Avaya Solution & Interoperability Test Lab

Application Notes for Nectar Converged Management Platform with Avaya Aura® Session Manager - Issue 1.0

Abstract

These Application Notes describe the configuration procedures required for the Nectar Converged Management Platform to interoperate with Avaya Aura® Session Manager. Nectar Converged Management Platform is an intelligent platform that converges monitoring and management of the different layers of a network and system infrastructure to provide a unified business service view of an entire application or its delivery system.

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 configuration procedures required for Nectar CMP to interoperate with Avaya Aura® Session Manager. The purpose of the testing was to verify that Nectar CMP recorded each phone call's performance metrics.

Nectar CMP is a Network Management Platform that is delivered as a service. In a converged architecture, the interoperable framework is designed with many individual parts working together for overall network functionality. Nectar CMP is an intelligent platform that converges monitoring and management of the different layers of a network and system infrastructure to provide a unified business service view of an entire application or its delivery system, regardless of how many parts it is composed of.

2. General Test Approach and Test Results

The general approach was to place various types of calls to and from stations, collect VoIP call quality data from Nectar CMP, and compare collected values with Avaya SIP telephone's Network Audio Quality values. For feature testing, the types of calls included internal calls, inbound trunk calls, outbound trunk calls, transferred calls, conferenced calls. During the compliance test, a VoIP impairment tool was utilized to simulate VoIP delay and packet drop. For serviceability testing, failures such as cable pulls and resets were applied. Verification of each call was made by performing queries into the Nectar CMP meta data, and looking at the results recorded in the Nectar CMP internal logs.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing. The feature testing evaluated the ability of Nectar CMP to provide quality of calls placed to and from stations. The serviceability testing introduced failure scenarios to see if Nectar CMP can resume monitoring and recording after failure recovery.

2.2. Test Results

Nectar CMP successfully provided VoIP call quality data on various types of calls. For serviceability testing, Nectar CMP was able to resume collecting VoIP call quality data after restoration of connectivity to the CLAN, and after resets of Nectar CMP and Avaya Media.

2.3. Support

Technical support for the CMP can be obtained by contacting Nectar Support via the support link at http://www.nectarcorp.com/support or by calling support at (888) 8-N-E-C-T-A-R.

3. Reference Configuration

Figure 1 illustrates the network configuration used to verify the Nectar CMP solution. The figure shows two separate communication systems, each running Avaya Aura® Communication Manager on separate Avaya servers. Site A was comprised of an S8300 Server with a G450 Media Gateway, and SIP Trunks to an Avaya Aura® Session Manager located in another network segment to which three 9600 Series SIP Telephones registered. Site B was comprised of an S8500 Server with 9600 Series IP Telephones registered to it. An IP trunk connected the two Avaya Aura® Communication Manager systems. A Nectar CMP server was located in the Site A, and had IP connection to all devices. A Packet Storm network device was used in various places on the network during the tests in order to inject delays and packet loss to verify phone and Nectar CMP properly measured network performance.

The primary focus of this test was to verify interoperability with SIP Endpoints and Avaya Aura® Session Manager at Site A. The Avaya Aura® Communication Managers at both sites, and Site B were present primarily for the ability to connect external calls to the SIP endpoints at Site A. The Nectar CMP solution was separately tested with Avaya Aura® Communication Manager R5 and R6, re-testing these was not the focus of this effort.

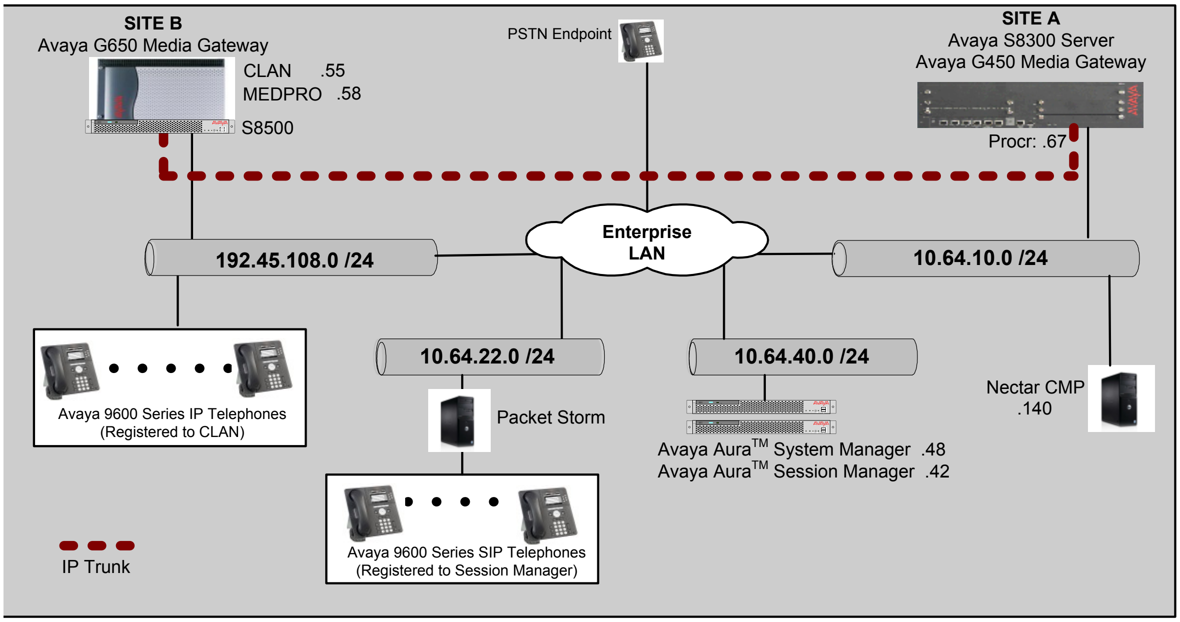


Figure 1 - Test configuration of Nectar CMP with Avaya Aura® Session Manager

4. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8800 Servers	Avaya Aura® System Manager 6.0 Avaya Aura® Session Manager 6.0
Avaya S8300 Server with Avaya G450 Media Gateway	Avaya Aura® Communication Manager 6.0 (R016x.00.0.345.0)
Avaya 9600 Series IP Telephones	
9630 (SIP) 9650 (SIP)	2.6 2.6
Nectar CMP OS –Windows 2008R2 Server	2.1

5. Configuring Avaya Aura® Session Manager

Nectar CMP utilizes a combination of the following methods to collect data for generating a report on VoIP devices.

- RTCP Monitor Server – Nectar CMP received RTCP reports from the endpoints or the media processor (medpro) board to provide the VoIP path and call quality information.
- SNMP/TRAP – Nectar CMP queried Avaya Aura® Session Manager utilizing SNMP walk, to collect status information. Nectar CMP was set up as a trap receiver, and thus received alarms from Avaya Aura® Session Manager.

This section provides the procedures used for configuring the above mentioned methods in Avaya Aura® Session Manager.

5.1. Creating RTCP Monitor Server

Nectar CMP utilizes RTCP packets to calculate and report the call path and quality of calls. An RTCP monitor server must be configured in Communication Manager to collect information on calls connecting disparate endpoints or conferences (3 or more parties). For calls directly connected to SIP endpoints which do not use Media Gateway resources, the phone firmware settings file is used to configure the RTCP server for the phones to directly send information. The following clip is from the 46xxsettings file the SIP phones used in this test:

```
####################  RTCP MONITORING  #####################
## The RTCP monitor
##   One RTCP monitor (VMM server) IP address in
##   dotted-decimal format or DNS name format (0 to 15
##   characters). Note that for H.323 telephones only this
##   parameter may be changed via signaling from Avaya
##   Communication Manager. For 96xx SIP models in Avaya
##   environments, this parameter is set via the PPM server.
##   This parameter is not supported on 16cc model phones.
SET RTCPMON 10.64.10.140
## RTCPMONPORT sets the port used to send RTCP information
## to the IP address specified in the RTCPMON parameter.
## RTCPMONPORT is only supported on 46xx SIP telephones and
## 96xx telephones in non-Avaya environments.  For 96xx SIP
## models in Avaya environments, this parameter is set via
## the PPM server. The default is 5005.
SET RTCPMONPORT  "5005"
## RTCP Monitor Report Period
##   Specifies the interval for sending out RTCP monitoring
##   reports (5-30 seconds).  Default is 5 seconds. This
##   parameter applies only to 96xx SIP telephones.
SET RTCPMONPERIOD 5
```

The RTCP monitor server settings were administered on Communication Manager for separate testing and are covered in separate application notes titled “Application Notes for Nectar Converged Management Platform with Avaya Aura® Communication Manager”.

5.2. Configuring SNMP / TRAP Agents

For Nectar CMP to query the status information on Session Manager, the SNMP and TRAP services need to be enabled. Once SNMP is enabled, Nectar CMP utilizes SNMPwalk to extract information from Session Manager. Enabling the SNMP service for Session Manager can be configured through the server's console interface.

Launch Telnet or PuTTY and connect to the Session Manager console. Supply the login and password for an account with super-user privileges, in the test configuration, the craft user account was used.

Enter the **setup_snmp public** command to enable the "**public**" SNMP community.

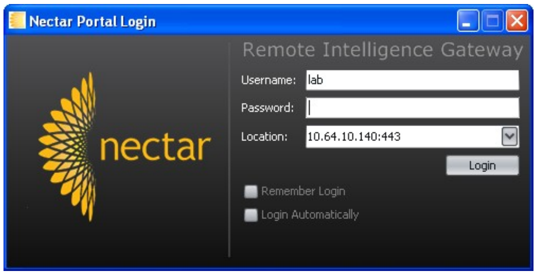
```
[craft@avaya-asm ~]$ setup_snmp public
Community being set to public
Restarting/Starting SNMP Daemon
Stopping snmpd:                                          [  OK  ]
Starting snmpd:                                          [  OK  ]
Session Manager basic SNMP agent configuration complete.
[craft@avaya-asm ~]$
```

6. Configuring the Nectar CMP Remote Intelligence Gateway

The first step is to setup the configuration of Nectar CMP to receive RTCP packets from the VoIP endpoints and media gateways in order to record performance metrics. The second task is to configure the Session Manager object in the application. For additional information on configuring Nectar CMP, refer to [2], [3] and [4].

6.1. Configure Nectar CMP to receive RTCP Packets

Launch a web browser and connect to Nectar CMP by entering http://<Nectar CMP IP address> to login to the Nectar Portal Login page. Provide credentials.

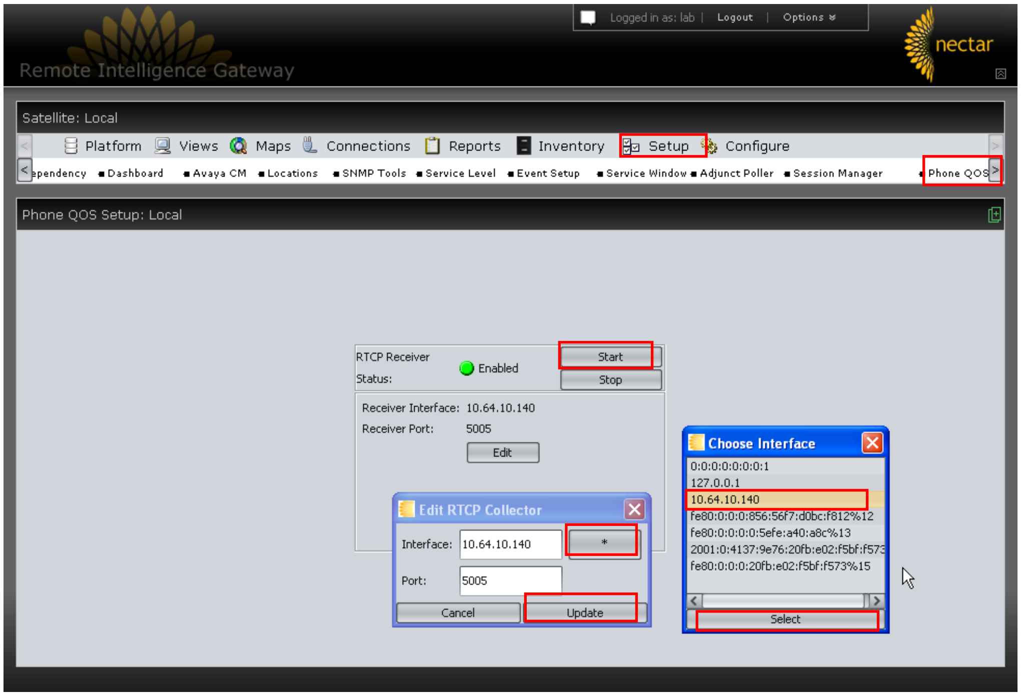


Username: lab

Location: 10.64.10.140:443

Navigate to **Setup >Phone QOS** and edit the RTCP Receiver settings.

- Click **Edit** to set the **Receiver Interface** and **Receiver Port**.
- Choose the Interface by clicking the * icon, highlighting the address of the server and click on the **Select** button.
- On the **Edit RTCP Collector** dialog, select **Update** to commit the changes.
- Click **Start** to enable the server to start collection RTCP data.



RTCP Receiver Status: Enabled

Receiver Interface: 10.64.10.140
Receiver Port: 5005

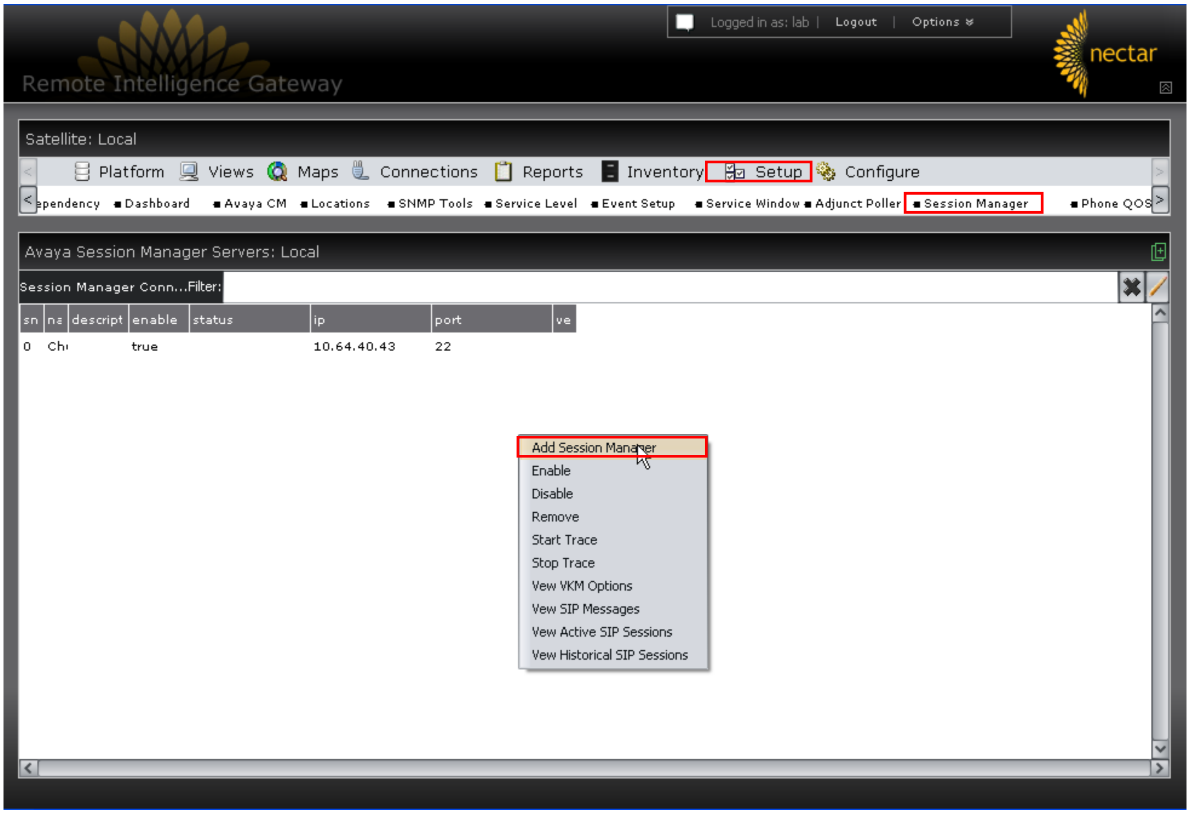
Interface: 10.64.10.140
Port: 5005

0:0:0:0:0:0:0:1
127.0.0.1
10.64.10.140
fe80:0:0:0:856:56f7:d0bc:f812%12
fe80:0:0:0:0:5efe:a40:a8c%13
2001:0:4137:9e76:20fb:e02:f5bf:f573
fe80:0:0:0:20fb:e02:f5bf:f573%15

Then press the **Start** button to enable the RTCP receiver.

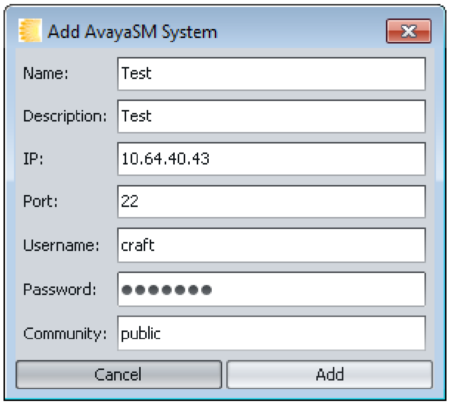
6.2. Add Session Manager to the Remote Intelligence Gateway

Navigate to **Setup->Session Manager.** Right click and select **Add Session Manager**:



sn	na	descript	enable	status	ip	port	ve
0	Ch		true		10.64.40.43	22	

Enter the **Name**, **Description**, **IP**, **Port** (22 for SSH), **Username**, **Password**, and **Community** string. Press the **Add** button when complete.


Add AvayaSM System

Name: Test

Description: Test

IP: 10.64.40.43

Port: 22

Username: craft

Password: ●●●●●●●

Community: public

7. Verification Steps

The following steps were used to verify the configuration.

- Use the **ping** command to verify connectivity from Nectar CMP to all devices.
- Verify that calls can be successfully completed between the telephones.
- Compare VoIP quality data from the following sources:
  - A VoIP impairment tool
  - Avaya IP telephone's Network Audio Quality data
  - Nectar CMP

8. Conclusion

These Application Notes illustrate the procedures for configuring Nectar CMP to monitor and correctly provide VoIP call quality statistics on the various types of calls placed to and from SIP stations. In the configuration described in these Application Notes, Nectar CMP employs a combination of the following methods to collect data for generating a report on VoIP devices:

- RTCP Monitor Server
- SNMP/TRAP

During compliance testing, CMP successfully monitored call streams, correctly provided VoIP call quality data, and received traps from VoIP devices and Media Servers.

9. References

This section references the Avaya and Nectar 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^{TM} Session Manager*, Issue 3, Release 6.0 August 2010, Document Number 03-603324

Nectar provided the following documentation. For additional product and company information, visit http://www.nectarcorp.com.

[2] *Nectar CMP Supplement – Avaya CM VKM Preparing Avaya Communications Manager (IP Enabled) for CMP Interaction*, September 2010, Document Version 2.0

[3] *Nectar CMP Administrator Technical Guide Central Intelligence Platform (CIP),* July 2010, Document Version 2.3

[4] *Nectar CMP Operator Technical Guide Central Intelligence Platform (CIP),* July 2010, Document Version 2.3

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.