

Avaya Solution & Interoperability Test Lab

# Application Notes for Configuring Cybertech Pro with Avaya Communication Manager and Avaya Application Enablement Services – Issue 1.0

## Abstract

These Application Notes describe the compliance testing of the Cybertech Pro voice recording system with Avaya Communication Manager and Avaya Application Enablement Services. The document contains an extensive description of the configurations for both Cybertech Pro 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

The purpose of this document is to describe the compliance testing carried out with Cybertech Pro and Avaya Communication Manager and Avaya Application Enablement Services. It includes a description of the configuration of both the Avaya and the Cybertech solutions, a description of the tests that were performed and a summary of the results of those tests.

Cybertech Pro is a voice recording system which can be used to record the voice stream of Avaya telephone endpoints. It uses Avaya Communication Manager's 'Service Observe' feature via the Avaya Application Enablement Services (AES) Device, Media, and Call Control (DMCC) interface and the Telephony Services API (TSAPI) to capture the audio and call details for call recording.

The Device, Media and Call Control (DMCC) API associated with the AES server allows the creation of "Virtual" IP phones to monitor analogue, digital or VoIP extensions. A group of virtual IP phones is created in Avaya Communication Manager to be used by the CyberTech recorder application. These virtual phones are used to monitor the status of the target to be recorded. Recording can be activated using 'Service Observe' or 'Single Step Conference'. The method used is selected on the Cybertech recorder.

## 1.1. Interoperability Compliance Testing

The interoperability compliance tests included feature functionality and serviceability testing. The feature testing focused on testing scenarios that involve interaction between the Cybertech Pro server, Avaya Communication Manager and Avaya Application Enablement Services. The tests included the following:

- Verification of connectivity
- Verification of correct recording of basic internal and external calls
- Verification of correct recording for transfer, hold, and conference operations for internal and external calls
- Verification of call-back and bridged appearance operations
- Verification that agent information is included when monitoring calls to logged-in agents
- Verification of correct recovery after disconnection of various inter-device connections

The serviceability testing focused on verifying the Cybertech Pro's ability to recover from adverse conditions, such as disconnect from Avaya Communication Manager and Avaya Application Enablement Services.

## 1.2. Support

Technical support from Cybertech can be obtained through the following:

Cybertech Support Desk Email: supportdesk@Cybertech-int.com Telephone: +31 72 567 31 79

SF; Reviewed; SPOC 4/16/2009

# 2. Reference Configuration

Cybertech Pro is a voice recording system which can be used to record the voice stream of Avaya telephone endpoints. The voice traffic of selected endpoints can be monitored and recorded to a voice data archive, with the time and call participants recorded with each call segment file.

The Avaya IP Telephony configuration used to verify these Application Notes is shown in **Figure 1**. The Avaya Application Enablement Services (AES) server was used by Cybertech Pro to receive call status information. Cybertech Pro then used Avaya Communication Manager "Service Observe" facility and "Single Step Conference" to collect voice data streams of endpoints which were selected to be monitored.

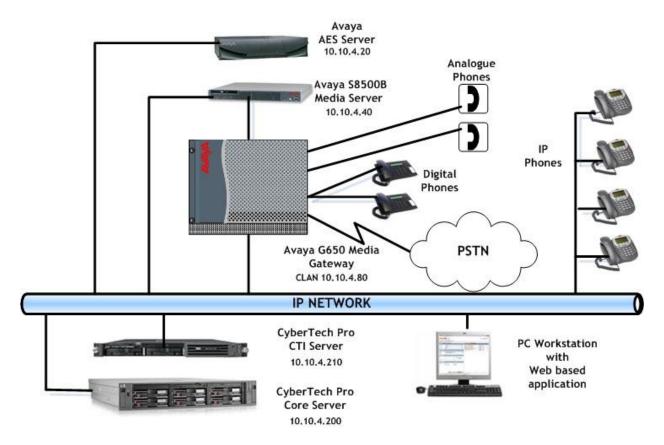


Figure 1: Cybertech Pro Test Configuration

# 3. Equipment and Software Validated

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

Equipment	Software Version
Avaya <sup>TM</sup> S8500B Server	Avaya Communications Manager
	5.1.2 (R015x.01.2.416.4)
Avaya <sup>™</sup> S8500B Server	Avaya Application Enablement Services
	4.2.1
Avaya <sup>™</sup> G650 Media Gateway	
IPSI TN2312BP	HW15, FM44
CLAN TN799DP	HW01, FM26
IP Media Processor TN2602AP	HW02, FM41
Analog Card TN793CP	HW09, FM010
DS1 Interface TN246CP	HW02, FM019
Digital Line TN2214CP	HW08, FM015
Avaya <sup>™</sup> 96xx and 46xx Series IP	
Telephones (H.323)	
9640	2.0
9620	2.0
4620SW	2.9
4621SW	2.9
2420	R5
Analog Telephones – POTS	N\A
Cybertech Recording server	Version 5.2.0.75
Cybertech CTI Server	Callcontroller – version 1.4.10.438
	AvayaLinkController – version .2.4.240

#### Table 1: Hardware and Software Version Numbers

# 4. Test Configuration

**Table 2** contains the extensions that are used for testing. The capital letter designationscorrespond to the telephones shown in Figure 1. The virtual phones are softphones which wereadded to act as recording extensions.

Type of Phone	Phone Extension	Station	Button Allocation	Comments	IP Address
IP9640	3002	S1	3 x call-appr, serv- obsrv		10.10.4.52
IP9640	3005	S2	3 x call-appr, serv- obsrv		10.10.4.54
Digital-2420	3009	А	3 x call-appr, auto- cback		
Digital-2420	3006	В	3 x call-appr, auto- cback, call-pkup	*Agent logged in	
IP4610	3000	C	3 x call-appr, brdg- appr D, call-pkup **Added auto- cback	*Agent logged in	
IP9620	3001	D	3 x call-appr		
POTS		Е			
POTS		F			
IP Softphone	3012	Virtual 1	3 x call-appr, serv- obsrv	*Recording extension not visible	
IP Softphone	3013	Virtual 2	3 x call-appr, serv- obsrv	*Recording extension – not visible	
External CM	2500	G			
External CM	2510	Н			

#### Table 2: Station Extensions and Details Used for Testing

# 5. Configuration of Avaya Communication Manager

The configuration and verification operations illustrated in this section were all performed using Avaya Communication Manager System Administration Terminal (SAT).

The information provided in this section describes the configuration of Avaya Communication Manager for this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in reference [1].

The configuration operations described in this section can be summarized as follows:

- Verify that the licenses allocated to the system are sufficient to support the required configuration
- Configure system parameters and system features
- Allocate Feature Access Codes
- Configure IP node names
- Configure the telephone stations that are to be used for testing
- Configure virtual CTI telephone stations
- Configure Class of Restriction for recording devices
- Allocate a call pickup group
- Allocate agent resources
- Configure the interface to AES

The configuration of the PRI interface to the PSTN is outside the scope of these application notes.

## 5.1. Verify System Parameters Customer Options

Use the **display system-parameters customer-options** command to verify that Avaya Communication Manager is licensed to meet the minimum requirements to interoperate with the Cybertech Pro server. Those items shown in bold in the screen below indicate required values or minimum capacity requirements. If these are not met in the configuration, please contact an Avaya representative for further assistance. On **Page 2**, the value configured for **Maximum Concurrently Registered IP Stations** must be sufficient to support the total number of IP stations used. For Voice Recording you need double the number of Maximum Concurrently Registered IP stations, than the number of targets.

display system-parameters customer-options		Page 2 of 11
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	100	0
Maximum Concurrently Registered IP Stations:	2400	0
Maximum Administered Remote Office Trunks:	0	0
Maximum Concurrently Registered Remote Office Stations:	0	0
Maximum Concurrently Registered IP eCons:	0	0
Max Concur Registered Unauthenticated H.323 Stations:	10	0
Maximum Video Capable H.323 Stations:	10	0
Maximum Video Capable IP Softphones:	10	0
Maximum Administered SIP Trunks:	10	0
Maximum Administered Ad-hoc Video Conferencing Ports:	10	0
Maximum Number of DS1 Boards with Echo Cancellation:	0	0
Maximum TN2501 VAL Boards:	10	0
Maximum Media Gateway VAL Sources:	0	0
Maximum TN2602 Boards with 80 VoIP Channels:	128	0
Maximum TN2602 Boards with 320 VoIP Channels:	128	1
Maximum Number of Expanded Meet-me Conference Ports:	0	0

Verify with your Avaya account team that the required licenses are installed. In this test the following parameters were used though not all may be required for your solution needs. On **Page 3** the parameters are set as follows:

- Answer Supervision by Call Classifier? to y
- **Computer Telephony Adjunct Links?** to y

display system-parameters customer-option	ns Page 3 of	11
OPTIONAL	FEATURES	
Abbreviated Dialing Enhanced List? n	Audible Message Waiting?	n
Access Security Gateway (ASG)? n	Authorization Codes?	n
Analog Trunk Incoming Call ID? n	CAS Branch?	n
A/D Grp/Sys List Dialing Start at 01? n	CAS Main?	n
Answer Supervision by Call Classifier? y	Change COR by FAC?	n
ARS? y	Computer Telephony Adjunct Links?	У
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net?	n
ARS/AAR Dialing without FAC? y	DCS (Basic)?	n
ASAI Link Core Capabilities? n	DCS Call Coverage?	n
ASAI Link Plus Capabilities? n	DCS with Rerouting?	n
Async. Transfer Mode (ATM) PNC? n		
Async. Transfer Mode (ATM) Trunking? n	Digital Loss Plan Modification?	n
ATM WAN Spare Processor? n	DS1 MSP?	n
ATMS? n	DS1 Echo Cancellation?	У
Attendant Vectoring? n		

