- SNMP Agents
- SNMP Traps
- Filters
- SNMP Test

Diagnostics

- Restarts
- System Logs
- Temperature/Voltage
- Ping
- Traceroute
- Netstat
- Modem Test
- Network Time Sync
- Raid Status

Server

- Status Summary
- Process Status
- Interchange Servers
- Busy-out Server
- Release Server
- Shutdown Server
- Server Date/Time
- Software Version

Server Configuration

- Configure Server

Agent Status

The Agent Status Web page shows the current state of the Master Agent and all the Sub Agents. It also allows for the ability to Start or Stop the Master Agent.

Master Agent status: Down **Start Agent**

Sub Agent Status

FP Agent:	UP
MVSubAgent:	UP
Load Agent:	UP
MIB2Agent:	UP

Sub Agents are NOT connected to the Master Agent.

Help

Figure 5: Agent Status

3.2. RTCP

This section describes the RTCP configuration. It is performed using the Avaya Communication Manager SAT interface.

Use the **change system-parameters ip-options** command to set the RTCP Monitor Server parameters. These values will be sent from Avaya Communication Manager to each Avaya IP Telephone so that the telephones will know where to send RTCP data. Set the **Default Server IP Address** to the IP address of the AppManager agent that will collect the data. The **Default Server Port** and **Default RTCP Report Period** must match the AppManager configuration in **Figure 22**. In the compliance test, the default values of **5005** and **5** were used, respectively.

```
change system-parameters ip-options                                     Page 1 of 4
                               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: 192.168.199.44
  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
```

Figure 6: System Parameters IP Options

Use the **change ip-network-region** command to enable RTCP reporting for H.323 IP telephones. In the compliance test, the H.323 IP telephones belonged to IP network region **1**. Set the **RTCP Reporting Enabled** field to **y**.

```
change ip-network-region 1                                     Page 1 of 19
                                                              IP NETWORK REGION
  Region: 1
Location: 1      Authoritative Domain:
  Name: Avaya region
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? n
  UDP Port Max: 65531
DIFFSERV/TOS PARAMETERS      RTCP Reporting Enabled? y
  Call Control PHB Value: 34      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: 7
  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
```

Figure 7: IP Network Region

3.3. CDR

This section describes the CDR configuration. It is performed using Avaya Communication Manager SAT interface.

Use the **change node-names ip** command to associate the IP address of the AppManager Agent to a node name. In the compliance test, the node name *NetIQ* was assigned to IP address **192.168.199.44**. Also, highlighted in the example below is the node name *clan2* which will be used in the next step. This node name represents the IP address of the CLAN circuit pack used as the source of the CDR data.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
clan2	192.45.100.70	
default	0.0.0.0	
medpro	192.45.100.69	
NetIQ	192.168.199.44	
(5 of 5 administered node-names were displayed)		
Use 'list node-names' command to see all the administered node-names		
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name		

Figure 8: IP Node Names

Use the **change ip-services** command to define the CDR link between Avaya Communication Manager and AppManager. In the **Service Type** field, enter **CDR1** for the primary CDR link. In the **Local Node** field, enter the node name that will terminate the CDR link on Avaya Communication Manager. In the compliance test, which used an Avaya G650 Media Gateway, the **Local Node** was the CLAN circuit pack discussed above. The **Remote Node** field is set to the node name defined in **Figure 8** for AppManager. The **Remote Port** may be set to a value between 5000 and 64500 inclusive and must match the port configured on AppManager in **Figure 22**.

change ip-services					Page	1 of	4
IP SERVICES							
Service	Enabled	Local	Local	Remote	Remote		
Type		Node	Port	Node	Port		
CDR1		clan2	0	NetIQ	9000		

Figure 9: IP Services – Page 1

On **Page 3**, set the **Reliable Protocol** field to **n** to disable the use of Avaya's Reliable Session Protocol (RSP) for CDR transmission. In this case, the CDR link will use TCP without RSP.

change ip-services						Page 3 of 4
SESSION LAYER TIMERS						
Service Type	Reliable Protocol	Packet Resp Timer	Session Connect Message Cntr	SPDU Cntr	Connectivity Timer	
CDR1	n	30	3	3	60	

Figure 10: IP Services – Page 3

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 settings for the compliance test are described below. AppManager used a customized CDR format which is defined in **Figure 12**. Other standard CDR formats may be used, but would require the **AvayaCDRFormat.txt** file to be modified with the appropriate CDR format on AppManager (see reference [3] for more details).

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

The remaining parameters define the type of calls that will be recorded and what data will be included in the record. See reference [1, 2] for a full explanation of each field. The test configuration used some of the more common fields described below.

- **Intra-switch CDR? y** This allows call records for internal calls involving specific stations.
- **Record Outgoing Calls Only? n** This allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls.
- **Outg Trk Call Splitting? y** This allows a separate call record for any portion of an outgoing call that is transferred or conferenced.
- **Suppress CDR for Ineffective Call Attempts? y** This prevents calls that are blocked from appearing in the CDR record.
- **Inc Trk Call Splitting? y** This allows a separate call record for any portion of an incoming call that is transferred or conferenced.

Default values may be used for all other fields.

change system-parameters cdr		Page 1 of 2
CDR SYSTEM PARAMETERS		
Node Number (Local PBX ID): 1	CDR Date Format: month/day	
Primary Output Format: customized	Primary Output Endpoint: CDR1	
Secondary Output Format:		
Use ISDN Layouts? n	Enable CDR Storage on Disk? 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? y	Outg Attd Call Record? n	
Disconnect Information in Place of FRL? 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		
Record Agent ID on Incoming? n	Record Agent ID on Outgoing? n	
Inc Trk Call Splitting? y	Inc Attd Call Record? n	
Record Non-Call-Assoc TSC? n	Call Record Handling Option: warning	
Record Call-Assoc TSC? n	Digits to Record for Outgoing Calls: dialed	
Privacy - Digits to Hide: 0	CDR Account Code Length: 6	

Figure 11: System Parameters CDR – Page 1

On **Page 2**, the customized CDR format used by AppManager is defined. Each field in the CDR record is entered in the **Data Item** column, followed by the expected length of the field in the **Length** column. This is the format that Avaya Communication Manager will use when sending CDR records to AppManager.

change system-parameters cdr			Page 2 of 2		
CDR SYSTEM PARAMETERS					
Data Item - Length		Data Item - Length		Data Item - Length	
1: acct-code	- 15	17:	-	33:	-
2: attd-console	- 2	18:	-	34:	-
3: auth-code	- 13	19:	-	35:	-
4: clg-num/in-tac	- 15	20:	-	36:	-
5: code-dial	- 4	21:	-	37:	-
6: code-used	- 4	22:	-	38:	-
7: cond-code	- 1	23:	-	39:	-
8: date	- 6	24:	-	40:	-
9: dialed-num	- 23	25:	-	41:	-
10: in-crt-id	- 3	26:	-	42:	-
11: in-trk-code	- 4	27:	-	43:	-
12: out-crt-id	- 3	28:	-	44:	-
13: sec-dur	- 5	29:	-	45:	-
14: time	- 4	30:	-	46:	-
15: return	- 1	31:	-	47:	-
16: line-feed	- 1	32:	-	48:	-
Record length = 104					

Figure 12: System Parameters CDR – Page 2

If the **Intra-switch CDR** field is set to **y** in **Figure 11**, 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 3	
INTRA-SWITCH CDR					
Assigned Members:				3	of 5000 administered
Extension	Extension	Extension	Extension	Extension	
24511					
24513					
24515					
Use 'list intra-switch-cdr' to see all members, 'add intra-switch-cdr' to add new members and 'change intra-switch-cdr <ext>' to change/remove other members					

Figure 13: Intra-Switch CDR

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 trunk group types. The example below shows the H.323 trunk between Sites A and B.

```
change trunk-group 6                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 6                Group Type: isdn          CDR Reports: y
  Group Name: To devcon13      COR: 1                TN: 1          TAC: 106
    Direction: two-way        Outgoing Display? n      Carrier Medium: H.323
  Dial Access? y              Busy Threshold: 255    Night Service:
Queue Length: 0
Service Type: tie                Auth Code? n
                                   Member Assignment Method: manual
```

Figure 14: Trunk Group

4. Configure NetIQ AppManager

This section describes the configuration of NetIQ AppManager. It assumes that the application and all required software components have been installed and properly licensed. The procedures fall into the following areas:

- Launch AppManager for Avaya Communication Manager
- Add Computer
- Configure SNMP, CDR, and RTCP Parameters
- Discover Avaya Communication Manager
- Retrieve Configuration Data
- Add Avaya IP Telephones

4.1. Launch AppManager for Avaya Communication Manager

NetIQ AppManager is configured using the **Operator Console**. Launch the **Operator Console** from the Windows Start menu by navigating to **All Programs→NetIQ→AppManager→Operator Console**. The logon screen is displayed as shown below. Enter the appropriate values for **Server** and **Repository** fields and then click on the **Logon** button. The main Operator Console window appears as shown in **Figure 16**.



