Avaya Solution & Interoperability Test Lab

Application Notes for Nexidia Extractor with Avaya Communication Manager and Avaya Application Enablement Services - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Nexidia Extractor to monitor and record calls placed to and from stations on Avaya Communication Manager.

The Extractor is an application, built upon Nexidia's Scalable Media Processing (SMP) Framework that captures calls processed by an Avaya VoIP solution and records them along with any associated metadata. The Extractor is composed of the SMP, the Avaya stream control/capture extension, and the recording sink extension. The Extractor interfaces with Avaya Communication Manager through Avaya Application Enablement Services (AES), using TSAPI to associate recordings with important CTI information, and DMCC to acquire media. The system uses the DMCC Streaming capability to record extension, and inbound or outbound calls. Voice is recorded at the server in wave format.

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 comprised of an Avaya Communication Manager, an Avaya Application Enablement Services (AES) server, and the Extractor. The Extractor is a subset of the Nexidia Enterprise Speech Intelligence (ESI) system which utilizes Speech Analytics Technology to provide a scalable, accurate, affordable and fast solution to analyze all recorded audio.

The Extractor monitors, records, stores, and plays back phone calls for verification. The Extractor uses TSAPI with an Avaya AES server to monitor stations to obtain recording triggers and call information. The Extractor also uses the Device, Media and Call Control (DMCC) service with the Avaya AES server to register DMCC softphones that the Extractor uses as recording ports.

Figure 1 provides the test configuration used for the compliance test. Note that actual configurations may vary. The solution described herein is also extensible to other Avaya Servers and Media Gateways. An Avaya S8300 Server with an Avaya G700 Media Gateway was included during the test, to provide an IP trunk between two Avaya Communication Manager systems.

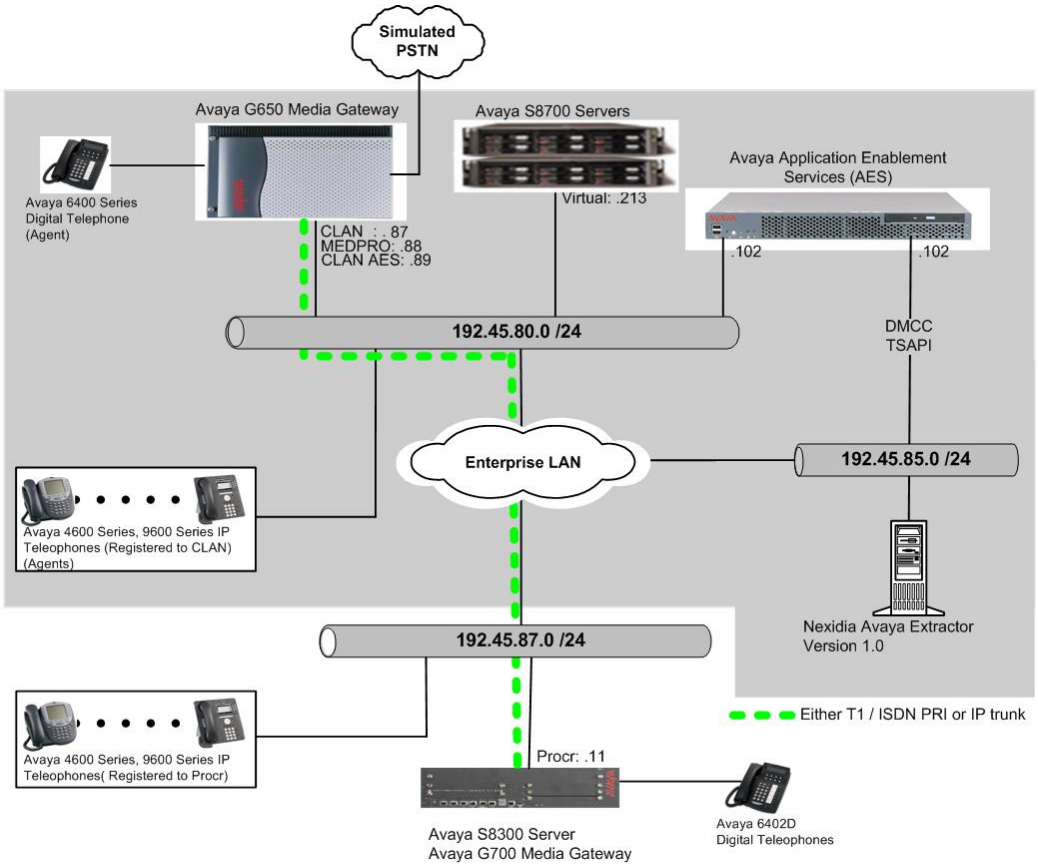


Figure 1: Sample Test Configuration for the Extractor Solution

2. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya S8720 Server		Avaya Communication Manager 5.1 (01.0.414.3) with SP # 15842
Avaya G650 Media Gateway		-
	TN2312BP IP Server Interface TN799DP C-LAN Interface TN2302AP IP Media Processor	HW11 FW030 HW20 FW017 HW01 FW108
Avaya S8300 Server with Avaya G700 Media Gateway		Avaya Communication Manager 5.1 (01.0.414.3) with SP # 15842
Avaya Application Enablement Services Server		4.2 (R4.2.0.19.4)
Avaya 4600 Series IP Telephones		
	4620SW (H.323) 4625SW (H.323)	2.8 2.8
Avaya 9600 Series IP Telephones		
	9630 (H.323) 9650 (H.323)	1.5 1.5
Avaya 6408D+ Digital Telephone		-
Extractor on Linux Fedora 9		1.0.0 Bld:1023

3. Configure Avaya Communication Manager

This section provides the procedures for configuring an ip-codec-set and ip-network region, a switch connection and Computer Telephony Integration (CTI) links, monitored stations, and recording stations on Avaya Communication Manager. All the configuration changes in Avaya Communication Manager are performed through the System Access Terminal (SAT) interface. The highlights in the following screens indicate the values used during the compliance test.

