



Avaya Solution & Interoperability Test Lab

Application Notes for the Amcom PC/PSAP, utilizing Amcom CTI Layer, with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services - Issue 1.0

Abstract

These Application Notes describe a compliance-tested configuration comprised of Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services, Avaya IP and Digital Telephones, and Amcom PC/PSAP desktop applications.

Amcom PC/PSAP is a Windows-based intelligent E911 workstation solution for a campus or municipality. Using the existing PBX telephone system as an “Automatic Number Identification (ANI)/Automatic Location Information (ALI) controller”, Amcom PC/PSAP eliminates the need for external proprietary switching solutions and is able to perform all necessary telephony functions from the call taker’s PC keyboard. Amcom PC/PSAP integrates with Amcom CTI Layer, which is a middleware between Amcom PC/PSAP and Avaya Aura® Application Enablement Services, to control and monitor phone states.

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 Avaya Aura® Communication Manager, Avaya Aura® Application Enablement Services, Avaya IP and Digital Telephones, and Amcom PC/PSAP applications.

Amcom Communications PC/PSAP is a PC and LAN based system, which allows Communication Manager to be used in a PSAP (Public Safety Answering Position – a physical location where 911 emergency telephone calls are received and then routed to the proper emergency services by the security agent or “911 operator” at the PSAP). Campuses or municipalities can set up a public or private PSAP using Amcom PC/PSAP, which has the capabilities to extract ANI (Automatic Number Identification – phone number of the caller) from Emergency 911 trunks and retrieve corresponding ALI (Automatic Location Information – information about the call based on the ANI such as name, phone number, address, nearest cross street, etc.). Amcom PC/PSAP integrates with Amcom CTI Layer, which is a middleware between Amcom PC/PSAP and Avaya Aura® Application Enablement Services, to control and monitor phone states.

It is the Amcom CTI Layer service that actually uses the Avaya Aura® Application Enablement Services Device and Media Call Control (DMCC) Application Programming Interface (API) to share control of and monitor a physical telephone and receive the same terminal and first party call information received by the physical telephone. Amcom PC/PSAP in turn uses the Amcom CTI Layer service to control and monitor a physical telephone. The PC/PSAP applications regularly provide the Database server with call and lamp state information concerning the controlled telephones.

2. General Test Approach and Test Results

The general approach was to exercise basic telephone and call operations on Avaya IP and Digital telephones using the aforementioned Amcom desktop application. The main objectives were to verify that:

- The user may successfully use PC/PSAP to perform off-hook, on-hook, dial, answer, hold, retrieve, transfer, conference, and release operations on the physical telephone.
- The agent user may successfully use PC/PSAP to log into and out of an ACD, and move between agent work modes.
- Manual operations performed on the physical telephone are correctly reflected in the PC/PSAP GUI.
- PC/PSAP and manual telephone operations may be used interchangeably; for example, go off-hook using PC/PSAP and manually dial digits.
- Display and call information on the physical telephone is accurately reflected in the PC/PSAP GUI.
- Call states are consistent between PC/PSAP and the physical telephone.

For serviceability testing, failures such as cable pulls and resets were applied. All test cases passed.

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 interoperability compliance test included features and serviceability. The focus of the compliance test was primarily on verifying the interoperability between Amcom PC/PSAP, Application Enablement Services, and Communication Manager.

2.2. Support

Technical support for the Amcom PC/PSAP solution can be obtained by contacting Amcom:

- URL – <http://amcomsoftware.com>
- Phone – (888) 797-7487

3. Reference Configuration

Figure 1 illustrates the configuration used in these Application Notes. The sample configuration shows an enterprise with an Application Enablement Services server and an Avaya S8300D Server running Communication Manager software with an Avaya G450 Media Gateway. The PC/PSAP was located in a different VLAN. Endpoints include Avaya 9600 Series H.323 IP Telephones and an Avaya 6408D Digital Telephone. Avaya S8720 Servers with an Avaya G650 Media Gateway was included in the test to provide an inter-switch scenario.

Note: Basic administration of Application Enablement Services server is assumed. For details, see [2].