Figure 15: Console Logon

4.2. Add Computer

Initially, a host computer must be added to the tree view to serve as the proxy agent for gathering data from Avaya Communication Manager. In order to add an agent computer to the Operator Console, navigate to **TreeView→Add Computer**.

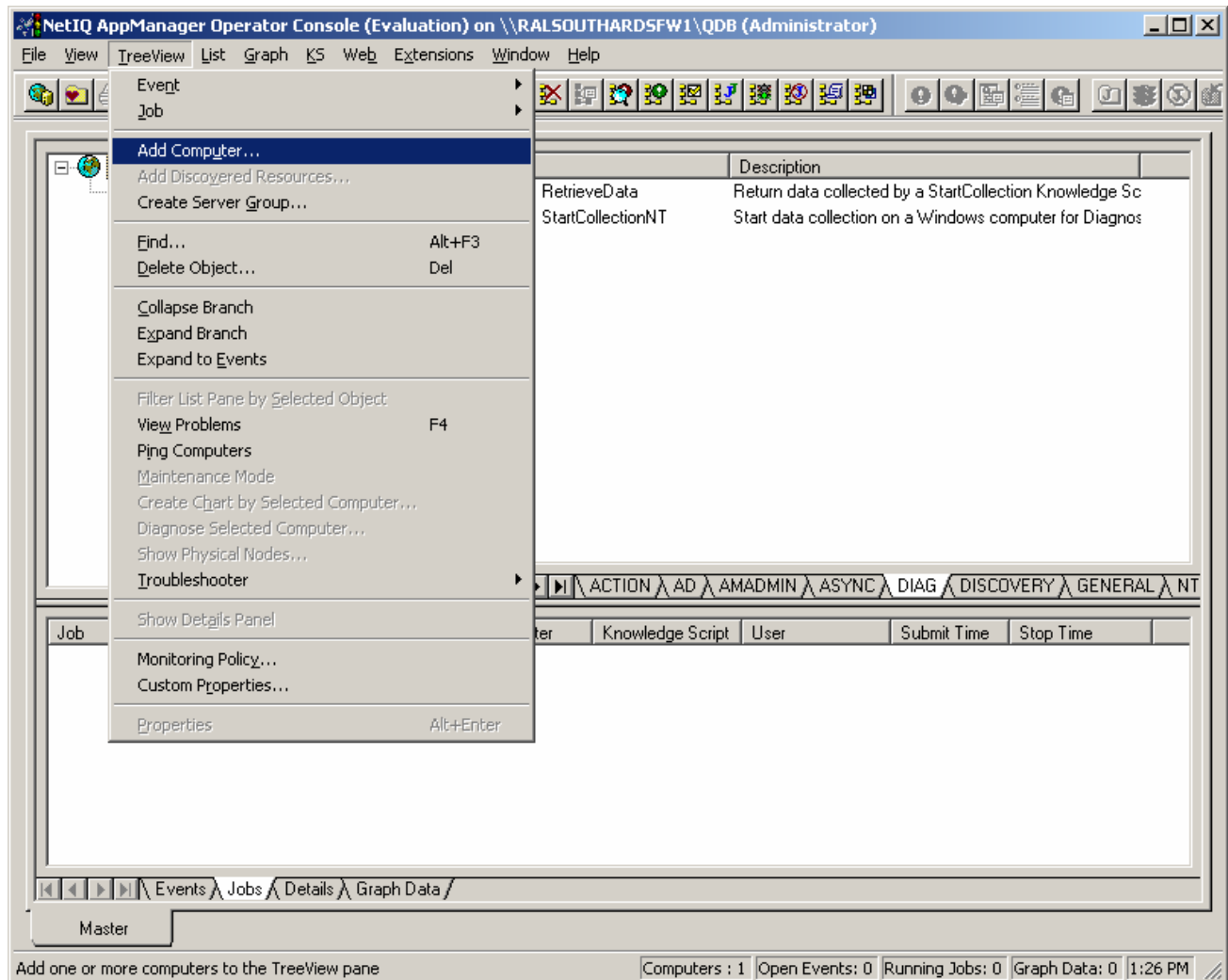


Figure 16: Main Operator Console Window

The pop-up window shown in **Figure 17** appears. Select the appropriate radio button for **Windows Computers** or **Unix Computers**. Enter the host name of the agent computer in the text box. In the case of **Windows Computers**, click the box for **Discover Windows objects automatically**. Click **OK**. This will populate the tree view in **Figure 18** with the following Window objects for the agent computer.

- CPU
- Memory
- File System
- Network
- Automatic Updates
- Common Language Runtime

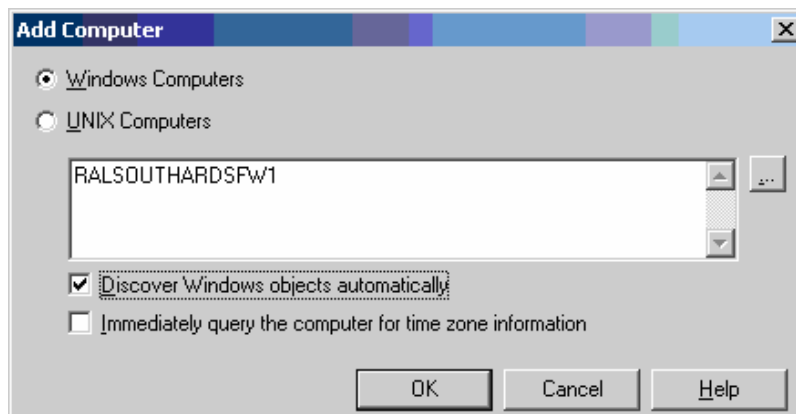


Figure 17: Add Computer

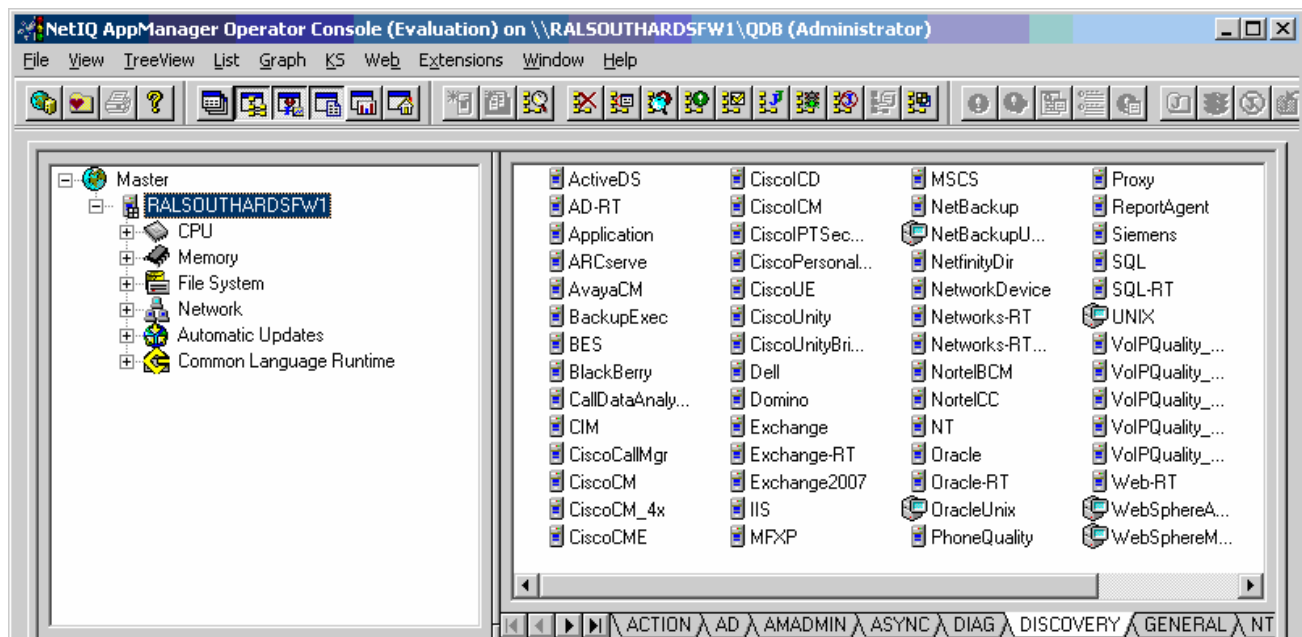


Figure 18: Main Operator Console Window with TreeView

4.3. Configure SNMP, CDR and RTCP Parameters

The agent computer created in **Figure 17** must be configured to connect to Avaya Communication Manager. From the main window shown in **Figure 16**, navigate to **Extensions→Security Manager** from the tool bar across the top of the window as shown below.

