Avaya Solution & Interoperability Test Lab

Application Notes for CA NetQoS Unified Communications Monitor with Avaya Aura™ Communication Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the CA NetQoS Unified Communications Monitor to successfully interoperate with Avaya Aura™ Communication Manager.

CA NetQoS Unified Communications Monitor is a network-based voice and video monitoring product that tracks the quality of end-user experience, provides alerts on performance problems and isolates performance issues to speed troubleshooting.

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 a compliance-tested configuration consisting of an Avaya VoIP environment, which included Avaya Aura™ Communication Manager, Avaya IP and Digital Telephones, and CA NetQoS Unified Communications Monitor.

The overall objective of this interoperability compliance testing is to verify that CA NetQoS Unified Communications Monitor (herein referred to as CA NetQoS UC Monitor) can operate in an Avaya VoIP environment and accurately report call quality problems if they arise.

CA NetQoS UC Monitor utilizes the Avaya RTCP Monitor feature to automatically collect VoIP quality information. In addition, UC Monitor provides an optional feature to collect and correlate CDRs with the RTCP information to provide greater insight into the caller and called party, as well as the identity of the digital phone number on the other side of the Avaya gateway.

In an Avaya environment, CA NetQoS UC Monitor provides metrics to ensure UC quality of experience, to enable easier troubleshooting by isolation of an issue to specific locations or network paths, and to evaluate long-term call activity and volume for capacity planning purposes.

These Application Notes assume that Communication Manager is already installed and configuration steps have been performed. Only steps relevant to this compliance test will be described in this document.

1.1. Interoperability Compliance Testing

The focus of the interoperability compliance testing was primarily on verifying whether CA NetQoS UC Monitor can interoperate in an Avaya VoIP environment and can accurately report degradation in call quality caused by network impairments. The specific environment used in this testing consisted of Communication Manager, Avaya IP and Digital Telephones. The serviceability testing introduced failure scenarios to verify if CA NetQoS UC Monitor can recover from failures.

Please refer to Section 6 for complete test results, known limitations, observations and any necessary workarounds.

1.2. Support

Technical support for CA NetQoS UC Monitor can be obtained by contacting CA NetQoS by calling (800) 225-5224.

2. Reference Configuration

Figure 1 illustrates a sample configuration consisting of a redundant pair of Avaya S8720 Servers running Communication Manager and an Avaya G650 Media Gateway at Site A, and Avaya S8300 Server running Communication Manager with an Avaya G450 Media Gateway at Site B. CA NetQoS UC Monitor is located in a different VLAN. A network impairment tool was positioned in line between Site A and Site B. Site C is included to provide Avaya IP telephones in a different subnet than Site A. The calls between Site A and Site C will not go through the network impairment tool.