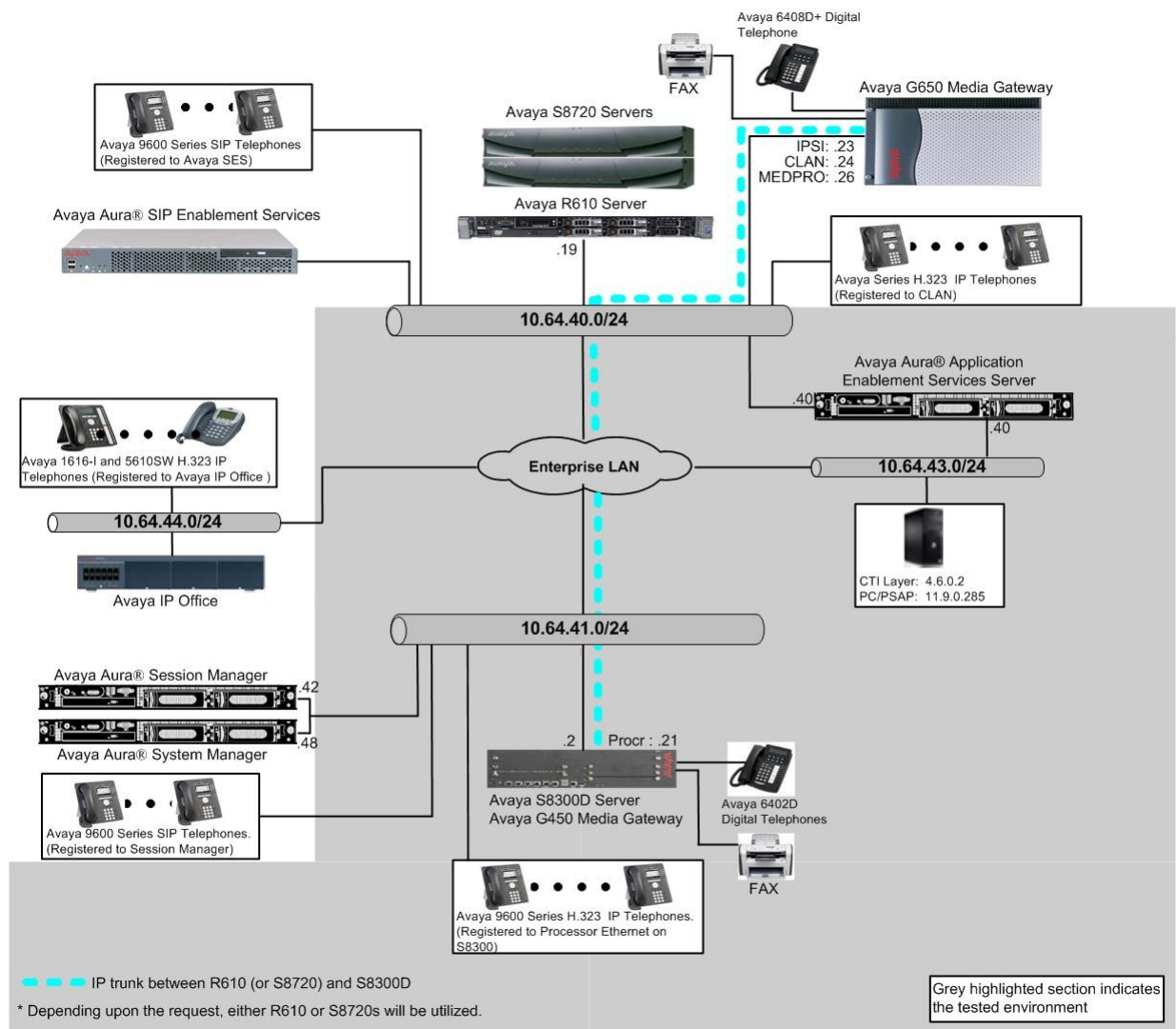


Figure 1: Amcom PC/PSAP Test Configuration.

4. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya Aura® Communication Manager running on Avaya S8300D Server with Avaya G450 Media Gateway		6.0.1(R016x.00.1.510.1) w/ patch 00.1.510.1-19303
Avaya Aura® Application Enablement Services running on Avaya S8800 Server		6.1.1 (r6-1-1-30-0)
Avaya Aura® Communication Manager running on Avaya S8720 Servers with Avaya G650 Media Gateway (<i>used for inter-switch test scenarios</i>)		5.2.1 (R015x.02.1.016.4)
Avaya 9600 Series IP Telephones		
	9620 (H.323)	3.1
	9630 (H.323)	3.1
	9650 (H.323)	3.1
Avaya 6408D+ Digital Telephone		-
Amcom CTO Layer		4.6.0.2
Amcom PC/PSAP		11.9.0.285

5. Configure Avaya Aura® Communication Manager

This section describes the procedures for configuring IP Services, Feature Access Codes, Abbreviated Dialing, and controlled telephones.

5.1. Configure IP Services

Notes: Section 5.1 was performed at the Avaya S8300D Server with an Avaya G450 Media Gateway side.

Enter the **change node-names ip** command. In the compliance-tested configuration, the procr IP address was used for registering H.323 endpoints, and for connectivity to Application Enablement Services.

change node-names ip		Page 1 of 1
IP NODE NAMES		
Name	IP Address	
aes	10.64.43.40	
procr	10.64.41.21	
procr6	::	

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 **procr** that was configured previously in the IP NODE NAMES form in this section. During the compliance test, the default port was used for the Local Port field.

change ip-services

Page1 of 4

IP SERVICES

Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port
AESVCS	y	procr	8765		
CDR1		procr	0	rdtt	9002

On **Page 4**, enter the hostname of the Application Enablement Services server for the AE Services Server field. The server name may be obtained by logging in to the Application Enablement Services 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 Application Enablement Services server in **Section 6.2**.

change ip-services				Page 4 of 4
AE Services Administration				
Server ID	AE Services Server	Password	Enabled	Status
1:	aes	*	y	idle
2:				

5.2. Configure Feature Access Codes (FAC)

Notes: Sections, 5.2, 5.3, 5.5, and 5.6, were performed at the Avaya S8720 Servers with an Avaya G650 Media Gateway side.

Enter the **change feature-access-codes** command. On **Page 1** of the FEATURE ACCESS CODE (FAC) form, verify the Auto Route Selection (ARS) – Access Code 1 field is set to **9**.

change feature-access-codes	Page 1 of 9
FEATURE ACCESS CODE (FAC)	
Abbreviated Dialing List1 Access Code: *01	
Abbreviated Dialing List2 Access Code: *02	
Abbreviated Dialing List3 Access Code: *03	
Abbreviated Dial - Prgm Group List Access Code: *04	
Announcement Access Code: *05	
Answer Back Access Code: #06	
Auto Alternate Routing (AAR) Access Code: 8	
Auto Route Selection (ARS) - Access Code 1: 9	
Access Code 2:	
Automatic Callback Activation: *09 Deactivation: #09	
Call Forwarding Activation Busy/DA: #11 All: *10 Deactivation: #10	

5.3. Configure Dialplan

Enter the **change dialplan analysis** command. Create a single digit dial string with 9 and associate it with **Feature Access Code (fac)**.

change dialplan analysis	Page 1 of 12							
DIAL PLAN ANALYSIS TABLE								
Percent Full: 1								
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type
0	1	attd	4	5	ext			
10	4	dac	5	5	ext			
11	3	dac	6	5	ext			
12	3	fac	7	5	ext			
126	6	aar	8	1	fac			
13	3	fac	9	1	fac			
14	3	fac	*	3	fac			
15	3	fac	#	3	fac			

5.4. Configure Hunt Group

Notes: Section 5.4 was performed at the Avaya S8300D Server with an Avaya G450 Media Gateway side.