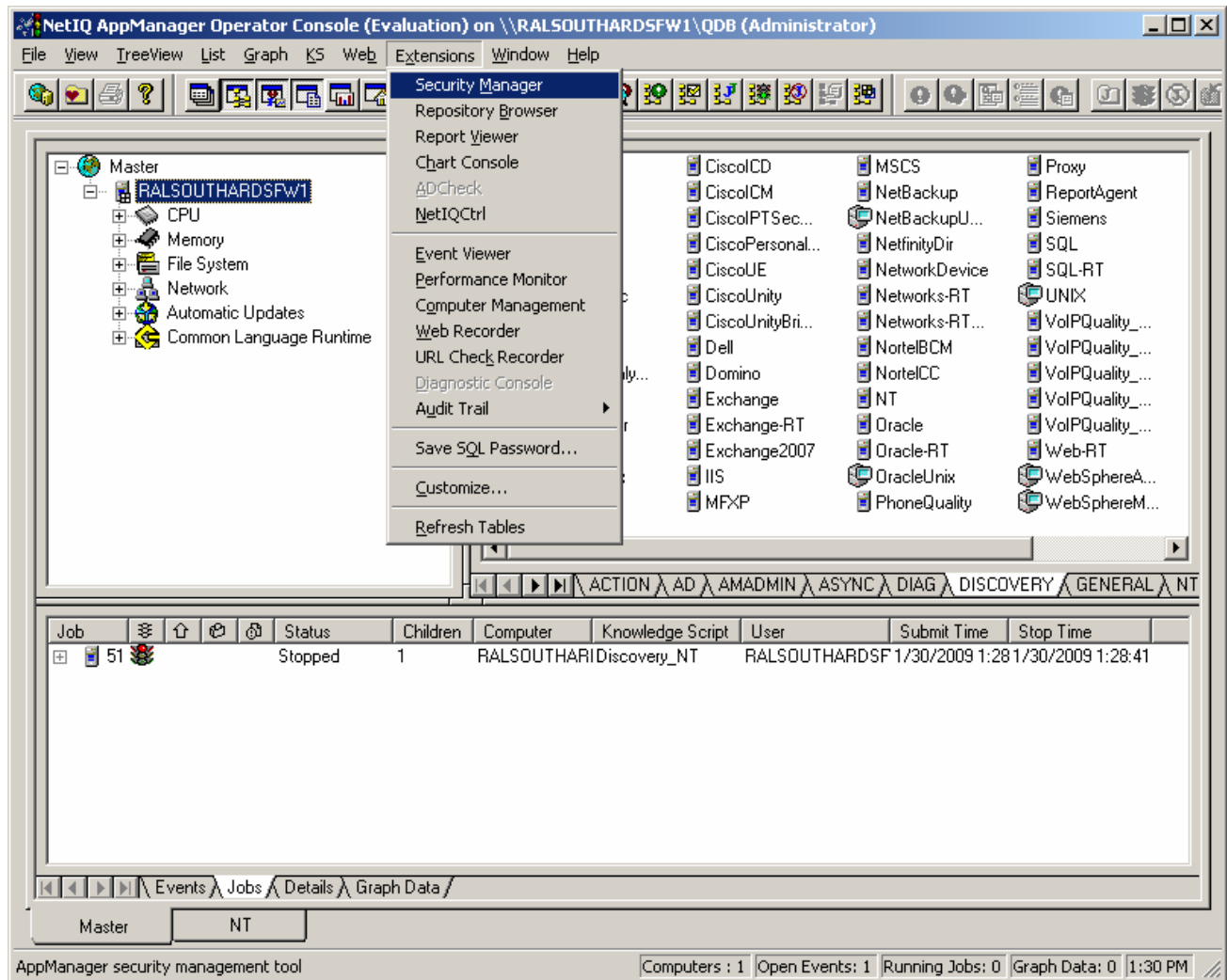


Figure 19: Navigate to Security Manager

The following window appears. Highlight the agent host name **RALSOUTHARDSFW1** and click on the **Custom** tab. The example below shows the two custom entries to communicate to Avaya Communication Manager via SNMP, CDR, and RTCP. The **AvayaCM_CallDataCollection** entry covers CDR and RTCP. These entries were originally created by clicking the **Add** button and will be covered next.

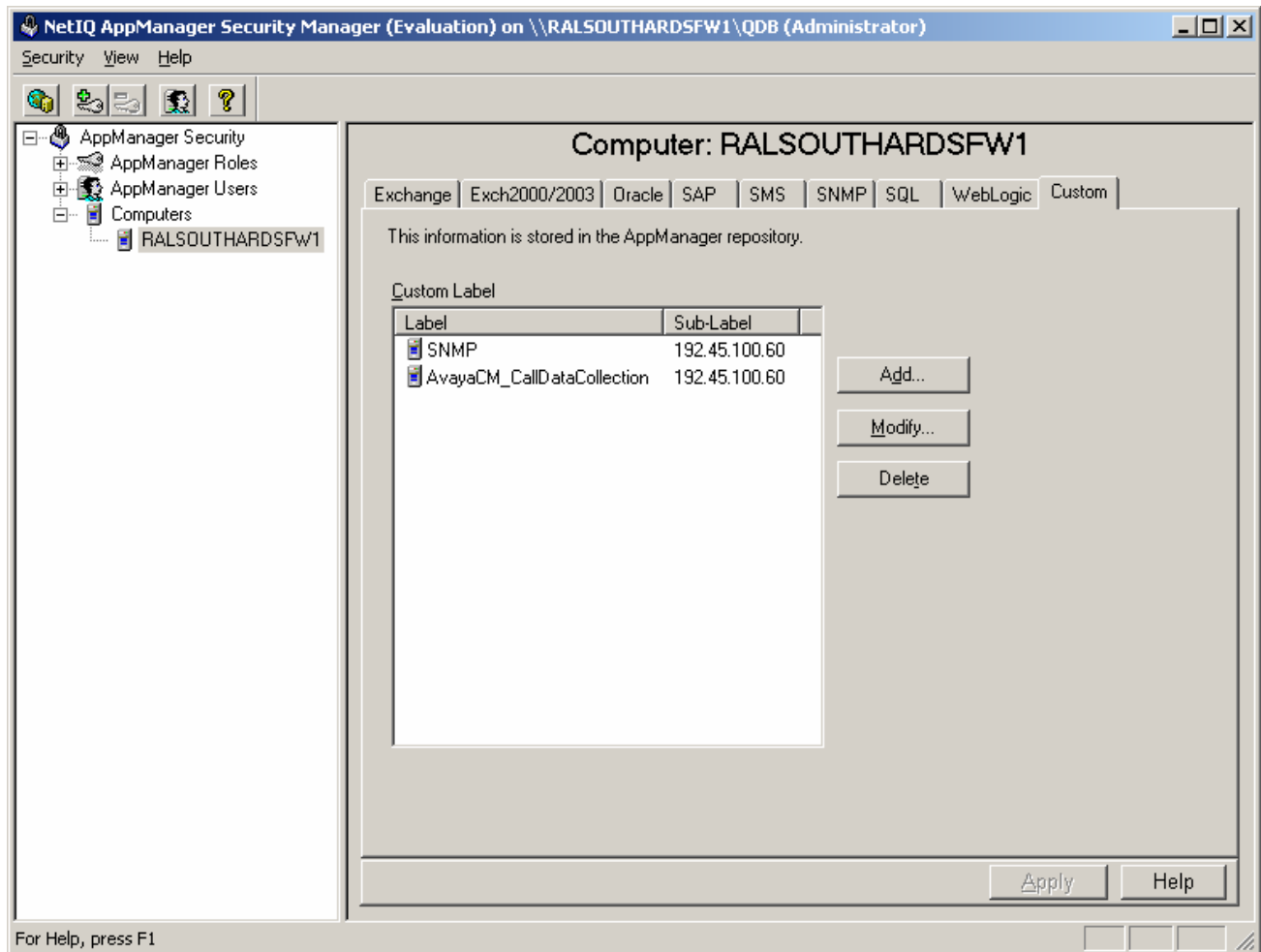
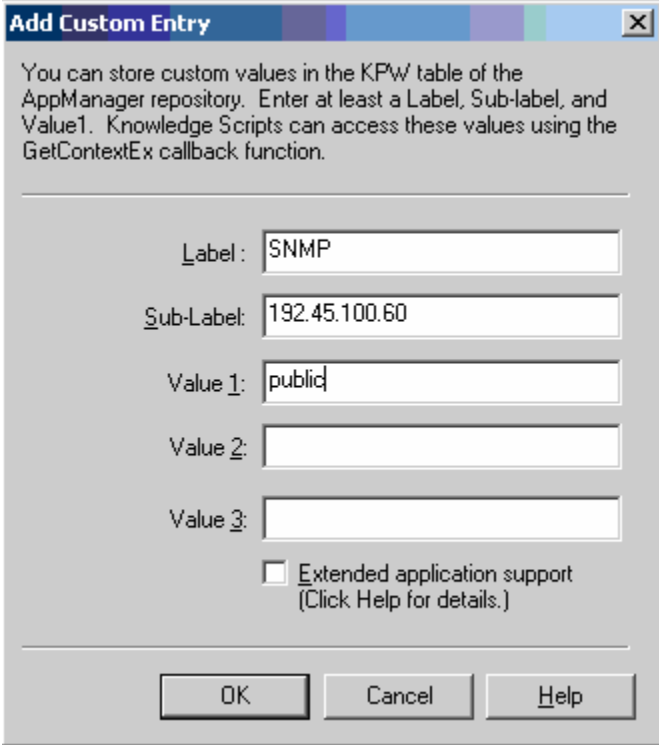


