

Avaya Solution & Interoperability Test Lab

Application Notes for Applied Network Intelligence Trunk Dashboard with Avaya Communication Manager and Avaya Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Applied Network Intelligence (ANI) Trunk Dashboard to interoperate with Avaya Communication Manager and Avaya Application Enablement Services.

ANI Trunk Dashboard is a monitoring tool that uses Avaya Application Enablement Services to monitor up to 16 Avaya Communication Managers for any indication of a problem with Trunks. The Trunk Group monitoring is based on both snapshots of trunk group data and on 10-minute averages of trunk group usage information. The Dashboard also monitors for Major Alarms, Minor Alarms, DS1 Alarms, and CDR Link Alarms.

The overall objective of this testing is to verify the ANI Trunk Dashboard can interoperate with Avaya Application Enablement Services and Avaya 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

These Application Notes describe the configuration steps required for Applied Network Intelligence (ANI) Trunk Dashboard to interoperate with Avaya Communication Manager and Avaya Application Enablement Services (AES). ANI Trunk Dashboard is a monitoring tool that uses Avaya AES to monitor up to 16 Avaya Communication Managers for any indication of a problem with Trunks. The Trunk Group monitoring is based on both snapshots of trunk group data and on 10-minute averages of trunk group usage information. The Dashboard also monitors for Major Alarms, Minor Alarms, DS1 Alarms, and CDR Link Alarms.

The overall objective of this testing is to verify the ANI Trunk Dashboard can interoperate with Avaya AES and Avaya Communication Manager.

Figure 1 provides the test configuration used for the compliance test. Note that actual configurations may vary.

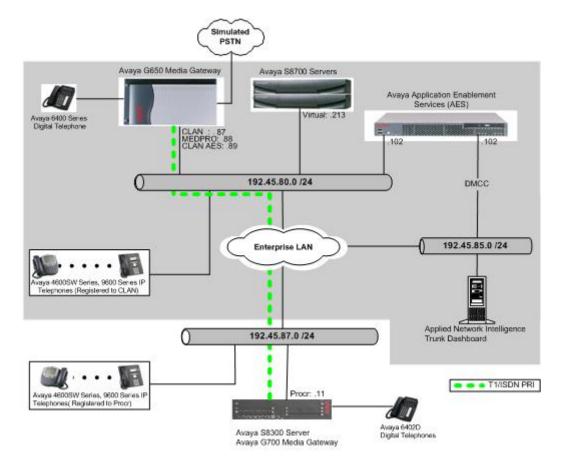


Figure 1: ANI Trunk Dashboard with Avaya Communication Manager and Avaya AES

2. Equipment and Software Validated

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

Equipment	Software/Firmware			
Avaya S8700 Servers	Avaya Communication Manager 4.0.1			
	(R014x.00.1.731.2)			
Avaya G650 Media Gateway				
TN2312BP IP Server Interface	HW11 FW030			
TN799DP CLAN Interface	HW01 FW017			
TN2302AP IP Media Processor	HW20 FW108			
Avaya S8300 Server	Avaya Communication Manager 4.0.1			
	(R014x.00.1.731.2)			
Avaya G700 Media Gateway	25.28.0			
Avaya Application Enablement Services	4.0 w/ Bundled Offer Build 47.3			
Avaya 4600 Series IP Telephones				
4620SW(H.323)	2.8			
4625SW (H.323)	2.8			
Avaya 9600 Series IP Telephones				
9630 (H.323)	1.5			
9650 (H.323)	1.5			
Avaya 6400D Series Digital Telephones	-			
Applied Network Intelligence Trunk	1.0			
Dashboard				

3. Configure Avaya Communication Manager

This section provides the procedures for configuring a T1 trunk, trunk group, and signal group on Avaya Communication Manager. The highlights in the following screens indicate the values used during the compliance test.

