



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Nu Technologies ORBi-TEL⁷ using ip.buffer with Avaya AuraTM Communication Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the Nu Technologies ORBi-TEL⁷ to successfully collect call detail records (CDRs) from Avaya AuraTM Communication Manager over Reliable Session Protocol (RSP) using ip.buffer. The ip.buffer is a data collection buffer and it is delivered as part of the ORBi-TEL⁷ solution.

ORBi-TEL⁷ is a set of integrated tools to measure quality of service, usage trends, and performance to optimize the network. ORBi-TEL⁷ consists of four modules. Cost Management, also referred to as Call Logging and Reporting Module, was the only module that was tested. The Call Logging and Reporting module collects, stores and processes these call records to provide usage analysis, call costing and billing capabilities.

Information in these Application Notes has been obtained through interoperability compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

The objective of this compliance test is to verify that Nu Technologies ORBi-TEL⁷ solution can interoperate with Avaya Aura™ Communication Manager 5.2.1. ORBi-TEL⁷ with ip.buffer interoperates with Avaya Aura™ Communication Manager over RSP for the collection of Call Detail Records (CDRs). During compliance testing, the CDR collection was verified for Avaya Aura™ Communication Manager running on an Avaya S8500 Server.

ORBi-TEL⁷ is a set of integrated tools to measure quality of service, usage trends, and performance to optimize the network. ORBi-TEL⁷ consists of four modules. Cost Management also referred to as Call Logging and Reporting module was the only module that was tested.

ORBi-TEL⁷ retrieves call details records via a buffer called the ip.buffer from Avaya Aura™ Communication Manager. The ip.buffer is configured via a web interface to receive and buffer call detail records over Reliable Session Protocol (RSP). ORBi-TEL⁷ polls the ip.buffer and converts the call records 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. ORBi-TEL⁷ can support any CDR format provided by Avaya Aura™ Communication Manager. ORBi-TEL⁷ creates a custom PBX configuration file to accurately parse the CDR data. For the compliance testing, a customized format was used.

The ORBi-TEL⁷ server and multiple ip.buffers are able to receive CDR outputs from more than one switch as it can listen on the same port configured on separate Avaya Aura™ Communication Manager systems. This multi-site configuration was not tested during compliance testing. The CDR collection was verified for one Avaya Aura™ Communication Manager running on an Avaya S8500 Server.

1.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing evaluated the ability of Nu Technologies' ORBi-TEL⁷ and ip.buffer to collect and process CDR records for various types of calls: intra-switch calls (calls between phones on the same switch), outbound/inbound calls to/from the PSTN and outbound/inbound calls to/from the phones between the two sites via the IP trunk. The Avaya Reliable Data Test Tool (RDTT) was also used in the interoperability testing to compare the records received by RDTT and those by ORBi-TEL⁷. The serviceability testing introduced failure scenarios to see if ORBi-TEL⁷ and ip.buffer can resume CDR collection after failure recovery.

1.2. 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>

2. Reference Configuration

Figure 1 illustrates a sample configuration that was used to compliance test the interoperability of Nu Technologies' ORBi-TEL⁷ and Communication Manager. The configuration consists of an Avaya S8500 Server running Communication Manager with a G650 Media Gateway. This system has connections to the following: Avaya 9600 Series IP Phones, Avaya Digital Phones and a PRI trunk to the PSTN. ORBi-TEL⁷ uses an ip.buffer to connect to and collect CDR records from each site using RSP. The phones connected to the system will be used to generate call traffic to the Avaya S8500 Server. These phones will be used to generate intra-switch calls (calls between phones on the same system) and outbound/inbound calls to/from the PSTN. In addition, the Avaya Reliable Data Test Tool (RDTT) will be connected to compare the records received by RDTT with the ORBi-TEL⁷ results.