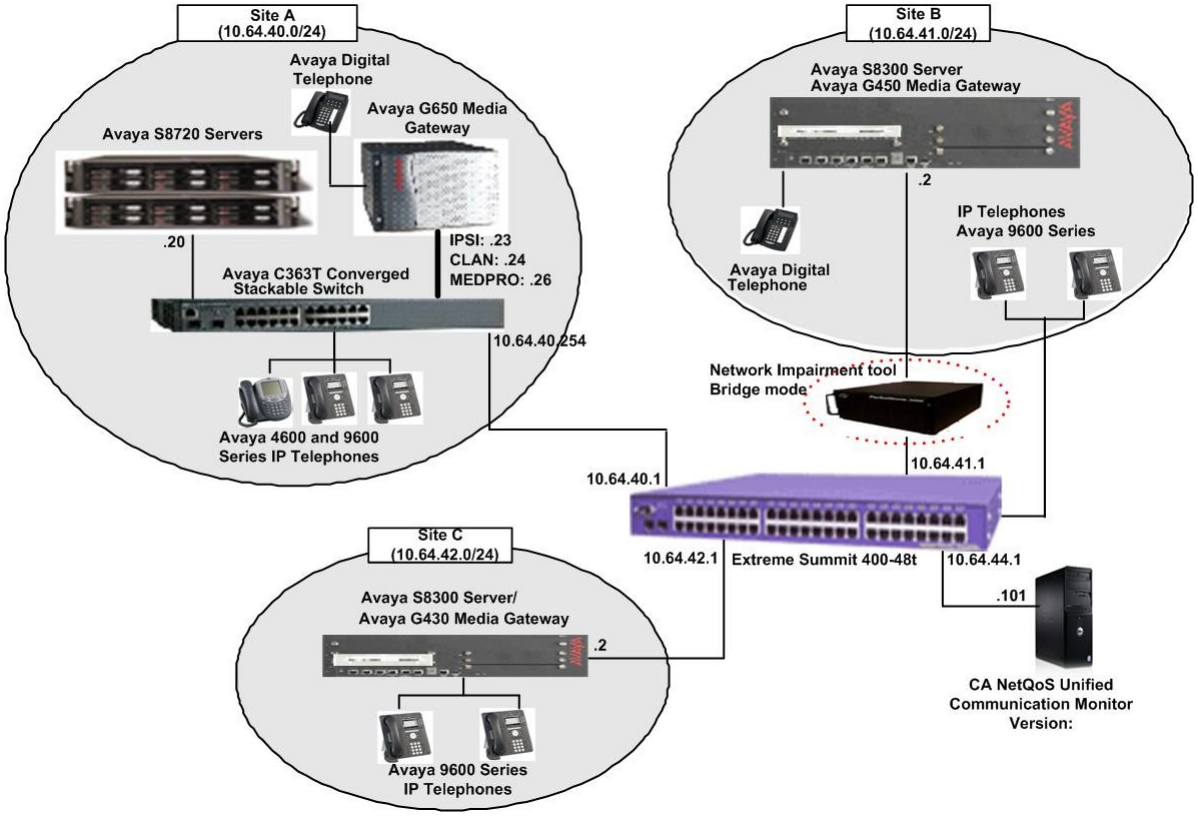


Figure 1. Test configuration of CA NetQoS UC Monitor in an Avaya VoIP Environment

3. Equipment and Software Validated

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

Equipment	Software
Avaya S8720 Servers with Avaya G650 Media Gateway	Avaya Aura™ Communication Manager 5.2.1 (R015x.02.1.016.4) with Patch 17963
Avaya S8300 Server	Avaya Aura™ Communication Manager 5.2.1 (R015x.02.1.016.4) with Patch 17963
Avaya G450 Media Gateway	28.17
Avaya 4625 IP Telephone (H.323)	2.9
Avaya 9600 Series IP Telephone 9620 (H.323) 9630 (H.323) 9650 (H.323) 9670 (H.323)	 3.1 3.1 3.1 3.1
Avaya 6408D+ Digital Telephone	-
CA NetQoS Unified Communications Monitor on Windows 2003 Server with Service Pack 2	3.0 Build 33

4. Configure Avaya Aura™ Communication Manager

This section provides procedures for configuring Communication Manager in preparation of the compliance test, with CA NetQoS UC Monitor. All configuration changes in Communication Manager were performed via the System Access Terminal (SAT). These steps describe the procedure used for the Avaya S8720 Server. The highlighted sections of the following screens indicate the parameter values used during the compliance test. During the test, CDR and RTCP were utilized. However, CDR collection is an optional step that enables CA NetQoS UC Monitor to collect additional data. This section describes procedures for setting up the following features:

- RTCP Monitor
- CDR (Optional)

4.1. Configure RTCP Monitor Server

This section provides the procedures for configuring the UC Monitor server as the RTCP Monitor Server. Since CA NetQoS UC Monitor utilizes RTCP packets to calculate and report the quality of the call stream, a RTCP Monitor Server needs to be specified in Communication Manager. The following screen describes the setting of the RTCP Monitor Server. Enter the **change system-parameters ip-options** command to configure the RTCP Monitor Server. Provide the following information:

- Default Server IP Address - IP address of CA NetQoS UC Monitor.

