



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Aura® Application Enablement Services R6.3 and Avaya Aura® Communication Manager R6.3 with Enghouse Interactive CT Connect using TSAPI – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for Enghouse Interactive CT Connect to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services using the Telephony Service API (TSAPI) interface. Enghouse Interactive CT Connect is a Computer Telephony Integration (CTI) middleware platform that provides call control and monitoring functionality through various application programming interfaces to end user applications.

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

Enghouse Interactive CT Connect is computer telephony call control server software capable of connecting a variety of TDM and VoIP telephone switches to distributed computer application environments.

Enghouse CT Connect can implement one of two mechanisms to integrate with Avaya Aura® Communication Manager, via Avaya Aura® Application Enablement Services (AES).

- Avaya Telephony Service API (TSAPI) interface
- Avaya Adjunct Switch Application Interface (ASAI) protocol

This document focuses on integration using TSAPI. Enghouse Interactive CT Connect implements TSAPI to provide Computer Telephony Integration (CTI) call control and monitoring functionality and application programming interfaces to end user business applications.

2. General Test Approach and Test Results

The general test approach was to validate the ability of CT Connect to correctly and successfully connect to Application Enablement Services and handle and control various Communication Manager endpoints in a variety of call scenarios.

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

Interoperability compliance testing consisted of using CT Connect to verify successful handling and control of a variety of endpoints as follows:

- Assign, unassign on devices and call monitor channels
- Make/answer internal/external incoming/outgoing call
- Hangup call
- Cancel call
- Snapshot to view current status of endpoint
- Display endpoint information
- Send DTMF
- Deflect call, Call Forward
- Enable/disable Do Not Disturb
- Hold/retrieve and reconnect
- Set, enable and disable call forwarding
- Attended transfer
- Blind transfer

- Swap calls
- Conferencing
- Single step conferencing
- Single step transfer
- Predictive calls
- Call pickup
- Obtain ACD status
- Obtain agent status
- Call Routing
- Obtain Global Reference Id
- Selective listen in conference
- Illuminate/extinguish message waiting indicator

2.2. Test Results

All test cases were executed successfully with the following observations:

- In the case of a supervised conference call where A calls B, A puts B on hold in order to conference in C, and B incorrectly attempts to retrieve the call, the call between A and B disconnects. This is acknowledged as unlikely to occur during implementation as only the relevant call handling features would be presented to the agent through the GUI.

2.3. Support

For technical support on Enghouse Interactive CT Connect products, please visit the website at <http://enghouseinteractive.com/> or contact an authorized Enghouse representative at info.ei@enghouse.com or via Tel: +44 203 357 3040

3. Reference Configuration

Figure 1 below shows Avaya Aura® Communication Manager R6.3 (serving H.323 endpoints with an Avaya G430 Media Gateway) was configured with Avaya Aura® Application Enablement Services R6.3 hosted on VMware providing a TSAPI interface to which the EngHouse Interactive CT Connect application connects. Avaya Aura® Session Manager R6.3 provides the point of registration for Avaya SIP endpoints. Avaya Aura® System Manager Server provides a means to manage and configure Session Manager. All of these applications were hosted on VMware ESXi 5.0 infrastructure.

Note: For the purposes of the compliance test the CtcTest application was used to validate the functions of CT Connect.

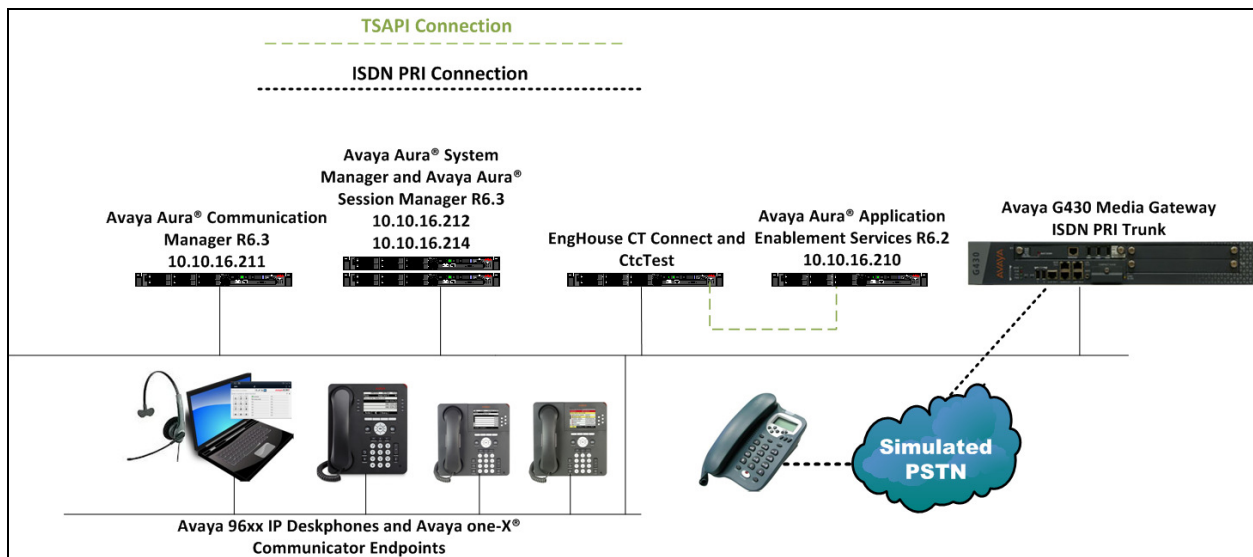


Figure 1: Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services with EngHouse Interactive CT Connect Solution

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager Virtual Appliance	R6.3 SP0.1
Avaya Aura® Application Enablement Services Virtual Appliance	R6.3
Avaya Aura® System Manager Virtual Appliance	R6.3.2 Patch 1
Avaya Aura® Session Manager Virtual Appliance	R6.3 SP2
Avaya G430 Media Gateway <ul style="list-style-type: none">• MM710	33.13.0 <ul style="list-style-type: none">• HW5 FW22
Avaya 9640 IP Deskphone	SIP 2.6.10.1
Avaya 9630 IP Deskphone	H323 3.2
Avaya 9608 IP Deskphone	SIP 6.2.1.26
Avaya one-X® Communicator	6.1704
EngHouse Syntellect CT Connect and CtcTest Tool	8.0.324.0