On Page 4, the IP Stations parameter must be set to v so that IP stations can be configured.

display system-parameters customer-op	tions Page 4 of 11
OPTIO	NAL FEATURES
Emergency Access to Attendant? y	IP Stations? y
Enable 'dadmin' Login? y	
Enhanced Conferencing? n	ISDN Feature Plus? n
Enhanced EC500? n	ISDN/SIP Network Call Redirection? n
Enterprise Survivable Server? n	ISDN-BRI Trunks? y
Enterprise Wide Licensing? n	ISDN-PRI? y
ESS Administration? n	Local Survivable Processor? n
Extended Cvg/Fwd Admin? n	Malicious Call Trace? n
External Device Alarm Admin? n	Media Encryption Over IP? y
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n
Flexible Billing? n	
Forced Entry of Account Codes? n	Multifrequency Signaling? y

On **Page 6**, the **EAS-PHD** parameter must be set to y so that skill levels greater that 3 can be selected. This is not mandatory for recording but was used in testing.

isplay system-parameters customer-option	s Page 6 of 11
CALL CENTER OPTI	ONAL FEATURES
Call Center Rel	ease: 5.0
ACD? y	Reason Codes? r
BCMS (Basic)? y	Service Level Maximizer? r
BCMS/VuStats Service Level? n	Service Observing (Basic)? y
BSR Local Treatment for IP & ISDN? n	Service Observing (Remote/By FAC)? y
Business Advocate? n	Service Observing (VDNs)? y
Call Work Codes? n	Timed ACW? n
DTMF Feedback Signals For VRU? n	Vectoring (Basic)? y
Dynamic Advocate? n	Vectoring (Prompting)? y
Expert Agent Selection (EAS)? y	Vectoring (G3V4 Enhanced)? y
EAS-PHD? y	Vectoring (3.0 Enhanced)? y
Forced ACD Calls? n	Vectoring (ANI/II-Digits Routing)? y
Least Occupied Agent? n	Vectoring (G3V4 Advanced Routing)? y
Lookahead Interflow (LAI)? n	Vectoring (CINFO)? y
ultiple Call Handling (On Request)? n	Vectoring (Best Service Routing)? y
Multiple Call Handling (Forced)? n	Vectoring (Holidays)? y
PASTE (Display PBX Data on Phone)? n	Vectoring (Variables)? y

### 5.2. Configure System Parameters Features

Use the **change system-parameters features** command to set the **Call Pickup Alerting?** and **Directed Call Pickup?** parameters to y. These features were used in testing but are not mandatory for recording.

```
change system-parameters features
                                                                     4 of 17
                                                               Page
                       FEATURE-RELATED SYSTEM PARAMETERS
         Reserved Slots for Attendant Priority Queue: 5
                          Time before Off-hook Alert: 10
              Emergency Access Redirection Extension:
Number of Emergency Calls Allowed in Attendant Queue: 5
Maximum Number of Digits for Directed Group Call Pickup: 4
              Call Pickup on Intercom Calls? y
                                                       Call Pickup Alerting? y
Temporary Bridged Appearance on Call Pickup? y
                                                       Directed Call Pickup? y
                 Extended Group Call Pickup: none
 Deluxe Paging and Call Park Timeout to Originator? n
Controlled Outward Restriction Intercept Treatment: tone
Controlled Termination Restriction (Do Not Disturb): tone
         Controlled Station to Station Restriction: tone
AUTHORIZATION CODE PARAMETERS
                                 Authorization Codes Enabled? n
```

Solution & Interoperability Test Lab Application Notes ©2009 Avaya Inc. All Rights Reserved. Page 8 of 48 CT52-ACM-DMCC On Page 11 ensure the features were set as follows to allow service observing.

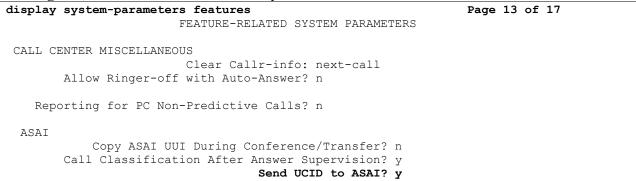
- Service Observing: Warning Tone? to y. It is not mandatory for recording but was used while testing.
- Allow Two Observers in Same Call? to y

```
display system-parameters features
                                                                     Page 11 of 17
                         FEATURE-RELATED SYSTEM PARAMETERS
CALL CENTER SYSTEM PARAMETERS
  EAS
         Expert Agent Selection (EAS) Enabled? y
        Minimum Agent-LoginID Password Length:
          Direct Agent Announcement Extension:
                                                                     Delay:
   Message Waiting Lamp Indicates Status For: station
  VECTORING
               Converse First Data Delay: 0 Second Data Delay: 2
Converse Signaling Tone (msec): 100 Pause (msec): 70
                     Prompting Timeout (secs): 10
   Reverse Star/Pound Digit For Collect Step? n
          Available Agent Adjustments for BSR? n
                             BSR Tie Strategy: 1st-found
   Store VDN Name in Station's Local Call Log? n
  SERVICE OBSERVING
              Service Observing: Warning Tone? y
                                                       or Conference Tone? n
     Service Observing Allowed with Exclusion? n
             Allow Two Observers in Same Call? y
```

Universal Call ID is used to uniquely identify calls. On **Page 5** of the system-parameters features form, set **Create Universal Call ID (UCID)** to **y** and **UCID Network Node ID** to an unassigned node ID.

```
5 of 17
display system-parameters features
                                                              Page
                      FEATURE-RELATED SYSTEM PARAMETERS
SYSTEM PRINTER PARAMETERS
 Endpoint:
                       Lines Per Page: 60
SYSTEM-WIDE PARAMETERS
                                   Switch Name:
           Emergency Extension Forwarding (min): 10
         Enable Inter-Gateway Alternate Routing? n
Enable Dial Plan Transparency in Survivable Mode? n
                            COR to Use for DPT: station
MALICIOUS CALL TRACE PARAMETERS
              Apply MCT Warning Tone? n MCT Voice Recorder Trunk Group:
SEND ALL CALLS OPTIONS
    Send All Calls Applies to: station Auto Inspect on Send All Calls? n
UNIVERSAL CALL ID
    Create Universal Call ID (UCID)? y
                                         UCID Network Node ID: 1
```

```
On Page 13, set Send UCID to ASAI to y.
```



## 5.3. Configure Feature Access Codes

Use the **change feature-access-codes** command to configure all of the access codes shown in the table below.

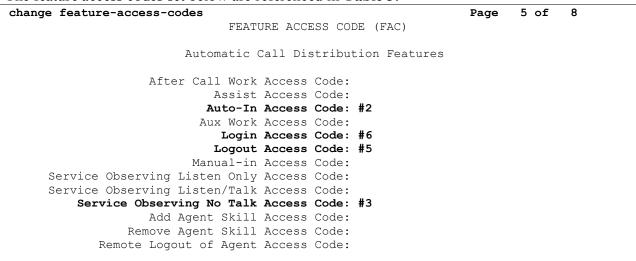
Parameter	Usage
Call Pickup	This is used by telephone users to initiate a call-pickup operation.
Access Code	
Auto-in	This is used by the agent to indicate readiness.
Login	Agent login.
Logout	Agent logout.
Service	This is used by the voice recorder to receive the voice stream without sending
Observing No	voice data. Value used below (#3) is a free choice; the value chosen must
Talk	match the Cybertech configuration settings.

#### **Table 3: Feature Access Codes**

The values set for each option can be seen highlighted on **Page 1** and **Page 5** in the figures below.

change feature-access-codes		Page	1 of	8
FEATURE ACC	ESS CODE (FAC)			
Abbreviated Dialing List1 Access	Code:			
Abbreviated Dialing List2 Access	Code:			
Abbreviated Dialing List3 Access	Code:			
Abbreviated Dial - Prgm Group List Access	Code:			
Announcement Access	Code:			
Answer Back Access	Code:			
Attendant Access	Code:			
Auto Alternate Routing (AAR) Access	Code:			
Auto Route Selection (ARS) - Access Co	de 1: Access Coo	de 2:		
Automatic Callback Activa	tion: Deactivat	cion:		
Call Forwarding Activation Busy/DA:	All: Deactivat	cion:		
Call Forwarding Enhanced Status:	Act: Deactivat	cion:		
Call Park Access	Code:			
Call Pickup Access	Code: #4			
CAS Remote Hold/Answer Hold-Unhold Access	Code:			
CDR Account Code Access	Code:			
Change COR Access	Code:			
Change Coverage Access	Code:			
Contact Closure Open	Code: Close (	Code:		

Solution & Interoperability Test Lab Application Notes ©2009 Avaya Inc. All Rights Reserved. The feature access codes set below are referenced in Table 3.



## 5.4. Configure Node Names

Ensure that the CLAN IP address is in the node-names form. Enter the **change node-names ip** command. In the compliance-tested configuration, the 'CLAN' IP address was used for registering H.323 endpoints, and the 'PresAES' IP address was used for connectivity to Avaya AES.

change node-names	s ip	Page	1 of	2
	IP NODE NAMES			
Name	IP Address			
CLAN	10.10.4.80			
MEDPRO	10.10.4.90			
PresAES	10.10.4.40			
default	0.0.0			
procr	10.255.255.100			

## 5.5. Configure Telephone Stations

Use the **add station** command to configure all of the telephones shown in **Section 4**, **Table 2**. Refer to this table when allocating names and button assignments for each test phone.

