



Configuring the Avaya Meeting Exchange S6200 Conferencing Server and Avaya Communication Manager to Manage Emergency/Crisis Scenarios Originating in an Enterprise Network - Issue 1.0

Abstract

These Application Notes present the procedures for configuring the Avaya Meeting Exchange S6200 Conferencing Server and Avaya Communication Manager to manage emergency/crisis scenarios originating in an enterprise network. For this sample configuration, Avaya Communication Manager was configured to provide Multiple Level Precedence and Preemption (MLPP), Malicious Call Trace (MCT) and off-hook alert features. The Avaya Meeting Exchange S6200 Conferencing Server was administered to generate auto blast dial conferences to a list of participants dedicated to resolving emergency/crisis scenarios. To further assist in the management of emergency/crisis scenarios, the Bridge Control API (BCAPI) on the Avaya Meeting Exchange S6200 Conferencing Server was utilized by a custom software application developed by Avaya to display events corresponding to emergency/crisis scenarios. These Application Notes resulted from a customer Proof of Concept request.

1. Introduction

These Application Notes present the procedures for configuring the Avaya Meeting Exchange S6200 Conferencing Server (Avaya Meeting Exchange) and Avaya Communication Manager to manage emergency/crisis scenarios originating in an enterprise network. For this sample configuration, this included:

- A standing conference utilized for meetings and a role call.
- A fire/emergency scenario.
- An off-hook alert scenario (see **Example 1**).

Figure 1 illustrates the sample network configuration utilized for this compliance tested solution. Avaya Communication Manager was configured to provide call routing, Multiple Level Precedence and Preemption (MLPP), Malicious Call Trace (MCT) and off-hook alert features. Avaya Meeting Exchange was administered to generate auto blast dial conferences to a list of participants dedicated to resolving emergency/crisis scenarios. To further assist in the management of emergency/crisis scenarios, the Bridge Control API (BCAPI) on Avaya Meeting Exchange was utilized by a custom software application developed by Avaya to display events corresponding to emergency/crisis scenarios. The software application was developed specifically for this Proof of Concept request, and is referred to as the Avaya Alarm Display Terminal (AADT). The AADT application runs on a Windows based PC installed with the Java Runtime Environment (JRE). Avaya Bridge Talk is an application for provisioning and managing conferencing applications on Avaya Meeting Exchange. For this sample configuration, Avaya Bridge Talk was utilized strictly for conference provisioning. The AADT application was utilized to manage conferences, and thus manage emergency/crisis scenarios. The AADT and Avaya Bridge Talk applications may reside on the same PC. Refer to [4] for information regarding Avaya Bridge Talk.

Example 1: The following example utilizes an off-hook alert to illustrate the concept of an emergency/crisis scenario, and the corresponding interoperability between Avaya Communication Manager, Avaya Meeting Exchange and the AADT application in managing the emergency/crisis scenario.

- If any station registered to Avaya Communication Manager in the Facility goes off-hook and does not enter a valid destination phone number within a prescribed time limit, Avaya Communication Manager will then alert Avaya Meeting Exchange of this emergency/crisis scenario by placing a call to Avaya Meeting Exchange from the station in the Facility that generated the off-hook alert.
- Avaya Meeting Exchange associates the call from Avaya Communication Manager with a pre-provisioned dial list and proceeds to create a conference to manage the emergency/crisis scenario. The conference is comprised of the station in the Facility that generated the off-hook alert, as well as the following participants on the dial list that were added via an auto blast dial:
 - All stations in the Response Team.
 - The station designated for the operator in the Control Room.
- Avaya Meeting Exchange generates events corresponding to the conference via BAPI.
- The AADT application captures and displays the events on a PC in the Control Room.

Signaling connectivity between Avaya Communication Manager and Avaya Meeting Exchange utilized SIP. To account for the SIP stations in this sample configuration, Avaya SIP Enablement Services was utilized as a SIP registration server only.