3.1. Codec Configuration

Enter the **change ip-codec-set t** command, where **t** is a number between 1 and 7, inclusive.

```
change ip-codec-set 1                                          Page   1 of   2

                           IP Codec Set
   Codec Set: 1

   Audio        Silence      Frames   Packet
   Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU           n          2        20
 2: G.729             n          2        20
```

3.2. IP Network Regions

During compliance testing, a C-LAN board dedicated for H.323 endpoint registration was assigned to IP network region 1. The Avaya IP Telephones and IP Softphones used by the

Extractor, registered with the C-LAN boards and were thus also assigned to IP network region 1. One consequence of assigning the aforementioned IP telephones, IP Softphones, and MedPro boards to a common IP network region is that the RTP traffic between them is governed by the same codec set. The second C-LAN board (CLAN-AES), which is dedicated for the AES server, was assigned to network region 2. The following screen shows only network region 1.

```
change ip-network-region 1                                    Page   1 of  19
                             IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain:
    Name:
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: 3929
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46       RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46        Use Default Server Parameters? y
        Video PHB Value: 46
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 0
        Audio 802.1p Priority: 0
        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
```

3.3. Configure Switch Connection and CTI Links between Avaya Communication Manager and Avaya Application Enablement Services

The Avaya AES server forwards CTI requests, responses, and events between the Extractor and Avaya Communication Manager. The AES server communicates with Avaya Communication Manager over a switch connection link. Within the switch connection link, CTI links may be configured to provide CTI services to CTI applications such as the Extractor. The following steps demonstrate the configuration of the Avaya Communication Manager side of the switch connection and CTI links. See **Section 4** for the details of configuring the AES side of the switch connection and CTI links.

Enter the **add cti-link m** command, where **m** is a number between 1 and 64, inclusive. Enter a valid extension under the provisioned dial plan in Avaya Communication Manager, set the Type field to **ADJ-IP**, and assign a descriptive Name to the CTI link.

```
add cti-link 4                                                Page   1 of   2
                                    CTI LINK
 CTI Link: 4
Extension: 20006
     Type: ADJ-IP
                                                                   COR: 1
     Name: TSAPI
```

Enter the **change node-names ip** command. In the compliance-tested configuration, the CLAN IP address was utilized for registering H.323 endpoints (Avaya IP Telephones, and IP Softphones, and AES Device, Media and Call Control API stations) and the CLAN-AES IP address was used for connectivity to Avaya AES.

```
change node-names ip                                          Page   1 of   2
                                  IP NODE NAMES
    Name                 IP Address
CLAN                   192.45.80.87
CLAN-AES               192.45.80.89
MEDPRO                 192.45.80.88
MEDPRO2                192.45.80.161
S8300G700              192.45.87.11
default                0.0.0.0
procr                  192.45.80.214
```

Enter the **change ip-services** command. On **Page 1**, configure the Service Type field to **AESVCS** and the Enabled field to **y**. The Local Node field should be pointed to the **CLAN-AES** board that was configured previously in the IP NODE NAMES form in this section. During the compliance test, the default port was utilized for the Local Port field.

```
change ip-services                                            Page   1 of   4

                                  IP SERVICES
 Service      Enabled      Local        Local       Remote      Remote
  Type                     Node         Port        Node        Port
AESVCS         y       CLAN-AES         8765
```

On **Page 4**, enter the hostname of the AES server for the AE Services Server field. The server name may be obtained by logging in to the AES server using ssh, and running the command **uname –a**. Enter an alphanumeric password for the Password field. Set the Enabled field to **y**. The same password will be configured on the AES server in **Section 4.1**.

```
change ip-services                                            Page   4 of   4
                           AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:       server2             xxxxxxxxxxxxxxxx      y        idle
      2:
      3:
```

3.4. Monitored Stations

Enter the **add station s** command, where **s** is an extension valid in the provisioned dial plan. During the compliance test, the following recorded stations were created.

- 22001 (Avaya 4620SW IP)
- 22002 (Avaya 4625SW IP)
- 22003 (Avaya 9630 IP)
- 22007 (Avaya 6408D+)
- 22009 (Avaya IP Agent)

3.5. Recording Stations

Enter the **add station s** command, where **s** is an extension valid in the provisioned dial plan. On **Page 1** of the STATION form, set the Type field to an IP telephone set type, enter a descriptive Name, specify the Security Code, and make sure that the IP Softphone field is set to **y**. For the compliance test, recording stations from 23001 to 23023 were created.

```
change station 23001                                          Page   1 of   5
                                    STATION

Extension: 23001                        Lock Messages? n               BCC: 0
     Type: 4620                         Security Code: *               TN: 1
     Port: S00046                     Coverage Path 1:                 COR: 1
     Name: DMCC-1                     Coverage Path 2:                 COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                          Time of Day Lock Table:
              Loss Group: 19          Personalized Ringing Pattern: 1
                                                Message Lamp Ext: 23001
           Speakerphone: 2-way                Mute Button Enabled? y
        Display Language: english                Expansion Module? n
 Survivable GK Node Name:
          Survivable COR: internal                Media Complex Ext:
   Survivable Trunk Dest? y                            IP SoftPhone? y

                                               IP Video Softphone? n


                                              Customizable Labels? y
```

4. Configure Avaya Application Enablement Services

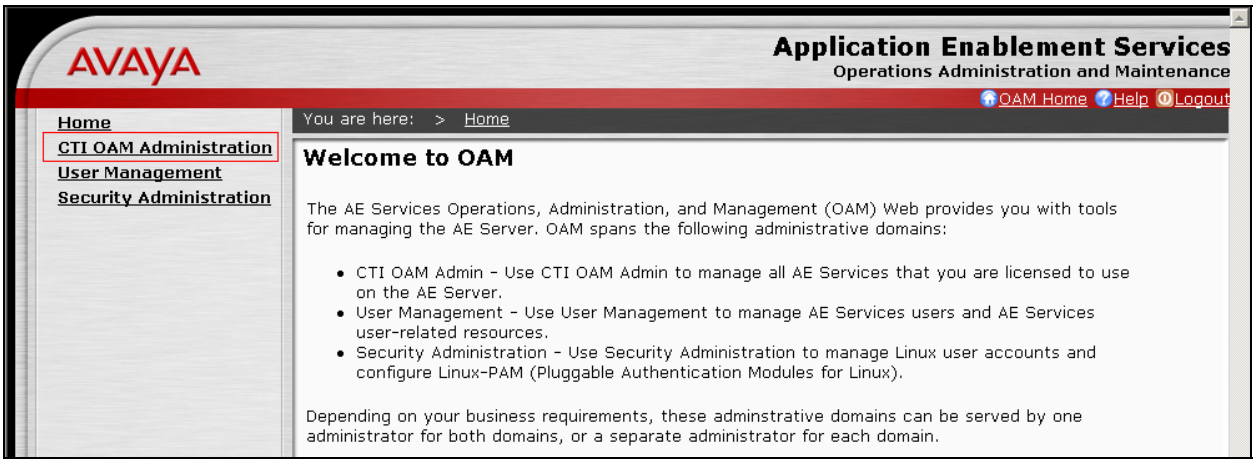
The Avaya Application Enablement Services (AES) server enables Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Avaya Communication Manager. The Avaya Application Enablement Services (AES) server receives requests from CTI applications, and forwards them to Avaya Communication Manager. Conversely, the Avaya Application Enablement Services (AES) server receives responses and events from Avaya Communication Manager and forwards them to the appropriate CTI applications.