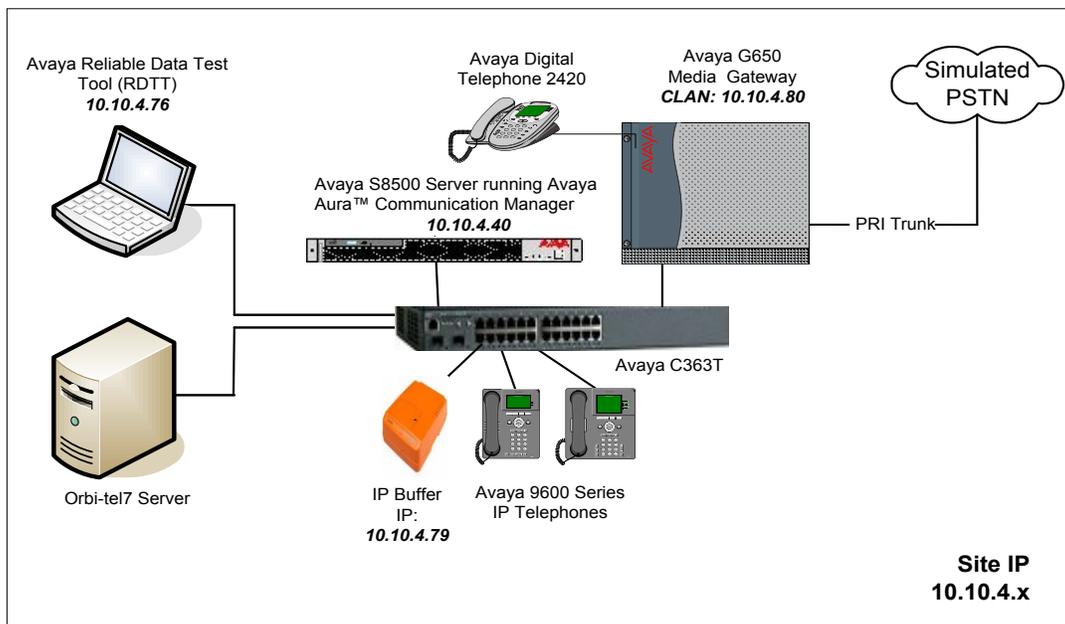


Figure 1: Network Configuration of ORBi-TEL⁷ with Avaya Aura™ Communication Manager

3. Equipment and Software Validated

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

Equipment	Software Version
Avaya S8500B Server	Avaya Aura™ Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya G650 Media Gateway - IPSI TN2312BP - CLAN TN799DP - IP Media Processor TN2602AP - DS1 Interface TN246CP	HW15, FM49 HW01, FM34 HW02, FM49 HW02, FM024
Avaya 96xx Telephones (H.323) - 9630 - 9620	3.0
Avaya Digital Telephones - 2420	-
Avaya C363T-PWR Converged Stackable Switch	4.3.12
Nu Technologies - ORBi-TEL ⁷	Release 18
Nu Technologies - ip.buffer	Release 2.41.133

4. Configure the Avaya Aura™ Communication Manager

This section provides the procedures for configuring Call Data Recording (CDR) features in Communication Manager. All the configuration changes in Communication Manager are performed through the System Access Terminal (SAT). These steps describe the procedures used for the Avaya S8500 Server. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 9**. Communication Manager was configured to generate CDR records to the IP address of the ORBi-TEL⁷ server over RSP. On the Avaya S8500 Server, the CDR link originates at the IP address of the C-LAN board that connects to the same network where the ORBi-TEL⁷ server is located. The configuration operations described in this section can be summarized as follows:

- Configure Node Names
- Configure CDR Links
- Change CDR System Parameters
- Set Intra-Switch Extensions
- Configure Trunks for CDR Reporting

The configuration of the PRI interface to the PSTN is outside the scope of these Application Notes.

4.1. Configure Node Names

Use the **change node-names ip** command to add a new node name for the **ip.buffer** by specifying the **Name** as **ip.buffer** and the **IP Address** as **10.10.4.79**. The RDTT which was used in the compliance test was also added here though this is not necessary for the functioning of the solution. The **RDTT** was given an **IP Address** of **10.10.4.76**.

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
CLAN	10.10.4.80	
CM2	10.1.0.10	
Gateway001	10.10.4.1	
MEDPRO	10.10.4.90	
ip.buffer	10.10.4.79	
PresAES	10.10.4.20	
RDTT	10.10.4.76	
procr	10.255.255.100	

4.2. Configure CDR Links

Use the **change ip-services** command to define the CDR link over RSP. To define a primary CDR link, the following information should be provided on **Page 1**:

- **Service Type: CDR1** If needed, a secondary link can be defined by setting Service Type to CDR2. I
- **Local Node: CLAN** On the Avaya S8500 Server, the Local Node is set to the node name of the C-LAN board.
- **Local Port: 0** The Local Port is fixed to 0.
- **Remote Node: ip.buffer** The Remote Node is set to the node name that was created in **Section 4.1** for the ORBi-TEL⁷ server.
- **Remote Port: 9000** The Remote Port may be set to a value between 5000 and 64500 inclusive and must match the port configured on the ORBi-TEL⁷ server in **Section 5.3.2**.