3.1. Configure T1/ISDN-PRI trunk

This section describes the steps for configuring the T1/ISDN-PRI trunk on Avaya Communication Manager. Enter the **list configuration all** command and note the Board Number for the DS1 circuit pack to be configured.

list con	figuration all								Pag	ge	3	
		SYSTEM CONF	IGURATION									
Board Number	Board Type	Code	Vintage	u=u	Ass: nassig	-				=psa		
01A10	DS1 INTERFACE	TN464F	000018		02 03							
				09	10 11	12	13	14	15	16		
				17	18 19	20	21	22	23	24		
				u	u u	u	u	u	u	u		

Enter the **add ds1 x** command, where **x** is the board number of the DS1 circuit pack noted previously. Enter a descriptive Name and set the other highlighted fields below to the values indicated.

add ds1 1a10		Page	1 (of	2	
		DS1 CIRCUIT PACK				
Location:	01A10	Name: ANI-test				
Bit Rate:	1.544	Line Coding: b8zs				
Line Compensation:	1	Framing Mode: esf				
Signaling Mode:	isdn-pri					
Connect:	pbx	Interface: user				
TN-C7 Long Timers?	n	Country Protocol: 1				
Interworking Message:	PROGress	Protocol Version: a				
Interface Companding:	mulaw	CRC? n				
Idle Code:	11111111					
	D	CP/Analog Bearer Capability: 3.1kHz				
		T303 Timer(sec): 4				

3.2. Configure Signaling Group

Enter the **add signaling-group s** command, where **s** is an unused signaling group number. Set the highlighted fields below to the values indicated. Note that the value for the Primary D-Channel field is set to channel 24 on the DS1 circuit pack for a T1.

```
add signaling-group 10 Page 1 of 1
SIGNALING GROUP
Group Number: 10 Group Type: isdn-pri
Associated Signaling? y Max number of NCA TSC: 10
Primary D-Channel: 01A1024 Max number of CA TSC: 10
Trunk Group for Channel Selection:
Supplementary Service Protocol: a
```

After the completion of the trunk group configuration in **Section 3.3**, enter the **change signaling-group s** command, where **s** is the number of the signaling group configured previously. Set the Trunk Group for Channel Selection field value to the trunk group number configured in **Section 3.3**.

```
change signaling-group 10 Page 1 of 1
SIGNALING GROUP
Group Number: 10 Group Type: isdn-pri
Associated Signaling? y Max number of NCA TSC: 10
Primary D-Channel: 01A1024 Max number of CA TSC: 10
Trunk Group for Channel Selection: 10
Supplementary Service Protocol: a
```

3.3. Configure Trunk Group

Enter the **add trunk-group t** command, where **t** is an unused trunk group number. On **Page 1** of the TRUNK GROUP form, enter a descriptive Group Name and enter a TAC that is valid under

CRK; Reviewed:	Solution & Interoperability Test Lab Application Notes	4 of 18
SPOC 2/15/2008	©2008 Avaya Inc. All Rights Reserved.	ANI-AES

the provisioned dial plan in Avaya Communication Manager. Set the other highlighted fields below to the values indicated.

add trunk-group 10		Page 1 of 21
	TRUNK GROUP	
Group Number: 10	Group Type: isdn	CDR Reports: y
Group Name: trunk-ANI	COR: 1	TN: 1 TAC: 111
Direction: two-way	Outgoing Display? n	Carrier Medium: PRI/BRI
Dial Access? n	Busy Threshold: 255	Night Service:
Queue Length: 0		
Service Type: tie	Auth Code? n	TestCall ITC: rest
	Far End Test Line No:	
TestCall BCC: 4		

On **Page 3**, set the highlighted fields below to the values indicated.

add trunk-group 10	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: internal
	Internal Alert? n Maintenance Tests? y
	Data Restriction? n NCA-TSC Trunk Member:
	Send Name: y Send Calling Number: y
Used for DCS? n	Send EMU Visitor CPN? n
Suppress # Outpulsing? n	Format: public
	UUI IE Treatment: service-provider
	Replace Restricted Numbers? n
	Replace Unavailable Numbers? n
	Send Connected Number: n
	Hold/Unhold Notifications? n
Send UUI IE? y	Modify Tandem Calling Number? n
Send UCID? n	
Send Codeset 6/7 LAI IE? y	

On **Page 5** of the trunk-group form, add trunk members by entering:

- **xxxxxzz** for Port, where **xxxxx** is the board number of the DS1 circuit pack configured in the SYSTEM CONFIGURATION form in **Section 3.1**, and **zz** is a channel in the T1/ISDN-PRI.
- The signaling group number configured in **Section 3.2** for the Sig Grp field.