Figure 20: Security Manager

Click on the **Add** button in the Security Manager window shown in **Figure 20** to configure the SNMP connection parameters. The dialog box in **Figure 21** is displayed. Enter **SNMP** for the **Label** field. Enter the virtual IP address of the Avaya S8730 Servers in the **Sub-Label** field. Enter the SNMP community string (read-only) configured in **Figure 3** in the **Value 1** field. Click **OK**.



The dialog box is titled "Add Custom Entry" and contains the following fields and controls:

- Label:** A text field containing the text "SNMP".
- Sub-Label:** A text field containing the IP address "192.45.100.60".
- Value 1:** A text field containing the community string "public".
- Value 2:** An empty text field.
- Value 3:** An empty text field.
- Extended application support:** A checkbox that is currently unchecked, with the text "(Click Help for details.)" below it.
- Buttons:** At the bottom are three buttons: "OK", "Cancel", and "Help".

Figure 21: Add Custom Entry for SNMP

Click the **Add** button in the Security Manager window shown in **Figure 20** again to configure the CDR and RTCP connection parameters and enter **AvayaCM_CallDataCollection** for the **Label** field. Enter the IP address of the Avaya S8730 Servers in the **Sub-Label** field. In the case of redundant servers, enter the virtual IP address. **Value 1** is the port number used for CDR data. This must match the value configured on Avaya Communication Manager in **Figure 9**. **Value 2** is the port number used for RTCP data. **Value 3** is the RTCP report period in seconds. These values must match the values configured on Avaya Communication Manager in **Figure 6**. Click **OK**.

Add Custom Entry

You can store custom values in the KPw table of the AppManager repository. Enter at least a Label, Sub-label, and Value1. Knowledge Scripts can access these values using the GetContextEx callback function.

Label: AvayaCM_CallDataCollection

Sub-Label: 192.45.100.60

Value 1: 9000

Value 2: 5005

Value 3: 5

☐ Extended application support
(Click Help for details.)

OK Cancel Help

Figure 22: Add Custom Entry for CDR/RTCP

4.4. Discover Avaya Communication Manager

Once the connection parameters have been defined as shown in **Figure 21** and **Figure 22**, then the components of Avaya Communication Manager can be discovered using SNMP. To do this, select the **DISCOVERY** tab. Drag the **AvayaCM** script to the agent host name (**RALSOUTHARDSFW1**) in the tree view.

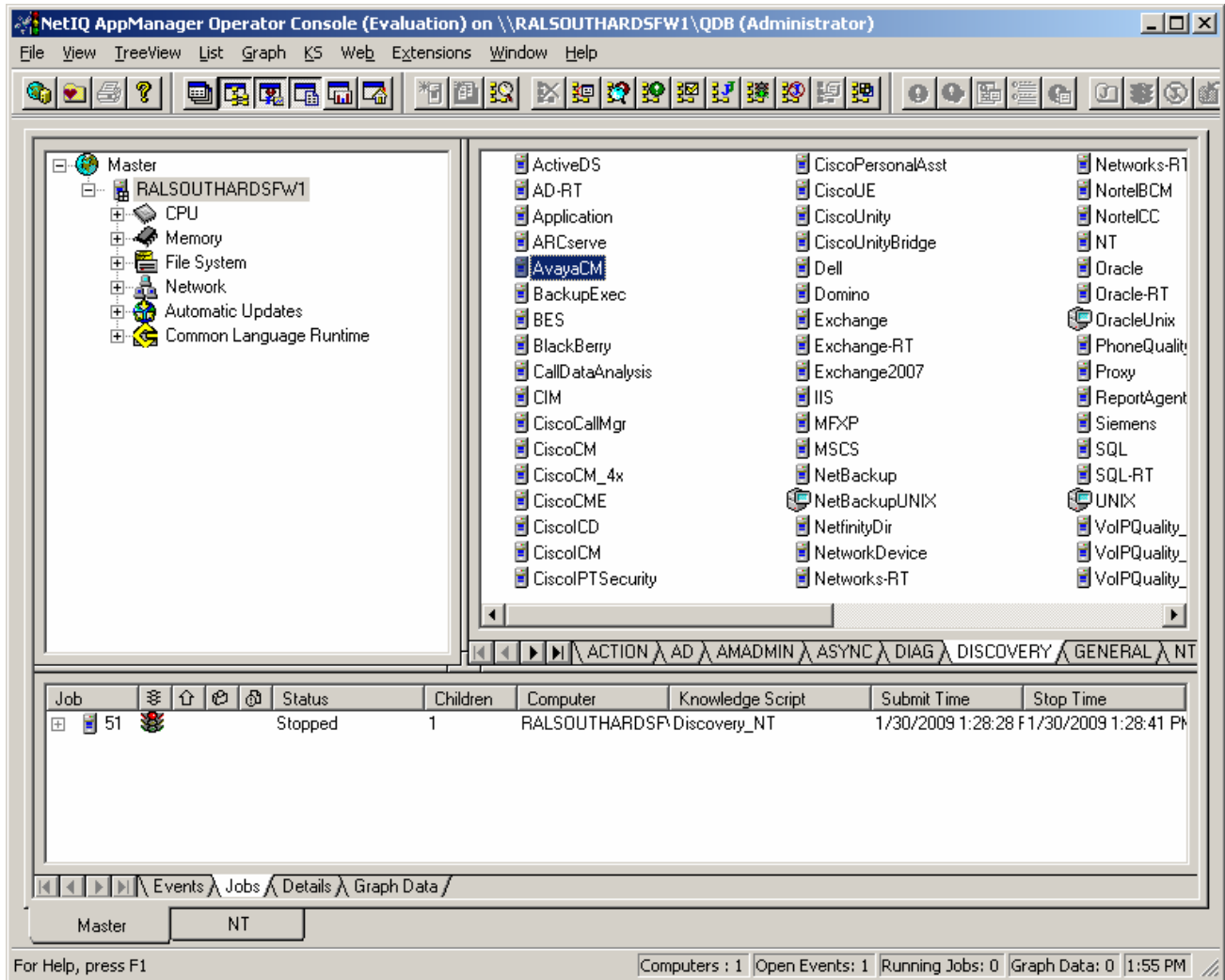


Figure 23: Discover Avaya Communication Manager

The following pop-up window will appear. Enter the virtual IP address of the Avaya S8730 Servers in the field labeled **Comma-separated list of active Communication Manager servers**. Optionally, the **Raise event if discovery succeeds** option may be enabled. Click **OK**.