Note: A different port number must be specified for each Media Server.

Set up a secondary CDR link, **CDR2**, for the **RDTT** in the same way. Specify a **Remote Port** of **9001** and repeat the remaining values.

change ip-services		IP SERVICES				Page 1 of 4
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port	
CDR1		CLAN	0	IP Buffer	9000	
CDR2		CLAN	0	RDTT	9001	

On **Page 3** of the ip-services form, enable the Reliable Session Protocol (RSP) for the CDR link **CDR1**, by setting the **Reliable Protocol** field to **y**. Enable the **Reliable Protocol** on the **CDR2** link by setting it to **y**.

change ip-services		SESSION LAYER TIMERS				Page 3 of 4
Service Type	Reliable Protocol	Packet Resp Timer	Session Connect Message Cntr	SPDU Cntr	Connectivity Timer	
CDR1	y	30	3	3	60	
CDR2	y	30	3	3	60	

4.3. Change CDR System Parameters

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

- **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 Output Format:** Set this to **customized** format.
- **Primary Output Endpoint:** Set to **CDR1** to correspond with CDR link set in **Section 4.2**.
- **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 4.4**.
- **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 not generate CDR records.
- **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
```

On **Page 2** of the **CDR SYSTEM PARAMETERS** form, define the customized CDR format as shown below. The data is entered as it should appear in the customized call records sent over the CDR link. For each field in the CDR record specify the **Data Item** and **Length**.

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

Record length = 135

4.4. Set Intra-Switch Extensions

If the **Intra-switch CDR** field is set to **y** in the **CDR SYSTEM PARAMETERS** form in **Section 4.3**, use the **change intra-switch-cdr** command to define the extensions that will be subject to call detail records. On **Page 1** of the **INTRA-SWITCH CDR** form, enter a specific extension whose usage will be tracked with a CDR record. 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			
3001			
3002			
3003			

4.5. Configure Trunks for CDR Reporting

For each trunk group for which CDR records are desired, verify that CDR reporting is configured to generate CDR records. 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 1                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 1                Group Type: isdn          CDR Reports: y
  Group Name: ToCM2              COR: 1                TN: 1          TAC: 101
  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
```

5. Configure ORBi-TEL⁷

This section provides the procedures to configure ORBi-TEL⁷ Server and ip.buffer to receive Call Data Records (CDRs) from the Avaya system. The procedures described below are normally carried out by Nu Technologies engineers during installation and subsequent re-configuration.

5.1. 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 the collection of CDRs.

5.1.1. Add Site Details

Add site details to the ORBi-TEL⁷ Server by logging onto the ORBi-TEL⁷ Linux server with the pre-configured ORBi-TEL⁷ Server username and password. From the UNIX prompt type the following command **isql -f sites**. Select **u** for update and enter the relevant fields as shown below:

- **sitenam** Enter **AVAYA1** as the site name
- **transprog** Set this parameter to **defvx**, which defines the a customized format.
- **transopts** Set it for the **cdm** translator option.

The remainder of the fields can be left as default. Select **esc** to save. The completed screen is displayed below.