For the compliance test, channels 1 - 15 and 16 - 23 (not shown) of the T1/ISDN-PRI were added. Channel 24, the Primary D-Channel configured in **Section 3.2**, was excluded.

add trunk-group 10			Page	5 of	21
	TRUNK GROUP				
		Administe	ered Members (min/max):	0/0	
GROUP MEMBER ASSIGNM	ENTS	Total	Administered Members:	0	
Port Code	Sfx Name	Night	Sig Grp		
1: 01A1001 TN464	F		10		
2: 01A1002 TN464	F		10		
3: 01A1003 TN464	F		10		
4: 01A1004 TN464	F		10		
5: 01A1005 TN464	F		10		
6: 01A1006 TN464	F		10		
7: 01A1007 TN464	F		10		
8: 01A1008 TN464	F		10		
9: 01A1009 TN464	F		10		
10: 01A1010 TN464	F		10		
11: 01A1011 TN464	F		10		
12: 01A1012 TN464	F		10		
13: 01A1013 TN464	F		10		
14: 01A1014 TN464	F		10		
15: 01A1015 TN464	F		10		

3.4. Configure Uniform Dialplan

Enter the **change uniform-dialplan d** command, where **d** is any digit that is valid under the provisioned dial plan. Enter the whole or a partial extension for the Matching Pattern field. Enter the length of the extension for the Len field. Set the Del field set to 0, and the Net field to **aar**.

change uniform-di	ialplan 4		Page	1 of 2		
UNIFORM DIAL PLAN TABLE						
					Percent	Full: 0
Matching		Insert		Node		
Pattern L	Len Del	Digits	Net Conv	r Num		
7	50		aar n			
			n			
			n			

3.5. Configure AAR

Enter the **change aar analysis d** command, where **d** is any digit that is valid under the provisioned dial plan. Enter the whole or a partial extension for the Dialed String field. Enter the number of an unused route pattern for the Route Pattern field. The route pattern will be defined in **Section 3.6**. The Call Type field is set to **aar**.

change aar analysis 444	AAR DIGIT A	ALYSIS TABLE	Page 1 of	2
	AAK DIGII A	ALISIS INDE	Percent Full:	2
Dialed	Total Rout	e Call Node		
String	Min Max Patte	rn Type Num	Reqd	
7	5 5 79	aar	n	

3.6. Configure Route Pattern

Enter the **change route-pattern r** command, where **r** is the number of the route pattern specified in **Section 3.5**. Enter the number of the trunk group configured in **Section 3.3** for the Grp No field. Assign a Facility Restriction Level to this routing preference for the FRL field. The FRL value is set to **0**, which is the least restrictive.

change route-pattern 79	Page 1 of 3
Pattern Number: 79 Pattern Name: Lyrix	
SCCAN? n Secure SIP? n	
Grp FRL NPA Pfx Hop Toll No. Inserted	DCS/ IXC
No Mrk Lmt List Del Digits	QSIG
Dgts	Intw
1: 10 0	n user
2:	n user
BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No	. Numbering LAR
0 1 2 3 4 W Request Dgt	s Format
Subadd	ress
1: yyyyn n rest	none
2: yyyyn n rest	none

3.7. Configure IP Services

Enter the **change node-names ip** command. Define node names for two CLANs. In the compliance-tested configuration, the CLAN IP address was utilized for registering H.323 endpoints, and the CLAN-AES IP address was used for connectivity to Avaya AES.

change node-nam	nes ip			Page	1 of	2
		IP NODE 1	JAMES			
Name	IP Address					
CLAN	192.45.80.87					
CLAN-AES	192.45.80.89					
MEDPRO	192.45.80.88					
S8300G700	192.45.87.11					
default	0.0.0.0					

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-s	ervices				Page	1 of	4	
			IP SERVICES					
Service	Enabled	Local	Local	Remote	Remote			
Туре		Node	Port	Node	Port			
AESVCS	У	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 run **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-ser	vices		Page	4 of	4	
		AE Services Administrat	tion			
Server ID	AE Services Server	Password	Enabled	Status		
1: 2:	server1	*****	У	idle		
3:						

4. Configure Avaya Application Enablement Services

Avaya AES enables Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Avaya Communication Manager. Avaya AES receives requests from CTI applications, and forwards them to Avaya Communication Manager. Conversely, Avaya AES 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 Avaya AES has been performed. The steps in this section describe configuring of a Switch Connection and creating a CTI user.

4.1. Configure Switch Connection

Launch a web browser, enter <u>https://<IP address of AES server>:8443/MVAP</u> in the URL, and log in with the appropriate credentials for accessing the AES CTI OAM pages.

Αναγα	
Application Enablement Services	? Hel
Please log on.	
Logon:	
Password:	
Login	
Login	

Select the **CTI OAM Admin** link from the left pane of the page.

Αναγα	Application Enablement Se Operations Administration and Mai
Home	You are here: > Home
<u>CTI OAM Admin</u> <u>User Management</u>	Welcome to OAM
	 The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains: CTI OAM Admin - Use CTI OAM Admin to manage all AE Services that you are licensed to use on the AE Server. User Management - Use User Management to manage AE Services users and AE Services user-related resources.
	Depending on your business requirements, these adminstrative domains can be served by one administrator for both domains, or a separate administrator for each domain.

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

Αναγα			on Enablement Services ons Administration and Maintenance
CTI OAM Home	You are here: > Administration_ > 9	witch Connections	OAM Home ?Help OLogout
 Administration 	Switch Connections		
Network Configuration	Switch Connections		
Switch Connections CTI Link Admin	S8700	Add Connection	
 <u>DMCC Configuration</u> <u>TSAPI Configuration</u> 	Connection Name	Number of Active Connections	Connection Type
Security Database Certificate Management	Edit Connection Edit CLAN IPs	Edit H.323 Gatekeeper	Delete Connection
TR87 Configuration Status and Control			
<u>Maintenance</u>			
<u>Alarms</u>			
▶ Logs			
 <u>Utilities</u> <u>Help</u> 			

The next window that appears prompts for the switch connection password. Select **CTI/Call Information** using the drop down menu on the Switch Connection Type field. Enter the same password that was administered on Avaya Communication Manager in **Section 3.7**. Default values may be used in the remaining fields. Click on **Apply**.

AVAYA		Application Enablement S Operations Administration and M	1ainte
CTI OAM Home	You are here: > <u>Administration</u> > S	Switch Connections	elp 🔘
 <u>Administration</u> <u>Network Configuration</u> 	Set Password - S8700		
Switch Connections CTI Link Admin DMCC Configuration TSAPI Configuration	Please note the following: * A password is not required for a H323 * Changing the password affects only n	3 Gatekeeper Connection. new connections, not open connections.	
Security Database	Switch Connection Type	CTI/Call Information 💌	
Certificate Management TR87 Configuration	Switch Password	*****	
<u>Status and Control</u>	Confirm Switch Password	*****	
 <u>Maintenance</u> <u>Alarms</u> Logs 	SSL Apply Cancel		

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

Αναγα		Application Enablement Serv Operations Administration and Maint		
CTI OAM Home	You are here: > <u>Administration</u> > <u>S</u>	Switch Connections	GOAM Home 🕜 Help 🔘	
 <u>Administration</u> <u>Network Configuration</u> 	Switch Connections			
Switch Connections CTI Link Admin		Add Connection		
 <u>DMCC Configuration</u> <u>TSAPI Configuration</u> 	Connection Name	Number of Active Connections	Connection Type	
Security Database	O \$8300G700	1		
<u>Certificate Management</u>	⊙ S8700	1	CTI/Call Information	
 TR87 Configuration Status and Control 	Edit Connection Edit CLAN IPs	Edit H.323 Gatekeeper	Delete Connection	

Enter the IP address of the CLAN used for AES connectivity from Section 3.7, and click on Add Name or IP.

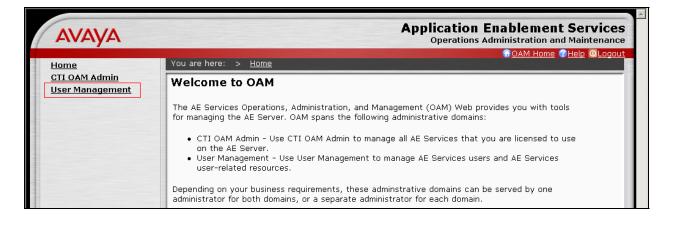
Αναγα	Application Enablement Services Operations Administration and Maintenance
CTI OAM Home	GOAM Home @Help Ologout You are here: > Administration > Switch Connections
<u>Network Configuration</u> Switch Connections	Edit CLAN IPs - \$8700
<u>CTI Link Admin</u> DMCC Configuration	192.45.80.89 Add Name or IP Name or IP Address Status
TSAPI Configuration Security Database	Delete IP
<u>Certificate Management</u> <u>TR87 Configuration</u>	
Status and Control Maintenance	
<u>Alarms</u> <u>Logs</u>	
 <u>Utilities</u> <u>Help</u> 	

4.2. Configure CTI User

The steps in this section describe the configuration of a CTI user. Launch a web browser, enter <u>https://<IP address of AES server>:8443/MVAP</u> in the URL, and log in with the appropriate credentials for accessing the OAM Home page.

AVAYA	
Application Enablement Services	? Help
Please log on.	
Logon:	
Password:	
Login	1

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 \rightarrow Add User page to add a CTI user.

AVAYA	Application Enablement Service: Operations Administration and Maintenanc
User Management Home	You are here: > User Management
✓ <u>User Management</u> List All Users	Welcome to User Management
Add User Search Users	User Management provides you with the following tools for managing AE Services users:
Modify Default User Change User Password Service Management Help	 List All Users Add User Search Users
• Help	Modify Default User Change User Password

On the Add User page, provide the following information:

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

Note: User ID and User Password must match with information configured in the **cmapi.properties** file in **Section 5**.

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

Αναγα		Application Enablement Services Operations Administration and Maintenance
and the second se	You are here: > <u>User Management</u> > <u>Add User</u> Add User Fields marked with * can not be empty * User Id ani	OAM Home O Help O Logout
User Management Home User Management List All Users Add User Search Users Modify Default User Change User Password Service Management Help	* Common Name ani * Surname ani * User Password ******* * Confirm Password ******* Admin Note Avaya Role None Business Category Car License CM Home Css Home	
	CT User Yes 💌 Department Number	

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

Αναγα						ion Enablement Servi tions Administration and Mainter	nance
CTI OAM Home Administration Network Configuration	You are here:		<u>stration > Se</u>	ecurity Databa	<u>se</u> > <u>CTI Use</u>	GOAM Home @Help @L ers_>_List ali users	ogout
Switch Connections CTI Link Admin DMCC Configuration TSAPI Configuration Security Database SDB Control CTI Users List All Users Search Users Worktops Devices Devices Tlinks	C C C C C C Edit List All	User ID access cmapi craft crkim ctiuser dssi ani	Common Na access cmapi craft crkim ctiuser dssi ani	ame Worktop N NONE NONE NONE NONE NONE NONE	lame Device ID NONE NONE NONE NONE NONE NONE		

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

Αναγα	Application Enablement Ser Operations Administration and Maint
CTI OAM Home Administration	@ <u>OAM Home</u> @Help @ You are here: > <u>Administration</u> > <u>Security Database</u> > <u>CTI Users</u> > <u>List All Users</u>
Administration Network Configuration Switch Connections CTI Link Admin DMCC Configuration TSAPI Configuration Security Database	Edit CTI User ani User ID ani Common Name ani Worktop Name NONE Unrestricted Access Enable
<u> CTI Users</u> <u> List All Users</u> <u> Search Users</u>	Call Origination and Termination None
<u>Worktops</u> Devices	Device / Device
<u>Device Groups</u> <u>Tlinks</u> <u>Tlink Groups</u>	Call / Device None Call / Call
<u>Certificate Management</u> <u>TR87 Configuration</u> <u>Status and Control</u>	Allow Routing on Listed Device None Apply Changes Cancel

5. Configure ANI Trunk Dashboard

ANI installs, configures, and customizes the Trunk Dashboard application for their end customers. For installation and configuration of the Trunk Dashboard, contact ANI technical support.

This section only illustrates the interface configuration of the Trunk Dashboard to communicate with Avaya AES utilizing DMCC service. The following shows the contents of the **cmapi.properties** file located in the **c:\Program Files\starfish\datacollector\config** directory.

- cmapi1.server_ip Enter the Client Connectivity IP address of AES.
- cmapi1.username Enter the CTI username configured in Section 4.2.
- cmapi1.password Enter the CTI password configured in Section 4.2.
- cmapil.server_port Enter the unencrypted DMCC server port. The default port, **4721**, was used during the compliance test.
- cmapi1.secure Since the unencrypted port was used, this field was set to false.

```
# CMAPI specific data.
cmapi1.server ip=192.45.85.102
cmapi1.username=ani
cmapi1.password=ani
cmapi1.server_port=4721
# Legal values for cmapil.secure are true and false.
cmapi1.secure=false
#cmapi.trust store location=C:\\Program Files\\starfish\\datacollector\\config\\avaya.jks
#Button specific data.
majorbutton=263
minorbutton=264
cdr1button=266
cdr2button=267
ds1button=265
nextbutton=285
# 3.1 to 4.0 transition related changes!
exitbutton=0
shared=false
waitfordisplayrefresh=0
restartcount=3
restartenable=false
```

6. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing evaluated the ability of ANI Trunk Dashboard to monitor and collect statistics of calls placed thru the trunk. The serviceability testing introduced failure scenarios to see if ANI Trunk Dashboard can resume recording after failure recovery.

6.1. General Test Approach

All test cases were performed manually. The general approach was to place trunk calls to and from stations. These trunk calls were monitored using ANI Trunk Dashboard, and trunk usage

CRK; Reviewed:	Solution & Interoperability Test Lab Application Notes	15 of 18
SPOC 2/15/2008	©2008 Avaya Inc. All Rights Reserved.	ANI-AES

statistics were verified. Alarms were manually created and verified using ANI Trunk Dashboard. For serviceability testing, failures such as cable pulls, busyouts and releases of the DS1 trunk group, and resets were applied.

6.2. Test Results

All test cases were executed and passed.

7. Verification Steps

This section provides the tests 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 ST	ATUS		
Srvr/ Link	AE Services Server	Remote IP	Remote Port	Local Node	Msgs Sent	Msgs Rcvd
01/01	serverl	192. 45. 80.102	36538	CLAN-AES	17	18

7.2. Verify Avaya Application Enablement Services

From the AES CTI OAM Admin web pages, verify the status of the DMCC Service by selecting **Status and Control** \rightarrow **Services Summary** from the left pane.

Αναγα	Application Enablement Services Operations Administration and Maintenance
CTI OAM Home <u>Administration</u> Status and Control	You are here: > <u>Status and Control</u> > <u>Services Summary</u>
 Status and Control Switch Conn Summary Services Summary Maintenance Alarms Logs Utilities Help 	Service Status Since Cause C CVLAN Service ONLINE 2007-12-12 20:47:41 NORMAL C DLG Service ONLINE 2007-12-12 20:47:36 NORMAL C TSAPI Service ONLINE 2007-12-12 20:47:43 NORMAL Image: C TSAPI Service ONLINE 2007-12-12 20:47:43 NORMAL Image: D DMCC Service ONLINE 2007-12-12 20:47:44 NORMAL

8. Support

Technical support on ANI Trunk Dashboard can be obtained through the following:

- **Phone:** (908) 203-4660 or (800) 771-6943
- Email: <u>info@starfishdevelopment.com</u>
- Web: <u>https://www.starfishdevelopment.com</u>

9. Conclusion

These Application Notes describe the configuration steps required for ANI Trunk Dashboard to interoperate with Avaya Communication Manager and Avaya Application Enablement Services. All feature and serviceability test cases were completed.

10. Additional References

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

 [1] Administrator Guide for Avaya Communication Manager, Document 03-300509, Issue 3.1, February 2007
 [2] Telecom Dashboard, Real-Time Monitoring of Trunk Performance

©2007 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by [®] and TM 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 <u>devconnect@avaya.com</u>.