This section assumes that installation and basic administration of the Avaya Application Enablement Services server has been performed. The steps in this section describe the configuration of a Switch Connection, a CTI user, a CMAPI port, and creating a CTI link for TSAPI.

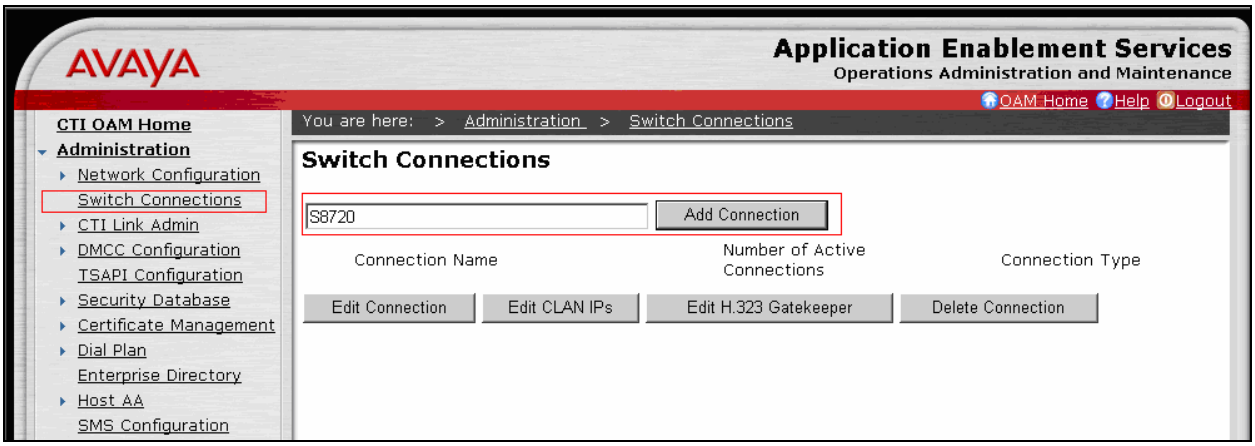
4.1. Configure Switch Connection

Launch a web browser, enter http://<IP address of AES server> in the address field, and log in with the appropriate credentials for accessing the AES CTI OAM pages.

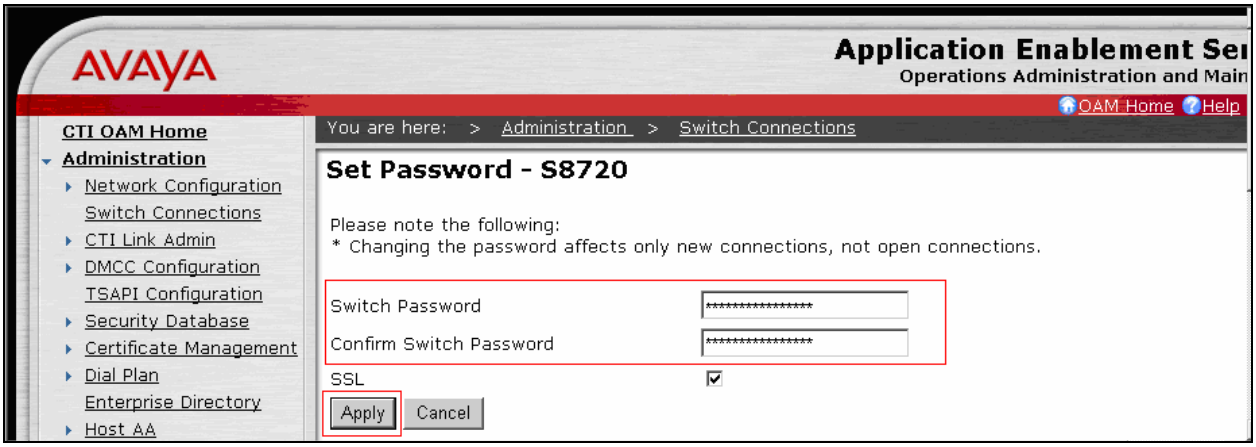
Select the **CTI OAM Administration** link from the left pane of the screen.



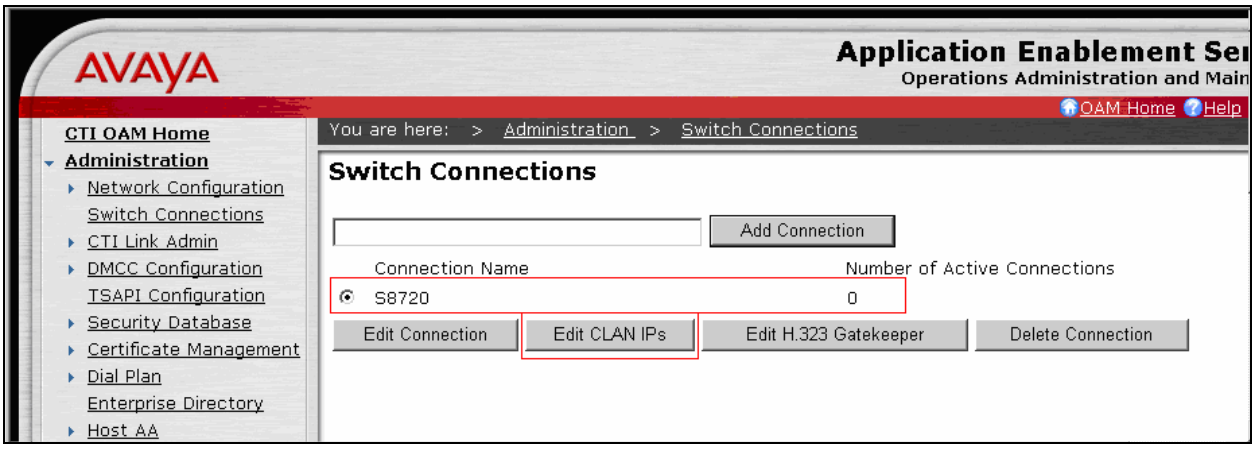
Click on **Administration → Switch Connections** in the left pane to invoke the Switch Connections page. A Switch Connection defines a connection between the Avaya AES and Avaya Communication Manager. Enter a descriptive name for the switch connection and click on **Add Connection**.