This action will continue to fill out the tree view with all the Avaya Communication Manager components in the main Operator Console window, except for the individual IP telephones.

Description	Value	Units
General Settings		
+ Job Failure Notification		
+ Set up supplemental database?	<input checked="" type="checkbox"/> Yes	
- SNMP		
Global SNMP timeout	30	Seconds
+ Raise event if discovery succeeds?	<input checked="" type="checkbox"/> Yes	
+ Raise event if discovery fails?	<input checked="" type="checkbox"/> Yes	
Discover Avaya Communication Manager servers		
Discovery timeout for all servers	10	Minutes
Maximum number of concurrent discoveries	10	Discoveries
Comma-separated list of active Communication Manager servers	192.45.100.60	
Comma-separated list of Communication Manager IP address pairs in a single NAT cluster		
Full path to file with list of active Communication Manager servers		

Discovers an Avaya Communication Manager cluster. Specify a list of active Communication Managers or the full path to a file containing a list of servers. If the proxy agent is on the same computer as the Operator Console, you can use the file selector to browse for the file, otherwise enter the full path to the file. NOTE: Before running this Knowledge Script, configure the proper security parameters in Security Manager; click Help for instructions. The SNMP Agent must be active on all the servers in the cluster.

OK Cancel Help

Figure 24: Discovery Properties

4.5. Retrieve Configuration Data

Even though the tree view is now populated with the Avaya Communication Manager components, additional detailed information must be retrieved using SNMP and stored in the Avaya CM supplemental database. To do this, select the **AVAYACM** tab and drag the **RetrieveConfigData** script to the **Active SPE** in the left pane.

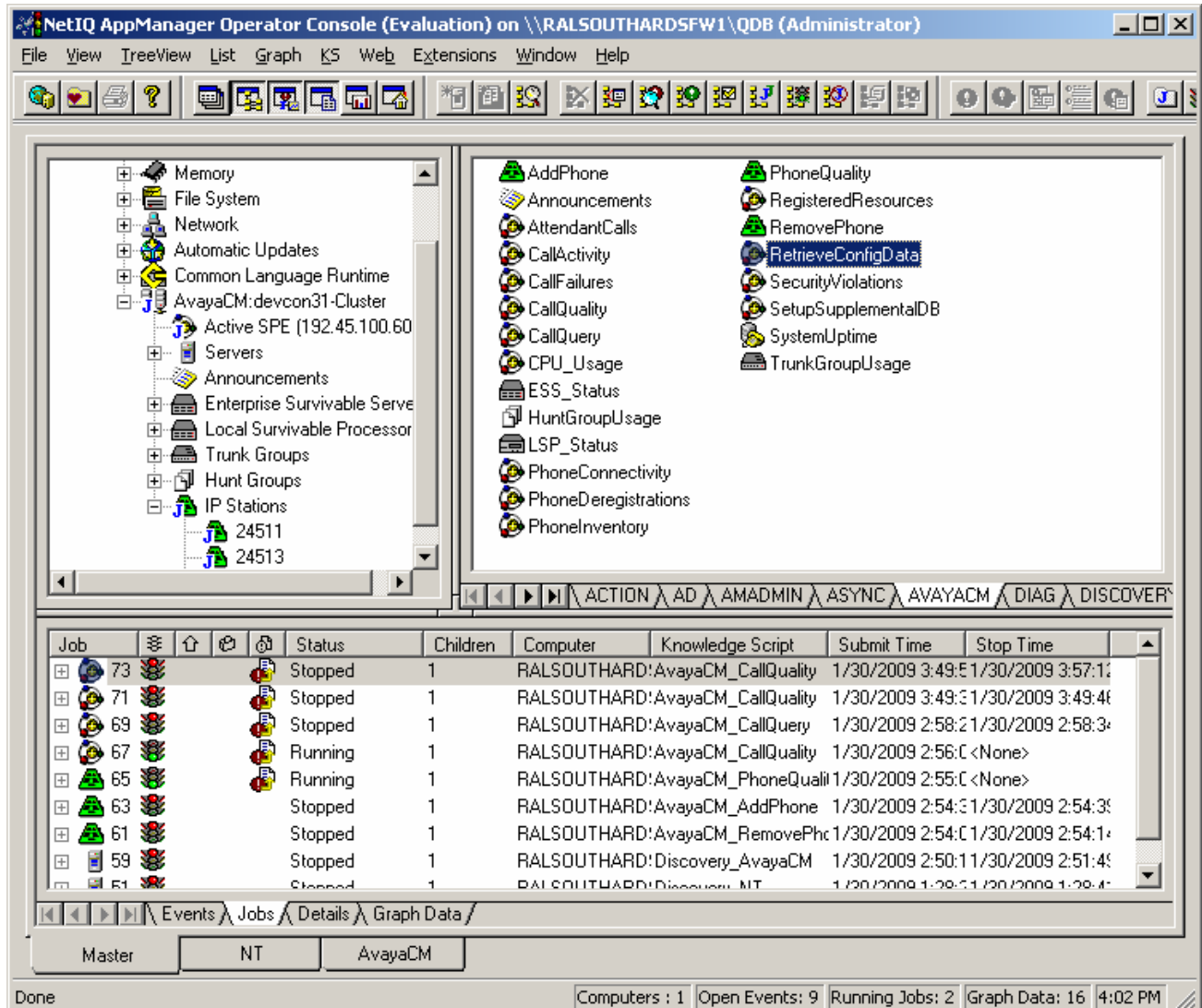


Figure 25: Retrieve Configuration Data

The following pop-up window appears. Retain the default values. Optionally, the **Raise event if configuration retrieval succeeds** option may be enabled. Click **OK**.

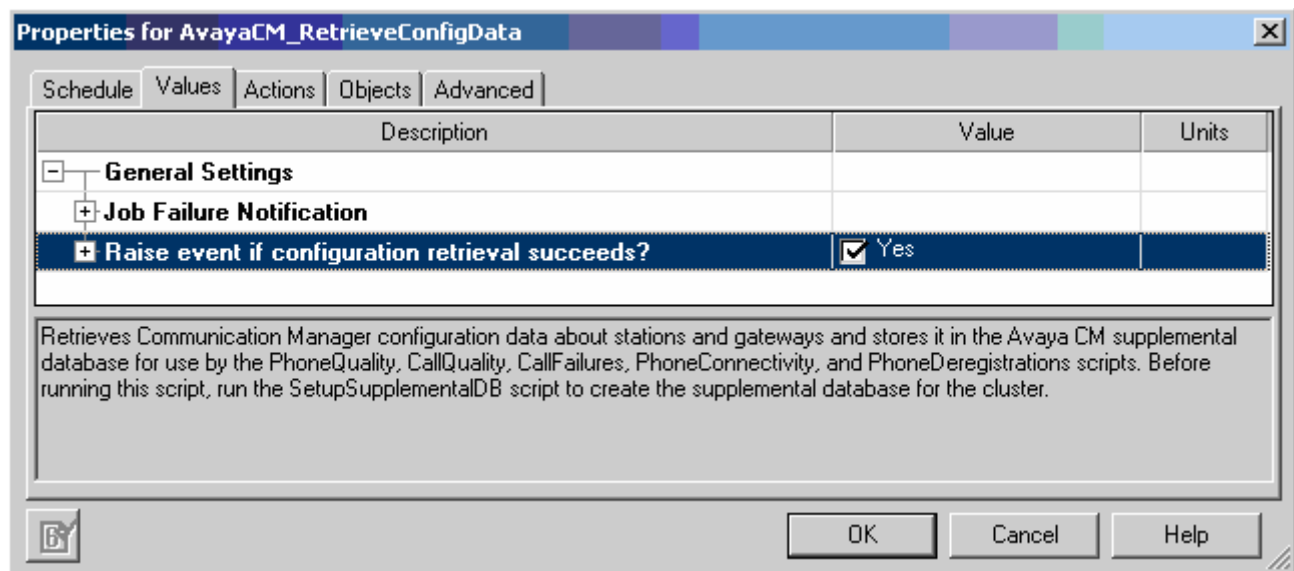


Figure 26: Retrieve Configuration Data Properties

4.6. Add Avaya IP Telephones

Lastly, in order to run a script (specifically the *PhoneQuality* script) on an individual IP telephone, that IP telephone must be entered in the tree view. To add an IP telephone to the tree view, select the **AVAYACM** tab and drag the **AddPhone** script to **IP Stations** in the left pane. The pop-up window in **Figure 28** will appear.