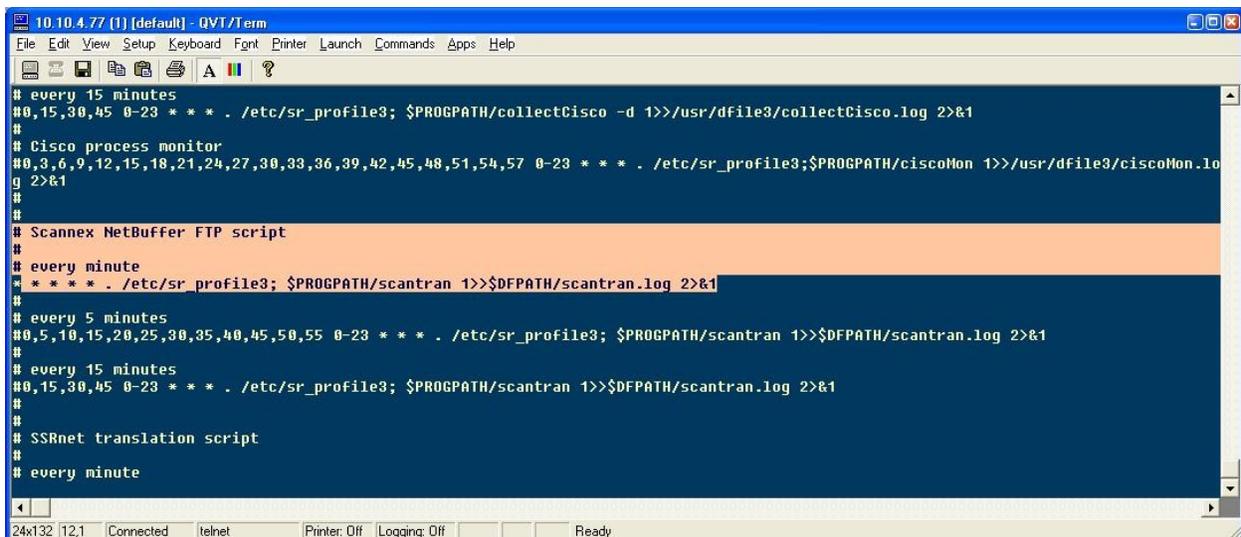
```
10.10.4.77 (1) [default] - QVT/Term
File Edit View Setup Keyboard Fgnt Printer Launch Commands Apps Help
PERFORM: Query Next Previous View Add Update Remove Table Screen ...
Searches the active database table.          ** 1: sites table**
sitenom          [6 ]
sitenam          [AVAYA1 ]
sitecode         [AVAYA1 ]
sitelive         [1 ]
auditdate        [21/12/2009]
lastesno         [65600 ]
lasttsno         [1304 ]
lastpsno         [0 ]
lastspno         [0 ]
lastcono         [0 ]
transprog        [defvx ]
transopts        [-cdm ]
protprog         [ ]
protdebug        [ ]
trafprog         [ ]
trafopts         [ ]
pbx_id           [ ]
timezone         [ ]
dialno           [ ]
dialno2          [ ]
1 row(s) found
24x132 1.9 Connected telnet Printer: Off Logging: Off Ready
```

5.1.2. Configure Collection and Translation Script

A script is configured for the automatic/on demand CDR collection and translation. From the UNIX prompt edit the file `/usr/prog3/scantran` using an appropriate editor (not shown). Enter in the parameters as follows:

- **sitenam** Enter in **AVAYA1** as named in **Section 5.1.1**.
- **transprog** This parameter defines the format, set for **defvx**, which is the customized format.
- **transopts** Set it for **cdm** translator option.

The remaining fields can be left as default. Save the file and exit. The completed screen is displayed below.



```
10.10.4.77 [1] [default] - QVT/Term
File Edit View Setup Keyboard Font Printer Launch Commands Apps Help
# every 15 minutes
#0,15,30,45 0-23 * * * . /etc/sr_profile3; $PROGPATH/collectCisco -d 1>>/usr/dfile3/collectCisco.log 2>&1
#
# Cisco process monitor
#0,3,6,9,12,15,18,21,24,27,30,33,36,39,42,45,48,51,54,57 0-23 * * * . /etc/sr_profile3;$PROGPATH/ciscoMon 1>>/usr/dfile3/ciscoMon.log 2>&1
#
# Scannex NetBuffer FTP script
#
# every minute
# * * * * . /etc/sr_profile3; $PROGPATH/scantran 1>>$DFPATH/scantran.log 2>&1
#
# every 5 minutes
#0,5,10,15,20,25,30,35,40,45,50,55 0-23 * * * . /etc/sr_profile3; $PROGPATH/scantran 1>>$DFPATH/scantran.log 2>&1
#
# every 15 minutes
#0,15,30,45 0-23 * * * . /etc/sr_profile3; $PROGPATH/scantran 1>>$DFPATH/scantran.log 2>&1
#
# SSRnet translation script
#
# every minute
```

5.2. Add Extensions to the ORBi-TEL⁷ Server Database

The database on the ORBi-TEL⁷ Server must be populated with Communication Manager extensions and trunks 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 **AVAYA1** as the Site Name to correspond with **Section 5.1.1**
- **Extension** Enter in a valid extension as configured on Communication Manager
- **Status** Choose **Ext Owner**

Click the **Add Extension** button.