Enter the **add hunt-group n** command, where **n** is an unused hunt group number. On **Page 1** of the HUNT GROUP form, assign a descriptive Group Name and Group Extension valid in the provisioned dial plan at the S8300D Server with a G450 Media Gateway side.

add hunt-group 11		Page 1 of 60
HUNT GROUP		
Group Number: 11	ACD? n	
Group Name: 911-hunt	Queue? n	
Group Extension: 72082	Vector? n	
Group Type: ucd-mia	Coverage Path:	
TN: 1	Night Service Destination:	
COR: 1	MM Early Answer? n	
Security Code:	Local Agent Preference? n	
ISDN/SIP Caller Display:		

On **Page 3**, add the 911 member extensions, which will be forwarded when a caller dials 911.

add hunt-group 11		Page 3 of 60
HUNT GROUP		
Group Number: 11	Group Extension: 72082	Group Type: ucd-mia
Member Range Allowed: 1 - 1500	Administered Members (min/max): 1 / 3	
Total Administered Members: 3		
GROUP MEMBER ASSIGNMENTS		
Ext	Name (24 characters)	Ext Name (24 characters)
1: 72001		14:
2: 72002		15:
3: 72003		16:
4:		17:
5:		18:

5.5. Configure Auto Route Selection (ARS)

Enter the **change ars analysis 11** command. When a caller dials 911, the first digit (9) indicates that it is an ARS call. Therefore, the next two digits (11) are utilized in the ARS table.

change ars analysis 11		Page 1 of 2
ARS DIGIT ANALYSIS TABLE		
Location: all		Percent Full: 1
Dialed String	Total Min Max	Route Pattern Call Type Node Num ANI Req
11	2 2	51 emer n
120	11 11	deny fnpa n
1200	11 11	deny fnpa n
121	11 11	deny fnpa n

5.6. Configure Route Pattern – Send 911 call to Hunt Group extension

Enter the **change route-pattern r** command, where r is a route-pattern number. In the following route-pattern, two digits (11) are removed and replace it with 72082 (Hunt Group extension). The extension, 72082, will be sent to the trunk group 51.

change route-pattern 51															Page 1 of 3																	
Pattern Number: 51 Pattern Name: temp-911																																
SCCAN? n Secure SIP? n																																
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted						DCS/	IXC																		
No			Mrk	Lmt	List	Del	Digits						QSIG																			
													Intw																			
1:	51	0					2	72082						n	user																	
2:													n	user																		
3:													n	user																		
BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR																																
0 1 2 3 4 W Request Dgts Format Subaddress																																
1:	y	y	y	y	y	n	n	rest								none																
2:	y	y	y	y	y	n	n	rest								none																
3:	y	y	y	y	y	n	n	rest								none																

5.7. Configure Route Pattern – Send 911 call to VDN extension

Another way to accomplish the 911 task is using ACD. In this case, the 911 call will be sent to 72072 (VDN extension) in previous route pattern form. When used ACD, the following sections, 5.8 and 5.9, need to be configured.

5.8. Configure Feature Access Code

Enter the **change feature-access-codes** command. On **Page 5** of the **feature-access-codes** form, configure and enable the following access codes:

- After Call Work Access Code
- Auto-In Access Code
- Aux Work Access Code
- Login Access Code
- Logout Access Code

change feature-access-codes															Page 5 of 11	
FEATURE ACCESS CODE (FAC)																
Call Center Features																
AGENT WORK MODES																
After Call Work Access Code: 120																
Assist Access Code: 121																
Auto-In Access Code: 122																
Aux Work Access Code: 123																
Login Access Code: 124																
Logout Access Code: 125																
Manual-in Access Code: 126																
SERVICE OBSERVING																
Service Observing Listen Only Access Code: 127																
Service Observing Listen/Talk Access Code: 128																
Service Observing No Talk Access Code: 129																
Service Observing Next Call Listen Only Access Code:																

5.9. Configure Abbreviated Dialing

Enter the **add abbreviated-dialing group g** command, where **g** is the number of an available abbreviated dialing group. In the **DIAL CODE** list, enter the Feature Access Codes for ACD Login and Logout from **Section 5.8**.

add abbreviated-dialing group 1		Page	1 of	1
ABBREVIATED DIALING LIST				
Group List: 1	Group Name: Call Center			
Size (multiple of 5): 5	Program Ext:		Privileged? n	
DIAL CODE				
11: 124				
12: 125				
13:				

5.10. Configure Controlled Telephones

Enter the **change station r** command, where **r** is the extension of a registered, physical Avaya IP or Digital telephone. On **Page 1** of the **station** form, enter a phone Type, descriptive name, Security Code and set IP SoftPhone field to **y** to allow the physical station to be controlled by a softphone such as the Amcom PC/PSAP application.