- Default Server Port – 5005 [This port number must match the CA NetQoS UC Monitor RTCP Listening Port. The default value for the Default Server Port field is 5005]
- Default RTCP Report Period(secs) – 5 [The report period determines the frequency at which Avaya Communication Manager forwards RTCP packets to the RTCP Monitor Server, which is the CA NetQoS UC Monitor server. The value for the Default RTCP Report Period(secs) field is 5]

Default values may be used in the remaining fields.

```
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
                  Enable Voice/Network Stats? n
 RTCP MONITOR SERVER
         Default Server IP Address: 10 .64 .44 .101
                 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
```

4.2. Configure Avaya Call Detail Recording (Optional)

CDR collection is an optional step that enables CA NetQoS UC Monitor to collect additional data. Use the **change node-names ip** command to create a new node name, for example, **CDR-NetQoS**. This node name is associated with the IP Address of the PC running the CA NetQoS UC Monitor application. Also, take note of the node name – **CLAN**. It will be used in the next step.

```
change node-names ip                                             Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
CDR-NetQoS              10.64.44.101
CLAN                    10.64.40.24
G450                    10.64.41.21
MEDPRO                  10.64.40.26
RDTT                    10.64.43.10
```

Use the **change ip-services** command to define the CDR link running over the TCP/IP 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: **CLAN** [For the Avaya S8720 Server, the Local Node is set to the node name of the CLAN board. If an Avaya S8300 Server were utilized, Local Node would be set to **procr**.]
- Local Port: **0** [The Local Port is fixed to 0 because Communication Manager initiates the CDR link.]
- Remote Node: **CDR-NetQoS** [The Remote Node is set to the node name previously defined.]
- Remote Port: **9000** [The Remote Port may be set to a value between 5000 and 64500 inclusive, and must match the port configured in CA NetQoS UC Monitor, which is 9000 by default.]

```
change ip-services                                              Page   1 of   4

                                    IP SERVICES
 Service      Enabled      Local       Local        Remote       Remote
  Type                     Node        Port         Node         Port
CDR1                  CLAN             0        CDR-NetQoS       9000
CDR2                  CLAN             0        RDTT             9001
```

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
 CDR2            y          30               3            3         60
```

Enter the **change system-parameters cdr** command from the SAT to set the parameters for the type of calls to track and the format of the CDR data. The example below shows the settings used during the compliance test. Provide the following information:

- 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 the data that will be included in the record. See reference [2] for a full explanation of each field. The test configuration used some of the more common fields described below.

- Use Legacy CDR Formats?: **n** [Allows CDR formats to use 5.x CDR formats. If the field is set to **y**, then CDR formats utilize the 3.x CDR formats.]
- 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?: **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): 1                       CDR Date Format: month/day
      Primary Output Format: unformatted   Primary Output Endpoint: CDR1
    Secondary Output Format: unformatted Secondary Output Endpoint: CDR2
           Use ISDN Layouts? n                    Enable CDR Storage on Disk? y
       Use Enhanced Formats? n      Condition Code 'T' For Redirected Calls? y
      Use Legacy CDR Formats? n                  Remove # From Called Number? n
Modified Circuit ID Display? n                                Intra-switch CDR? y
                  Record Outgoing Calls Only? n      Outg Trk Call Splitting? y
  Suppress CDR for Ineffective Call Attempts? n       Outg Attd Call Record? 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? y       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
```

If the Intra-switch CDR field is set to **y** on Page 1 of the system-parameters cdr form, then use the **change intra-switch-cdr** command to define the extensions that will be subject to call detail records when involved in an internal call. In the Assigned Members field, enter the specific extensions whose usage will be tracked.