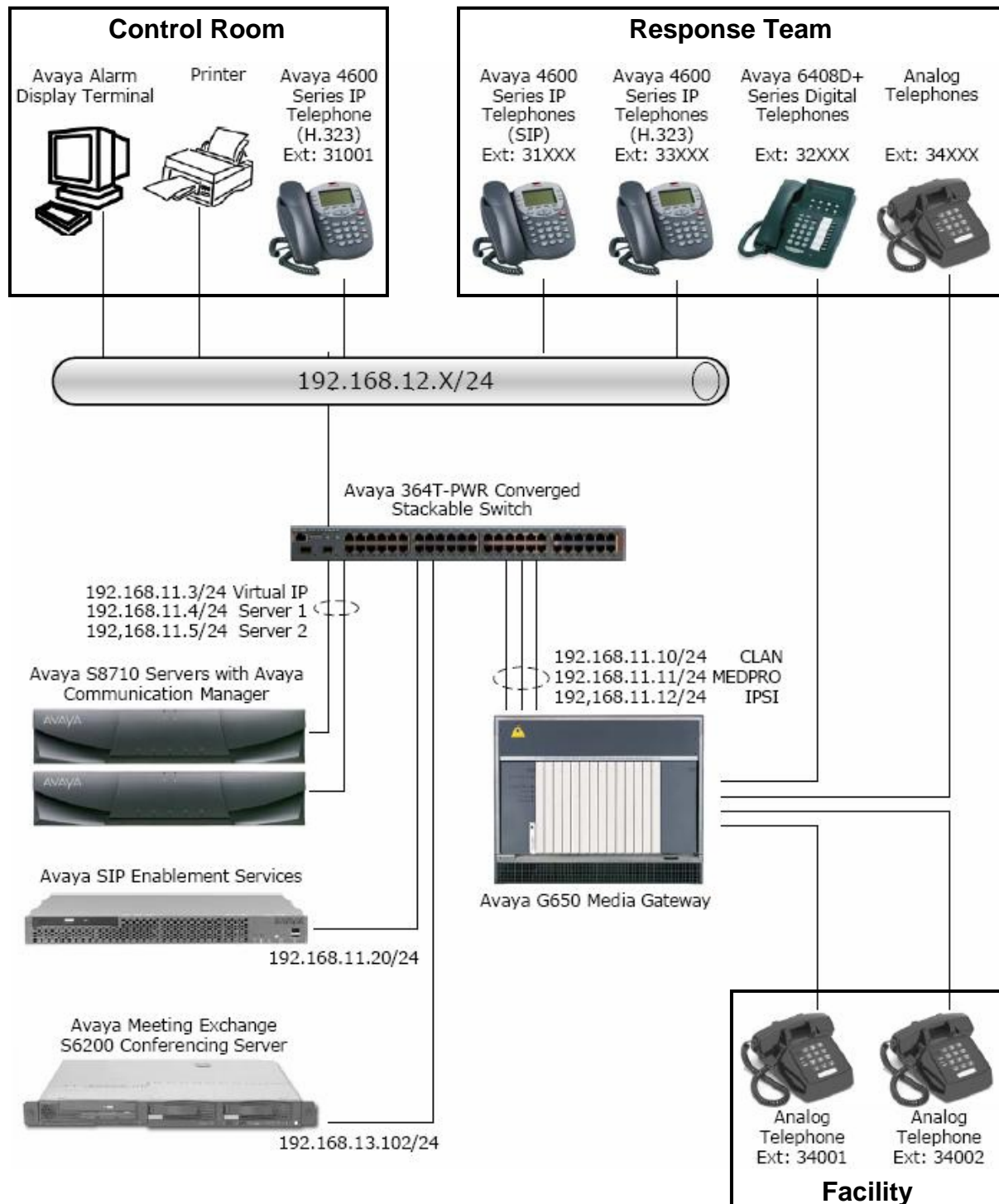


Figure 1: Sample Network Configuration

2. Equipment and Software Validated

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

Equipment	Software
Avaya S8710 Servers	Avaya Communication Manager 4.0 (S8710-014-00.0.730.5)
Avaya G650 Media Gateway <ul style="list-style-type: none">Avaya TN2312BP (IPSI)Avaya TN799DP (C-LAN)Avaya TN2302AP (MEDPRO)	HW12 FW038 HW01 FW024 HW20 FW115
Avaya Meeting Exchange S6200 Conferencing Server <ul style="list-style-type: none">Software versionIPCB build version	40102h mx7_1.3.00-84
Avaya Bridge Talk	4.0.03a
Avaya Alarm Display Terminal <ul style="list-style-type: none">Avaya Alarm Display Terminal applicationJava Runtime Environment	1.0 1.5.0_11-b03
Avaya SIP Enablement Services	SES-3.1.2.0-309.0
Avaya C364T-PWR Converged Stackable Switch	4.5.14
Avaya 4600 Series IP Telephones	2.8 (H.323)
Avaya 4600 Series IP Telephones	2.2.2 (SIP)
Avaya 6408D+ Digital Telephones	--
Analog Telephones	--

Table 1: Hardware and Software Versions

3. Assumptions and Limitations

For this sample configuration, the following are assumed:

- Avaya Meeting Exchange and Avaya Communication Manager are configured and operational.
- Signaling and media connectivity (e.g., trunking) between Avaya Communication Manager and Avaya Meeting Exchange is configured. Refer to [1] for details on configuring secure SIP connectivity utilizing Transport Layer Security (TLS) between Avaya Communication Manager and Avaya Meeting Exchange (S6200).