5. Configure Avaya Aura® Communication Manager

The configuration and verification operations illustrated in this section are performed using the Communication Manager System Access Terminal (SAT). The information provided in this section describes the configuration of Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation as referenced in **Section 10**. The configuration operations described in this section can be summarized as follows:

- Configure Interface to Avaya Aura® Application Enablement Services
- Configure Call Center Features
- Configure SIP Endpoints for Third Party Call Control

5.1. Configure Interface to Avaya Aura® Application Enablement Services

Enter the command **change node-names ip** and enter the node **Name** and **IP Address** for Application Enablement Services, in this case **AES63RP** and **10.10.16.170** respectively. Take a note of the **procr** node **Name** and **IP Address** as it is used later in this section.

```
change node-names ip                                     Page 1 of 2
                                                    IP NODE NAMES
  Name          IP Address
AES63RP      10.10.16.210
SM63RPSIG      10.10.16.214
default        0.0.0.0
procr        10.10.16.211
procr6         ::
```

In order for Communication Manager to establish a connection to Application Enablement Services, administer the CTI Link by entering the command **add cti-link n** as shown below. Take a note of the **CTI Link** number, specify an available **Extension** number, set the **Type** as **ADJ-IP**, which denotes that this is a link to an IP connected adjunct, and name the link for easy identification, in this instance, the node-name is used.

```
add cti-link next                                     Page 1 of 3
                                                    CTI LINK
  CTI Link: 1
Extension: 1999
  Type: ADJ-IP
                                                    COR: 1
  Name: aes63rp
```

Configure IP-Services for the AESVCS service using the **change ip-services** command and configure as follows:

- **Service Type** – enter **AESVCS**
- **Enabled** – ensure this is set to **y**
- **Local Node** – set to the **procr** node name noted above

change ip-services			IP SERVICES			Page 1 of 4
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port	
AESVCS	y	procr	8765			

Navigate to **Page 4**, set the **AE Services Server** node-name and the **Password** AES will use to authenticate with Communication Manager, ensure **Enabled** is set to **y**.

change ip-services			AE Services Administration		Page 4 of 4
Server ID	AE Services Server	Password	Enabled	Status	
1:	aes62vm	Avaya1234567	y	in use	

5.2. Configure Call Center Features

For the purposes of the Predictive Call feature and ACD functionality of CT Connect, the following must be configured:

- Configure Hunt Group
- Configure Vector
- Configure Vector Directory Number (VDN)
- Configure Agents

5.2.1. Configure Hunt Group

Enter the command **add hunt-group x** where **x** is an appropriate hunt group number and configure as follows:

- **Group Number** – this is used as the Skill Number when configuring the agent and vector
- **Group Name** – enter an appropriate name
- **Group Extension** – enter an extension appropriate to the dialplan. This is used for the ACD monitor feature of CT Connect
- **Group Type** – set to **ead-mia**
- **ACD?** – set to **y**
- **Queue?** – set to **y**
- **Vector?** – set to **y**

```
add hunt-group 2000                                     Page 1 of 4
                                                    HUNT GROUP
      Group Number: 2000                                ACD? y
      Group Name: HuntGroup For EngHouse                Queue? y
      Group Extension: 1992                             Vector? y
      Group Type: ead-mia
                TN: 1
                COR: 1                                MM Early Answer? n
      Security Code:                                    Local Agent Preference? n
ISDN/SIP Caller Display:

      Queue Limit: unlimited
Calls Warning Threshold:      Port:
Time Warning Threshold:      Port:
```

On Page 2, set **Skill** to **y**.

```
change hunt-group 2000                                 Page 2 of 4
                                                    HUNT GROUP
      Skill? y                                           Expected Call Handling Time (sec): 180
      AAS? n
      Measured: none
Supervisor Extension:

      Controlling Adjunct: none

      Multiple Call Handling: none

Timed ACW Interval (sec):      After Xfer or Held Call Drops? n
```


5.2.2. Configure Vector

Enter the command **change vector x** where **x** is the required vector number. Configure as shown below so that calls **queue-to skill 2000**. Skill 2000 is the hunt group configured in the previous section.

```
change vector 2000                                     Page 1 of 6
                                                    CALL VECTOR

Number: 2000                Name: Vector For EngH
Multimedia? n      Attendant Vectoring? n      Meet-me Conf? n      Lock? n
Basic? y      EAS? y      G3V4 Enhanced? y      ANI/II-Digits? y      ASAI Routing? y
Prompting? y      LAI? y      G3V4 Adv Route? y      CINFO? y      BSR? y      Holidays? y
Variables? y      3.0 Enhanced? y
01 queue-to      skill 2000 pri m
02 wait-time      999 secs hearing ringback
03 goto step      2      if unconditionally
04
```

5.2.3. Configure Vector Directory Number (VDN)

Enter the command **add vdn x** where **x** is the required VDN number appropriate to the dialplan. Configure the VDN to send calls to the vector configured in the previous section as follows:

- **Extension** – note the VDN extension number which will be used to place calls to the Skill vector and on to the Skill.
- **Name** – enter an appropriate name
- **Destination** – enter the **Vector Number** configured in the previous section

```
add vdn 2000                                           Page 1 of 3
                                                    VECTOR DIRECTORY NUMBER

      Extension: 2000
      Name*: VDN For EngHouse
      Destination: Vector Number      2000
Attendant Vectoring? n
Meet-me Conferencing? n
Allow VDN Override? n
COR: 1
TN*: 1
Measured: none

VDN of Origin Annc. Extension*:
1st Skill*:
2nd Skill*:
3rd Skill*:

* Follows VDN Override Rules
```

5.2.4. Configure Agents

Agents must be configured with the appropriate Skill Number. Enter the command **add agent-loginID x** where **x** is an agent extension number appropriate to the dialplan and configure as follows:

- **Login ID** – take a note of the configured **Login ID**
- **Name** – enter an identifying name

```

add agent-loginID 3000                                     Page 1 of 3
                                     AGENT LOGINID

      Login ID: 3000                                         AAS? n
      Name: Agent 3000                                       AUDIX? n
      TN: 1                                                  LWC Reception: spe
      COR: 1                                                 LWC Log External Calls? n
Coverage Path:                                             AUDIX Name for Messaging:
Security Code:

                                     LoginID for ISDN/SIP Display? n
                                     Password:
                                     Password (enter again):
                                     Auto Answer: station
                                     MIA Across Skills: system
ACW Agent Considered Idle: system
Aux Work Reason Code Type: system
Logout Reason Code Type: system
Maximum time agent in ACW before logout (sec): system
Forced Agent Logout Time:      :

WARNING: Agent must log in again before changes take effect
  
```

On **Page 2**, enter the hunt group number configured in **Section 5.2.1** in the **SN** (Skill Number) column and enter an appropriate **SL** (skill level).

```

add agent-loginID 3000                                     Page 2 of 3
                                     AGENT LOGINID

      Direct Agent Skill:                                     Service Objective? n
Call Handling Preference: skill-level                       Local Call Preference? n

      SN  RL  SL          SN  RL  SL          SN  RL  SL          SN  RL  SL
1: 2000  1           16:           31:           46:
2:           17:           32:           47:
  
```

5.3. Configure SIP Endpoints for Third Party Call Control

In order to control a SIP endpoint via Application Enablement Services, enter the command **change station x** where **x** is an appropriate endpoint extension number. On **Page 6**, set **Type of 3PCC Enabled** to **Avaya**.

```
change station 1002                                     Page 6 of 6
                                                         STATION
SIP FEATURE OPTIONS
    Type of 3PCC Enabled: Avaya
    SIP Trunk: aar
```

6. Configure Avaya Aura® Application Enablement Services

Configuration of Application Enablement Services is performed from the OAM web pages. Navigate to the URL of the AES OAM, in this case <https://10.10.16.210/index.jsp> and login using the appropriate credentials (not shown). Upon successful login, the screen below will appear.

The screenshot shows the Avaya Application Enablement Services Management Console. The header includes the Avaya logo, the title "Application Enablement Services Management Console", and a welcome message for user "craft" with system details. A navigation menu on the left lists various services. The main content area displays a "Welcome to OAM" message and a list of administrative domains with brief descriptions of their functions.

AVAYA Application Enablement Services Management Console

Welcome: User craft
Last login: Wed Aug 14 13:29:58 2013 from 10.10.16.62
Number of prior failed login attempts: 14
HostName/IP: aes63rp/10.10.16.210
Server Offer Type: VIRTUAL_APPLIANCE_ON_VMWARE
SW Version: 6.3.0.0.212-0
Server Date and Time: Wed Aug 14 17:34:30 UTC 2013

Home Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
- ▶ Licensing
- ▶ Maintenance
- ▶ Networking
- ▶ Security
- ▶ Status
- ▶ User Management
- ▶ Utilities
- ▶ Help

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:

- 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.
- Help - Use Help to obtain a few tips for using the OAM Help system

Depending on your business requirements, these administrative domains can be served by one administrator for all domains, or a separate administrator for each domain.

Copyright © 2009-2012 Avaya Inc. All Rights Reserved.

6.1. Configure Switch Connection

To establish the connection between Communication Manager and AE Services, click **Communication Manager Interface** → **Switch Connections**. In the field next to **Add Connection**, enter an appropriate name, in this case **CM63** and click on **Add Connection**.

The screenshot shows the "Communication Manager Interface | Switch Connections" page. The navigation menu is expanded to show "Switch Connections". A text input field contains the name "CM63", and an "Add Connection" button is visible next to it.

Communication Manager Interface | Switch Connections Home | Help | Logout

- ▶ AE Services
- ▶ Communication Manager Interface
 - Switch Connections

Switch Connections

CM63 Add Connection

The following screen is displayed. Complete the configuration as shown and enter the password specified in **Section 5.1** when configuring AESVCS in ip-services and check the **Processor Ethernet** box. Click on **Apply** when done.

Communication Manager Interface | Switch Connections

AE Services
 Communication Manager Interface
 Switch Connections
 Dial Plan
 Licensing
 Maintenance
 Networking
 Security

Connection Details - CM63

Switch Password [.....]
 Confirm Switch Password [.....]
 Msg Period 30 Minutes (1 - 72)
 SSL
 Processor Ethernet
 Apply Cancel

The following screen will be shown displaying the newly added switch connection, click **Edit PE/CLAN IPs**.

Communication Manager Interface | Switch Connections Home | Help | Logout

AE Services
 Communication Manager Interface
 Switch Connections
 Dial Plan
 Licensing
 Maintenance
 Networking

Switch Connections

[] Add Connection

Connection Name	Processor Ethernet	Msg Period	Number of Active Connections
<input checked="" type="radio"/> CM63	Yes	30	1

Edit Connection Edit PE/CLAN IPs Edit H.323 Gatekeeper Delete Connection Survivability Hierarchy

Enter the IP Address of the procr noted in **Section 5.1** and click **Add/Edit Name or IP**.