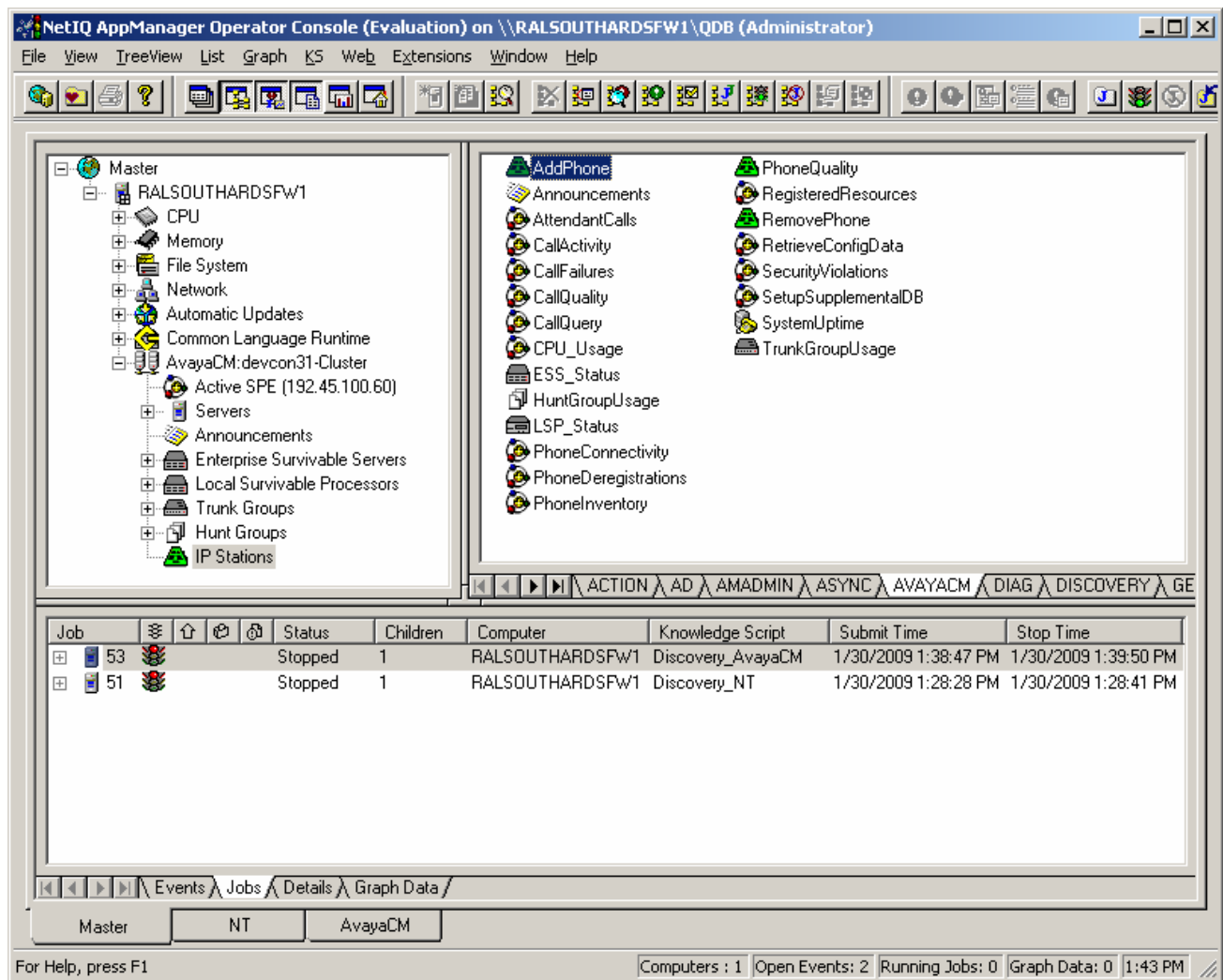


Figure 27: Add Phone

Enter the IP telephone extension or list of extensions in the **List of phone extensions** field as shown in **Figure 28**. Optionally, the **Raise event if all phones are added successfully** option may be enabled. Click **OK**. This action will fill out the tree view with the individual IP telephones shown in the tree view in **Figure 29**. Sample AppManager reports are shown in **Section 6.2**.