Repeat the above steps to add all necessary extensions. The complete list of extensions added for the site is displayed below.

Search	Name	Extension	Site Name	Node	Status	Job Title	Id
	Unknown	3000	AVAYA1	AVAYA1 EXTNS	Ext Owner		140233
	Unknown	3001	AVAYA1	AVAYA1 EXTNS	Ext Owner		140233
	Unknown	3002	AVAYA1	AVAYA1 EXTNS	Ext Owner		140233
	Unknown	3003	AVAYA1	AVAYA1 EXTNS	Ext Owner		140233
	Unknown	3004	AVAYA1	AVAYA1 EXTNS	Ext Owner		140233
	Unknown	3005	AVAYA1	AVAYA1 EXTNS	Ext Owner		140233

5.3. Configure the ip.buffer

The ip.buffer is configured to work with ORBi-TEL⁷ and the Avaya solution.

5.3.1. Setting the ip.buffer IP Address

The ip.buffer is shipped with a default factory set IP Address. The ip.buffer IP address is set by associating the ip.buffer with its MAC address. Open a DOS window on the ORBi-TEL⁷ Server by clicking on **Start**, **Run** and type **cmd** and issue the following command: **arp -s x.x.x.x yy-**

yy-yy-yy-yy-yy, where x.x.x.x will be the new IP Address of ip.buffer and yy-yy-yy-yy-yy-yy is the MAC address found on the ip.buffer. Power off the ip.buffer for 30 seconds and re-connect the power. Ping the new IP address to check the ip.buffer IP configuration and verify a successful reply.

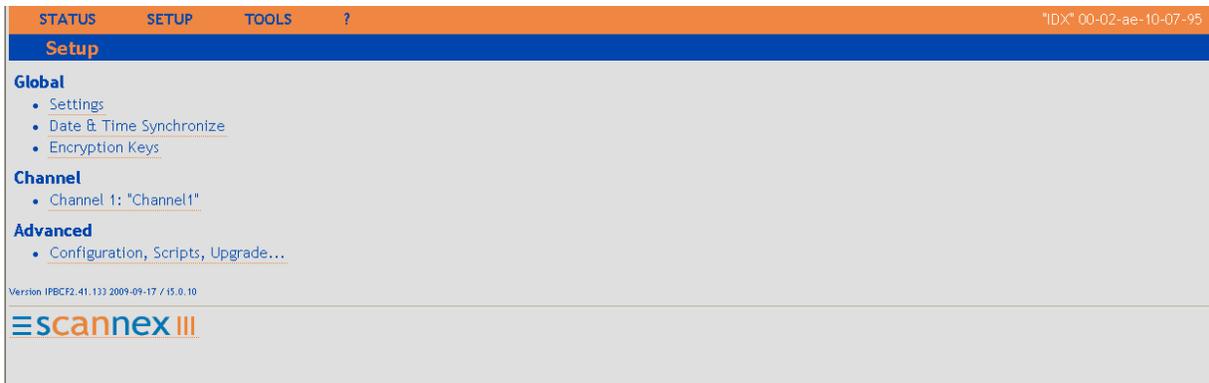
5.3.2. Configuring the ip.buffer Using a Web Browser

Enter the following URL Address in the web browser (IE) address bar <http://x.x.x.x>, where x. x. x. x is the selected IP address of the ip.buffer. Select the Setup Menu tab located on the opening Status screen to access the **Setup Menu**.

In the windows login box that appears, enter the appropriate username and password for the ip.buffer.



After a successful login the Setup Menu screen is shown.



In the **Setup Menu** screen select **Settings** and **Network/show**. The following screen is displayed. In the **Name** field enter the name that matches the ORBi-TEL⁷ site name configured on the ORBi-TEL⁷ Server in **Section 5.1.1**. Select the **Fixed IP** option for **Assignment** under the **LAN/Ethernet** section. The **IP address** of the ip.buffer is pre-populated with the **arp** command issued in **Section 5.3.1**. Enter the **Gateway** and **Subnet IP** address as shown below. The remaining fields can be left with the default values. Click on **Save**.