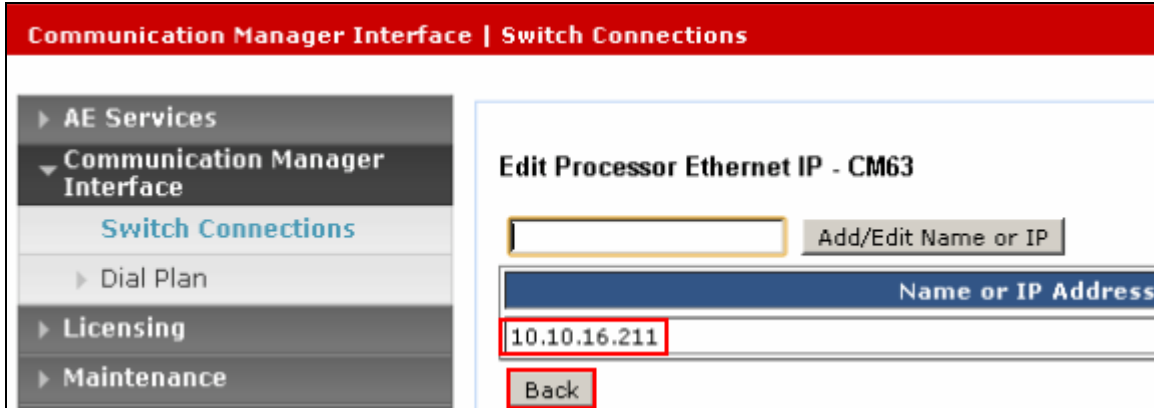
Communication Manager Interface | Switch Connections

AE Services
 Communication Manager Interface
 Switch Connections

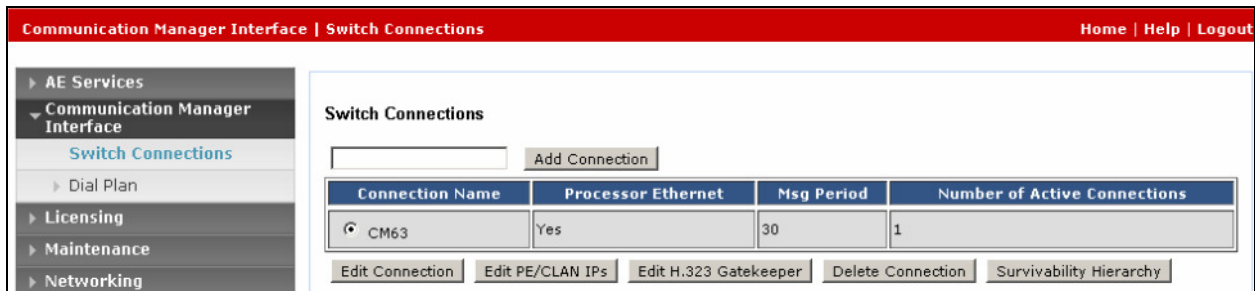
Edit Processor Ethernet IP - CM63

10.10.16.211 Add/Edit Name or IP

The following screen will appear showing the newly added procr IP address, click **Back**.

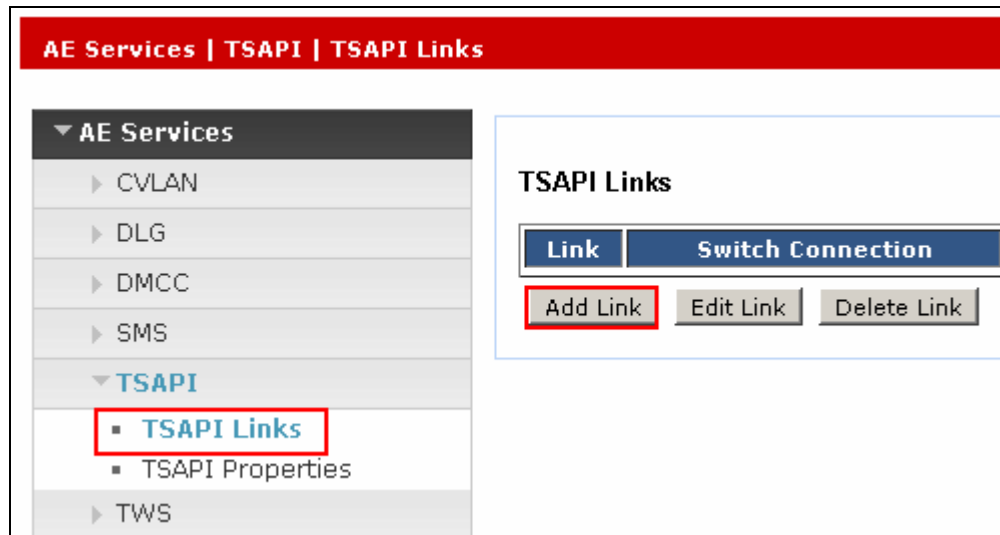


The newly added **Switch Connection** will appear once more.



6.2. Administer TSAPI Link

Select **AE Services** → **TSAPI** → **TSAPI Links** from the left pane. The **TSAPI Links** screen is displayed, click **Add Link**.



Configure the TSAPI Link using the newly configured **Switch Connection**, the **Switch CTI Link Number** configured in **Section 5.1** and set **Security** to **Both** as shown below and click **Apply Changes**.

AE Services

- CVLAN
- DLG
- DMCC
- SMS
- TSAPI**
 - TSAPI Links**
 - TSAPI Properties
- TWS

Communication Manager Interface

Add TSAPI Links

Link: 1

Switch Connection: CM63

Switch CTI Link Number: 1

ASAI Link Version: 4

Security: Both

Apply Changes **Cancel Changes**

The screen below will be displayed with instructions to restart the TSAPI Server. Click **Apply** taking note of the instructions given.

AE Services

- CVLAN
- DLG
- DMCC
- SMS
- TSAPI**
 - TSAPI Links**

Apply Changes to Link

Warning! Are you sure you want to apply the changes?
These changes can only take effect when the TSAPI server restarts.

⚠ Please use the Maintenance -> Service Controller page to restart the TSAPI server.

Apply **Cancel**

The screen below will appear displaying the newly added TSAPI link.

Link	Switch Connection	Switch CTI Link #	ASAI Link Version	Security
1	CM63	1	4	Both

Buttons: Add Link, Edit Link, Delete Link

6.3. Restart TSAPI Service

Select **Maintenance** → **Service Controller** from the left pane, to display the **Service Controller** screen in the right pane. Check the **TSAPI Service** box, and click **Restart Service**.

Service	Controller Status
<input type="checkbox"/> ASAI Link Manager	Running
<input type="checkbox"/> DMCC Service	Running
<input type="checkbox"/> CVLAN Service	Running
<input type="checkbox"/> DLG Service	Running
<input type="checkbox"/> Transport Layer Service	Running
<input checked="" type="checkbox"/> TSAPI Service	Running

Buttons: Start, Stop, Restart Service, Restart AE Server, Restart Linux, Restart Web Server

6.4. Obtain Tlink Name

Select **Security** → **Security Database** → **Tlinks**. Note the value of the **Tlink Name**, this will be needed for configuring the CT Connect server in **Section 7.4**.