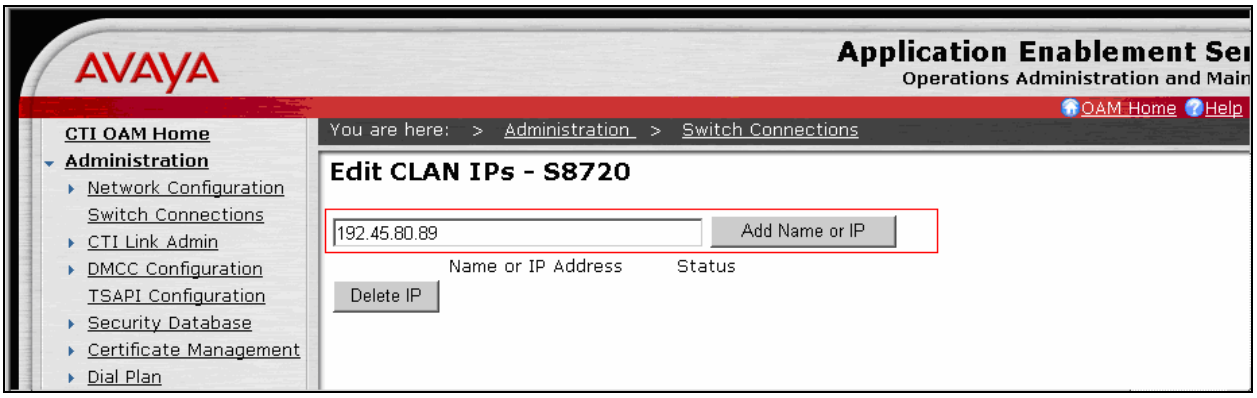
The next window that appears prompts for the Switch Connection password. Enter the same password that was administered in Avaya Communication Manager in **Section 3.3**. Click on **Apply**.



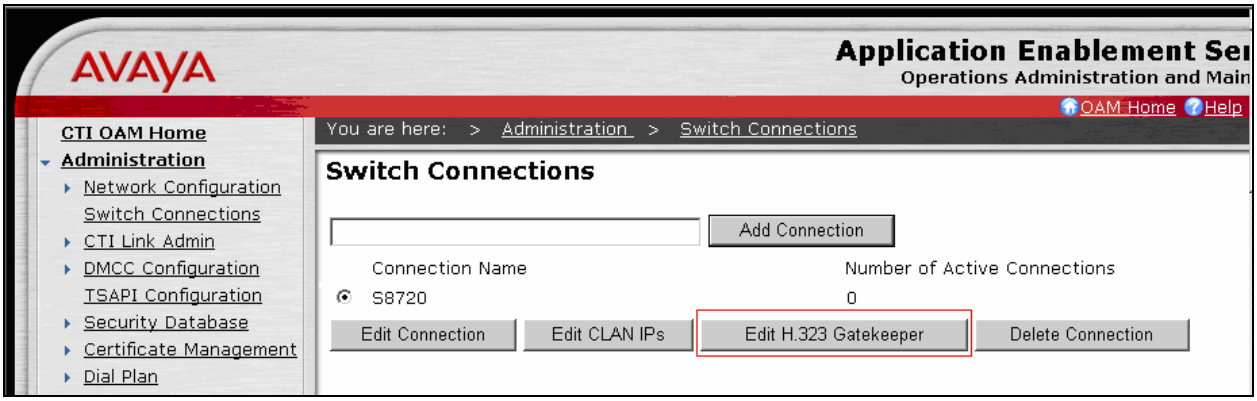
After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on **Edit CLAN IPs**.



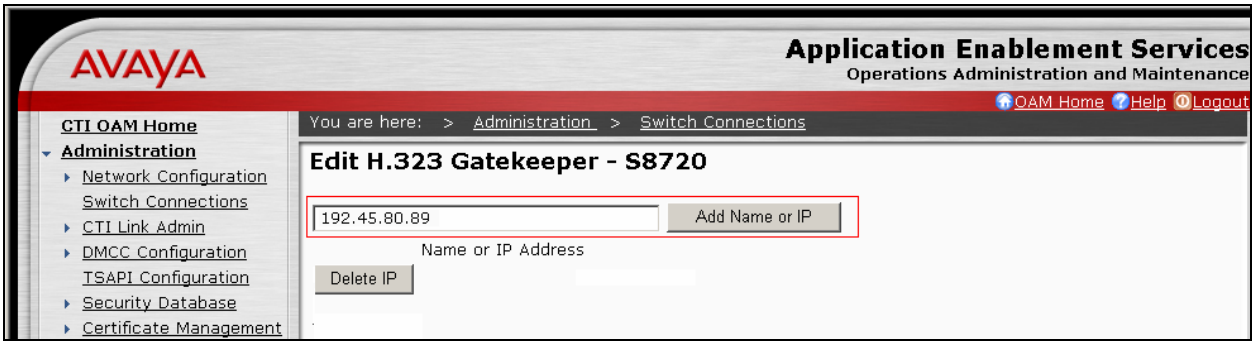
Enter the CLAN-AES IP address which was configured for AES connectivity in **Section 3.3** and click on **Add Name or IP**. Repeat this step as necessary to add other C-LAN boards enabled with Application Enablement Services.



After the completion, navigate back to **Administration → Switch Connections** in the left pane to invoke the Switch Connections page. Click on **Edit H.323 Gatekeeper** for DMCC call control and monitor.

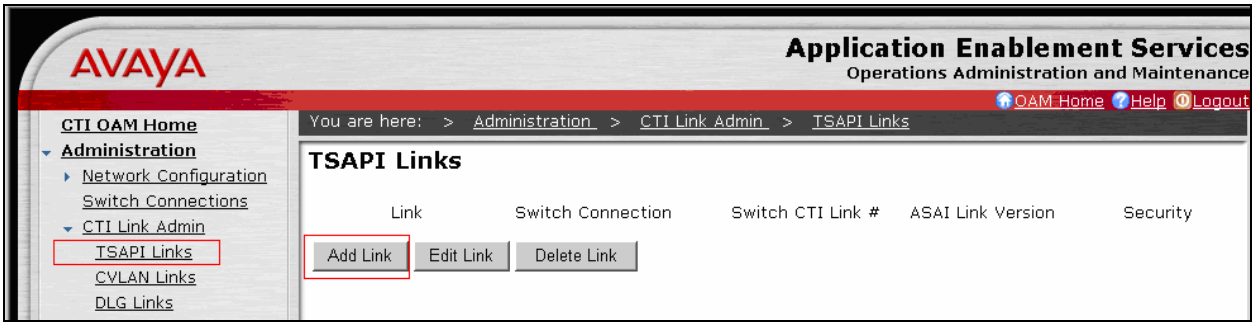


On the **Edit H.323 Gatekeeper – S8720** page, enter the C-LAN IP address which will be used for the DMCC service. During the compliance test, CLAN-AES was utilized for the DMCC service. Click on **Add Name or IP**. Repeat this step as necessary to add other C-LAN boards enabled with Application Enablement Services.

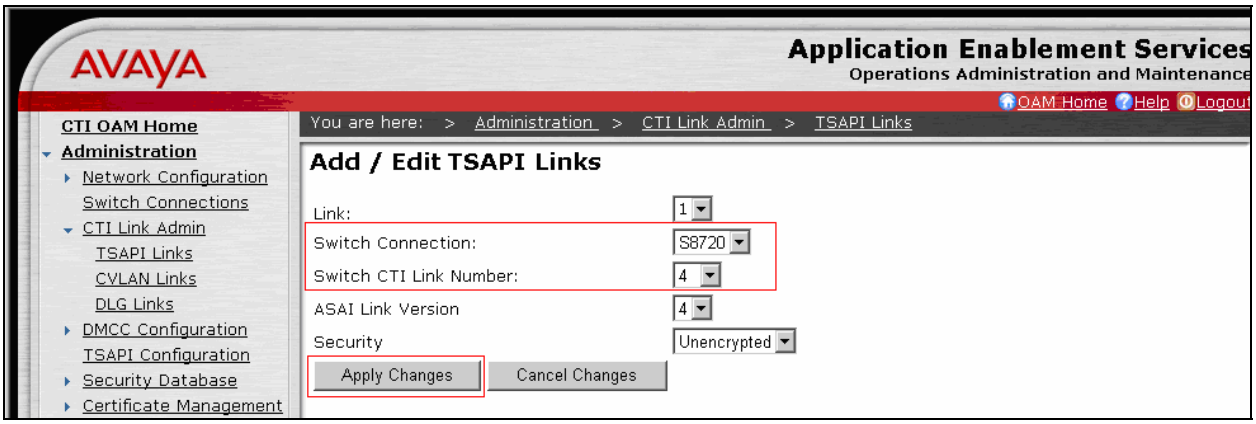


4.2. Configure the TSAPI CTI link

Navigate to **Administration → CTI Link Admin → TSAPI Links** in the left pane, and click on the **Add Link** button to create a TSAPI CTI link.



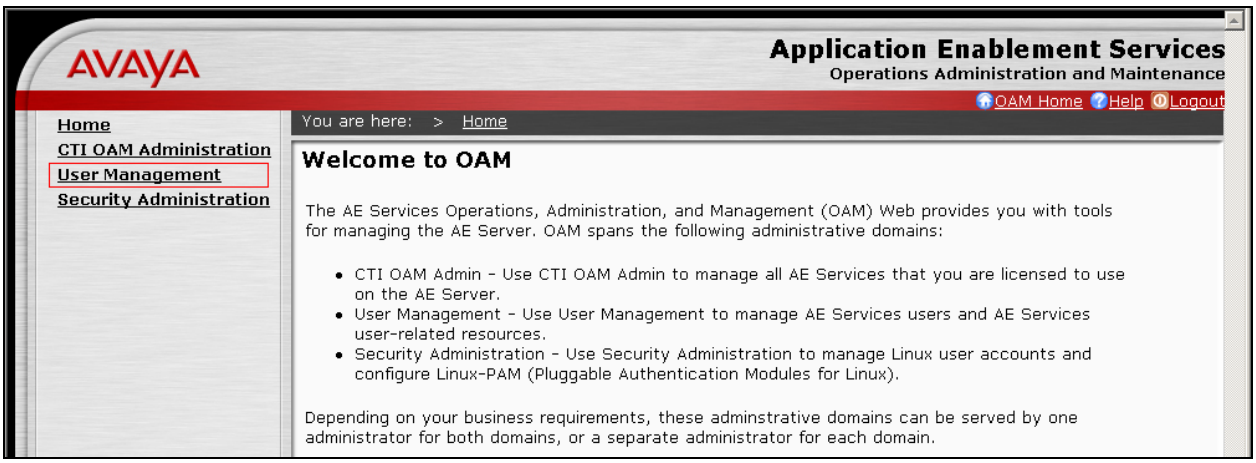
Select a Switch Connection using the drop down menu. The Switch Connection is configured in **Section 4.1**. Select the Switch CTI Link Number using the drop down menu. Switch CTI Link Number should match with the number configured in the cti-link form **in Section 3.3**. Click the **Apply Changes** button. Default values may be used in the remaining fields.



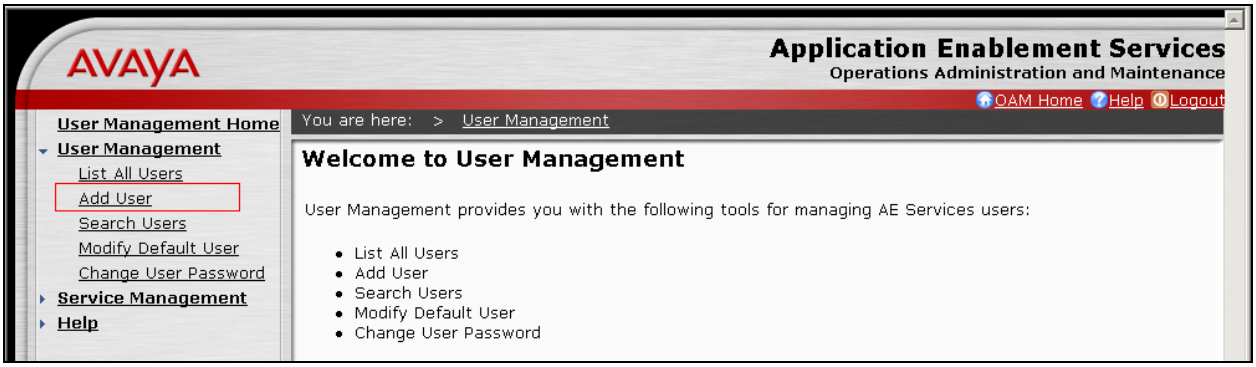
4.3. Configure the CTI Users

The steps in this section describe the configuration of a CTI user. Launch a web browser, enter http://<IP address of AES server> in the URL, and log in with the appropriate credentials to access the relevant administration pages.