Note: *To simplify the process of adding multiple extensions in the Assigned Members field, the Intra-switch CDR by COS feature may be utilized in the SPECIAL APPLICATIONS form under the system-parameters section. To utilize this feature, contact an authorized Avaya account representative to obtain the license.*

```
change intra-switch-cdr                                         Page   1 of   2
                           INTRA-SWITCH CDR

Assigned Members:   6    of 5000   administered
   1: 22001     19:          37:          55:          73:          91:
   2: 22002     20:          38:          56:          74:          92:
   3: 22003     21:          39:          57:          75:          93:
   4: 22004     22:          40:          58:          76:          94:
   5: 22005     23:          41:          59:          77:          95:
   6: 22007     24:          42:          60:          78:          96:
```

For each trunk group whose CDR records are required, verify that CDR reporting is enabled. Use the **change trunk-group *n*** command, where ***n*** is the trunk group number, to verify that the CDR Reports field is set to **y**. This applies to all types of trunk groups.

Note: *These steps assume that a trunk group, a signaling group, and a route pattern are configured correctly. Configuring these is outside the scope of these Application Notes.*

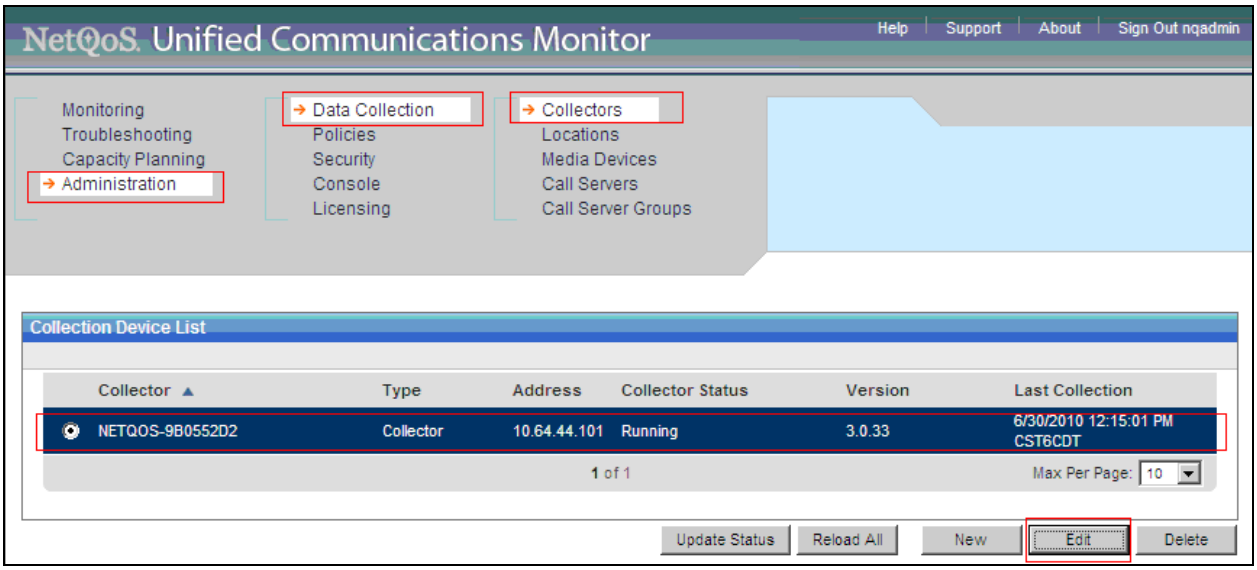
```
change trunk-group 10                                          Page   1 of  21
                                TRUNK GROUP

Group Number: 10                    Group Type: isdn          CDR Reports: y
  Group Name: G450-IP trunk                COR: 1        TN: 1        TAC: 111
   Direction: two-way         Outgoing Display? y         Carrier Medium: H.323
 Dial Access? y               Busy Threshold: 255  Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 10
                                                     Number of Members: 4
```