change station 72001		Page	1 of	5
STATION				
Extension: 72001	Lock Messages? n	BCC: 0		
Type: 9620	Security Code: *	TN: 1		
Port: S00002	Coverage Path 1:	COR: 1		
Name: Console-72001	Coverage Path 2:	COS: 1		
	Hunt-to Station:			
STATION OPTIONS				
Location:	Time of Day Lock Table:			
Loss Group: 19	Personalized Ringing Pattern: 1			
	Message Lamp Ext: 72001			
Speakerphone: 2-way	Mute Button Enabled? y			
Display Language: english				
Survivable GK Node Name:				
Survivable COR: internal	Media Complex Ext:			
Survivable Trunk Dest? y	IP SoftPhone? y			
IP Video Softphone? n				
Short/Prefixed Registration Allowed: default				
Customizable Labels? y				

On **Page 4** of the station form, for **ABBREVIATED DIALING List 2**, enter the abbreviated dialing group configured in **Section 5.8**. On **Pages 4** and **5** of the station forms, configure the following **BUTTON ASSIGNMENTS** in addition to the call-appr (call appearance) buttons:

- auto-in (on Page 4)
- aux-work (on Page 4)
- abrv-dial – configure two of these buttons, one for Login and one for Logout, along with the Dial Codes from Abbreviated Dialing List 2 for ACD Login and Logout, respectively (on Page 5)
- release (On Page 5)

```

change station 72001                                     Page 4 of 5
                                     STATION

SITE DATA
  Room: 1001                                           Headset? n
  Jack:                                              Speaker? n
  Cable:                                           Mounting: d
  Floor:                                           Cord Length: 0
  Building: Store1                                   Set Color:

ABBREVIATED DIALING
  List1: personal 1      List2: group      1      List3:

BUTTON ASSIGNMENTS
  1: call-appr                                4: brdg-appr B:2 E:72002
  2: call-appr                                5: auto-in      Grp:
  3: brdg-appr B:1 E:72002                    6: aux-work    RC:      Grp:

```

```

change station 72001                                     Page 5 of 5
                                     STATION

BUTTON ASSIGNMENTS
  7: abrv-dial List: 2 DC: 01      HL? n 10: ec500      Timer? n
  8: abrv-dial List: 2 DC: 02      HL? n 11: extnd-call
  9: release                        12:

```

Repeat the instructions provided in this section for each physical station that is to be controlled / monitored by an Amcom CTI Layer.

6. Configure Application Enablement Services

The Application Enablement Services server enables Computer Telephony Interface (CTI) applications to control and monitor telephony resources on Communication Manager.

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

6.1. Device and Media Call Control API Station Licenses

The Amcom PC/PSAP Service instances appear as “virtual” stations/softphones to Communication Manager. Each of these virtual stations, hereafter called Device and Media Call Control API station, requires a license. Note that this is separate and independent of Avaya IP Softphone licenses, which are required for Avaya IP Softphones but not required for Device and Media Call Control API stations. To check and verify that there are sufficient DMCC licenses, log in to <https://<IP address of the Application Enablement Services server>/index.jsp>, and enter appropriate login credentials to access the Application Enablement Services Management Console page.

Select the **Licensing** → **WebLM Server Access** link from the left pane of the window.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Thu Dec 1 14:28:33 2011 from 10.64.43.10
HostName/IP: aes.avaya.com/10.64.43.40
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-1-30-0

Licensing Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▼ **Licensing**
 - WebLM Server Address
 - WebLM Server Access**
 - Reserved Licenses
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

Licensing

If you are setting up and maintaining the WebLM, you need to use the following:

- WebLM Server Address

If you are importing, setting up and maintaining the license, you need to use the following:

- WebLM Server Access

If you want to administer TSAPI Reserved Licenses or DMCC Reserved Licenses, you need to use the following:

- Reserved Licenses

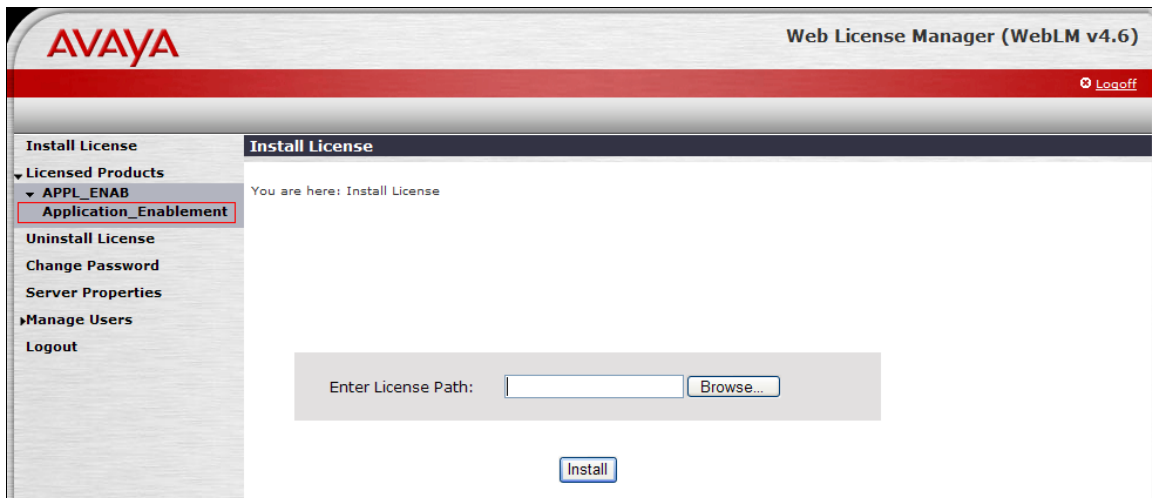
NOTE: Please disable your pop-up blocker if you are having difficulty with opening this page

Provide appropriate login credentials to access the Web License Manager page.



The image shows the login page of the Avaya Web License Manager (WebLM v4.6). The page has a red header with the Avaya logo and the text "Web License Manager (WebLM v4.6)". Below the header, the word "Login" is centered. There are two input fields: "User Name:" and "Password:". A gray button with a right-pointing arrow is located below the password field.