STATUS		SETUP		TOOLS		?		
							"IDX" 00-02-ae-10-07-95	
Global: Settings								
Device Name	AVAYA1	Name of the ip.buffer						
Network	Network & System show / hide							
LAN/Ethernet								
Assignment	Fixed IP	Fixed or dynamic IP address						
Fixed IP	10.10.4.79	Address (changes are <i>immediate</i> on save!)						
Subnet	255.255.255.0	Network subnet						
Gateway	10.10.4.1	Default gateway						
Name Servers								
DNS 1	255.255.255.255	Primary DNS server						
DNS 2	255.255.255.255	Secondary DNS server						
SNMP Traps								
Destination	255.255.255.255						SNMP trap output. Default = 255.255.255.255 (broadcast)	
SNMP Agent								
Contact							Person responsible (available to SNMP client)	
Location							Location of this device (available to SNMP client)	
Syslog								
Server							Syslog server address (blank=no syslog)	
Bandwidth Limiting								
Max data	0	kbyte/s						Destination data rate across Ethernet. Off=0
Time	SNTP & DST show / hide							
Power	Power & Battery Settings show / hide							
SMTP	Email Servers show / hide							
Alerts &	Alerts show / hide							

In the Setup Menu screen under Channel, select the option **Channel1:"Channel1"** to display the Channel 1 setup screen shown below. Set **Source** to **TCP**. Enter a port number in the **Port** field where **9000** is the default. The port number used should match the **Remote Port** configured on the Communication Manager in **Section 4.2**. Select **Avaya RSP** as the **Protocol**. The remaining fields can be left with the default values. Click on **Save** (not shown).

The screenshot shows the 'Channel 1: "Channel1"' configuration page. At the top, there are tabs for 'STATUS', 'SETUP', 'TOOLS', and '?'. The page title is 'Channel 1: "Channel1"'. Below the title, there are several sections:

- Name:** Channel1 (The name of the channel (don't use spaces))
- Source:** TCP (Where to collect from)
- TCP/IP:**
 - Connect:** Device to ipbuffer (passive/server) (Active or Passive connection)
 - Address:** (Name or IP address of device)
 - Allow:** (Restrict incoming connections to this LAN name or IP)
 - Port:** 9000 (TCP port number)
- Match & Send:** Four rows of input fields for matching patterns, with options for CR/LF, hex, and other formats.
- Heartbeat:**
 - Interval:** 0 seconds (Default=0)
 - String:** (String to send at the interval)
- Protocol:** Avaya RSP (Which protocol or data type)
- Time Stamp:** (Prefix each record. See manual for formats. Blank = no prefix)

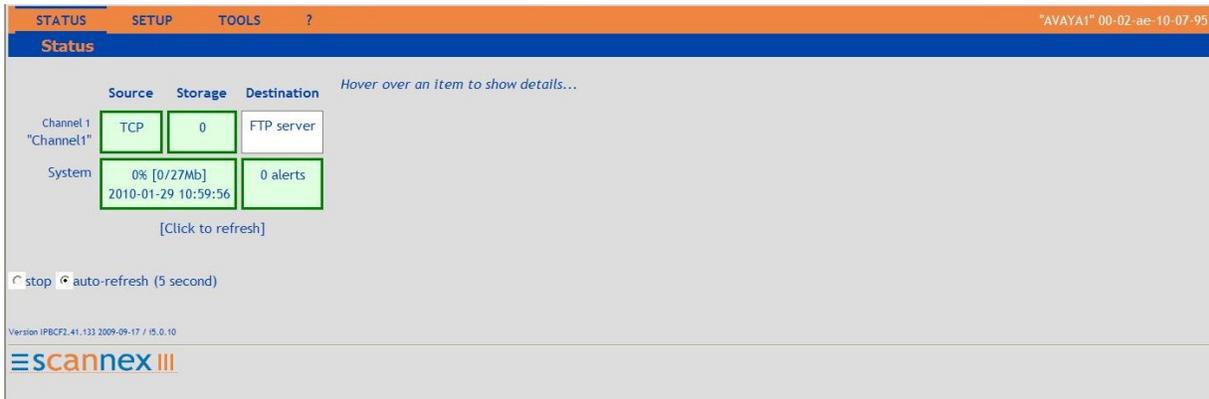
On the **Channel1:"Channel1"** screen set the **Destination** field show to display the **FTP server**. The ORBi-TEL⁷ Server acts as the FTP client with the ip.buffer being the FTP server. Set **Filename** to **download.dat**. Change **Username** and **Password** to the FTP client (ORBi-TEL⁷ Server) required values. Click on **Save**.