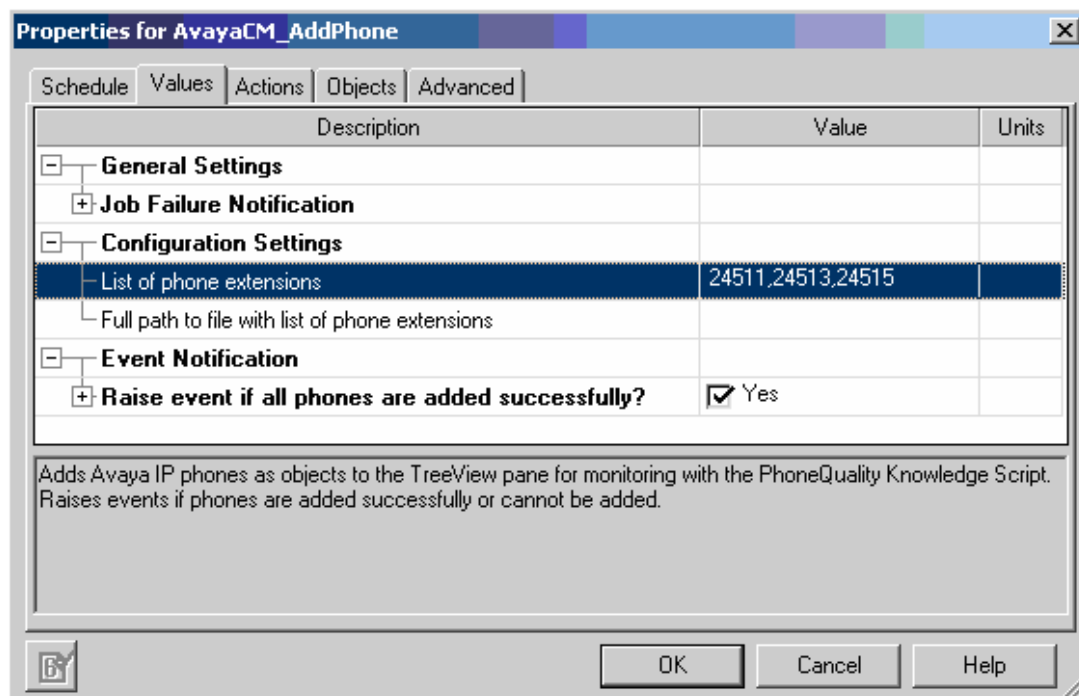


Figure 28: Add Phone Properties

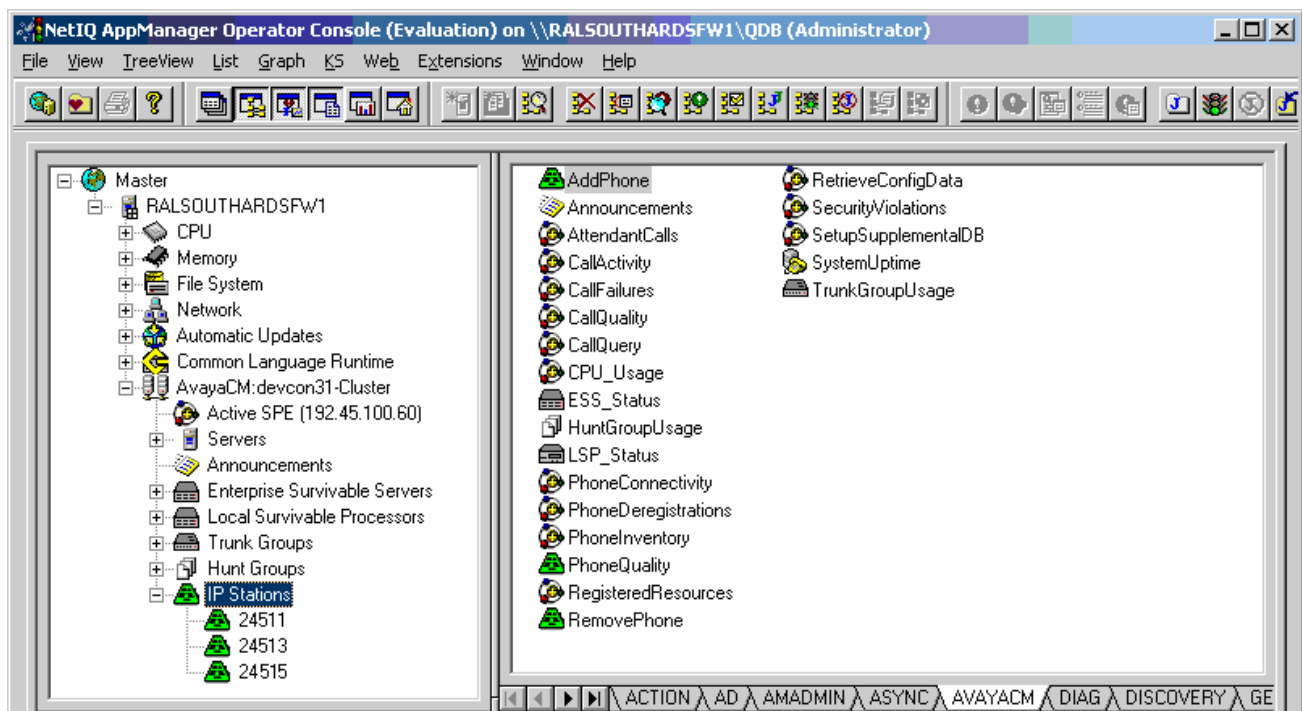


Figure 29: TreeView with IP Stations

5. Interoperability Compliance Testing

This section describes the compliance testing used to verify the interoperability of NetIQ AppManager with Avaya Communication Manager. This section covers the general test approach and the test results.

5.1. General Test Approach

The general approach was to place various types of calls to and from stations, collect VoIP call quality data on AppManager, and compare collected values with Avaya IP Telephone's Network Audio Quality values. In addition, CDR data displayed in the call query output from AppManager was compared to the CDR data received by an Avaya CDR test tool. For feature testing, the types of calls included internal calls, inbound trunk calls, outbound trunk calls, transferred calls, and conferenced calls. During the compliance test, a network impairment tool was utilized to simulate network delay and packet drop conditions in the corporate LAN. Verification of each call was made by performing queries into the AppManager data and looking at the results recorded. For serviceability testing, failures such as disconnecting the LAN cable were applied.

5.2. Test Results

AppManager passed compliance testing. Call quality metrics, CDR records, and the phone inventory were accurately collected on AppManager. The data was verified by running the *CallQuery*, *CallQuality*, *PhoneQuality*, and *RetrieveConfigData* Knowledge Scripts. Sample reports are shown in **Section 6.2**.

6. Verification Steps

This section provides the tests that can be performed to verify the configuration of Avaya Communication Manager and NetIQ AppManager.

6.1. Verify Avaya Communication Manager

The following steps may be used to verify the configuration on Avaya Communication Manager.

- Use the **ping** command to verify network connectivity from AppManager to all devices.
- Verify that calls can be successfully completed between the IP and digital telephones.
- From the SAT, use the **status cdr-link** command to verify that the CDR link to AppManager is up.

status cdr-link	
CDR LINK STATUS	
Primary	Secondary
Link State: up	CDR not administered
Date & Time: 2009/1 /26 10:35:6	0 /0 /0 0 :0 :0
Forward Seq. No: 0	0
Backward Seq. No: 0	0
CDR Buffer % Full: 0.00	0.00
Reason Code: OK	

Figure 30: CDR Link Status

- From the Avaya Communication Manager Web interface, click on the **Agent Status** link on the left pane to verify that the **Master Agent Status** is up as shown in **Figure 31**.

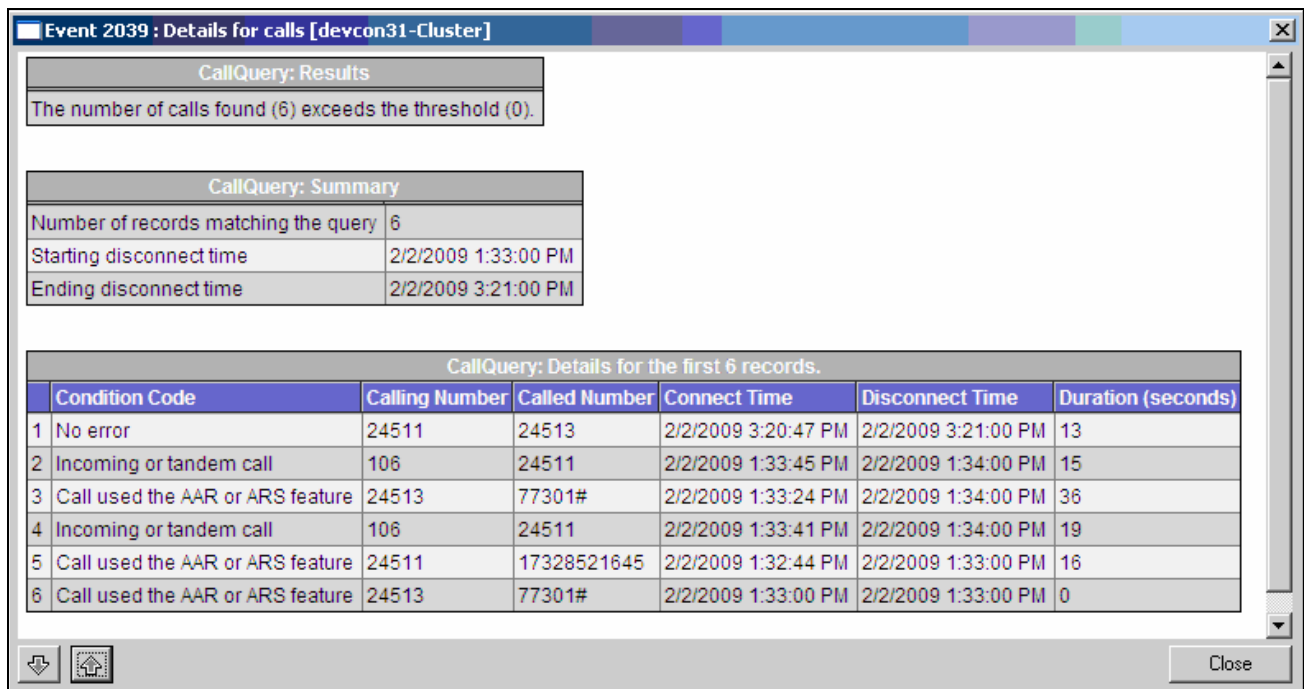


Figure 31: Agent Status

6.2. Verify NetIQ AppManager

The following steps may be used to verify the configuration of NetIQ AppManager. This section covers running various Knowledge Scripts to verify that data can be collected on AppManager. Note that running a script causes a job to be created in AppManager.

- Once the AppManager configuration is complete as detailed in **Section 4**, scripts can be run against the various components in the tree view. For example, to run the *CallQuery* script, which queries call detail records retrieved from Avaya Communication Manager and stored in the Avaya CM supplemental database, select the **AVAYACM** tab shown in **Figure 29** and drag the *CallQuery* script to the **Active SPE** in the tree view. A pop-up window appears (not shown) that allows parameters of the script to be modified, such as the date/time range. An example of the script output is shown below. It displays calls that match the criteria specified in the script parameters pop-up window.



Event 2039 : Details for calls [devcon31-Cluster]

CallQuery: Results

The number of calls found (6) exceeds the threshold (0).

CallQuery: Summary

Number of records matching the query	6
Starting disconnect time	2/2/2009 1:33:00 PM
Ending disconnect time	2/2/2009 3:21:00 PM

CallQuery: Details for the first 6 records.

	Condition Code	Calling Number	Called Number	Connect Time	Disconnect Time	Duration (seconds)
1	No error	24511	24513	2/2/2009 3:20:47 PM	2/2/2009 3:21:00 PM	13
2	Incoming or tandem call	106	24511	2/2/2009 1:33:45 PM	2/2/2009 1:34:00 PM	15
3	Call used the AAR or ARS feature	24513	77301#	2/2/2009 1:33:24 PM	2/2/2009 1:34:00 PM	36
4	Incoming or tandem call	106	24511	2/2/2009 1:33:41 PM	2/2/2009 1:34:00 PM	19
5	Call used the AAR or ARS feature	24511	17328521645	2/2/2009 1:32:44 PM	2/2/2009 1:33:00 PM	16
6	Call used the AAR or ARS feature	24513	77301#	2/2/2009 1:33:00 PM	2/2/2009 1:33:00 PM	0

Close

Figure 32: Call Query Report

- To run the *CallQuality* script, which monitors calls for quality metrics such as latency, packet loss, and jitter, select the **AvayaCM** tab in **Figure 29** and drag the *CallQuality* script to the **Active SPE** in the tree view. A pop-up window appears (not shown) that allows parameters of the script to be modified, such as event threshold levels. An example of the script output is shown below. It displays call quality metrics such as MOS, jitter and latency from both the calling and called parties.