5. Configure CA NetQoS Unified Communications Monitor

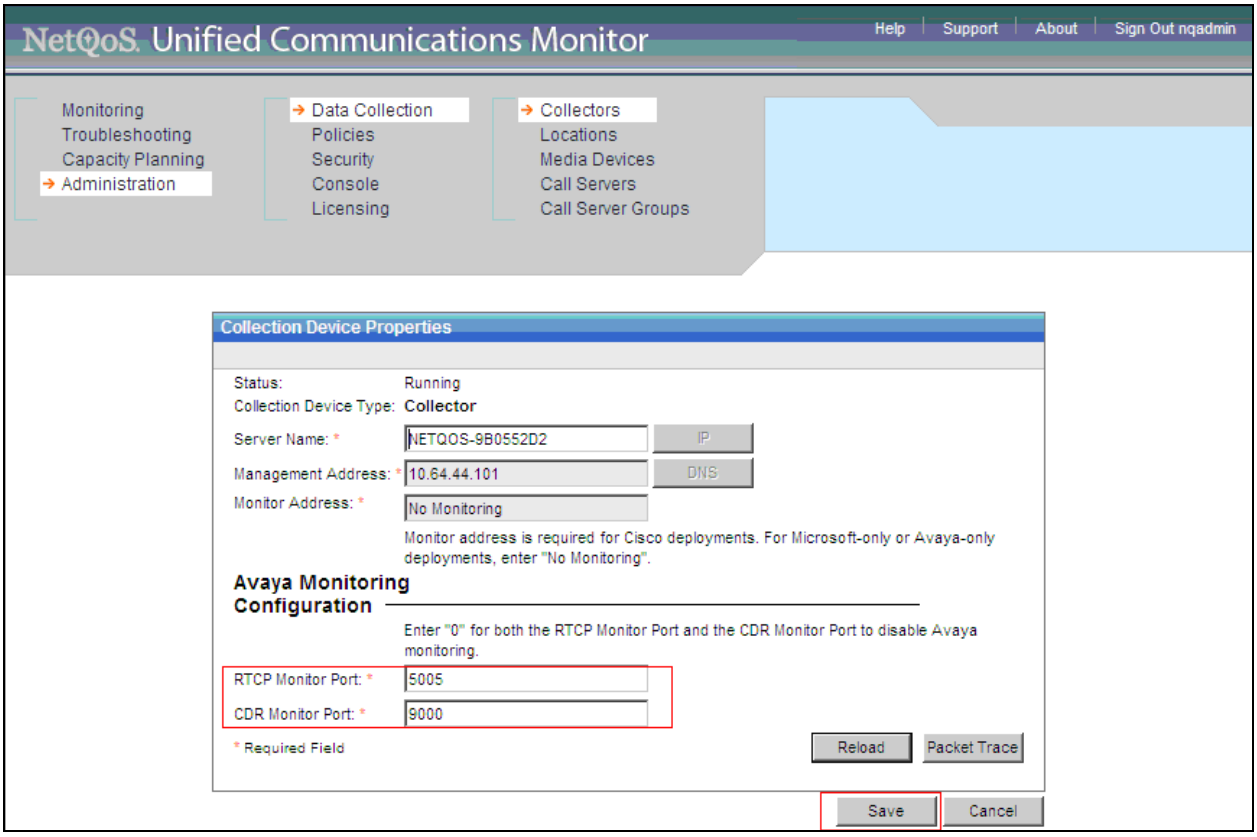
This section describes the configuration of CA NetQoS UC Monitor. During the compliance test, CA NetQoS UC Monitor receives CDR records on port 9000 (Default) and RTCP reports on port 5005 (Default). Thus, CA NetQoS UC Monitor should configure the listening ports for both CDR and RTCP.

Since the default port numbers for RTCP and CDR are automatically configured in UC Monitor, no additional configuration of ports was required for this test. However, the following screens show how to change those ports if necessary.

To configure listening ports on CDR and RTCP on CA NetQoS UC Monitor, click on the CA NetQoS UC Monitor icon. Navigate to the **Administration → Data Collection → Collectors** page. Select an appropriate Collector, and click on the **Edit** button.