The screenshot shows a web interface with a red header bar containing the text "Security | Security Database | Tlinks". On the left is a navigation menu with the following items: AE Services, Communication Manager Interface, Licensing, Maintenance, Networking, Security (expanded), Account Management, Audit, Certificate Management, Enterprise Directory, Host AA, PAM, Security Database (expanded), Control, CTI Users, Devices, Device Groups, and Tlinks (highlighted in blue). The main content area is titled "Tlinks" and contains a "Tlink Name" label, two radio button options, and a "Delete Tlink" button. The first radio button is selected and its label "AVAYA#CM63#CSTA#AES63RP" is enclosed in a red rectangular box. The second radio button is unselected and its label is "AVAYA#CM63#CSTA-S#AES63RP".

6.5. Administer Enghouse CTI User

Select **User Management** → **User Admin** → **Add User** from the left pane to display the **Add User** screen in the right pane. Enter desired values for **User Id**, **Common Name**, **Surname**, **User Password** and **Confirm Password**. For **CT User**, select **Yes** from the drop-down list. Retain the default value in the remaining fields. Click **Apply** at the bottom of the screen (not shown).

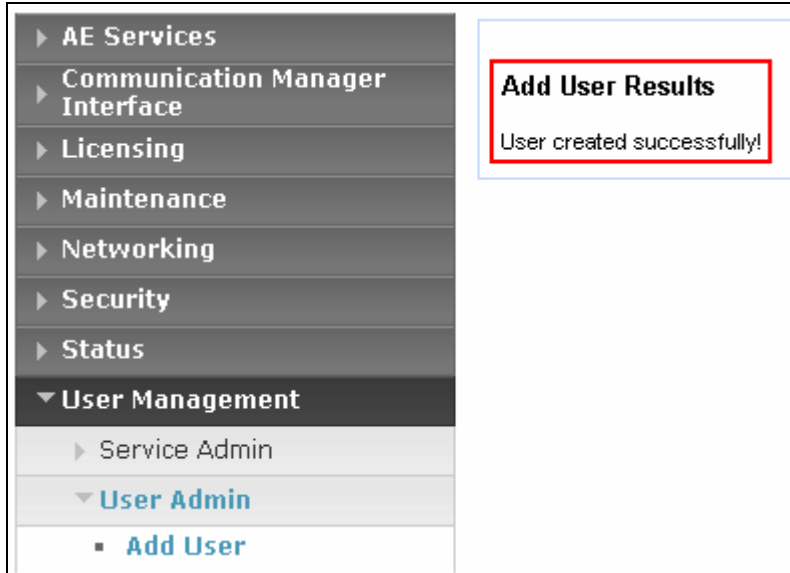
User Management | User Admin | Add User

Add User

Fields marked with * can not be empty.

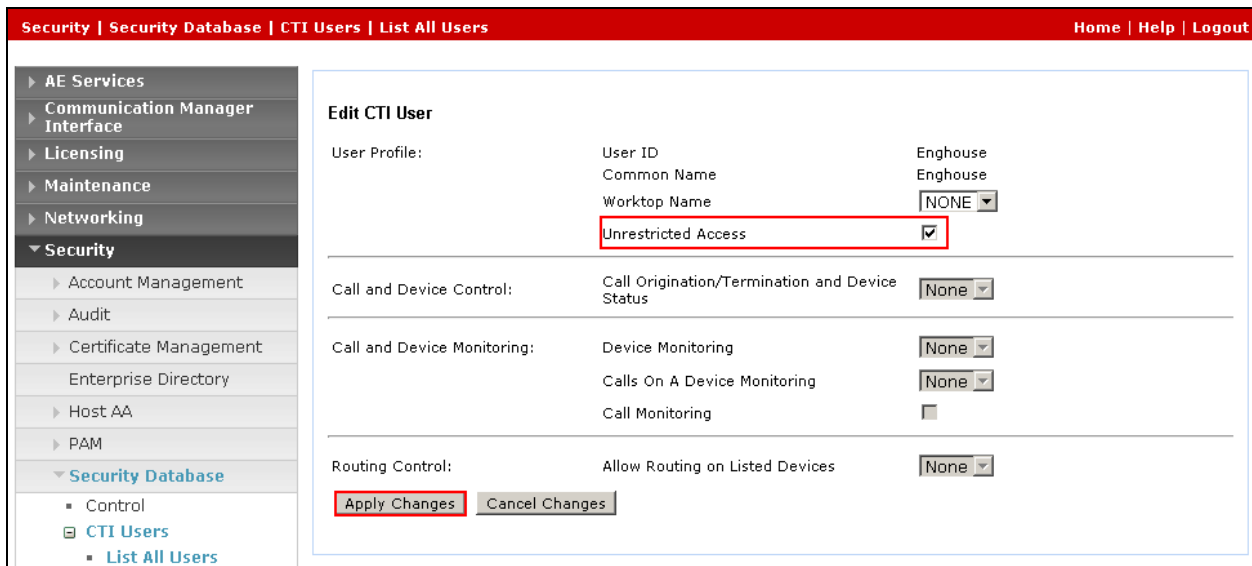
* User Id	Enghouse
* Common Name	Enghouse
* Surname	Enghouse
* User Password
* Confirm Password
Admin Note	
Avaya Role	None
Business Category	
Car License	
CM Home	
Css Home	
CT User	Yes

The following screen will appear confirming the successful creation of the new user.



6.6. Configure User Unrestricted Access

Select **Security** → **Security Database** → **CTI Users** → **List All Users** from the left pane, click on the radio button beside the user created above, in this case, **Enghouse** and click **Edit** (not shown). Place a tick in the box next to **Unrestricted Access**, as shown in the image below. Click **Apply Changes** when done.