The screenshot shows the 'Channel 1: "Channel1"' configuration page, now with the 'Destination' field set to 'FTP server'. Below the title, there are several sections:

- Name:** Channel1 (The name of the channel (don't use spaces))
- Source:** TCP (Where to collect from)
- Destination:** FTP server (How to deliver the data)
- FTP server:**
 - Username:** scannex (FTP Global / hide) (Username for this channel (case sensitive))
 - Password:** qjerty1 (RADIUS settings / hide) (Password (case sensitive))
 - Filename:** download.dat (Filename)
 - Compression:** none (Send normal or compressed)
 - Limit:** 0 kb (Limit transfer size. 0=no limit)
 - Autodelete:** Delete after download (Automatically delete the data when downloaded?)
- Data Markers:**
 - Prefix:** (Prefix string. Blank = no prefix. See manual for formats.)
 - Suffix:** (Suffix string. Blank = no suffix. Note: Suffix not used for TCP real-time connections)
- Data Security:**
 - Data Encryption:** Unencrypted (Whether to protect the data sent. Note: You must also program an encryption key in Setup/Encryption Keys!)
- Storage:** Storage settings show / hide

At the bottom, there are 'SAVE' and 'Cancel' buttons.

Select **Status** and the completed **Status** screen is displayed. The **TCP Source** displays in green indicating that the ip.buffer has successfully connected to the Avaya solution.



6. General Test Approach and Test Results

The general test approach was to manually place intra-switch calls, inbound and outbound PSTN trunk calls to and from telephones attached to the Avaya S8500 Server, and verify that ORBi-TEL⁷ with ip.buffer collects the CDR records and properly classifies and reports the attributes of the call. For serviceability testing, logical links were disabled/re-enabled, and the Avaya S8500 Server was rebooted.

All executed test cases were passed. ip.buffer successfully collected the CDR records from Communication Manager via the CDR link for all types of calls generated including intra-switch calls, inbound / outbound PSTN trunk calls, transferred calls and conference calls. It passed them on to the ORBi-TEL⁷ Server. For serviceability testing, the ORBi-TEL⁷ server was able to resume collecting CDR records automatically after failure recovery, including buffered CDR records for calls that were placed during the outages.

7. Verification Steps

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

7.1. Verify Avaya Aura™ Communication Manager

The following steps can ensure that the communication between Communication Manager and the ORBi-TEL⁷ is functioning correctly.

- Use the **ping** utility on the ORBi-TEL⁷ server to verify the IP connectivity to the Avaya S8500 Server.
- On the SAT of the Avaya S8500 Server, enter the **status cdr-link** command and verify that the CDR **Link State** shows **up** for both the **Primary** and **Secondary** links. This represents the CDR link of the ip.buffer and the CDR link for the RDTT. Data is only shown in the Secondary column only when there is a second CDR link.

status cdr-link	
CDR LINK STATUS	
Primary	Secondary
Link State: up	up
Date & Time: 2010/1 /28 15:41:27	2010/1 /28 15:41:27
Forward Seq. No: 43	43
Backward Seq. No: 0	0
CDR Buffer % Full: 0.00	0.00
Reason Code: OK	OK

7.2. Verify ORBi-TEL⁷ and the ip.buffer

Verify the connection between ORBi-TEL⁷ Server and the ip.buffer through the following steps.

7.2.1. Connection Between ORBi-TEL⁷ Server and the ip.buffer

Access the ip.buffer from a DOS or UNIX prompt and issue the following command:

#ftp x.x.x.x where **x.x.x.x** is the IP address of ip.buffer.

Enter Username and Password of the ftp server (ip.buffer).

Ensure that you received the following message:

#Connected

Enter in the following:

DIR

The return will display

#download.dat

Enter **BYE** to return to Unix or DOS.

BYE

9. Additional References

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

[1] *Avaya Aura™ Communication Manager Feature Description and Implementation*, Release 5.2, May 2009, Document Number 555-245-205.

[2] *Administering Avaya Aura™ Communication Manager*, Release 5.2, May 2009, Document Number 03-300509.

The Nu Technologies documentation can be found at <http://www.nut.eu.com>.

©2010 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.