On Page 1, Phone A, Extension 3009, is a digital phone therefore a Type of 2420 is chosen.

add station 3009	Page	1 of 5	
	STATION		
Extension: 3009	Lock Messages? n	BCC:	0
Туре: 2420	Security Code:	TN:	1
Port: 01A0607	Coverage Path 1:	COR:	1
Name: Phone A	Coverage Path 2:	COS:	1
	Hunt-to Station:		
STATION OPTIONS			
	Time of Day Lock Table:		
Loss Group: 2	Personalized Ringing Pattern:	1	
Data Option: none	Message Lamp Ext:		
Speakerphone: 2-way	Mute Button Enabled?	V	
Display Language: english	Expansion Module?	n	
Survivable COR: internal	Media Complex Ext:		
Survivable Trunk Dest? y	IP SoftPhone?	n	
	Customizable Labels?	Y	

Add the appropriate button assignments as shown in the screen on Page 4 below.

add station 3009		Page	4 of	5
	STATION	_		
SITE DATA				
Room:		Headset? n		
Jack:		Speaker? n		
Cable:		Mounting: d		
Floor:		Cord Length: 0		
Building:		Set Color:		
ABBREVIATED DIALING				
List1:	List2:	List3:		
BUTTON ASSIGNMENTS	_			
1: call-appr	5:			
2: call-appr	6:			
3: call-appr	7:			
4: auto-cback	8:			
voice-mail Number:				

Repeat this process to add stations for telephones B, C, D, S1 and S2 as displayed in **Table 2**, **Section 4**.

## 5.6. Configure CTI Telephone Stations

Use the **add station** command to configure a station for each of the virtual endpoints shown in **Table 2, Section 4**. Each of the virtual stations has a **Type** of **4620**. Enter in a descriptive **Name** and **Security Code** for each one. Set the **IP Softphone** to **y**.

change station 3012		P	age	1 of	5
		STATION	-		
Extension: 3012		Lock Messages? n		BCC:	0
Type: 4620		Security Code: 3012		TN:	1
Port: S00013		Coverage Path 1:		COR:	1
Name: Virtual 1		Coverage Path 2:		COS:	1
		Hunt-to Station:			
STATION OPTIONS					
		Time of Day Lock Table	:		
Loss Group:	19	Personalized Ringing Pattern	: 1		
		Message Lamp Ext	: 3012	2	
Speakerphone:	2-way	Mute Button Enabled	?у		
Display Language:	english	Expansion Module	? n		
Survivable GK Node Name:					
Survivable COR:	internal	Media Complex Ext	:		
Survivable Trunk Dest?	У	IP SoftPhone	?у		
		IP Video Softphone	? n		
		Customizable Labels	? Y		

Allocate the button assignments as shown in the screen below. Create a **serv-obsrv** button to initiate a service observe from the CTI server.

change station 3012			Page	4 of	5
	STATION				
SITE DATA					
Room: [B		Headset?	n		
Jack:		Speaker?	n		
Cable:		Mounting:	d		
Floor:		Cord Length:	0		
Building:		Set Color:			
ABBREVIATED DIALING					
List1:	List2:	List3:			
BUTTON ASSIGNMENTS					
1: call-appr	5:				
2: call-appr	6:				
3: call-appr	7:				
4: serv-obsrv	8:				

## 5.7. Configure COR

Set the class of restriction so that the stations can all service observed by a recording device. Set the values in the following screen as follows:

- Can Be Service Observed? as y
- Can Be A Service Observer? as y

change cor 1 Page 1 of 23 CLASS OF RESTRICTION COR Number: 1 COR Description: FRL: 0 APLT? y APLT? y Calling Party Restriction: none Can Be Service Observed? y Can Be A Service Observer? y Called Party Restriction: none Partitioned Group Number: 1 Priority Queuing? n Forced Entry of Account Codes? n Priority Queuing? n Direct Agent Calling? y Restriction Override: none Facility Access Trunk Test? n Direct Agent Calling? y Restricted Call List? n Can Change Coverage? n Access to MCT? y Fully Restricted Service? n Group II Category For MFC: 7 Send ANI for MFE? n Add/Remove Agent Skills? y MF ANI Prefix: Automatic Charge Display? n Hear System Music on Hold? y PASTE (Display PBX Data on Phone)? n Can Be Picked Up By Directed Call Pickup? y Can Use Directed Call Pickup? y Group Controlled Restriction: inactive

#### On Page 2 set the value Service Observing by Recording Device? to y.

change cor 1	Page	2 of 23
CLASS OF RESTRICTION		
MF Incoming Call Trace? n		
Brazil Collect Call Blocking? n		
Block Transfer Display? n		
Block Enhanced Conference/Transfer Displays? y		
Remote Logout of Agent? n		
Station Lock COR: 1 TODSL Release Interval (hours): Outgoing Trunk Disconnect Timer (minutes):		
Station-Button Display of UUI IE Data? n		
Service Observing by Recording Device? y		
ERASE 24XX USER DATA UPON		
Dissociate or unmerge this phone: none		
EMU login or logoff at this phone: none		
Mask CPN/NAME for Internal Calls? n		

## 5.8. Configure Pickup Group

Create a pickup group which contains stations A, B, C, D. This is used in conjunction with the "call-pkup" button which is allocated to endpoint B, as shown in **Section 4**, **Table 2**. Use the command **add pickup-group 1** to add this group as shown below. Assign a name and add extensions.

```
add pickup-group 1
                                                                  Page
                                                                          1 of
                                                                                 4
                                PICKUP GROUP
           Group Number: 1
             Group Name: CallPickUP
GROUP MEMBER ASSIGNMENTS
    Extension
                    Name
1: 3009
2: 3006
 3: 3000
 4: 3001
 5:
 6:
```

## 5.9. Configure Agents

A hunt group, Vector Directory Number (VDN), vector and two agent logins were created as in the following table. These were created for testing purposes only.

	Value	Name
VDN	1800	VDN1800
Vector	1	Vector1
Skill Ext\Hunt Groups	35001/1	Agent HG1
Agent Login	6001	AgentB
	6002	AgentC

**Table 4: Call Center Agent Details** 

#### 5.9.1. Configure Agent Hunt Group

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 **Group Name** and **Group Extension** valid under the provisioned dial plan. Set the following options to yes (y) as shown below.

- ACD? to y
- Queue? to y
- Vector? to y
- Group Type to ucd-mia to specify that the system hunts for the "most idle agent".

```
add hunt-group 1
                                                             Page
                                                                   1 of 61
                                HUNT GROUP
           Group Number: 1
                                                        ACD? y
            Group Name: Agent HG1
                                                      Queue? y
        Group Extension: 35000
                                                     Vector? y
            Group Type: ucd-mia
                    TN: 1
                                    MM Early Answer? n
                   COR: 1
                                    Local Agent Preference? n
          Security Code:
ISDN/SIP Caller Display:
            Queue Limit: unlimited
Calls Warning Threshold: Port:
 Time Warning Threshold:
                             Port:
```

On Page 2 set Skill? to y to indicate that this is a skilled hunt group.

add hunt-group 1	Page 2 of 61
daa hane group r	HUNT GROUP
	NONI GROOT
<b>Skill? y</b> AAS? n Measured: none Supervisor Extension:	Expected Call Handling Time (sec): 180
Controlling Adjunct: none	
	Redirect on No Answer (rings): Redirect to VDN: of Stroke Counts or Call Work Codes? N
	Redirect on No Answer (rings): Redirect to VDN: of Stroke Counts or Call Work Codes? n

#### 5.9.2. Configure Agent Queue Vector

Enter the **add vector n** command; where **n** is associated to hunt group 1. The **Vector number** is set to **1**. Enter the vector steps to queue to the  $1^{st}$  skill on the VDN as shown below.

```
add vector 1Page 1 of 6<br/>CALL VECTORNumber: 1Name: Vector1Basic? yEAS? y G3V4 Enhanced? y ANI/II-Digits? y<br/>LAI? n G3V4 Adv Route? y CINFO? y BSR? y<br/>3.0 Enhanced? y01 wait-time<br/>02 queue-to2 secs hearing ringback<br/>skill 1 prim03
```

#### 5.9.3. Configure Agent VDN

Use the **add vdn n** command to create a Vector Directory Number extension which can be used to reference the Operator queue vector. Set the values **Name** and **Vector Number 1** by referencing **Table 3**, **Section 5.8** above. The 1<sup>st</sup> **Skill** is set to 1.

```
add vdn 1800 Page 1 of 3

VECTOR DIRECTORY NUMBER

Extension: 1800

Name*: VDN1800

Vector Number: 1

Allow VDN Override? n

COR: 1

TN*: 1

Measured: none

1st Skill*: 1

2nd Skill*:

3rd Skill*:
```

Set **Observe on Agent Answer?** to y on **Page 2**. This will initiate service observe after the agent has answered the call.

add vdn 1800	Page 2 of	3
VECTOR DIRECTORY	NUMBER	
AUDIX Name:		
BSR Available Agent Strategy*:	1st-found	
BSR Tie Strategy*:	system	
	-	
Observe on Agent Answer?	У	
Display VDN for Route-To DAC*?	n	
VDN Override for ISDN Trunk ASAI Messages*?	n	
Reporting for PC Predictive Calls?	Ν	