4. Avaya Communication Manager Configuration

This section describes the steps for configuring Avaya Communication Manager to interoperate with Avaya Meeting Exchange and to provide security applications for an enterprise network.

In these Application Notes, Avaya Communication Manager administrative software screens are shown with a gray shaded background. These screens are also referred to as System Access Terminal (SAT) screens. In some instances, the information from the original screen has been edited or annotated for brevity or clarity in presentation. For example, entries and/or fields in the SAT screens that were either modified or were required for these Application Notes are displayed with boldface type. After completion of the configuration in this section, perform a **save translation** command to make the changes permanent.

The administrative steps in this section have been divided into the following sub-sections:

- Verifying licensing on Avaya Communication Manager that is required to support the configuration displayed in these Application Notes.
- Configuring a Dial Plan on Avaya Communication Manager with Automatic Alternate Routing (AAR), Automatic Route Selection (ARS) Dial Access Code (DAC) and Feature Access Code (FAC) entries.
- Configuring call routing from Avaya Communication Manager to Avaya Meeting Exchange.
- Configuring MLPP on Avaya Communication Manager to allow users to request priority processing of their calls during critical situations.
- Administering the MCT feature on Avaya Communication Manager to track malicious calls.
- Configuring the off-hook alert feature on Avaya Communication Manager to enable an alerting/emergency call to be routed from Avaya Communication Manager to Avaya Meeting Exchange if an invalid call is attempted from a station registered to Avaya Communication Manager.
- Administering a station on Avaya Communication Manager to utilize the MLPP, MCT and off-hook alert features.

4.1. Verify Licensing

The following steps show procedures to verify licensing on Avaya Communication Manager that is required to support the configuration displayed in these Application Notes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.

Step	Description
4.1.1	<p>Issue the command “display system-parameters customer-options”, and proceed to page 3. Verify that the ARS/AAR Dialing without FAC field is enabled.</p> <p><i>Note: The ARS/AAR Dialing without FAC feature allows direct access to both the AAR and ARS digit analysis tables from the dial plan analysis table.</i></p> <pre> display system-parameters customer-options Page 3 of 11 OPTIONAL FEATURES Abbreviated Dialing Enhanced List? n Audible Message Waiting? y Access Security Gateway (ASG)? n Authorization Codes? n Analog Trunk Incoming Call ID? n Backup Cluster Automatic Takeover? n A/D Grp/Sys List Dialing Start at 01? n CAS Branch? n Answer Supervision by Call Classifier? n CAS Main? n ARS? y Change COR by FAC? n ARS/AAR Partitioning? y Computer Telephony Adjunct Links? y ARS/AAR Dialing without FAC? y Cvg Of Calls Redirected Off-net? n ASAI Link Core Capabilities? n DCS (Basic)? n ASAI Link Plus Capabilities? n DCS Call Coverage? n Async. Transfer Mode (ATM) PNC? n DCS with Rerouting? n Async. Transfer Mode (ATM) Trunking? n ATM WAN Spare Processor? n Digital Loss Plan Modification? n ATMS? n DS1 MSP? n Attendant Vectoring? y DS1 Echo Cancellation? n (NOTE: You must logoff & login to effect the permission changes.) </pre>

Step	Description
4.1.2	<p>Proceed to page 4, and verify that the Malicious Call Trace field is enabled.</p> <pre> display system-parameters customer-options Page 4 of 10 OPTIONAL FEATURES Emergency Access to Attendant? y IP Stations? y Enable 'dadmin' Login? y Enhanced Conferencing? y ISDN Feature Plus? n Enhanced EC500? y ISDN Network Call Redirection? n Enterprise Survivable Server? n ISDN-BRI Trunks? n Enterprise Wide Licensing? n ISDN-PRI? y ESS Administration? n Local Survivable Processor? n Extended Cvg/Fwd Admin? n Malicious Call Trace? y External Device Alarm Admin? n Media Encryption Over IP? n 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 Global Call Classification? n Multimedia Call Handling (Basic)? y Hospitality (Basic)? y Multimedia Call Handling (Enhanced)? y Hospitality (G3V3 Enhancements)? n IP Trunks? y IP Attendant Consoles? n (NOTE: You must logoff & login to effect the permission changes.) </pre>
4.1.3	<p>Proceed to page 5, and verify that the Multiple Level Precedence & