



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Communication Manager 6.3 with Nu Technologies™ ORBi- TEL⁷ using an IP Buffer - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Avaya Aura® Communication Manager 6.3 with Nu Technologies ORBi-TEL⁷ 18.3.3 using an IP Buffer. The ORBi-TEL⁷ collects Call Detail Records of inbound and outbound calls from the Avaya Aura® 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.

1. Introduction

Nu Technologies ORBi-TEL⁷ is a set of integrated tools to measure quality of service, usage trends, and performance to optimize the network. Nu Technologies ORBi-TEL⁷ consists of four modules. Cost management, also referred to as call logging and reporting module, was the only module that was tested. Call logging and Reporting module collects, stores and processes Call Detail Records to provide usage analysis, call costing and billing capabilities. The other modules that were not tested include Performance management, Traffic management, Operations management and Alarm management. Nu Technologies ORBi-TEL⁷ retrieves Call Detail Records via an IP Buffer from Avaya Aura® Communication Manager. The IP Buffer is configured via a web interface to receive and buffer Call Detail Records from the Avaya Aura® Communication Manager which then pushes these reports to the ORBi-TEL⁷ at scheduled intervals where they are converted into a common internal format. Avaya Aura® Communication Manager can generate Call Detail Records for intra-switch calls, inbound trunk calls and outbound trunk calls. In addition, split records can be generated for transferred calls and conference calls. Nu Technologies ORBi-TEL⁷ can support any Call Detail Records format provided by Avaya Aura® Communication Manager. Nu Technologies ORBi-TEL⁷ creates a custom PBX configuration file to accurately parse the CDR data. For the compliance testing, a customized format was used. Nu Technologies ORBi-TEL⁷ server is capable of receiving Call Details Records from multiple sites.

2. General Test Approach and Test Results

The general test approach was to configure the ORBi-TEL⁷ to communicate with the Avaya Aura® Communication Manager (Communication Manager) as implemented on a customer's premises. Testing focused on verifying that Call Detail Records (CDR) are collected by the IP buffer and received in the format as generated by the Communication Manager. The ORBi-TEL⁷ application would collect the CDR data using File transfer Protocol from the IP Buffer. Various call scenarios were performed to simulate real call types as would be observed on a customer premises. See **Figure 1** for a network diagram. The interoperability compliance test included feature functionality and defence tests.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The testing included:

- Verification of connectivity between ORBi-TEL⁷/IP buffer and Communication Manager using a TCP connection.
- Verification that CDR data was collected as output by the Communication Manager.
- Link Failure\Recovery was also tested to ensure successful reconnection after link failure.
- CDR data collected included:
 - Local internal call handling
 - Handling of Incoming Network calls over PRI and SIP trunks
 - Handling of External Calls
 - Call Forwarding on busy or No Answer
 - Transfers – Blind and Supervised
 - Conference Calls
 - Call Park and Call Pick Up
 - Account Codes
- Daylight Savings
- Handling of calls to and from Avaya H323, SIP, and Soft phones
- Handling of calls over SIP and QSIG trunks
- Defence Tests to ensure recovery following LAN interruptions

2.2. Test Results

Tests were performed to insure full interoperability between ORBi-TEL⁷/IP buffer and Communication Manager. The tests were all functional in nature and performance testing was not included. All the test cases passed successfully.

2.3. Support

Technical support from Nu Technologies can be obtained through the following:

Phone: +44 1582 814700
E-mail: support@nut.eu.com
Web: <http://www.nut.eu.com>

3. Reference Configuration

Figure 1 illustrates the network topology used during compliance testing. The Avaya solution consists of a Communication Manager, System Manager, Session Manager and a G250 Gateway. The Communication Manager is configured to output Call Detail Records data over a TCP/IP port. A Node is configured on the Communication Manager to point to the Scannex IP buffer. The Call Detail Records are sent in customized format, stored in the buffer and retrieved by the ORBi-TEL⁷ application at defined periods. A variety of Avaya 96XX H323 and Digital phones were used to generate intra-switch calls (calls between phones on the same system), and outbound/inbound calls to/from the PSTN. QSIG and SIP trunks were configured to connect to the PSTN.

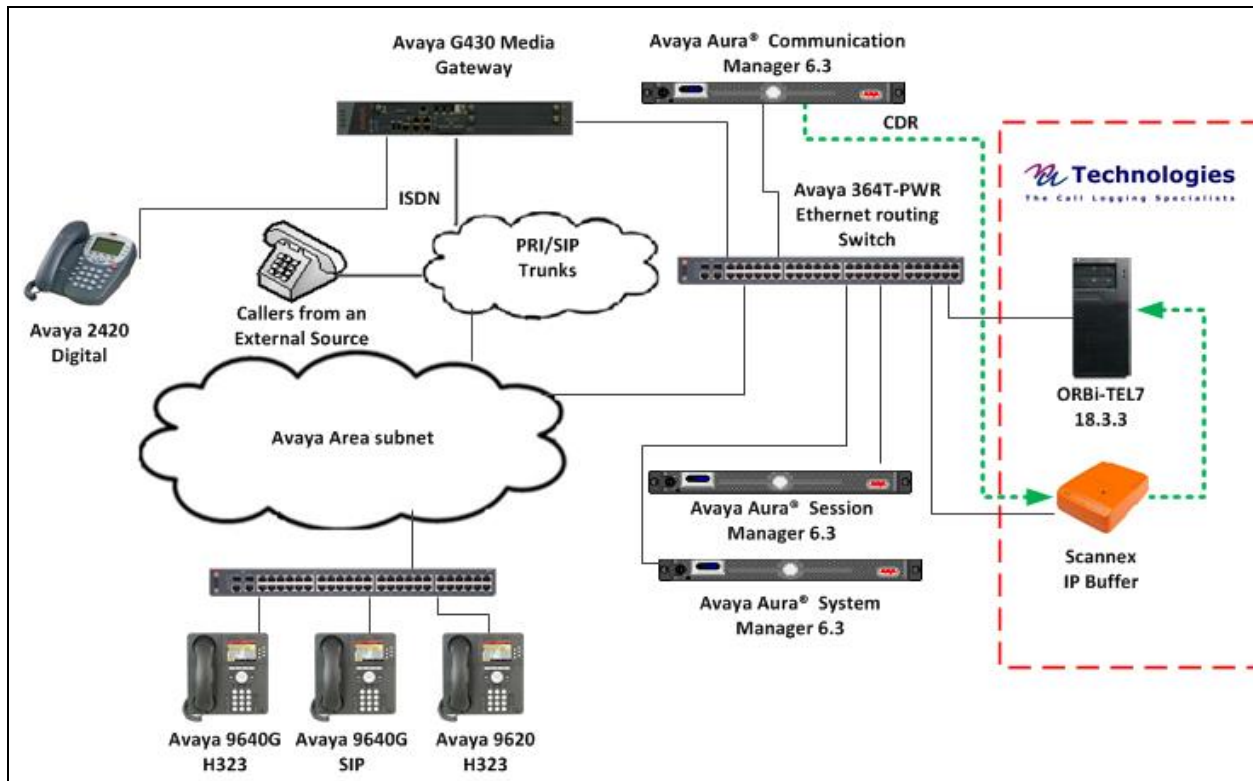


Figure 1: Avaya Aura[®] Communication Manager and Nu Technologies ORBi-TEL⁷ Reference Configuration

4. Equipment and Software Validated

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

Avaya Equipment	Software / Firmware Version
Avaya Aura® Communication Manager	R6.3 Build R016x.03.0.124.0 Update 03.0.124.0-20850
Avaya Aura® System Manager	R6.3 Build 6.3.0.8.5682-6.3.8.1814 Update 6.3.3.5.1719
Avaya Aura® Session Manager	R6.3 Build 6.3.0.8.5682-6.3.8.1814 Update 6.3.3.5.1719
Avaya G430 Media Gateway	31.22.0
Avaya 96xx Deskphones - H323 9620D - H323 9640G - SIP 9640D	3.101S 3.105S 2.6.10.1
Avaya Digital 2420	F/W 6
Nu Technologies Equipment	Software / Firmware Version
ORBi-TEL ⁷	Version 18.3.3
Scannex IP Buffer	Release IPBCF2.75.199 2012-02-09 / i5.0.10

5. Configure Avaya Aura® Communication Manager

Configuration and verification operations on the Communication Manager illustrated in this section were all performed using Avaya Site Administrator Emulation Mode. The information provided describes the configuration of the Communication Manager for this solution. It is implied that a working system is already in place. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

The configuration operations described in this section can be summarized as follows:

- Create Node Name for IP buffer
- Define the CDR Link
- Change system-parameters cdr
- Set Intra-Switch Extensions
- Configure Trunks for CDR Reporting

5.1. Create Node Name for IP buffer

A Node Name needs to be created to associate the IP buffer with the Communication Manager. Use the **change node-names ip** command to configure the following:

Page 1

- **Name** Enter an informative name i.e. **IP buffer**
- **IP address** Enter the IP address of the **IP buffer**

Press **F3** button to save the new settings.

change node-names ip		Page 1 of
2		
IP NODE NAMES		
Name	IP Address	
IP buffer	10.10.60.71	

5.2. Define the CDR Link

A CDR link needs to be defined between the Communication Manager and the IP buffer. Use the **change ip-services** command to configure the following:

- **Service Type** Enter **CDR1**
- **Local Node** Enter **procr**
- **Remote Node** Enter **IPBuffer1**
- **Remote Port** Enter **9000**

change ip-services				Page 1 of	3
IP SERVICES					
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port
CDR1		Procr	0	IPBuffer1	9000

Navigate to **Page 3** and set the **Reliable Protocol** field to **y**. This will enable Reliable Session Protocol (RSP) for CDR transmission. In this case, the CDR link will use TCP with RSP.

- **Reliable Protocol** Enter **y**

Press **F3** button to save the new settings.

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

5.3. Change CDR System Parameters

Certain parameter changes are required for Communication Manager to interoperate with ORBi-TEL⁷. The screen shots below show the settings used during compliance testing. Use the **change system-parameters cdr** command to configure the following:

- **CDR Date Format:** Set it to **month/day**. The date format will be used for the date stamp that begins each new day of call records.
- **Primary Out Format:** Set this to **customized** format.
- **Primary Output Endpoint:** Set to **CDR1** to correspond with CDR link set in **Section 5.2**.
- **Intra-switch CDR:** Set this to **y** to allow call records for internal calls involving specific stations. Those stations must be specified in the **inter-switch-cdr** form as set in **Section 5.4**.
- **Record Outgoing Calls Only:** Set this to **n** to allow incoming trunk calls to appear in the CDR records along with the outgoing trunk calls.
- **Suppress CDR for Ineffective Call Attempts?** Set this to **n** so that calls that are blocked do generate a CDR record.
- **Outg Trk Call Splitting:** Set this to **y** to allow a separate call record for any portion of an outgoing call that is transferred or conferenced.
- **Inc Trk Call Splitting:** Set this to **y** to allow a separate call record for any portion of an incoming call that is transferred or conferenced.

```
change system-parameters cdr                               Page 1 of 2
                  CDR SYSTEM PARAMETERS

Node Number (Local PBX ID):                               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? 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? n            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? 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: 15
```

Navigate to **Page 2** and enter the following information.

- Enter **Data Item** and **Length** as shown in the screen below

Press **F3** button to save the new settings.

```

change system-parameters cdr                                     Page 2 of 2
                                CDR SYSTEM PARAMETERS

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

                                Record length = 135
  
```

5.4. Set Intra-Switch Extensions

If the Intra-switch CDR field is set to **y** in the CDR SYSTEM PARAMETERS form in **Section 5.3**, use the **change intra-switch-cdr** command to define the extensions that will be subject to CDR. On **Page 1** of the **INTRA-SWITCH CDR** form, enter a specific extension whose usage will be tracked with a CDR. Add an entry for each additional **Extension**

```

change intra-switch-cdr                                     Page 1 of 3
                                INTRA-SWITCH CDR

                                Assigned Members: 0 of 5000 administered
                                Extension           Extension           Extension
Extension

3000
3004
3015
3016
  
```


5.5. Configure Trunks for CDR Reporting

For each trunk group for which CDRs are desired, verify that CDR reporting is configured to generate CDRs. Use the **change trunk-group n** command, where **n** is the trunk group number, to verify that the **CDR Reports** field is set to **y**. This applies to all types of trunk groups.

```
change trunk-group 9                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 9                                         Group Type: isdn           CDR Reports: y
  Group Name: OUTSIDE CALL                               COR: 1                    TN: 1            TAC: 109
  Direction: two-way                                   Outgoing Display? y      Carrier Medium: PRI/BRI
  Dial Access? y                                       Busy Threshold: 255      Night Service:
Queue Length: 0
Service Type: public-ntwrk                             Auth Code? n             TestCall ITC: rest
                                     Far End Test Line No:
TestCall BCC: 4
```

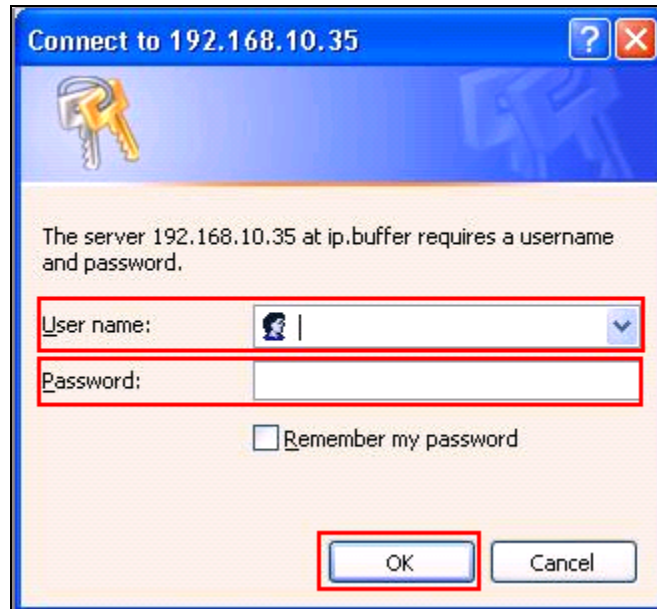
6. Configuration of Scannex IP buffer

This section provides the procedures to configure the Scannex IP buffer. It is implied that the Scannex IP buffer is already in place and configured with an IP address on the same subnet as the Communication Manager. For all other provisioning information, such as initial installation and configuration, please refer to the product documentation in **Section 10**.

Note: The procedures described below are normally carried out by a Nu Technologies engineer during installation and subsequent re-configuration.

6.1. Logging into the Scannex IP Buffer

To access the web-based interface of the Scannex IP Buffer, use the URL <http://x.x.x.x>, where **x. x. x. x** is the selected IP address of the IP Buffer. In the windows login box that appears, enter the default username and password and click on the **OK** button.



The image shows a Windows-style dialog box titled "Connect to 192.168.10.35". The dialog has a blue header bar with a question mark icon and a close button (X). Below the header is a blue banner with a key icon. The main area is white and contains the text: "The server 192.168.10.35 at ip.buffer requires a username and password." Below this text are two input fields: "User name:" with a dropdown arrow and a "Password:" field. A checkbox labeled "Remember my password" is located below the password field. At the bottom of the dialog are two buttons: "OK" and "Cancel". Red rectangular boxes highlight the "User name:" field, the "Password:" field, and the "OK" button.

6.2. Setup Scannex IP Buffer

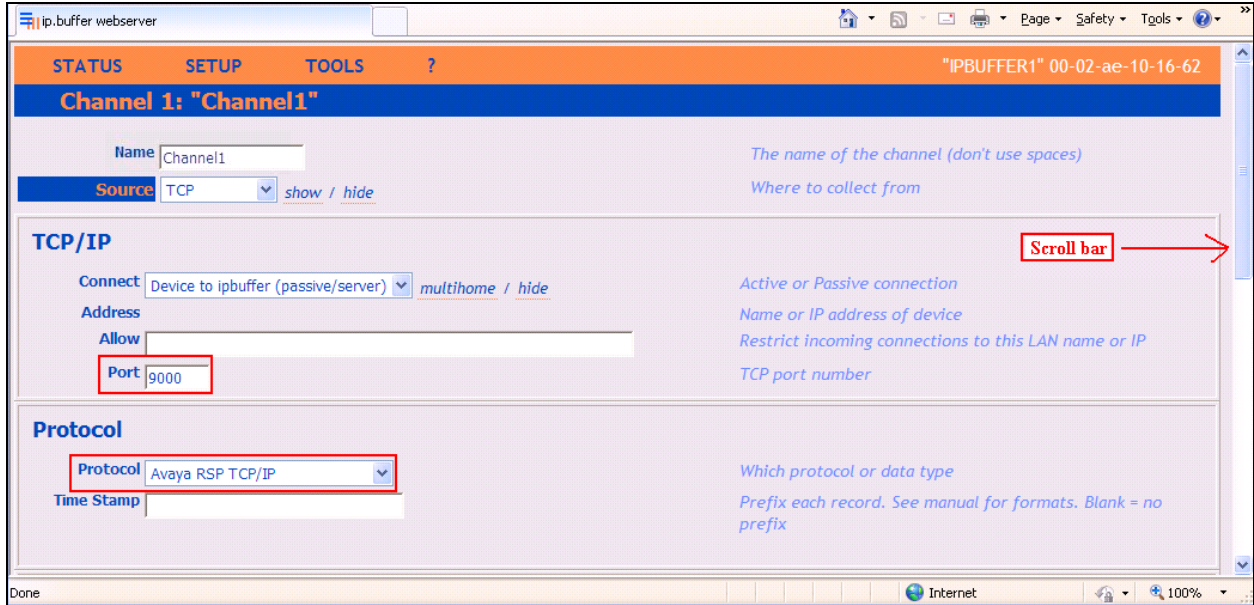
After logging in, the **Status** page is displayed. Select **SETUP** followed by **Channel 1** (Not shown).

The screenshot shows the Scannex III web interface. The top navigation bar includes 'STATUS', 'SETUP', and 'TOOLS'. The 'Status' page displays a table with columns for 'Source', 'Storage', and 'Destination'. Under 'Channel 1 Source', the 'Source' is set to 'TCP', 'Storage' is '0', and 'Destination' is 'FTP server'. The 'System' row shows '0% [0/123Mb]' and '0 alerts'. The 'Channel 1 Source' details include 'Last data 2012-08-21 22:54:56', 'Protocol ASCII Lines', 'Status Listening', 'Remote IP 0.0.0.0', and 'Match 1'. There is a '[Click to refresh]' link and a control for 'auto-refresh (5 second)'. The Scannex III logo is at the bottom.

Once the **Channel 1** page is opened, select **TCP** from the **Source** dropdown box, then select **show**.

The screenshot shows the Scannex III web interface for the 'Channel 1: "Channel1"' setup page. The 'Name' field contains 'Channel1'. The 'Source' dropdown is set to 'TCP' and the 'show' button is highlighted. The 'Destination' dropdown is set to 'COM1 Serial' and the 'show' button is highlighted. The 'Storage' dropdown is set to 'FTP server' and the 'show' button is highlighted. There are 'SAVE' and 'Cancel' buttons. A red message says 'Press SAVE to store changes!'. The Scannex III logo is at the bottom.

Once the next page opens, enter **9000** in the **TCP/IP port** box. The port number used should match the **Remote Port** configured on the Communication Manager in **Section 5.2**. From the **Protocol** drop down box select **Avaya RSP TCP/IP**. Use the scroll bar on the right side of the page and scroll to the bottom.



From the **Destination** dropdown box, select **FTP push (client)** and then select **show**.



Once the **FTP push (Client)** window opens, enter the following:

- **Address** Enter the IP Address of the ORBi-TEL⁷ Server
- **Username** Enter the **Username** of the ORBi-TEL⁷ Server
- **Password** Enter the **Password** of the ORBi-TEL⁷ Server
- **Directory** Enter the file location where the CDR data is stored
- **Command** Select **Append** from the drop down box
- **Filename** Enter **FILE1**

Use the scroll bar on the right side of the page and scroll down to **Push Schedule** (see next screen shot).

STATUS SETUP TOOLS ? "Scannex" 00-02-ae-10-16-62

Channel 1: "Channel1"

Name Channel1 *The name of the channel (don't use spaces)*

Source TCP *Where to collect from*

Destination FTP push (client) *How to deliver the data*

FTP push (client)

Address 10.10.60.73 *Name or IP address of FTP server*

Port 21 *TCP/IP port number*

Username *FTP username*

Password *FTP password*

Directory /usr/dfile3/SSR/AVAYA1 *FTP directory (use forward slashes)*

Command Append *Whether to overwrite or append on the FTP server*

Filename FILE1 *Filename (%Q=hex, %D=date, %T=time, etc)*

Compression none *Send normal or zlib compressed*

Limit 0 kb *File limit (0=no limit)*

Info Filename *Device Info file (blank = don't push)*

Event Filename *FTP Event CSV file (blank = don't push)*

Data Markers

Scroll bar

The screen shot below shows the Push Schedule as set during compliance testing. Once the schedule is complete, click on the **Save** button.

Push Schedule

Condition: Only when data

Zone A

Deliver Every: 1 minutes
At/Between: 08:00 HH:MM ...and 18:00 HH:MM
Variance: 0 minutes

On These Days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday

Zone B

At all other times
Deliver Every: 1 minutes

Failures

Retry time: 60

Storage settings show / hide

Press SAVE to store changes!

SAVE Cancel

7. Configure ORBi-TEL⁷

This section provides the procedures to configure ORBi-TEL⁷ server to receive CDR data from the Communication Manager via the IP buffer.

7.1. Configure the ORBi-TEL⁷ Server

The ORBi-TEL⁷ server needs to be configured for site details and setting up the Collection and Translation script for receiving CDR data. This procedure is normally carried out by a Nu Technologies engineer during installation and subsequent re-configuration.

7.2. Add Extensions to the ORBi-TEL⁷ Server Database

The database on the ORBi-TEL⁷ Server must be populated with Communication Manager extensions prior to running reports. Enter the following url **http://<IPaddr ORBi-TEL⁷>/orbitel.html**. Select **dbAdmin** and then select **New** on the dbAdmin page (not shown) to access the **Add Extension** form.

On the Add Extension form complete the following fields:

- **Site Name** Choose a pre-configured site name.
- **Extension** Enter a valid extension as configured on Communication Manager
- **Status** Choose **Ext Owner**

Click the **Add Extension** button. Repeat these steps to add all necessary extensions

Personal	Location
Name: Unknown	Site Name: AVAYA1
Job Title:	Node: AVAYA1 EXTNS
Extension: 3000	Code:
Status: Ext Owner	

Contact	Notes
Email:	
Mobile:	
Fax:	

Buttons: Close, Add Extension, Clear

8. Verification Steps

This section provides tests that can be performed to verify correct configuration of the Avaya and ORBi-TEL⁷ solution.

8.1. Verify the Avaya Aura® Communication Manager CDR Link

Use the **status cdr-link** command to verify that the link between the Communication Manager and the IP buffer is in service. **Link State: up** and **Reason Code: OK** confirms successful connection.

```
status cdr-link
                                CDR LINK STATUS
                                Primary                Secondary
                                Link State: up          CDR administered
Number of Retries: 999
Date & Time: 2013/11/20 18:01:12      0000/00/00 00:00:00
Forward Seq. No: 0                    0
Backward Seq. No: 0                  0
CDR Buffer % Full: 0.03                0.00
Reason Code: OK
```

8.2. Verify the connection between Scannex IP buffer and Avaya Aura® Communication Manager

On the IP Buffer select **Status**, the completed **Status** screen is displayed. The **TCP Source** displays in green indicating that the IP Buffer has successfully connected to the Avaya solution.



Once some test calls, including internal, inbound trunk and outbound trunk calls, have been made then run the ORBi-TEL⁷ report to ensure correct collection of results. Compare to the IP Buffer output. The following screen shows a sample report after some calls were made.

Date	Start Time	End Time	Duration (hh:mm:ss)	Ring Time	Source Extn	Source Trunk	Dest Extn	Dest Trunk	Auth Code	Dialled Digits	OLI	Destination	Exch	Cost
20/11/2013	15:39:48	15:40:00	00:12			505010	6611				1610			0.00
20/11/2013	15:56:39	15:57:00	00:21		3015			505002		50502075551610				0.00
20/11/2013	16:29:44	16:30:00	00:16			505005	6621				1610			0.00
20/11/2013	16:33:46	16:34:00	00:14			508001	6620				1610			0.00
20/11/2013	16:39:44	16:40:00	00:16		3016			505003		5051610				0.00
20/11/2013	17:48:54	17:49:00	00:06			505010	6620				1610			0.00
20/11/2013	17:52:54	17:53:00	00:06			505001	6620				1610			0.00

9. Conclusion

A full and comprehensive set of feature functional test cases were performed during Compliance testing. ORBi-TEL⁷ 18.3.3 is considered compliant with Avaya Aura® Communication Manager 6.3. All test cases have passed and met the objectives outlined in **Section 2.2**.

10. Additional References

These documents form part of the Avaya official technical reference documentation suite. Further information may be had from <http://support.avaya.com> or from your Avaya representative.

- [1] *Administering Avaya Aura® Communication Manager, Release 6.3, October 2013, Document Number 03-300509, Issue 9.0.*
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation, Release 6.3, May 2013, Document Number 555-245-205, Issue 10.0.*
- [3] *Administering Avaya Aura® Session Manager, Release 6.3, Issue 3 October 2013*
- [4] *Administering Avaya Aura® System Manager, Release 6.3, Issue 3, October, 2013 Administration for the Avaya G430, 03-603228, Issue 1, May, 2009*

Product Documentation for ORBi-TEL⁷ and Scannex IP Buffer can be obtained from Nu Technologies Ltd. or may be requested at <http://www.nut.eu.com/nutech/contactus.html>

©2014 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.