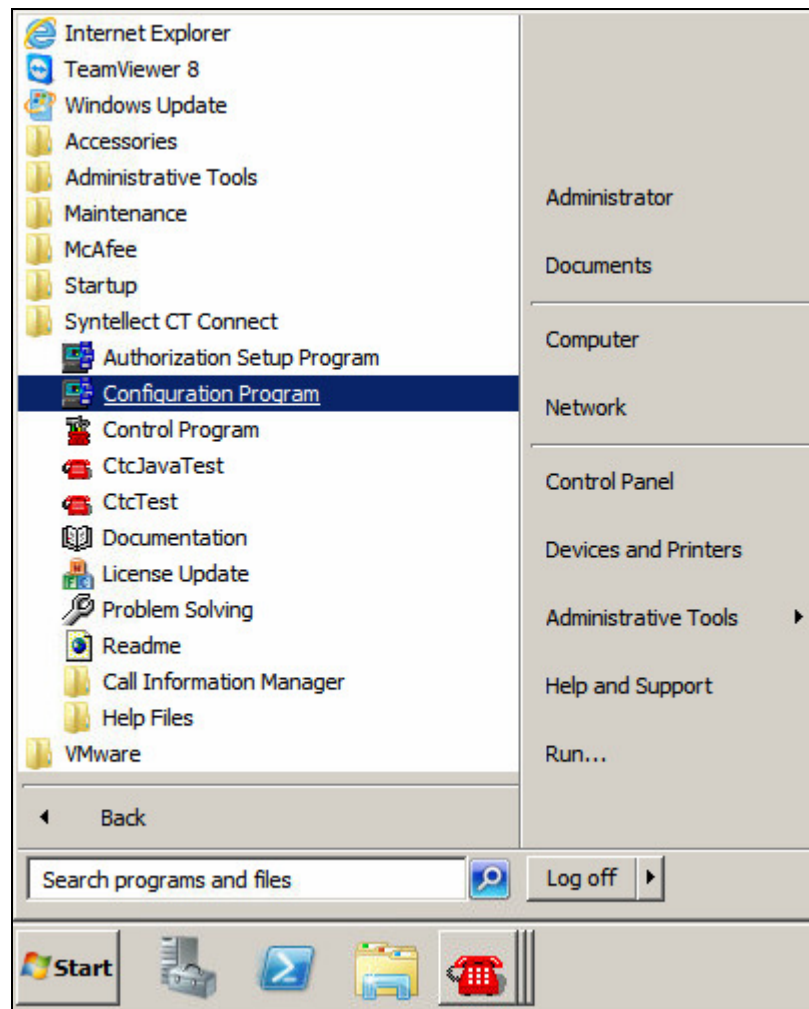
7. Configure EngHouse Interactive CT Connect

This section provides the procedures for configuring CT Connect. The procedures include the following areas:

- Launch configuration program
- Administer link
- Administer switch type
- Administer IP address and link number

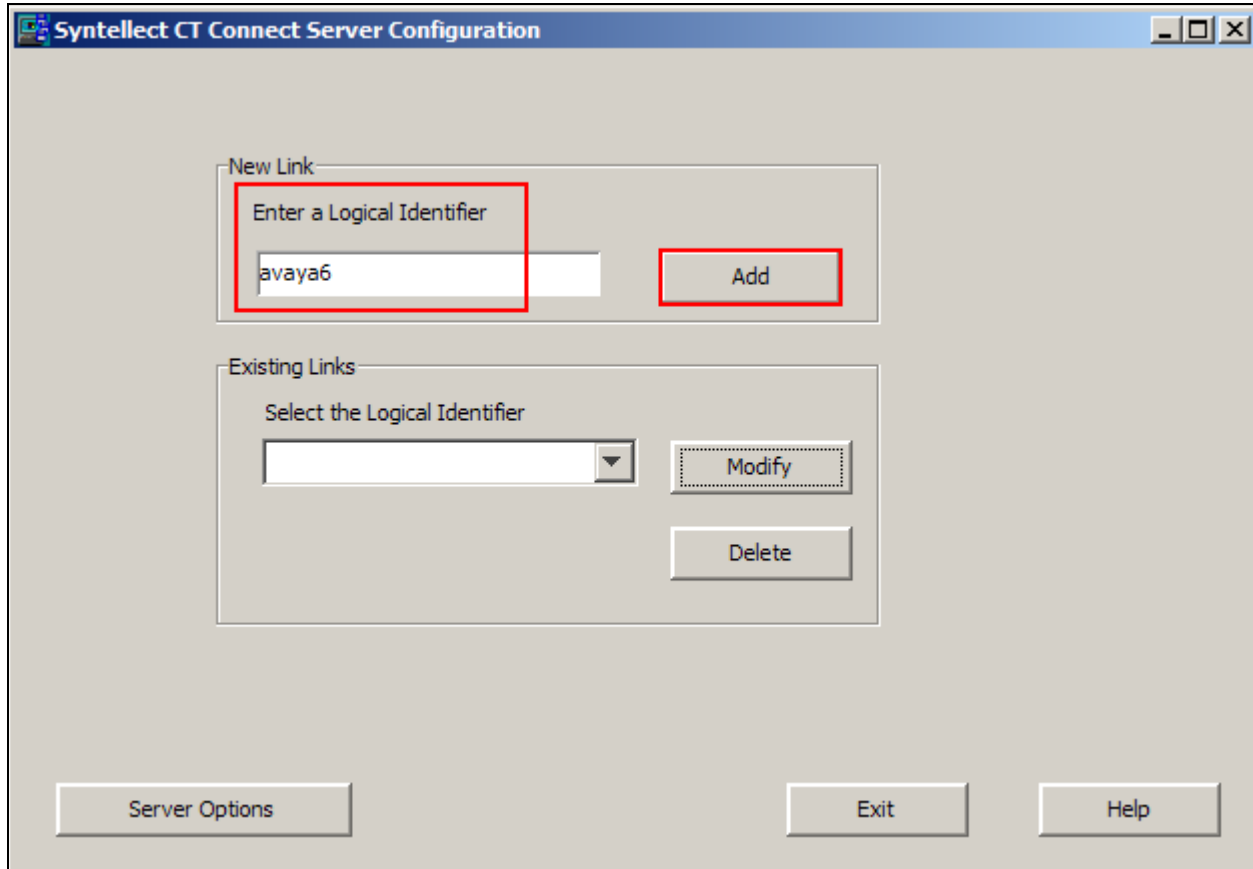
7.1. Launch configuration program

CT Connect uses a GUI based configuration program to configure the TSAPI connection between the CT Connect server and Application Enablement Services. From the CT Connect server, launch the configuration program by selecting **Start → All Programs → Syntellect CT Connect → Configuration Program** as shown below.