## 5.9.4. Configure Agent Login

Use the **add agent-loginID n** command; where **n** is a valid extension under the provisioned dial plan. Two agents are created at stations B and C as in **Table 2**, **Section 4**. The agent loginID chosen is **6001**. Enter a descriptive name for the agent in the **Name** field and set **Password**.

add agent-loginID 6001		Page	1 of 2
	AGENT	LOGINID	
Login ID:	60.01	AAS?	n
5		AUDIX?	
	AgentB		
TN:		LWC Reception:	-
COR:	1	LWC Log External Calls?	n
Coverage Path:		AUDIX Name for Messaging:	
Security Code:			
_		LoginID for ISDN/SIP Display?	n
		Password:	6001
		Password (enter again):	6001
		Auto Answer:	station
		MIA Across Skills:	system
		ACW Agent Considered Idle:	system
		Aux Work Reason Code Type:	system
		Logout Reason Code Type:	system
Max	ximum time ag	ent in ACW before logout (sec):	system
		Forced Agent Logout Time:	:

Specify the list of skills assigned to the login and the skill level for each of them in the SN/SL field as shown below. Set the Skill Number to 1, it should be the same as that configured for the associated vector number. The Skill Level is set to 1.

agent-	-loginID	6001				Page	2 of	2
			AGENI	LOGINID				
Dire	ect Agen	t Skill:						
l Handl	ling Pre	ference: ski	ll-level		Local (	Call Prefer	ence? n	
SN	SL	SN	SL	SN	SL	SN	SL	
1	1	16:		31:		46:		
		17:		32:		47:		
	Dire L Handi SN	Direct Agen L Handling Pre SN SL	SN SL SN 1 1 16:	AGENT Direct Agent Skill: L Handling Preference: skill-level SN SL SN SL 1 1 16:	AGENT LOGINID Direct Agent Skill: L Handling Preference: skill-level SN SL SN SL SN <b>1 1</b> 16: 31:	AGENT LOGINID Direct Agent Skill: L Handling Preference: skill-level Local ( SN SL SN SL SN SL 1 1 16: 31:	AGENT LOGINID Direct Agent Skill: L Handling Preference: skill-level Local Call Prefer SN SL SN SL SN SL SN 1 1 16: 31: 46:	AGENT LOGINID Direct Agent Skill: Handling Preference: skill-level Local Call Preference? n SN SL SN SL SN SL SN SL 1 1 16: 31: 46:

## 5.10. Configure Interface to Avaya AES

The Avaya Application Enablement Services server has a TSAPI interface which provides Cybertech Pro with a means of communicating with Avaya Communication Manager to perform telephony operations. Avaya Communication Manager requires the configuration parameters shown in this section.

Use the **add ip-interface** command to allocate a call control interface. The slot value specified should be the CLAN interface. The value used as **Node Name** must be one of the names from the list defined by the **change node-names ip** command. The **Subnet Mask** and **Gateway Address** should be assigned to the values used by the Ethernet network to which the CLAN is attached.

add ip-interface 01a02		Page 1 of	2
-	IP INTERFACES	2	
	_		
Type: C-LAN			
Slot: 01A02	2		
Code/Suffix: TN79	9 D		
Node Name: CLAN			
IP Address: 10 .:	10.4.80		
Subnet Mask: 255.2	255.255.0	Link: 1	
Gateway Address: 10 .:	10.4.1		
Enable Ethernet Port? y		low H.323 Endpoints? y	
Network Region: 1	A	Allow H.248 Gateways? y	
VLAN: n		Gatekeeper Priority: 5	
Target socket load and Warn:	ing level: 400		
Receive Buffer TCP Win	ndow Size: 8320		
	ETHERNET OPTIONS		
Auto? y			

Use the **change ip-services** command to set the parameters for **AESVCS** service for the CLAN as shown below. This was defined above to serve as the interface to the Avaya AES server. On **Page 1** add **CLAN** as the **Local Node** and accept default of **8765** as **Local Port**.

change ip-s	services		<b>*</b>		Page	1 of	3	
Service	Enabled	Local	IP SERVICES Local		Domoto			
Service	Ellabied	LOCAL	LOCAL	Remote	Remote			
Type		Node	Port	Node	Port			
AESVCS	у С:	LAN	8765					

On **Page 3** an entry for the Avaya AES server must be made in the list in the screen shown below. The name assigned to the Avaya AES server when it was installed must be entered in the **AE Services Server** field for that entry. The **Password** entry must the same as that assigned to the switch connection as shown in **Section 6.2** of this document

change ip-ser	vices			Page	3 of	3
		Services Administ:	ration			
Server ID	AE Services Server	Password	Enabled	Status		
1: 2: 3:	PresAES	xxxxxxxxxxx xxxxxxxxxxxx	n <b>y</b>	idle <b>in use</b>		

Solution & Interoperability Test Lab Application Notes ©2009 Avaya Inc. All Rights Reserved. Page 19 of 48 CT52-ACM-DMCC Use the **add cti-link** command to add a CTI link for use by TSAPI. The link number can be any value between 1 and 64 which is not currently assigned to another link. The link number specified must be the same value that is used in the **Add / Edit TSAPI Links** configuration screen shown in **Section 6.3** of this document. Use an unused extension as the value for the **Extension** parameter. The value chosen for the **Name** parameter is a matter of personal preference. Specify a **Type** of **ADJ-IP**, as required for a TSAPI link.

	Page	1 of 3	
CTI LINK			
		COR: 1	
	CTI LINK		

Use the **add data-module n** command; where **n** is an unassigned extension, to allocate an extension to be used as the data interface for the clan module. The value used as **Data Extension** can be any free extension. The **Name** value is only used for identification purposes. The **Type** field must be **ethernet**. The **Port** should be assigned to port 17 of the CLAN interface. The **Link** number should be assigned a value between 1 and 99.

```
add data-module 3400
DATA MODULE
Data Extension: 3400 Name: CLAN
Type: ethernet
Port: 01A0217
Link: 1
Network uses 1's for Broadcast Addresses? y
```

# 6. Configuration of Avaya AES

The information provided in this section describes the configuration of Avaya Application Enablement Services for this solution. The configuration includes the following areas:

- Verify Avaya Application Enablement Services License
- Create Switch Connection
- Administer TSAPI link
- Add CTI User
- Enable CTI Link User
- Set DMCC Port

## 6.1. Verify Avaya AES Licensing

The Avaya AES server is configured via a web browser by accessing the following URL: https://<Avaya AES server address>/

Once the login screen appears, enter the OAM Admin login ID/password to perform administrative activities on the AE Server. Verify that Avaya Communication Manager/AES is licensed for TSAPI and DMCC by consulting with your Avaya account manager or Business Partner to acquire the proper license for your solution.

From the OAM Home screen select **CTI OAM Admin** (not shown) to bring up the CTI OAM Home menu. Verify that the TSAPI service is licensed at the Welcome to CTI OAM Screens screen by ensuring that **TSAPI Service** and **DMCC Service** are in the list of services in the License Information section.

Αναγα				on Enableme	
	You are here: > CTI	OAM Home		OAM Hor	ne 🕜 Help 🛈 Logou
CTI OAM Home Administration Status and Control Maintenance	Welcome to CTI		5		
<u>Alarms</u> Logs	[craft] Last login: Mon	Feb 23 19:05:58 20(	09 from 135.64.21.180		
<ul> <li><u>Utilities</u></li> <li><u>Help</u></li> </ul>	IMPORTANT: AE Service Changes to the Securit		for administrative changes equire a restart.	to fully take effect.	
	Service	Status	State	Licenses P	urchased
	ASAI Link Manager	Running	N/A	N/A	
	DMCC Service	Running	ONLINE	Yes	
	CVLAN Service	Running	ONLINE	No	
	DLG Service	Running	OFFLINE	Yes	
	Transport Layer Service	Running	N/A	N/A	
	TSAPI Service	Running	ONLINE	Yes	
	SMS	N/A	N/A	No	
	For status on actual se	rvices, please use <u>St</u>	tatus and Control.		
	You are licensed to rur	Application Enablem	ent (CTI) version 4.2.		

Solution & Interoperability Test Lab Application Notes ©2009 Avaya Inc. All Rights Reserved.

## 6.2. Create Switch Connection

Navigate to Administration  $\rightarrow$  Switch Connections. Enter the name of the Switch Connection to be added and click on the Add Connection button. The screen below displays the active switch connection once it has been added.

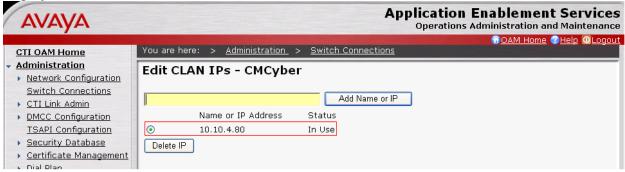
Αναγα	Application Enablement Services Operations Administration and Maintenance
and the second	GOAM Home @Help @Logout
CTI OAM Home	You are here: > <u>Administration</u> > <u>Switch Connections</u>
<ul> <li><u>Administration</u></li> </ul>	Switch Connections
Network Configuration	Switch connections
Switch Connections	
<u>CTI Link Admin</u>	Add Connection
DMCC Configuration	Connection Name Number of Active Connections
TSAPI Configuration	O CMCyber 1
Security Database	Edit Connection Edit CLAN IPs Edit H.323 Gatekeeper Delete Connection
<u>Certificate Management</u>	
Dial Plan	
Enternrise Directory	

Following the addition of the switch connection the AES Set Switch Connection Password screen is displayed. Enter the screen fields as described below and click the **Apply** button.

- Switch Password: The Switch Password must be the same as that entered into Avaya Communication Manager AE Services screen via the change ip-services command, described in Section 5.10.
- **SSL:** This is enabled

Αναγα		Application Enablement Service Operations Administration and Maintenar	
CTI OAM Home	You are here: > <u>Administration</u> >	Switch Connections	<u>out</u>
<u>Administration</u> <u>Network Configuration</u>	Set Password - New		_
Switch Connections CTI Link Admin DMCC Configuration	Please note the following: * Changing the password affects only	/ new connections, not open connections.	
TSAPI Configuration  Security Database	Switch Password	•••••	
<u>Certificate Management</u>	Confirm Switch Password	••••••	
Dial Plan	SSL		
Enterprise Directory Host AA SMS Configuration	Apply Cancel		

The CLAN IP address must then be set on the AES. From the Administration  $\rightarrow$  Switch Connections screen (not shown), click the Edit CLAN IPs button. Enter the IP address of the CLAN which the Avaya AES is to use for communication with Avaya Communication Manager as defined in Section 5.10. Click the Add Name or IP button (not shown). The following screen displays the added CLAN IP address.



The H.323 Gatekeeper should be set up to point to the Avaya Communication Manager where the virtual extensions are registered. Enter the CLAN IP address which will be used for the DMCC service.

Navigate to CTI OAM Home  $\rightarrow$  Administration  $\rightarrow$  Switch Connection  $\rightarrow$  Edit H323 Gatekeeper. Enter the IP Address and click Add Name or IP button. The screen below shows the added IP address.

<u>Network Configuration</u> Edit H.323 Gatekeeper - CMCyber	ment Services ation and Maintenance
Network Configuration	Home (7Help OLogout
Switch Connections	
Switch Connections CTI Link Admin Add Name or IP	
DMCC Configuration     Name or IP Address	
TSAPI Configuration 0 10.10.4.80	
Security Database     Delete IP	
<u>Certificate Management</u> Dial Plan	

## 6.3. Administer TSAPI Link

From the CTI OAM Home menu, select Administration  $\rightarrow$  CTI Link Admin  $\rightarrow$  TSAPI Links. On the TSAPI Links screen (not shown), select Add Link. On the Add/Edit TSAPI Links screen, enter the following values:

- Link: Select an unused link number. The link number chosen is 1.
- Switch Connection: The "Switch Connection" parameter should be the name of the Avaya Media Server which is to be controlled by this link. Choose the switch connection CMCyber, which has already been configured from the drop-down list.
- Switch CTI Link Number: Use the corresponding CTI link number configured in Section 5.10 which is 10.
- Security: Both is the option chosen here. The customer can choose Secure\UnSecure\Both.

#### Once completed, select Apply Changes.

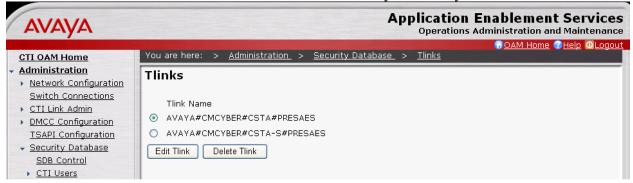
Αναγα		Application Enablement Services Operations Administration and Maintenance
CTI OAM Home  Administration  Network Configuration	You are here: > <u>Administration</u> > <u>C</u> Add / Edit TSAPI Links	িOAM Home @Help @Logout TI Link Admin_ > TSAPI Links
Switch Connections CTI Link Admin TSAPI Links CVLAN Links DLG Links DMCC Configuration TSAPI Configuration Security Database	Link: Switch Connection: Switch CTI Link Number: ASAI Link Version Security Apply Changes Cancel Changes	1 CMCyber V 10 V 4 V Both V
<u>Certificate Management</u> <u>Dial Plan</u> <u>Enterprise Directory</u>		

The AES must be restarted to effect the changes made in this section. From the CTI OAM Home menu, select **Maintenance**  $\rightarrow$  Service Controller. On the Service Controller screen, select **Restart AE Server**.



Solution & Interoperability Test Lab Application Notes ©2009 Avaya Inc. All Rights Reserved. Restart AE Server screen (not shown), select **Restart**. Wait at least 10 minutes and select **Maintenance**  $\rightarrow$  Service Controller. On the Service Controller screen, verify that all services are showing **Running** in the Controller Status column (not shown).

Navigate to the Tlinks screen by selecting Administration  $\rightarrow$  Security Database  $\rightarrow$  Tlinks. Note the value of the Tlink Name, as this will be needed for configuring the Cybertech server in Section 7.3. The Tlink Name shown below is automatically created by the AES server.



## 6.4. Create Avaya CTI User

A User ID and password needs to be configured for the Cybertech Pro server to communicate as a TSAPI Client with the AES server to monitor stations and initiate switching operations.

Click on OAM Home  $\rightarrow$  User Management and log into the User Management page. Click on User Management and then Add User.

In the Add User screen shown below, enter the following values:

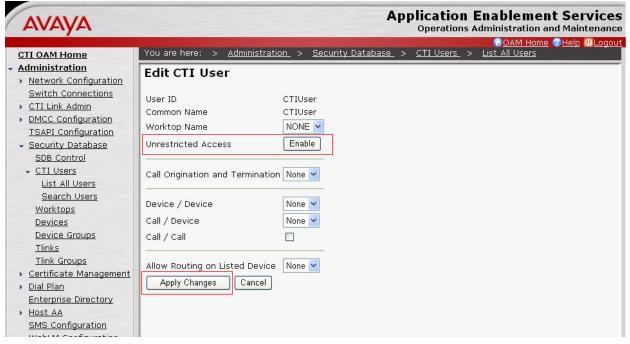
- User ID This will be used by the Cybertech server in Section 7.3.
- Common Name and Surname A descriptive name needs to be entered.
- New Password and Confirm Password This will be used with the User Id in Section 7.3.
- **CT User** Select **Yes** from the drop-down menu

Complete the process by choosing Apply (not shown) at the bottom of the screen.

AVAYA		Application Enablement Services Operations Administration and Maintenance
AVAYA User Management Home User Management List All Users Add User Search Users Modify Default User Change User Password Service Management Help	You are here: > User Management > Add Add User Fields marked with * can not be empty. * User Id CTIUser * Common Name CTIUser * Surname CTIUser * User Password * Confirm Password	Operations Administration and Maintenance
	Admin Note Avaya Role None Avaya Role None Avaya Role Car License CAT License CAT Home CSS Home CT User Yess V Department Number Display Name	

## 6.5. Enable CTI User

Navigate to the CTI Users by selecting Administration  $\rightarrow$  Security Database  $\rightarrow$  CTI Users  $\rightarrow$  List All Users. Select the CTIUser user that was set up in Section 6.4 and select the Edit option. For the Unrestricted Access option, select the Enable button and Apply Changes at the bottom of the screen.



## 6.6. Configure DMCC Ports

Navigate to CTI OAM Home  $\rightarrow$  Administration  $\rightarrow$  Network Configuration  $\rightarrow$  Ports to set the DMCC server port. During the compliance test, the Encrypted Port was enabled as shown in the following screen. Click the Apply Changes button (not shown) at the bottom of the screen to complete the process.

DMCC Server Ports			Enabled Disat
	Unencrypted Port	4721	. • •
	Encrypted Port	4722	• •
	TR/87 Port	4723	$\circ \circ$

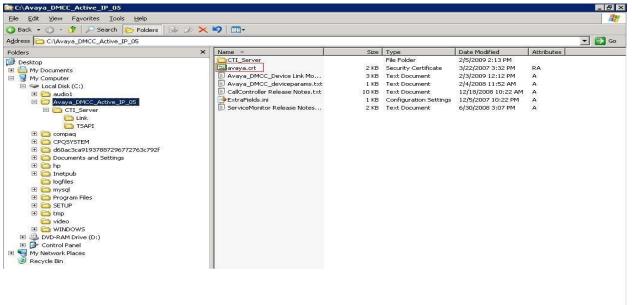
# 7. Configure Cybertech CTI Server

The Cybertech Pro CTI server is largely pre-configured for the customer by Cybertech prior to delivery. This section shows those configuration steps which need to be made after delivery. The configuration includes the following areas:

- Install of the SSL Certificate
- Install of the Avaya Link Controller, Call Controller and the TSAPI Client
- Configure the Cybertech Pro Voice Recorder

## 7.1. Install the SSL Certificate for the AES Connection

The Cybertech CTI server requires a certificate to communicate with the Avaya AES Server. After installation the following files are present on the CTI server. Double click on the 'avaya' certificate in the directory containing the distribution files. Please check CyberTech Connectivity Manual for latest details.



Click Install Certificate on the subsequent screen.

Certificat	e Information	
	<b>s intended for the following p</b> 114187.7.1.1.1 n policies	ourpose(s):
	fication authority's statement for Avaya Product Root CA	details.
Issued by:	Avaya Product Root CA	
¥alid from	8/22/2003 <b>to</b> 8/14/2033	

The Certificate Import Wizard is displayed. Click Next to begin the import.



Solution & Interoperability Test Lab Application Notes ©2009 Avaya Inc. All Rights Reserved. Click **Browse** to select the certificate destination.

Certificate stores are syste	m areas where certificates are kept.
Windows can automatically	select a certificate store, or you can specify a location fo
C Automatically select	the certificate store based on the type of certificate
Place all certificates i	in the following store
Certificate store:	
	Browse
	N.
	4
	k

Select the Local Computer, as shown.



Click Next after confirming the destination.

rtificate Import Wizard	×
Certificate Store	
Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a location for	
$\odot$ Automatically select the certificate store based on the type of certificate	
Place all certificates in the following store	
Certificate store:	
Trusted Root Certification Authorities\Local Computer	
	_
< <u>B</u> ack <u>N</u> ext > Cancel	

#### Click Finish after the certificate installation is complete.

Certificate Import Wizard	ominica in compress.	×
Tokal	Completing the Certificate Import Wizard	
	You have successfully completed the Certificate Import wizard.	
	You have specified the following settings:	
	Certificate Store Selected by User Content Certificate	
	< <u>B</u> ack Finish Cancel	

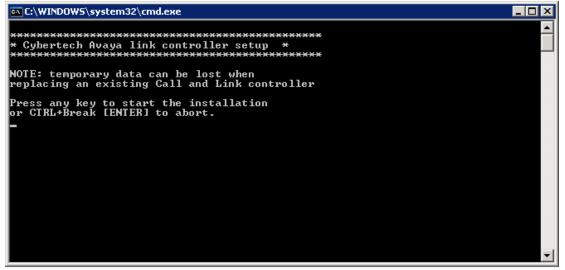
Solution & Interoperability Test Lab Application Notes ©2009 Avaya Inc. All Rights Reserved.

# 7.2. Install Avaya Link Controller, Call Controller and the TSAPI Client on CTI Server

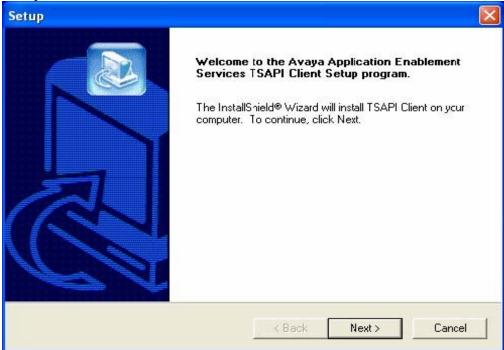
The Avaya Link Controller, Call Controller and the TSAPI Client must be installed on the CTI Server, as shown by the following steps. First, execute the 'setup.bat' file as shown in the default directory in the following screen. Make sure you run this batch file on the CTI server.

ack 👻 🕤 🚽 🍿 🔎 Search 🌔 Folders 🛛 😼 🗙	<b>19</b>					
ss 🛅 C:\Avaya_DMCC_Active_IP_05\CTI_Server						⇒
rs X	Name 🔺	Size	Туре	Date Modified	Attributes	
esktop	(Can Link		File Folder	2/5/2009 2:13 PM		
My Documents	C TSAPI		File Folder	2/5/2009 2:13 PM		
My Computer	cti_controller.exe	440 KB	Application	12/18/2008 10:17 AM	A	
🖙 Local Disk (C:)	🔊 EmailDll.dll	486 KB	Application Extension	6/9/2005 4:18 PM	A	
E Caudio1	🛐 Err_Beep.dll	60 KB	Application Extension	11/1/2007 4:13 PM	A	
Avaya DMCC Active_IP_05	err_core.dll	184 KB	Application Extension	11/1/2007 4:13 PM	A	
E CTI Server	💽 Err_Mail.dll	481 KB	Application Extension	11/1/2007 4:13 PM	A	
	err_snmp.dll	88 KB	Application Extension	12/19/2007 1:53 PM	A	
TSAPI	🔊 HealthReport.dll	212 KB	Application Extension	9/1/2008 12:50 PM	A	
	libmySQL.dll	228 KB	Application Extension	3/13/2003 8:21 PM	A	
	Temove.bat	2 KB	Windows Batch File	1/17/2008 4:54 PM	A	
	service_monitor.exe	220 KB	Application	6/30/2008 3:05 PM	A	
	setup.bat	2 KB	Windows Batch File	4/1/2008 2:31 PM	A	
E C hp	SetupDB.exe	3,144 KB	Application	10/24/2007 2:09 PM	A	
E C Inetpub	SNMP_DLL.dll	401 KB	Application Extension	6/9/2005 4:09 PM	A	
C logfiles			201	635		
mysql	1					
🗄 🥶 mysqi 🗄 🧰 Program Files	1					
	1					
E C tmp	1					
🖿 🛄 tmp						
WINDOWS						
E S Control Panel						
My Network Places						

This will open a dialog box as follows. Press any key to automatically install the Avaya Link controller and the Call controller to the CTI server.



Solution & Interoperability Test Lab Application Notes ©2009 Avaya Inc. All Rights Reserved. Page 32 of 48 CT52-ACM-DMCC After these steps the TSAPI installer will start.



Retain the default installation folder and click Next.

Setup 🔀			
Choose Destination Location Select folder where Setup will install files.			
To install in this folder, click Next. To install in a another folder.	different folder, click browse and select		
Destination Folder			
C:\Program Files\Avaya\AE Services\TSAPI	Client\ Browse		
InstallShield			
	< Back Next > Cancel		

Enter the IP address of the Avaya AES server in the Host Name or IP Address field, retaining the default port of 450. Click Add to List and then Next.

TCP/IP Name Server Co	nfiguration	×
	Your workstation will be configured for access to the TSAPI Service via TCP/IP. You must specify the host name or IP address and port number of each TSAPI Service you wish to use. Host Name or IP Address TCP Port 10.10.4.20 450 Add to List Configured Telephony Servers Configured Telephony Servers Delete The configured TSAPI Service will be placed in the TSLIB.INI file.	
	< <u>B</u> ack <u>N</u> ext > Cancel	

Click Finish after the installation completes.

Setup	
	Installation Complete. Setup has finished installing TSAPI Client on your computer.
	< <u>B</u> ack <b>Finish</b> Cancel

Solution & Interoperability Test Lab Application Notes ©2009 Avaya Inc. All Rights Reserved.

## 7.3. Configure the Cybertech Pro Voice Recorder

The Cybertech Pro Voice Recorder is configured for each of "Service Observe" and "Single Step Conference" modes in this section.

Enter the URL of the Cybertech Voice Recorder in the web browser and enter the User name and **Password** and click on the ">" button or press Enter.

C Log on [ct-c08090113] - Windows Internet Explorer		- 7 🗙
	🖌 🗲 🗙 Live Search	<b>P</b> •
Eile Edit View Favorites Iools Help		
😪 🏟 📾 Log on [ct-c08090113]	🟠 🔹 🔝 🐇 🖶 Page	• 💮 T <u>o</u> ols • 🎇
Dure	Titernet	€ 100% ·

Once logged in, select the **cti integration** tab which initially displays the **devices** on the secondary tab. Click on the Pencil symbol in the upper right portion of the screen.

CyberTech Pro [SER	ICE / ct-c08090113] - Win	dows Internet Explorer				
🗫 http://10.10.4.200/login.	nainadmin.asp					~
my account syst	TECH PRO minstallation cti integratik election overview linked chanr		user admini	stration system status	evaluation recorded calls	quit
Overview of all devices						2
Device name Avaya_Link	Device enabled Cor     TOP		Device state	Linked channel group None	Date last modified	2 0
			1			
		Choose an device t	to edit it or add a ni	ew one to the list.		
13:14:33 Welcome to C this information		ssful logon for service was on	16 February 2009	12:14:41. Contact your security ad		w to clipboard ar messages overview
Done					🏹 😜 Internet	🔍 100% 🔻 🛒

Solution & Interoperability Test Lab Application Notes ©2009 Avaya Inc. All Rights Reserved. Page 35 of 48 CT52-ACM-DMCC In the next screen **General device parameters** form below ensure that the **Device Parameters** values in **Table 5** are entered. Then select **Device Enabled** as **Yes**. The **TSAPIServerName** value depends on whether the TSAPI link is set to Encrypted, Unencrypted or Both. Refer to **Section 6.3**.

Parameter	Value
SwitchName	CMCyber
ObserveCode	#3
TSAPIServerName	AVAYA#CMCYBER#CSTA#PRESAES or AVAYA#CMCYBER#CSTA-S#PRESAES
ConnectionUseSSL	Yes
ConnectionProtocol	4.2

#### **Table 5: Cybertech Device Parameter Settings**

Under the **Connections settings** parameters in the same form, configure the **Connection settings** as shown in the **Table 6** below.

Parameter	Usage
Connection host	Enter the IP address of the Avaya AES Server.
IP port	Enter the default port address of "4722".
Connection user	Enter the user name which was defined in Section 6.4.
Connection password	Enter the "User Password" which was defined in Section 6.4.

#### **Table 6: Cybertech Pro Connection Settings**

Click Save changes once the values have been added.

CyberTech Pro [SERVICE / ct	-c08090113] - Windows Internet Ex	qlorer			
🖦 http://10.10.4.200/login.mainadmir	i.asp				~
CYBERTE my account system instal devices targets selection of	PRO	figuration user a	dministration system stat	us evaluation recorded calls quit	
Overview of all devices					3
Device name Avaya_Link	Device enabled Connection t Auto-	discove Device st Logged i	2 1	Date last modified	20
General device settings		1	Connection settings	ē	2
Device name	Avaya_Link		Connection host	10.10.4.20	
Device enabled	Yes	~	IP port	4722	
Auto-discovery enabled			Connection user	CTIUser	
Device parameters	SwitchName=CMCyber ObserveCode=#3	~	Connection password	•••••	
	TSAPIServerName=AVAYA#CMCYBER#	CSTA#PRE	Password (retype)	•••••	
	SAES ConnectionUpoSSL=Vee	<u>~</u>	Linked channel group	Avaya cert	~
17:51:06 You are editing an exist	ing record.			Cancel Sa	ve changes
17:46:46 You are editing an exist				Show statusbar messar	nerd
Done					

Select the **targets** secondary tab and click the "+" symbol for each target to be added. A target is any extension added either as active or a recording extension.