On the Install License page, select **License Products** → **Application_Enablement** link from the left pane of the window.



The image shows the "Install License" page of the Avaya Web License Manager (WebLM v4.6). The page has a red header with the Avaya logo and the text "Web License Manager (WebLM v4.6)". A "Logout" link is in the top right corner. On the left, there is a navigation pane with the following items: "Install License", "Licensed Products" (expanded), "APPL_ENAB" (expanded), "Application_Enablement" (highlighted with a red box), "Uninstall License", "Change Password", "Server Properties", "Manage Users", and "Logout". The main content area has a breadcrumb "You are here: Install License". Below this, there is a text input field labeled "Enter License Path:" with a "Browse..." button next to it. At the bottom, there is an "Install" button.

On the Licensed Features page, verify that there are sufficient DMCC licenses.

Web License Manager (WebLM v4.6)

[Logoff](#)

Install License

Licensed Products

APPL_ENAB

Application Enablement

Uninstall License

Change Password

Server Properties

Manage Users

Logout

Application Enablement (CTI) - Release: 6 - SID: 10503000 (Standard License File)

You are here: Licensed products > Application Enablement (CTI)

License installed on: Jun 2, 2011 9:55:08 AM MDT

[View Peak Usage](#)

Licensed Features

Feature (Keyword)	Expiration Date	Licensed	Acquired
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	16	0
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	1000	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	3	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	16	0
Product Notes (VALUE_NOTES)	permanent	SmallServerTypes: s8300c;s8300d;icc;premio;tn8400;laptop;CtiSmallServer MediumServerTypes: ibmx306;ibmx306m;dell1950;xen;hs20;hs20_8832_vm;CtiMediumServer LargeServerTypes: isp2100;ibmx305;d1380g3;d1385g1;d1385g2;unknown;CtiLargeServer TrustedApplications: IPS_001, BasicUnrestricted, AdvancedUnrestricted, DMCCUnrestricted; 1XP_001, BasicUnrestricted, AdvancedUnrestricted, DMCCUnrestricted; 1XM_001, BasicUnrestricted, AdvancedUnrestricted, DMCCUnrestricted; PC_001, BasicUnrestricted, AdvancedUnrestricted, DMCCUnrestricted; CIE_001, BasicUnrestricted, AdvancedUnrestricted, DMCCUnrestricted; OSCP_001, BasicUnrestricted, AdvancedUnrestricted, DMCCUnrestricted; VP_001, BasicUnrestricted, AdvancedUnrestricted, DMCCUnrestricted; SAMETIME_001, VALUE_AES_UNIFIED_CC_DESKTOP,; CCE_001, BasicUnrestricted, AdvancedUnrestricted, DMCCUnrestricted; CSI_T1_001, BasicUnrestricted, AdvancedUnrestricted, DMCCUnrestricted; CSI_T2_001, BasicUnrestricted, AdvancedUnrestricted, DMCCUnrestricted; AVAYAVERINT_001, BasicUnrestricted, AdvancedUnrestricted, DMCCUnrestricted;	Not counted
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	3	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	1000	0
DLG (VALUE_AES_DLG)	permanent	16	1
Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	1000	8
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	permanent	3	0

6.2. Configure Switch Connection

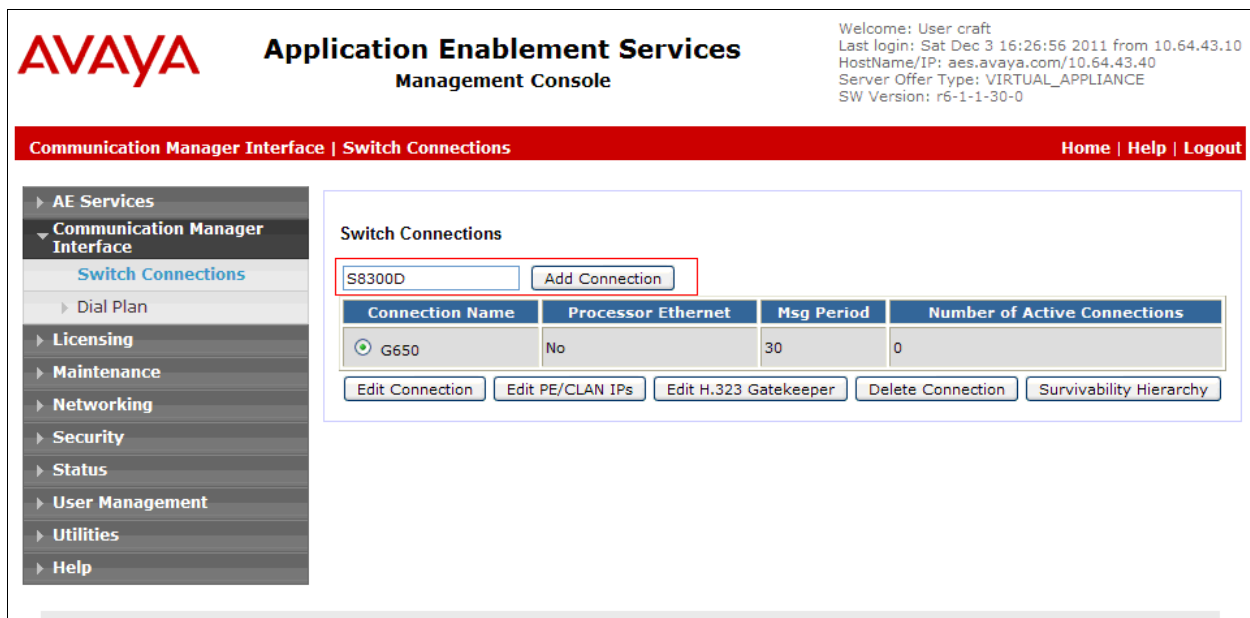
Launch a web browser, enter <https://<IP address of the Application Enablement Services server>> in the address field, and log in with the appropriate credentials for accessing the Application Enablement Services Management Console pages.