7.2. Administer Link

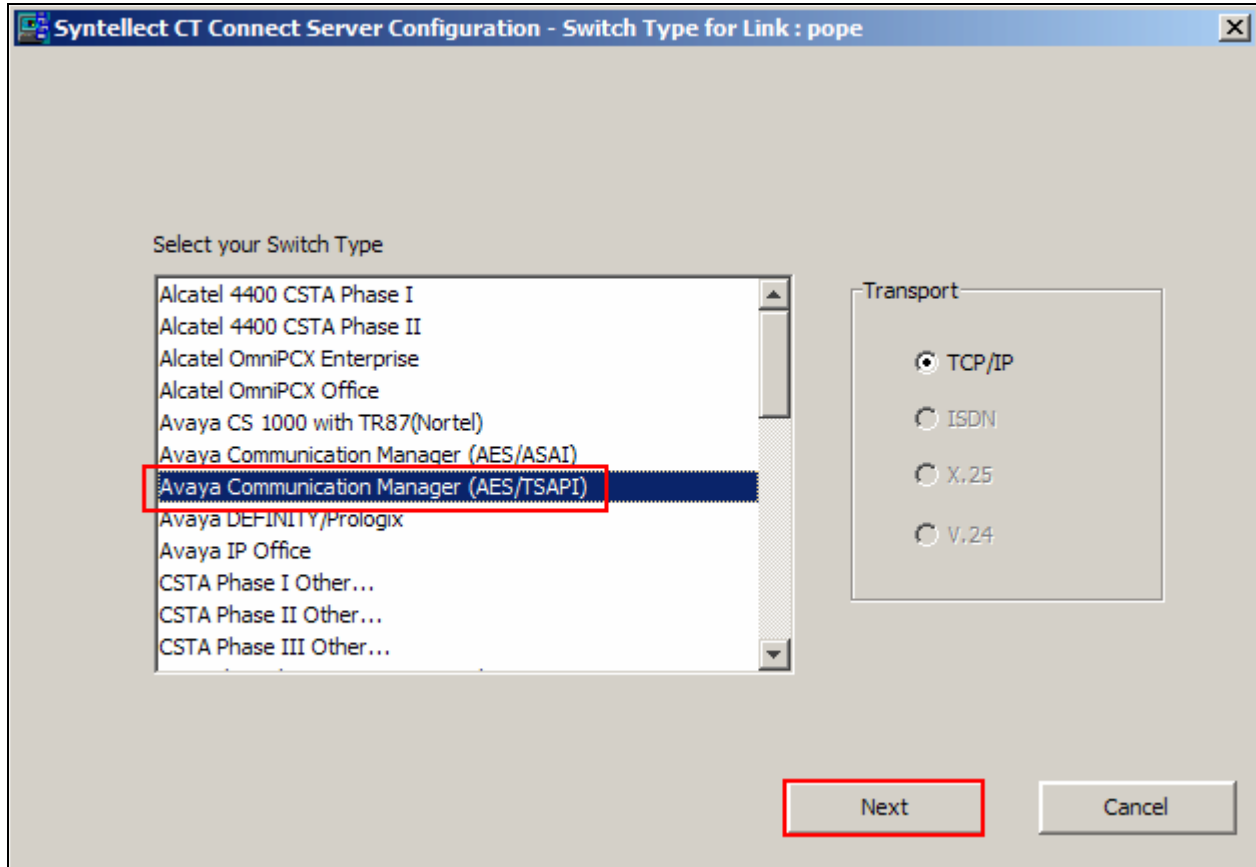
The **Syntellect CT Connect Server Configuration** screen is displayed. In the **Enter a Logical Identifier** field, enter a descriptive name, in this case **avaya6** and click **Add**.



The screenshot shows the 'Syntellect CT Connect Server Configuration' window. It features two main sections: 'New Link' and 'Existing Links'. In the 'New Link' section, there is a text input field labeled 'Enter a Logical Identifier' containing the text 'avaya6', and an 'Add' button. In the 'Existing Links' section, there is a dropdown menu labeled 'Select the Logical Identifier', a 'Modify' button, and a 'Delete' button. At the bottom of the window, there are three buttons: 'Server Options', 'Exit', and 'Help'. Red boxes highlight the 'Enter a Logical Identifier' field and the 'Add' button.

7.3. Administer switch type

In the **Select your Switch Type** list, select **Avaya Communication Manager (AES/TSAPI)** and click **Next**.



7.4. Administer IP address and link number

Enter the following values for the specified fields, and retain the default values in the remaining fields. Click **Save** when done.

- **AES Server Address** – enter the IP address of Application Enablement Services, in this case **10.10.16.210** as shown in **Figure 1**
- **TSAPI Service Name** - enter the **Tlink Name** obtained in **Section 6.4**
- **Username** - enter the CT User configured in **Section 6.5**
- **Password** - enter CT User **Password** configured in **Section 6.5**

The screenshot shows a configuration window titled "Syntellect CT Connect Server Configuration - Configuring Link : avaya6". It is divided into several sections:

- Transport:** AES Server Address (10.10.16.210), Port Number (450).
- Protocol Specific:** TSAPI Service Name (AVAYA#CM63#CSTA#AES63RP), Username (Enghouse), Password (Enghouse123!).
- Common:** Auto Start Link (unchecked), Auto Restart Monitors (unchecked), Timestamp (Server), Call Information Manager (localhost).
- Device Level Authorization:** Authorization (Off).

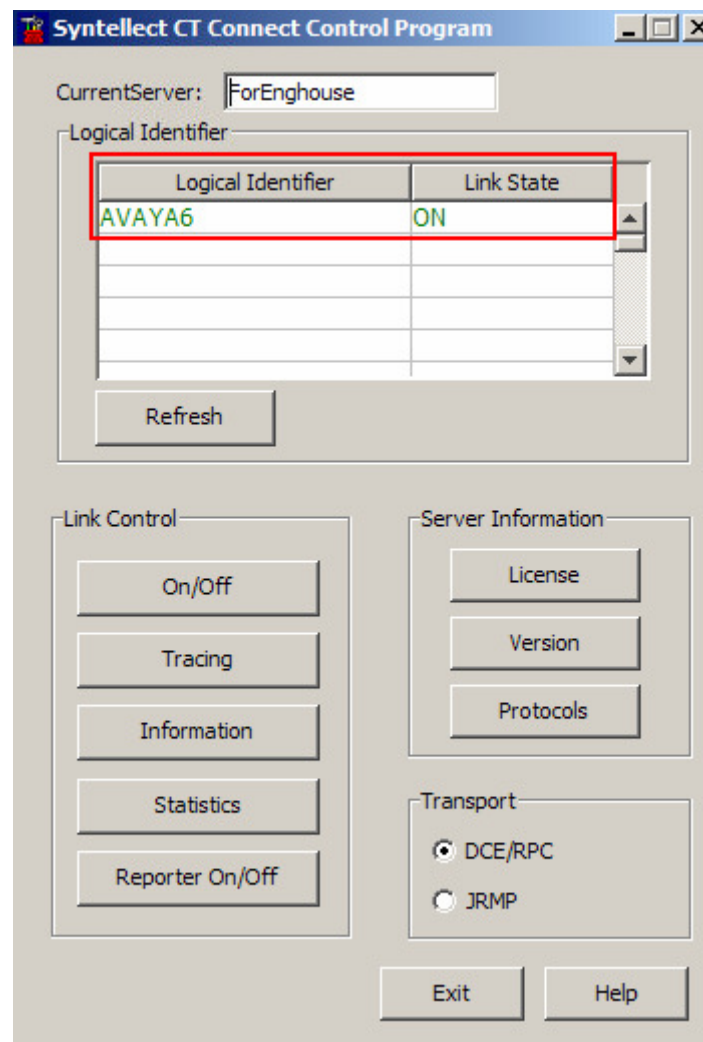
Buttons at the bottom include "Advanced", "Trace", "Save", and "Cancel".

8. Verification Steps

The correct configuration of the solution can be verified as follows:

8.1. Verify EngHouse Interactive CT Connect

From the CT Connect server, click **Start** → **All Programs** → **Syntellect CT Connect** → **Control Program** to load the **Syntellect CT Connect Control Program** screen. Ensure that the **Link State** associated with the administered **Logical Identifier** from **Section 7.2** in this case **avaya6** is **ON**.



Using the CtcTool, create a monitor on the required endpoint, in this case **1003**. Place a call to the monitored endpoint from another endpoint, in this case **1000**. Use the CtcTest tool to answer the call by executing the **ans** command. Ensure that the call is answered and CtcTest can be used to complete the full variety of call control scenarios.

```
CtcTest
Copyright Syntellect Inc. 2012. All rights reserved.
      CTC TEST Program Version 8.0
ctcTest>
ctcTest> assign 1003 localhost avaya6
ctcTest> setmon on
ctcTest> gete
ctcTest>

Event status
DN : 1003
Return Status : ctcSuccess
Channel Identifier : 5377416
The call reference is: 0x2ab
The state is RECEIVE and the event was INBOUND_CALL on channel 1
with qualifier 16
The Other party is DN 1000
The Other party is the Calling Device
The Other party dialing plan is 0
The Called party is DN 1003
The Called party dialing plan is 0
The Originating party is DN 1000
The Originating party dialing plan is 0
Timestamp: 27-Aug-2013 14:42:24:135
ctcTest> ans
ctcTest>

Event status
DN : 1003
Return Status : ctcSuccess
Channel Identifier : 5377416
The call reference is: 0x2ab
The state is ACTIVE and the event was TP_ANSWERED on channel 1
with qualifier 16
The Other party is DN 1000
The Other party is the Calling Device
The Other party dialing plan is 0
The Called party is DN 1003
The Called party dialing plan is 0
The Originating party is DN 1000
The Originating party dialing plan is 0
Timestamp: 27-Aug-2013 14:42:27:848
ctcTest>
```

8.2. Verify TSAPI Connection Status

Using the Application Enablement Services web interface, click **Status** → **Status and Control** → **TSAPI Service Summary** → **User Status** and select the Enghouse CT User configured in **Section 6.5** from the **CTI Users** drop down box and click **Submit**. Verify the number of **Open Streams** listed accurately reflects the number of endpoints being monitored and controlled by CT Connect.

The screenshot shows the 'CTI User Status' page for the 'Enghouse' user. It includes a navigation menu on the left with 'Status and Control' expanded to 'TSAPI Service Summary'. The main content area shows 'Open Streams: 2' and 'Closed Streams: 1'. Below this is a table of open streams.

Name	Time Opened	Time Closed	Tlink Name
Enghouse	Tue 27 Aug 2013 02:23:55 PM UTC		AVAYA#CM63#CSTA#AES63RP
Enghouse	Tue 27 Aug 2013 02:24:15 PM UTC		AVAYA#CM63#CSTA#AES63RP

Buttons for 'Show Closed Streams' and 'Back' are located below the table.

9. Conclusion

These Application Notes describe the compliance testing of Enghouse Interactive CT Connect with Avaya Aura® Communication Manager, and Avaya Aura® Application Enablement Services. All test cases were executed successfully with observations noted in **Section 2.2**.

10. Additional References

This section references the product documentations that are relevant to these Application Notes.

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

- *Administering Avaya Aura® Communication Manager, Release 6.3*, 03-300509, Issue 8.0 May 2013
- *Avaya Aura® Application Enablement Services Administration and Maintenance Guide, Release 6.3*, Issue 1.0, May 2013

©2013 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.