Event 2012 : Details for call(s) which fell below the average R-Value threshold [192.45.100.60] [devcon31-Cluster]																	
CallQuality: Results																	
2 calls fell below the average R-Value threshold (70).																	
The minimum average R-Value for a call was 49.94.																	
CallQuality: Summary																	
Number of records matching the query 2																	
Starting disconnect time 1/30/2009 3:52:53 PM																	
Ending disconnect time 1/30/2009 3:56:33 PM																	
CallQuality: Details for the first 2 records.																	
	Side A	Side B	Connect Time	Disconnect Time	Duration (seconds)	Side A MOS	Side A R-Value	Side A Jitter (ms)	Side A Latency (ms)	Side A Lost Packets (%)	Side A Codec	Side B MOS	Side B R-Value	Side B Jitter (ms)	Side B Latency (ms)	Side B Lost Packets (%)	Side B Codec
1	24513	24515	1/30/2009 3:55:55 PM	1/30/2009 3:56:33 PM	38	2.62	50.87	2	151	15.01	G711u	2.57	49.94	0	151	15.40	G711u
2	24511	24513	1/30/2009 3:53:45 PM	1/30/2009 3:54:50 PM	65	3.46	67.20	2	101	9.46	G711u	3.46	67.10	2	102	9.50	G711u

Figure 33: Call Quality Report

- To run the *PhoneQuality* script, which collects real-time voice quality statistics for active calls on Avaya IP phones, select the **AvayaCM** tab in **Figure 29** and drag the **PhoneQuality** script to the **Active SPE** in the tree view. A pop-up window appears (not shown) that allows parameters of the script to be modified. An example of the script output is displayed in the bottom half of the Operator Console window. It displays the real-time voice quality metrics for an active call established between extensions 24513 and 24515.

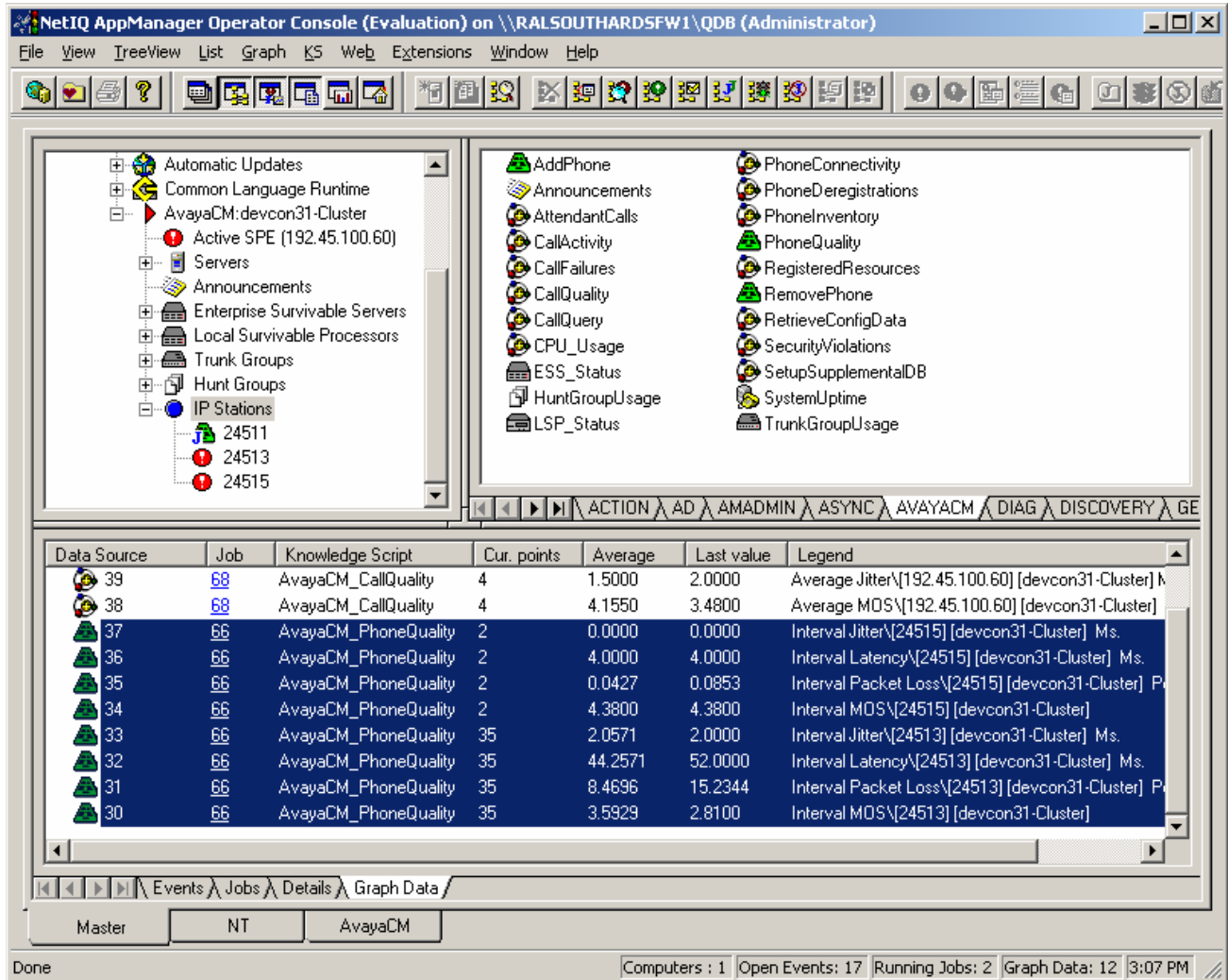


Figure 34: Phone Quality Report

- In **Section 4.5**, the *RetrieveConfigData* script was run to retrieve Avaya Communication Manager configuration data about stations and stores it in the Avaya CM supplemental database. This script generates a data file with the phone inventory as shown below. This data file is stored on the AppManager server in the **Program Files\NetIQ\Temp\NetIQ_debug** directory.

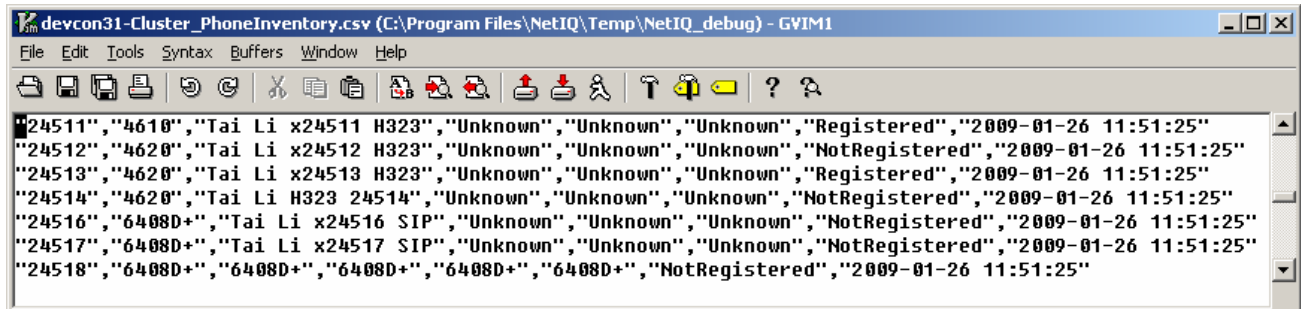


Figure 35: Phone Inventory

7. Support

For technical support on AppManager, contact NetIQ via the **Support & Services** link at www.netiq.com.

8. Conclusion

These Application Notes describe the steps required to configure NetIQ AppManager to interoperate with Avaya Communication Manager, including establishing a CDR link, sending RTCP packets from the Avaya H.323 IP Telephones to NetIQ AppManager, and enabling SNMP for collecting configuration data.

9. References

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

- [1] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 4.0, Release 5.0, January 2008, available at <http://support.avaya.com>.
- [2] *Feature Description and Implementation for Avaya Communication Manager*, Doc # 555-245-205, Issue 6, January 2008, available at <http://support.avaya.com>.
- [3] *NetIQ AppManager for Avaya Communication Manager Management Guide*, October 2008, available at <http://www.netiq.com/support>.

©2009 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.