The screenshot shows the login page of the Application Enablement Services Management Console. At the top, the title "Application Enablement Services Management Console" is displayed in bold black text. Below the title is a red horizontal bar. In the center, there is a light gray box with a blue border containing the login form. The form includes the text "Please login here:" followed by two input fields labeled "Username" and "Password". Below these fields is a "Login" button.

Click on **Communication Manager Interface** → **Switch Connection** in the left pane to invoke the Switch Connections page.

The screenshot shows the home page of the Application Enablement Services Management Console. The top header features the Avaya logo and the title "Application Enablement Services Management Console". To the right of the title, there is a welcome message: "Welcome: User craft", "Last login: Sat Dec 3 16:26:56 2011 from 10.64.43.10", "HostName/IP: aes.avaya.com/10.64.43.40", "Server Offer Type: VIRTUAL_APPLIANCE", and "SW Version: r6-1-1-30-0". Below the header is a red navigation bar with "Home" on the left and "Home | Help | Logout" on the right. On the left side, there is a vertical menu with the following items: "AE Services", "Communication Manager Interface" (highlighted with a red border), "Licensing", "Maintenance", "Networking", "Security", "Status", "User Management", "Utilities", and "Help". The main content area on the right is titled "Welcome to OAM" and contains a paragraph: "The AE Services Operations, Administration, and Management (OAM) Web provides you with tools for managing the AE Server. OAM spans the following administrative domains:". This is followed by a bulleted list of administrative domains and their functions: "AE Services - Use AE Services to manage all AE Services that you are licensed to use on the AE Server.", "Communication Manager Interface - Use Communication Manager Interface to manage switch connection and dialplan.", "Licensing - Use Licensing to manage the license server.", "Maintenance - Use Maintenance to manage the routine maintenance tasks.", "Networking - Use Networking to manage the network interfaces and ports.", "Security - Use Security to manage Linux user accounts, certificate, host authentication and authorization, configure Linux-PAM (Pluggable Authentication Modules for Linux) and so on.", "Status - Use Status to obtain server status infomations.", "User Management - Use User Management to manage AE Services users and AE Services user-related resources.", "Utilities - Use Utilities to carry out basic connectivity tests.", and "Help - Use Help to obtain a few tips for using the OAM Help system". At the bottom of the main content area, there is a paragraph: "Depending on your business requirements, these administrative domains can be served by one administrator for both domains, or a separate administrator for each domain."

A Switch Connection defines a connection between the Application Enablement Services server and Communication Manager. Enter a descriptive name for the switch connection and click on **Add Connection**.



AVAYA Application Enablement Services Management Console

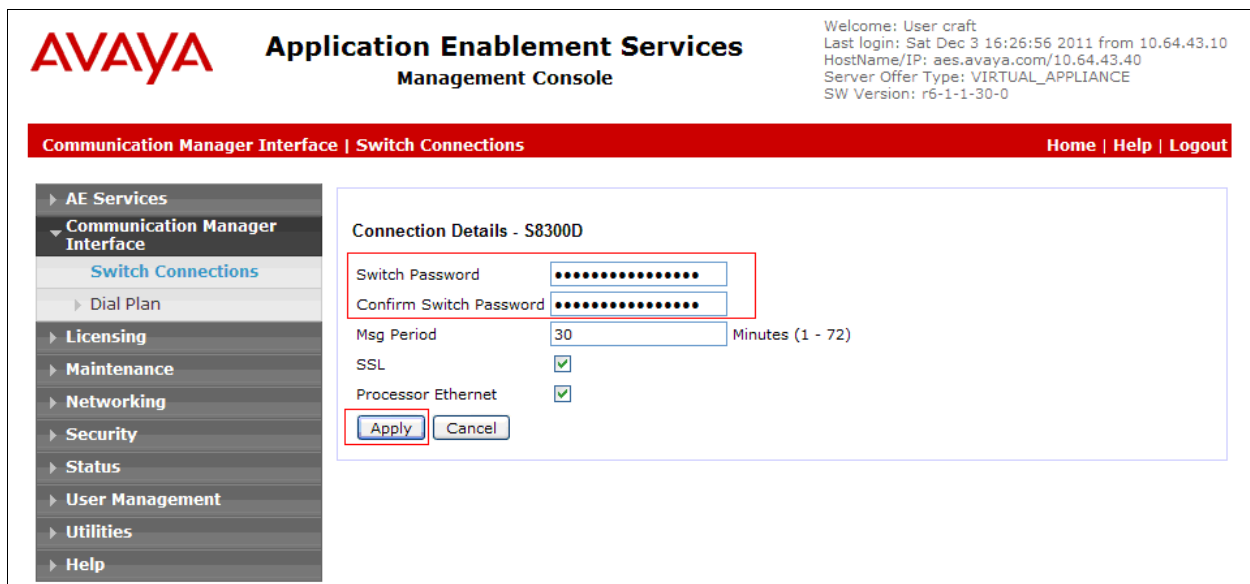
Welcome: User craft
Last login: Sat Dec 3 16:26:56 2011 from 10.64.43.10
HostName/IP: aes.avaya.com/10.64.43.40
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-1-30-0

Communication Manager Interface | Switch Connections [Home](#) | [Help](#) | [Logout](#)

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
G650	No	30	0

The next window that appears prompts for the Switch Password. Enter the same password that was administered in Communication Manager in **Section 5.1**. Click on **Apply**.



AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Sat Dec 3 16:26:56 2011 from 10.64.43.10
HostName/IP: aes.avaya.com/10.64.43.40
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-1-30-0

Communication Manager Interface | Switch Connections [Home](#) | [Help](#) | [Logout](#)

Connection Details - S8300D

Switch Password

Confirm Switch Password

Msg Period Minutes (1 - 72)

SSL ☒

Processor Ethernet ☒

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

Communication Manager Interface | Switch Connections Home | Help | Logout

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> S8300D	No	30	0


Enter the IP address of Procr used for Application Enablement Services connectivity from **Section 5.1**, and click on **Add Name or IP**.

Communication Manager Interface | Switch Connections Home | Help | Logout

Edit CLAN IPs - S8300D

Name or IP Address	Status
--------------------	--------

After returning to the Switch Connections page, select the radio button corresponding to the switch connection added previously, and click on the **Edit H.323 Gatekeeper** button for DMCC call control and monitor.



Application Enablement Services
Management Console

Welcome: User craft
Last login: Sat Dec 3 16:26:56 2011 from 10.64.43.10
HostName/IP: aes.avaya.com/10.64.43.40
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-1-30-0


Communication Manager Interface | Switch Connections
Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Switch Connections

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input type="radio"/> G650	No	30	0
<input checked="" type="radio"/> S8300D	Yes	30	1

On the **Edit H.323 Gatekeeper – S8300D** page, enter the procr IP address which will be used for the DMCC service. Click on **Add Name or IP**.



Application Enablement Services
Management Console

Welcome: User craft
Last login: Sat Dec 3 16:26:56 2011 from 10.64.43.10
HostName/IP: aes.avaya.com/10.64.43.40
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-1-30-0

Communication Manager Interface | Switch Connections
Home | Help | Logout

AE Services
Communication Manager Interface
Switch Connections
Dial Plan
Licensing
Maintenance
Networking
Security
Status
User Management
Utilities
Help

Edit H.323 Gatekeeper - S8300D

Name or IP Address

6.3. Configure the CTI Users

Navigate to **User Management** → **User Admin** → **Add User** link from the left pane of the window. 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 Amcom PC/PSAP Configuration page in **Section 7**.

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.

The screenshot displays the Avaya Application Enablement Services Management Console. The top header includes the Avaya logo, the title 'Application Enablement Services Management Console', and a welcome message for 'User craft' with login details. A red navigation bar contains links for 'User Management', 'User Admin', 'Add User', 'Home', 'Help', and 'Logout'. The left sidebar shows a tree view with 'User Management' expanded, and 'User Admin' and 'Add User' highlighted. The main content area is titled 'Add User' and contains a form with the following fields: '* User Id' (Amcom), '* Common Name' (Amcom), '* Surname' (Amcom123&), '* User Password' (masked), '* Confirm Password' (masked), 'Admin Note' (empty), 'Avaya Role' (None), 'Business Category' (empty), 'Car License' (empty), 'CM Home' (empty), 'Css Home' (empty), 'CT User' (Yes), 'Department Number' (empty), 'Display Name' (empty), and 'Employee Number' (empty). A red box highlights the first five fields, and another red box highlights the 'CT User' field.

Welcome: User craft
Last login: Sat Dec 3 16:26:56 2011 from 10.64.43.10
HostName/IP: aes.avaya.com/10.64.43.40
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-1-30-0

User Management | User Admin | Add User Home | Help | Logout


Add User

Fields marked with * can not be empty.

* User Id: Amcom
* Common Name: Amcom
* Surname: Amcom123&
* User Password:
* Confirm Password:

Admin Note:
Avaya Role: None
Business Category:
Car License:
CM Home:
Css Home:
CT User: Yes
Department Number:
Display Name:
Employee Number:

Once the user is created, navigate to the **Security → Security Database → CTI Users → List All Users** link from the left pane of the window. Select the User ID created previously, and click the **Edit** button to set the permission of the user.


Application Enablement Services
Management Console

Welcome: User craft
Last login: Sat Dec 3 16:26:56 2011 from 10.64.43.10
HostName/IP: aes.avaya.com/10.64.43.40
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-1-30-0

Security | Security Database | CTI Users | List All Users
Home | Help | Logout

▶ AE Services
▶ Communication Manager Interface
▶ Licensing
▶ Maintenance
▶ Networking
▼ Security
▶ Account Management
▶ Audit
▶ Certificate Management
Enterprise Directory
▶ Host AA
▶ PAM
▼ Security Database
▪ Control
▣ CTI Users
▪ List All Users

CTI Users

User ID	Common Name	Worktop Name	Device ID
amcom	Amcom123&	NONE	NONE

Edit
List All

Provide the user with unrestricted access privileges by checking the **Unrestricted Access** checkbox. Click on the **Apply Changes** button.

AVAYA

Application Enablement Services
Management Console

Welcome: User craft
Last login: Sat Dec 3 16:26:56 2011 from 10.64.43.10
HostName/IP: aes.avaya.com/10.64.43.40
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-1-30-0

Security | Security Database | CTI Users | List All Users

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▶ Networking

▼ Security

▶ Account Management

▶ Audit

▶ Certificate Management

Enterprise Directory

▶ Host AA

▶ PAM

▼ Security Database

▪ Control

▣ CTI Users

▪ List All Users

Edit CTI User

User Profile:

User IDamcom

Common NameAmcom123&

Worktop NameNONE

Unrestricted Access☒

Call and Device Control:

Call Origination/Termination and Device StatusNone

Call and Device Monitoring:

Device MonitoringNone

Calls On A Device MonitoringNone

Call Monitoring☐

Routing Control:

Allow Routing on Listed DevicesNone

Apply ChangesCancel Changes

6.4. Configure the DMCC Port

Navigate to the **Networking → Ports** link, from the left pane of the window, 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.