CyberTech Pro [SERVICE / ct-c08090113] - Windows Internet Explorer	
🗫 http://10.10.4.200/login.mainadmin.asp	<b>*</b>
	evaluation recorded calls quit
Overview of all device targets	0000
No records found in the database.	
Choose a target to edit it properties or add a new one to the list.	
13:34:14 You are editing an existing record.	Copy overview to dipboard Show statusbar messages overview
13:33:07 You are editing an existing record.	
Done	🧊 😜 Internet 🔍 100% 🔹 🖉

The **Device info** control appears each time the "+" control is clicked. Enter information for each of the targets to be monitored, as shown in the following table.

Name	Device	Туре	Range Start
			Start
3012	AvayaLink	Active Extension	3012
3013	AvayaLink Active Extension		3013
3006	AvayaLink Active Extension		3006
AgentB	AvayaLink	Extension	6001
AgentC	AvayaLink	Extension	6002
VDN	AvayaLink	Extension	1800
Huntgroup	untgroup AvayaLink Exter		3090
Target_B	AvayaLink	Recorded Extension	3006
Target_C	AvayaLink	Recorded Extension	3000

 Table 7: Cybertech Pro Target Device Info Parameters

#### An example of one target being added is shown in the following screen.

http://10.10.4.200/login.mainadmin.asp	~
CYBERTECH	
my account system installation cti integration system configuration user administration system status evaluation recorded calls quit devices targets selection overview linked channels	_
Dverview of all device targets	••
Add target	
Target name(s) ExtDig	
Device Avaya_Link	
Target type(s) Recorded Extension	
Target value range start 3006	
Target value range end (leave empty for single target)	
Target selection	
Cancel OK	

## Service Observe mode

After the targets have been entered, it should contain the following information in Service Observe mode.

-			configuration user administ	ration system status	evaluation recorded ca	alls quit
devices targets se verview of all device ta		ed channels				089
irget name	Target Sel	ection Device name	Target type	Target value	Date last modified	
DN	-	Avaya_Link	Extension	1800	2009-02-18	9 X
tVOIP	~	Avaya_Link	Recorded Extension	3000	2009-02-18	9 X.
ctDig	~	Avaya_Link	Recorded Extension	3006	2009-02-18	9 X
)12	~	Avaya_Link	Active Extension	3012	2009-02-16	∮ ¥.
13	~	Avaya_Link	Active Extension	3013	2009-02-16	∮ ¥.
intGroup	✓	Avaya_Link	Extension	3090	2009-02-17	1 ×
gentB	-	Avaya_Link	Extension	6001	2009-02-17	9 X
gentC		Avaya_Link	Extension	6002	2009-02-17	. ∮ ¥.
			1			

Solution & Interoperability Test Lab Application Notes ©2009 Avaya Inc. All Rights Reserved. Page 39 of 48 CT52-ACM-DMCC In the selection overview screen below the selected extensions which will be monitored in Service observe mode are displayed. The selected VDN is added as an extension.

CyberTech Pro [SEF	WICE / ct-c08090113] - Window	vs Internet Explorer				
http://10.10.4.200/login	n.mainadmin.asp					
my account sys devices targets Filter selection entries				n status evalua	tion recorded calls q	uit
Devices [All]		arget types [All]	*			Search
Overview of selection ( Farget name	entries Device name	Target type	Target value	▲ Target state	Date last modified	-
xtV0IP	Avaya_Link	Recorded Extension	3000	Set recording	2009-02-18	0
xtDig	Avaya_Link	Recorded Extension	3006	Set recording	2009-02-18	0
012	Avaya_Link	Active Extension	3012	Set recording	2009-02-16	0
013	Avaya_Link	Active Extension	3013	Set recording	2009-02-16	0
14:53:30 Record updi 14:53:27 You are edit		ght-click statusbar to send contents to the	windows		Copy overview to d	

Additional information about each of the targets is available via the I button. For example, this mechanism can be used to determine that endpoint C is being observed via virtual extension 3013.

CYBER	TECH					
my account syst	tem installation	system configuration user ad	Iministration system	n status evalua	ation recorded calls	quit
devices targets	selection overview linked channels	•				
evices [All]	,	Farget types [All]				Search
verview of selection e	entries					
arget name	Device name	Target type	Target value	<ul> <li>Target state</li> </ul>	Date last modified	
tVOIP	Avaya_Link	Recorded Extension	3000	Set recording	2009-02-18	0
				Out on a set is a	2009-02-18	0
	Avaya_Link	Recorded Extension	3006	Set recording	2005-02-10	
tDig	Avaya_Link Avaya_Link	Active Extension	3006 3012	Set recording	2009-02-16	0
tDig 12 13 ntGroup	Avaya_Link get message / alarms		3012			
tDig 12 13 intGroup	Avaya_Link get message / alarms	Active Extension	3012		2009-02-16	

Solution & Interoperability Test Lab Application Notes ©2009 Avaya Inc. All Rights Reserved.

#### Single Step Conference mode

The Cybertech Pro Recorder is configured for Single Step Conferencing for compliance testing. Targets are added as in Service Observe mode. After the targets have been entered, it should contain the following information in Single Step Conference mode.

http://10.10.4.200/login.		- Windows Interne	t Explorer			
	mainadmin.asp					
my account syste			configuration user administ	ration system status	evaluation recorded c	alls quit
Overview of all device t	argets					0800
Target name	Target Sel	ection Device name	Target type	Target value	Date last modified	
VDN	-	Avaya_Link	Extension	1800	2009-02-18	∮ ¥.
ExtVOIP	<ul> <li>Image: A second s</li></ul>	Avaya_Link	Conf. Rec. Extension	3000	2009-02-18	9 X
ExtDig	<ul> <li>✓</li> </ul>	Avaya_Link	Conf. Rec. Extension	3006	2009-02-18	∮ ¥.
3012	✓	Avaya_Link	Active Extension	3012	2009-02-16	∮¥.
3013	<ul> <li>✓</li> </ul>	Avaya_Link	Active Extension	3013	2009-02-16	∮ ¥.
HuntGroup	✓	Avaya_Link	Extension	3090	2009-02-17	9 X
AgentB		Avaya_Link	Extension	6001	2009-02-17	9 X
AgentC		Avaya_Link	Extension	6002	2009-02-17	1 ×
			1			
1960 CC		Cho	1	v one to the list.		
13:13:29 Record delete 13:13:25 Record delete		Cho	1	v one to the list.		eview to olicboard tubber mesages overview

In the **selection overview** tab on the screen below, the selected extensions are displayed which will be monitored in Single Step Conference mode. The selected Hunt group is added as an extension.

		system configuration user ad	ministration	status evalua	tion recorded calls d	quit
devices targets ilter selection entries	selection overview linked channels			1		
Devices [All]		get types [All]	~			Search
verview of selection e arget name	Device name	Target type	Target value	Target state	Date last modified	
xtVOIP	Avaya_Link	Conf. Rec. Extension	3000	Set recording	2009-02-18	0
xtDig	Avaya_Link	Conf. Rec. Extension	3006	Set recording	2009-02-18	0
012	Avaya_Link	Active Extension	3012	Selected	2009-02-16	0
013	Avaya_Link	Active Extension	3013	Selected	2009-02-16	0
untGroup	Avaya_Link	Extension	3090	Selected	2009-02-17	0

Solution & Interoperability Test Lab Application Notes ©2009 Avaya Inc. All Rights Reserved. Page 41 of 48 CT52-ACM-DMCC Additional information about each of the targets is available via the I button. For example, this mechanism can be used to determine that endpoint C is being observed in Single Step Conference mode.

🌈 CyberTe	ech Pro [SERVICE / ct-c08090113] -	Windows Internet Explorer				
🗫 http://10.	.10.4.200/login.mainadmin.asp					~
my acc devices		gration system configuration user	administration system	n status evalua	ntion recorded calls	quit
Filter selec	ction entries					3
Devices	[AII]	Target types [All]				Search
Oversiew	of selection entries					2
Target nam		Target type	Target value	Target state	Date last modified	
ExtVOIP	Avaya_Link	Conf. Rec. Extension	3000	Set recording	2009-02-18	0
ExtDig	Avaya_Link	Conf. Rec. Extension	3006	Set recording	2009-02-18	0
3012 3013	Avaya_Link	Active Extension	3012	Selected	2009-02-16	0
HuntGroup	Target message / alarn	15				0
		<u>_ 0K</u>	]			
(100)		1				200 (200)
13:11:33 13:10:25	Error starting java applet: The java applica	tion could not communicate with the server, de 3: Finger print matches, file is authentic).			Copy sverview to Show statuster or	

# 8. General Test Approach and Test Results

The test approach used placed calls using digital, VOIP and analogue phones. The tests were to verify the calls were being placed correctly and accurate audio recordings were being generated and collected by the Cybertech solution. Testing was performed manually. The tests were all functional in nature and performance testing was not included.

All of the test cases were executed and overall the solution was successful. One area of failure was a missing CLI on three calls.

The following results were obtained

- Confirmation of the ability of Cybertech Pro to correctly create voice recording files of various telephony operations
- Confirmation that the correct number of voice recording files is created for each operation performed
- Confirmation the voice content of each of the files is correct
- Confirmation the calling and called party for each of the files is correct
- Confirmation the start and stop times of each of the files is correct

The following was observed during testing:

A test had been included for bridged call appearance for Service Observe though the AES does not support this feature for Service Observe.