Enter the correct listening ports for RTCP Monitoring Port and CDR Monitoring Port fields, or verify that the defaults are appropriate. The listening ports should match the settings configured in **Section 4**. Click on the **Save** button.



6. General Test Approach and Test Results

All test cases were performed manually. The general approach was to place various types of calls to and from stations through a network impairment tool. During (or prior to) a call, network latency or packet drop was injected through the network impairment tool.

The compliance test included and verified the following:

- CA NetQoS UC Monitor was able to successfully receive correct RTCP data from Avaya IP Telephones.
- Individual inbound (no outbound transfer and conference calls) calls were successfully tested.
- Individual outbound (no transfer and conference calls) calls were successfully tested.
- Inbound transferred calls were successfully tested.
- Inbound conferenced calls were successfully tested.
- CA NetQoS UC Monitor was able to successfully receive correct CDR data from Communication Manager.

For serviceability testing, CA NetQoS UC Monitor was able to resume collection of CDR records and RTCP data after failure recovery including a network disconnection/reconnection, CA NetQoS UC Monitor reboot, and Communication Manager reboot.

For all calls, real-time performance metrics were reported in the UC Monitor Call Watch report. Typical point-to-point calls were correctly monitored and reported, with accurate call leg identification ad correlation. Detailed information about Avaya endpoints is available in the UC Monitor Phones report if SNMP access is configured (this configuration is not described in these Application Notes but is provided in the UC Monitor product documentation).

During compliance testing, it was observed that CDR data from the Avaya Communication Manager may be misleading when reporting on transferred or conference calls. For that reason, it is suggested that either CDR not be enabled for use by UC Monitor in these environments, or that care be taken when reviewing the UC Monitor results. In the latter case, UC Monitor will indicate (with an asterisk) that the CDR information could not be accurately correlated with the RTCP data to allow call direction to be determined; however, all other quality data will still be valid.

7. Verification Steps

The following steps may be used to verify the configuration:

- Place internal, inbound trunk, and outbound trunk calls to and from various telephones, generate an appropriate report in CA NetQoS UC Monitor and verify the report's accuracy.
- Using a network impairment tool, inject call latency and packet drop in the network, and compare results from the network emulator, Avaya IP telephones, and CA NetQoS UC Monitor.

If you have chosen to send CDR data to UC Monitor, which is an optional method for collecting additional data, you can verify that CDR data are correctly configured by:

- From Communication Manager, enter the **status cdr-link** command and verify that the CDR link state is up.
- Place a call and verify that CA NetQoS UC Monitor 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.

8. Conclusion

These Application Notes describe the procedures for configuring CA NetQoS UC Monitor to receive RTCP and CDR data from Communication Manager and various Avaya IP Telephones. CA NetQoS UC Monitor successfully received RTCP and CDR data from Communication Manager and various Avaya IP Telephones. All test cases were completed successfully.

During compliance testing, it was observed that CDR data from the Avaya Communication Manager may be misleading when reporting on transferred or conference calls. For that reason, it is suggested that either CDR not be enabled for use by UC Monitor in these environments, or that care be taken when reviewing the UC Monitor results. In the latter case, UC Monitor will indicate (with an asterisk) that the CDR information could not be accurately correlated with the RTCP data to allow call direction to be determined; however, all other quality data will still be valid

9. References

This section references the Avaya and CA NetQoS documentation that are relevant to these Application Notes.

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

[1] *Administering Avaya Aura™ Communication Manager*, Issue 5.0, May 2009, Document Number 03-300509

[2] *Avaya Aura™ Communication Manager Feature Description and Implementation*, Issue 7, Release 5.2, May 2009, Document 555-245-205

The following CA NetQoS documentation was provided by CA NetQoS engineer.

[3] *NetQoS Unified Communication Monitor User Guide*, V3.0

[4] *NetQoS Unified Communication Monitor Administrator Guide*, V3.0

[5] *NetQoS Unified Communications Monitor 3.0 Installation Steps*

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.