AVAYA **Application Enablement Services**
Management Console

Welcome: User craft
Last login: Sat Dec 3 16:26:56 2011 from 10.64.43.10
HostName/IP: aes.avaya.com/10.64.43.40
Server Offer Type: VIRTUAL_APPLIANCE
SW Version: r6-1-1-30-0

Networking | Ports

Home | Help | Logout

▶ AE Services

▶ Communication Manager Interface

▶ Licensing

▶ Maintenance

▼ Networking

AE Service IP (Local IP)

Network Configure

Ports

TCP Settings

▶ Security

▶ Status

▶ User Management

▶ Utilities

▶ Help

Ports

CVLAN Ports

Unencrypted TCP Port9999Enabled Disabled

Encrypted TCP Port9998Enabled Disabled

DLG PortTCP Port5678

TSAPI Ports

TSAPI Service Port450Enabled Disabled

Local TLINK Ports

TCP Port Min1024

TCP Port Max1039

Unencrypted TLINK Ports

TCP Port Min1050

TCP Port Max1065

Encrypted TLINK Ports

TCP Port Min1066

TCP Port Max1081

DMCC Server Ports

Unencrypted Port4721Enabled Disabled

Encrypted Port4722Enabled Disabled

TR/87 Port4723Enabled Disabled

7. Configure Amcom PC/PSAP

Amcom installs, configures, and customizes the PC/PSAP applications for their end customers. Amcom PC/PSAP integrates with Amcom CTI Layer, which is a middleware between Amcom PC/PSAP and Application Enablement Services, to control and monitor the phone states. Thus, only the Amcom CTI layer will be discussed in these Application Notes.

The following shows the **Amcom AES CTI Services Setup** page. Provide the following information:

Under DMCC Settings

- **AES Server** – Enter the IP address of the Application Enablement Services server.
- **Switch IP Address** – Enter the procr IP address of Avaya S8300D server.
- **Port** – Enter the DMCC port (4721).
- **User** – Enter the user name created for Amcom PC/PSAP in **Section 6.3**.
- **Password** – Enter the password created for Amcom PC/PSAP in **Section 6.3**.

Under Phone Device Settings

- **Extension** – Enter the extension that will be controlled by the Amcom PC/PSAP.
- **Security Code** – Enter the security code for the controlled station.
- **Release Button** – Enter the Release button assigned for the controlled station.
- **Line Appearances** – Enter the line appearances used for the controlled station.

The screenshot displays the 'Amcom AES CTI Service Setup' window, which is divided into four main sections: DMCC Settings, Phone Device Settings, Service Settings, and Debug Settings. The DMCC Settings section includes fields for AES Server (10.64.43.40), Switch Name, Switch IP Address (10.64.41.21), Port (4721), Application Id (1123), User (amcom), Password, Media Mode (No Media), Shared Control (False), Dependency Mode (Dependent), AES Version (6.1), and Telecommuter Extension. The Phone Device Settings section includes fields for Extension (72001), Security Code (****), RLT Transfer Button Id, Release Button Id (9), and Toggle-Swap Button Id. The Line Appearances section shows a table with Line 1 (Button id = 1), Line 2 (Button id = 2), Line 3 (Button id = 3), and Line 4 (Button id = 4). The Service Settings section includes fields for Listener Port (973), Home Directory (c:\Program Files\Amcom), Configuration File Name (cmapi.cfg), DLL File Name (C:\Program Files\Amcom\bin\amcom_cmapi.dll), LUA Agent Function File, LUA Agent State File, and LUA App Specific File. The Debug Settings section includes fields for File Name (Amcom_CTI_services), Number of Files (10), File Size (10000), Directory (c:\program files\amcom\trace), and a list of log levels (Level 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048) with checkboxes. The bottom of the window features a status bar with buttons for OK, Cancel, Restart Service, Phone Server, and Smart Console.

8. Verification Steps

The following steps may be used to verify the configuration:

- From the Amcom client computers, ping IP interfaces, in particular the Application Enablement Services server, and verify connectivity.
- For the physical IP telephones, verify that the physical telephones are registered by using the **list registered-ip-stations** command on the Communication Manager System Access Terminal (SAT). For the physical Digital telephones, verify that the telephones are attached to the correct ports.
- Go off-hook and on-hook on the controlled telephones manually and use PC/PSAP to verify consistency.
- Place and answer calls from the controlled telephones manually and use PC/PSAP to verify consistency.

9. Conclusion

These Application Notes described a compliance-tested configuration comprised of Communication Manager, Application Enablement Services, Avaya IP and Digital Telephones, and the Amcom PC/PSAP application. Amcom PC/PSAP allows a user to operate a physical telephone and view call and telephone display information through a graphical user interface (GUI). During compliance testing, calls were successfully placed to and from Avaya IP and Digital Telephones that were controlled and monitored by the Amcom PC/PSAP application.

10. Additional References

Product documentation for Avaya products may be found at <http://support.avaya.com>.

[1] *Administering Avaya Aura™ Communication Manager, Release 6.0, 03-300509, Issue 6.0, June 2010*, available at <http://support.avaya.com>

[2] Avaya Aura® Application Enablement Services Administration and Maintenance Guide, Release 6.1, Issue 2, February 2011, available at <http://support.avaya.com>.

Product information for Amcom products may be found at <http://www.amcomsoft.com/products.cfm>.

©2012 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.