The test plan details the results and contains a complete summary report.

SF; Reviewed;	Solution & Interoperability Test Lab Application Notes	Page 42 of 48
SPOC 4/16/2009	©2009 Avaya Inc. All Rights Reserved.	CT52-ACM-DMCC

# 9. Verification Steps

## 9.1. Verify Avaya Communication Manager Status

The following steps can ensure that the communication between Avaya Communication Manager and the Avaya Application Enablement Services server is functioning correctly.

Verify that the service state of the TSAPI link is established. Check the TSAPI link status with AES by using the command below. The CTI Link is 10.

statu	s aesvcs	cti-li	nk				
			AE SERVICES	CTI LINK STAT	TUS		
CTI Link	Version	Mnt Busy	AE Services Server	Service State	Msgs Sent	Msgs Rcvd	
10	4	no	PresAES	established	12	13	

Verify that the status of AES interface is connected and listening.

status aesvcs :	interface		
	A	E SERVICES INT	TERFACE STATUS
Local Node	Enabled?	Number of Connections	Status
CLAN	yes	1	listening

Verify that the there is a link with the AES and that messages are being sent and received.

status	aesvcs link				
		AE SERVICES	LINK STATUS		
Srvr/ Link	AE Services Server	Remote IP	Remote Local Node Port	e Msgs Sent	Msgs Rcvd
02/01	PresAES	10.10.4.20	51158 CLAN	25	25

## 9.2. Verify Avaya AES Status

The following steps are carried out on the Application Enablement Services to ensure that the communication link between Avaya Communication Manager and the Avaya Application Enablement Services server is functioning correctly.

## 9.2.1. TSAPI Link

Verify the status of the TSAPI link by selecting **Status and Control**  $\rightarrow$  **Services Summary**. Select **TSAPI Service** (not shown), followed by **Details**.

The TSAPI Link Details screen is displayed as shown below.

Αναγα						Арј			stration and M	
CTI OAM Home	Υοι	ı are l	nere: > <u>St</u> .	atus and Cont	<u>rol</u> > <u>Serv</u>	ices Summary		<u>,</u>	<u>OAM Home 🕜H</u>	elp OLogo
Administration Status and Control TSAPI Link Details										
Switch Conn Summary Services Summary Maintenance		Link	Switch Conn Name	Switch CTI Link Number	Conn Status	Since	Service State	Switch Version	Number of Associations	ASAI Message Rate
<ul> <li><u>Alarms</u></li> <li><u>Logs</u></li> </ul>	0	1	CMCyber	10	Talking	2009-02-24 13:31:59.0	Online	15	0	15
<ul> <li><u>Utilities</u></li> <li><u>Help</u></li> </ul>										

Verify the status of the TSAPI link by checking that the **Connection Status** is **Talking** and the **Service State** is **Online**.

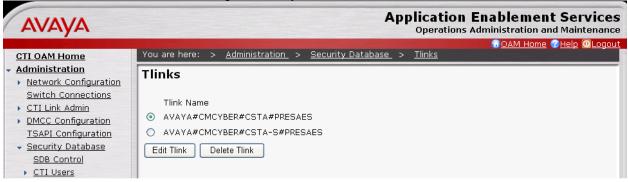
#### 9.2.2. DMCC Service

Verify the status of the DMCC service by selecting Status and Control  $\rightarrow$  Services Summary. Select DMCC Service (not shown), followed by Details. The DMCC Services Summary screen is displayed as shown below. It shows a connection to the Cybertech CTI Server, IP address '10.10.4.210'.

Αναγα					ment Service
CTI OAM Home	You are here: > <u>Status and (</u>	<u>Control</u> > <u>Services Su</u>	<u>mmary</u>	MAO O AM	Home @Help @Logo
Administration Status and Control	DMCC Service Summ	ary - Session Su	mmary		
Switch Conn Summary Services Summary	Session Summary Device Sum Generated on Mon, Feb 16, 200				
<u>Maintenance</u> <u>Alarms</u> Logs Utilities Help	Service Uptime: Number of Active Sessions: Number of Sessions Created Sir Number of Existing Devices: Number of Devices Created Sin	1 nce Service Boot: 4 0	, 2:07 hours		
	Session ID	User Application	<u>Far-end</u> Identifier	Connection Type	<u># of Associated</u> <u>Devices</u>
	226303EE7C00E9534           588430B04816585-8           Terminate Sessions	CTIUser Avaya_Link Show Terminated Session	_	XML Encrypted	0

### 9.2.3. TLinks

Navigate to Administration  $\rightarrow$  Security Database  $\rightarrow$  TLinks. Verify the value of the Tlinks name. This will be needed to configure the Cybertech server.



### 9.2.4. TSAPI Test

Make a call between two stations on Avaya Communication Manager using the TSAPI Link. Navigate to the screen as follows CTI OAM Home  $\rightarrow$  Utilities  $\rightarrow$  TSAPI Test. Use the username and password set up as in Section 6.4.

Αναγα			Application Enablement Services Operations Administration and Maintenance
CTI OAM Home	You are he	re: > <u>Utilities</u> > <u>TSAPI Test</u>	G <u>OAM Home</u> @Help @Logout
Administration     Status and Control	TSAPI	Test	
<ul> <li>Maintenance</li> <li>Alarms</li> </ul>	TLink	AVAYA#CMCYBER#CSTA-S#PRESAES	
▶ <u>Logs</u> ▼ <u>Utilities</u>	User: Password:	CTIUser	
<u>ASAI Test</u> <u>Ping Host</u>	From:	2500	
<u>TSAPI Test</u> <u>TR/87 Test</u>	To: Dial	2510	
• <u>Help</u>			

### 9.2.5. ASAI Test

Additional tests can be carried out by the using the ASAI Test. Open this screen under CTI **OAM Home**  $\rightarrow$  **Utilities**  $\rightarrow$  **ASAI Test**. This verifies that the TSAPI Link set up in Section 6.3 is communicating

is communicating.	•					
<u>Administration</u> Otatus and Control	ASAI Test					
<u>Status and Control</u> <u>Maintenance</u>						
<u>Alarms</u>	· · · · · · · · · · · · · · · · · · ·	Check the link numbers you would like to run ASAI Test on:				
▶ Logs	CVLAN Link	TSAPI Link				
<ul> <li><u>Utilities</u></li> </ul>	🗌 link 1	🗹 link 1				
ASAI Test	🗌 link 2	🔲 link 2				
Ping Host TSAPI Test	🔲 link 3	🗌 link 3				
TR/87 Test	🔲 link 4	🗌 link 4				
• <u>Help</u>	🗌 link 5	🗌 link 5				
	🗌 link 6	🗌 link 6				
	🗌 link 7	link 7				
	🔲 link 8	🗌 link 8				
	🗌 link 9	🗌 link 9				
	🗌 link 10	🗌 link 10				
	🗌 link 11	link 11				
	🗌 link 12	link 12				
	🗌 link 13	🗌 link 13				
	🗌 link 14	link 14				
	🗌 link 15	🗌 link 15				
	🗌 link 16	link 16				
	Select All Deselect /					

Run the ASAI Test and check the TSAPI link number on which you would like to run the test. A successful test will display a result as in the following screen.

AVAYA		Application Enablement Services Operations Administration and Maintenance
CTI OAM Home	You are here: > <u>Utilities</u>	GOAM Home @Help @Logout
Administration     Status and Control	ASAI Test Result	
<ul> <li>Maintenance</li> <li>Alarms</li> <li>Logs</li> <li>Utilities</li> </ul>	<ul> <li>ASAI Test</li> <li>\n=== Test for TSAPI Link 1 ===</li> <li>=== Test Completed ===</li> </ul>	

## 9.3. Verify Cybertech Configuration

The following steps can be performed to verify the basic operation of the system components:

- Make calls local and external to and from monitored stations to verify that the correct call records are produced
- Perform hold, transfer, blind transfer, and conferencing operations to verify that correct call records are produced
- Make calls to and from bridged appearances to verify that correct call records are produced
- Make calls from external telephones to a VDN to verify that correct call records are produced
- Make calls to agents and verify that correct call records are produced

SF; Reviewed; SPOC 4/16/2009

## 10. Conclusion

These Application Notes describe the conformance testing of the Cybertech Pro with Avaya Communication Manager and Avaya Application Enablement Services. All functionality and serviceability test cases were completed successfully by the Cybertech Pro solution.

# 11. Additional References

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

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

- 1. Administrator Guide for Avaya Communication Manager, Document No 03-300509, Issue 4, January 2008
- 2. Change Description for Release 5.1 of Avaya Communication Manager, SIP Enablement Services, Avaya Servers, and Media Gateways, Document No 03-602958, Issue 1, June 2008
- 3. Avaya MultiVantage® Application Enablement Services Administration and Maintenance Guide - Release 4.2, Document No 02-300357, Issue 10, May 2008
- 4. Developing Client-side IP Recording Applications using Avaya Application Enablement Services, An Avaya DevConnect Application Note, October 2008

The following documentation is available on request from Cybertech <u>http://www.cybertech-int.com</u>

- 1. Cybertech CT Recording Solutions R5 Installation Manual v5.3
- 2. Cybertech Parrot DSC VOIP installation manual
- 3. Cybertech CT Recording Solutions R5 CTI manual
- 4. Cybertech AVAYA DMCC connectivity manual

#### ©2009 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by  $\mathbb{R}$  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>.