The Welcome to OAM page is displayed next. Select **User Management** from the left pane.



From the Welcome to User Management page, navigate to the **User Management → Add User** page to add a CTI user.

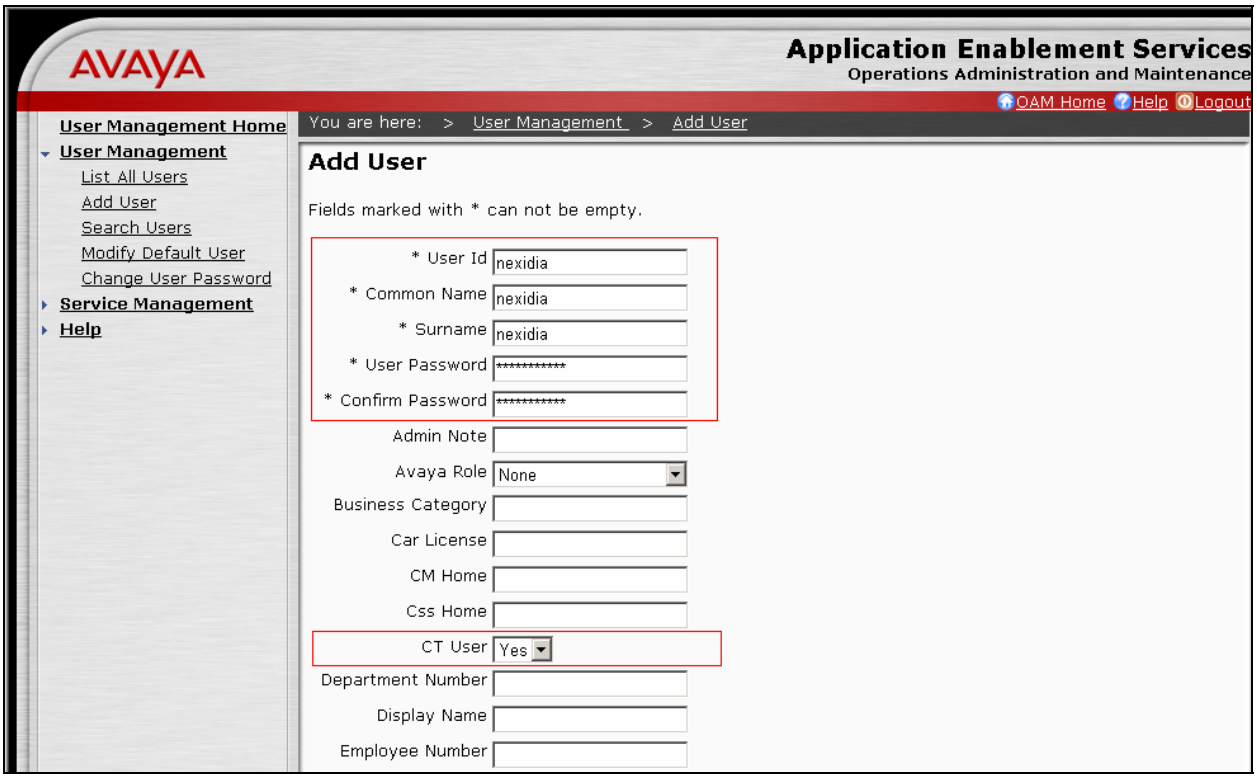


On the Add User page, provide the following information:

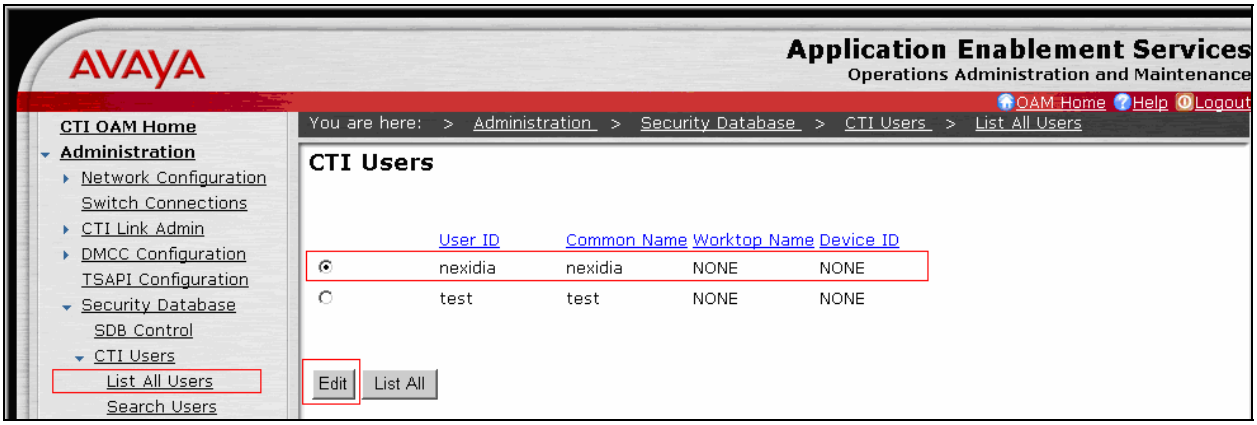
- User Id
- Common Name
- Surname
- User Password
- Confirm Password

The above information (User ID and User Password) must match with the information configured in the Extractor Configuration page in **Section 5**.

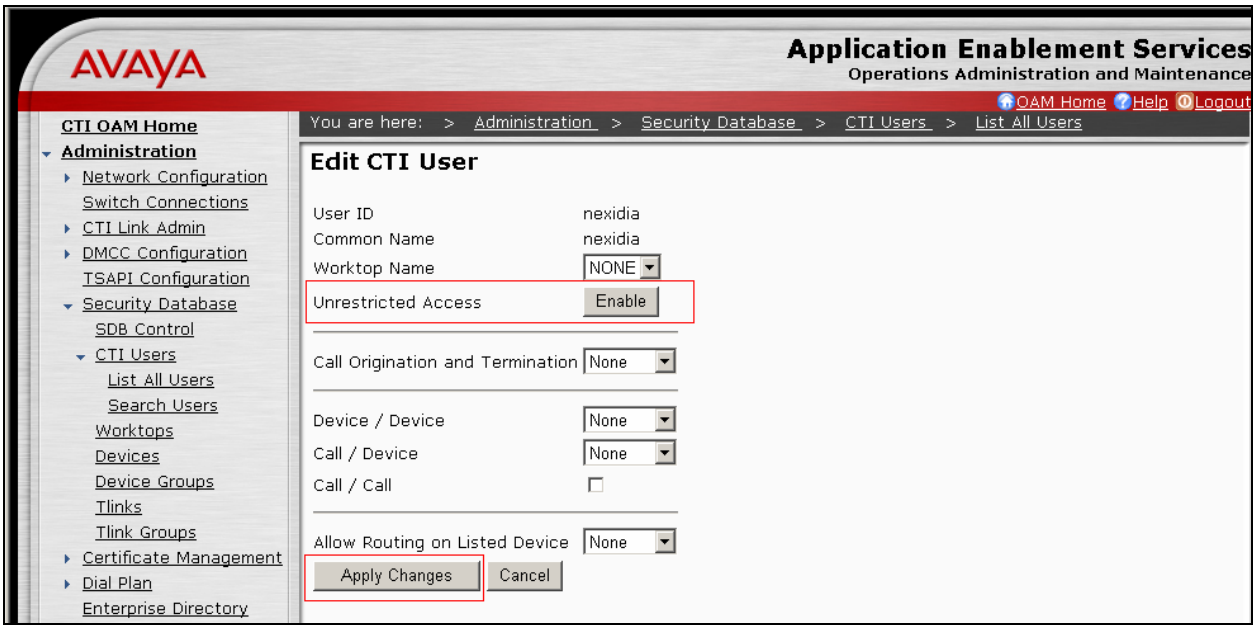
Select **Yes** using the drop down menu on the CT User field. This enables the user as a CTI user. Default values may be used in the remaining fields. Click the **Apply** button (not shown) at the bottom of the screen to complete the process.



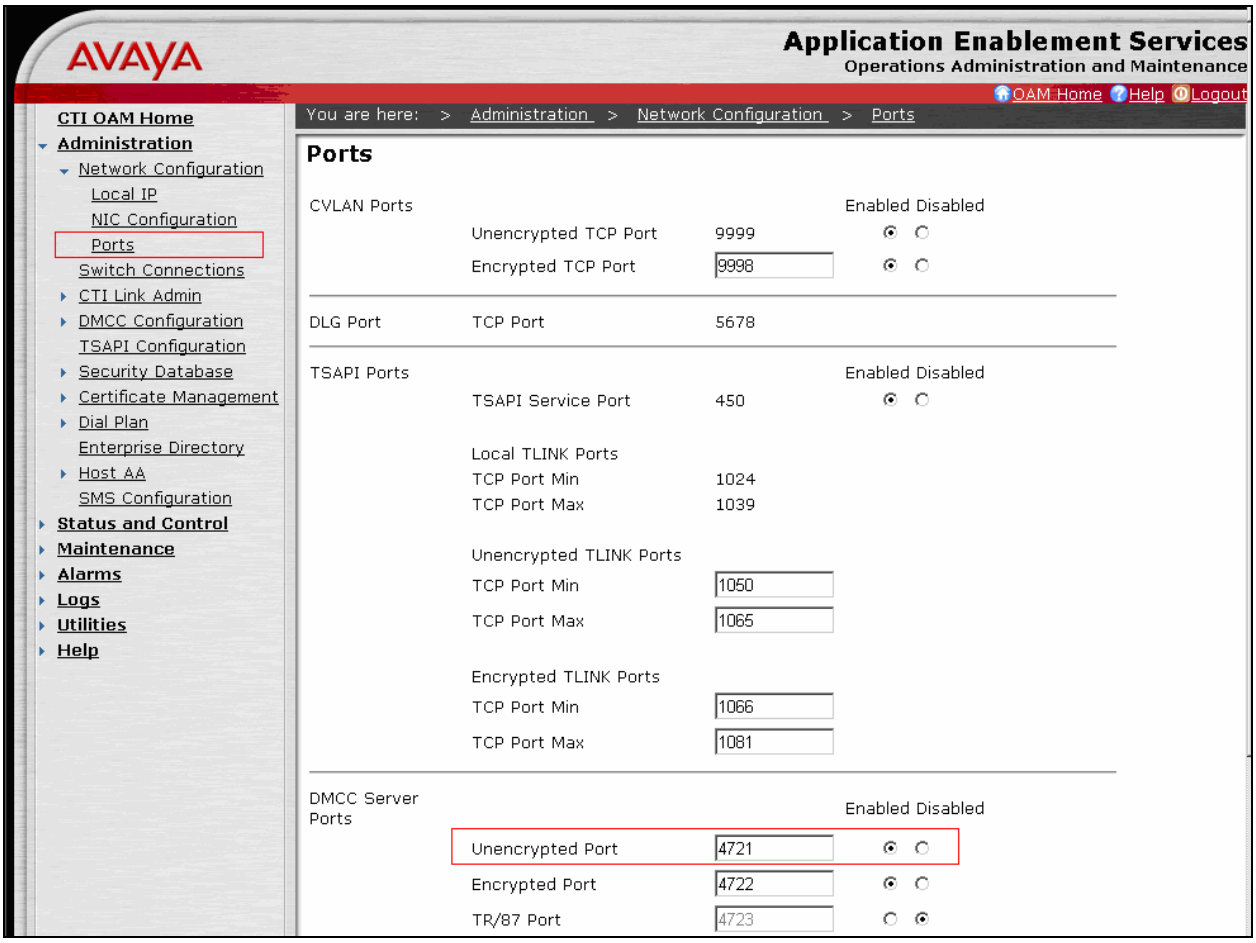
Once the user is created, select **OAM Home** in upper right and navigate to the **CTI OAM Administration → Security Database → CTI Users → List All Users** page. Select the User ID created previously, and click the **Edit** button to set the permission of the user.



Provide the user with unrestricted access privileges by clicking the **Enable** button on the Unrestricted Access field. Click the **Apply Changes** button.



Navigate to the **CTI OAM Home → Administration → Ports** page to set the DMCC server port. During the compliance test, the default port values were utilized. The following screen displays the default port values. Since the unencrypted port was utilized during the compliance test, set the Unencrypted Port field to **Enabled**. Default values may be used in the remaining fields. Click the **Apply Changes** button (not shown) at the bottom of the screen to complete the process.



5. Configure Nexidia Extractor

This section only describes the interface configuration for the Extractor application to communicate with Avaya AES and Avaya Communication Manager.
Refer to [3] [4] and [5] for configuring the Extractor application. The following screen shows the global.properties file. During the compliance test, the highlighted values were utilized:

```
################################################################################
# Avaya properties
################################################################################
#
# Avaya defined properties
# IP of the server running AE Services.
cmapi.server_ip=192.45.85.103

# Port that AE Services will be listening on. Use:
#   4721 for unsecured, or
#   4722 for secured.
cmapi.server_port=4721

# Username of the application.
cmapi.username=nexidia
```

```
# Password of the application.
cmapi.password=Nexidia123&

.
.
.

# Extensions for the AvayaManager to monitor
nx.manager.monitor0.extension=22001
nx.manager.monitor0.password=22001
nx.manager.monitor1.extension=22002
nx.manager.monitor1.password=22002
nx.manager.monitor2.extension=22003
nx.manager.monitor2.password=22003
nx.manager.monitor3.extension=22007
nx.manager.monitor3.password=22007
nx.manager.monitor4.extension=22009
nx.manager.monitor4.password=22009
#
# Extensions to use for AvayaCapture channels.
nx.capture.channel0.extension=23001
nx.capture.channel0.password=1234
nx.capture.channel1.extension=23002
nx.capture.channel1.password=1234
nx.capture.channel2.extension=23003
nx.capture.channel2.password=1234
nx.capture.channel3.extension=23004
nx.capture.channel3.password=1234
nx.capture.channel4.extension=23005
nx.capture.channel4.password=1234

.
.
.

nx.capture.channel21.extension=23022
nx.capture.channel21.password=1234
nx.capture.channel22.extension=23023
nx.capture.channel22.password=1234

# Capture codec
# Legal values are: g711U, g711A, g729A
#
nx.capture.codecs=g711U

# Capture encryption
# Legal values are: none, aes
#
nx.capture.encrypts=none
```

6. Interoperability Compliance Testing

The interoperability compliance test included basic recording, serviceability, and performance testing. The basic recording testing evaluated the ability of the Extractor to monitor and record calls placed to and from stations. The serviceability testing introduced failure scenarios to see if the Extractor can resume recording after failure recovery. The performance testing stressed the Extractor by continuously placing calls over extended periods of time.

6.1. General Test Approach

The general approach was to manually place calls to and from stations, monitor and record them using the Extractor, and verify the recordings. The types of calls included internal calls, inbound and outbound trunk calls. Performance tests verified that the Extractor could record calls during a sustained, high volume of calls. For serviceability testing, failures such as cable pulls, CTI link busyouts and releases, and resets were applied.

6.2. Test Results

All test cases were executed and passed.

7. Verification Steps

This section provides the steps that can be performed to verify proper configuration of Avaya Communication Manager and Avaya AES.

7.1. Verify Avaya Communication Manager

Verify the status of the administered AES link by using the **status aesvcs link** command.

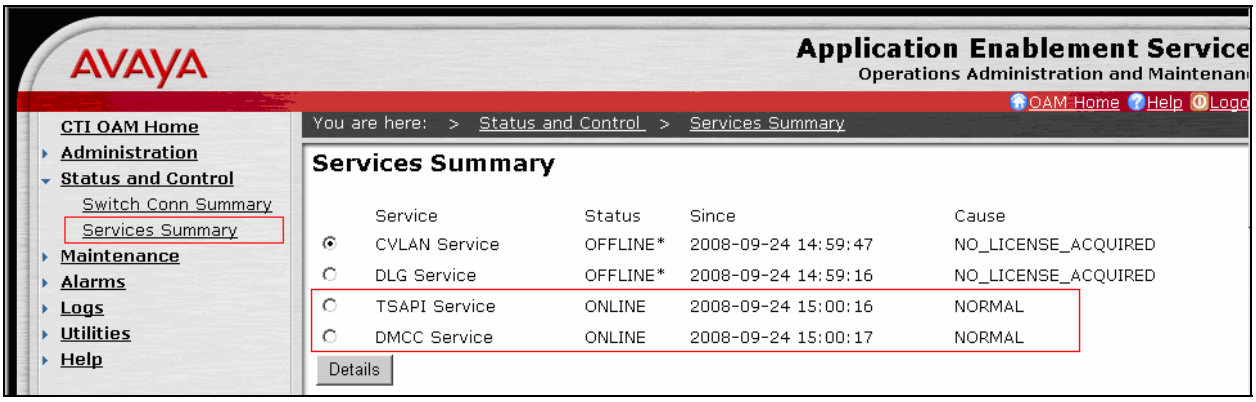
```
status aesvcs link

                          AE SERVICES LINK STATUS

Srvr/  AE Services     Remote IP        Remote  Local Node      Msgs    Msgs
Link   Server                          Port                    Sent    Rcvd

01/01  server2         192. 45. 80.103  60336   CLAN-AES        208     197
```

Verify the Service State field of the administered TSAPI CTI link is in **established** state, by using the **status aesvcs cti-link** command.

```
status aesvcs cti-link

                       AE SERVICES CTI LINK STATUS

CTI   Version  Mnt   AE Services      Service       Msgs     Msgs
Link           Busy  Server           State         Sent     Rcvd

4     4        no    server2          established   15       15
```

7.2. Verify Avaya Application Enablement Services

From the CTI OAM Admin web pages, verify the status of the TSAPI and DMCC Services are ONLINE, by selecting **Status and Control → Services Summary** from the left pane.



8. Support

Technical support on Nexidia Extractor can be obtained via email at, support@nexidia.com

9. Conclusion

These Application Notes illustrate the procedures for configuring the Extractor call recording solution to monitor and record calls placed to and from stations on an Avaya Communication Manager system. In the configuration described in these Application Notes, the Extractor employs Device, Media and Call Control Application Programming Interface virtual stations as recording ports. During compliance testing, the Extractor successfully monitored events and recorded calls placed to and from stations. The Extractor was also able to record calls under continuous call volumes over extended periods of time.

Note: *The compliance test included only the basic inbound and outbound station recordings. The features such as transfer, bridging, conferencing, call center environment, were not tested during the test, and will be covered with the next release of the Extractor.*

10. Additional References

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

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

[1] *Administrator Guide for Avaya Communication Manager*, Issue 4, January 2008, Document Number 03-300509

[2] *Application Enablement Services Administration and Maintenance Guide*, Release 4.1, Issue 9, February 2008, Document Number 02-300357

The following documentation was provided by Nexidia

[3] Extractor *Nexidia ESI Server Guide, Installation and Configuration*, Version 6.3, November 12, 2007
[4] *Nexidia ESI On-Line Help*, Version 6.3
[5] *Extractor Overview*, V1.0

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.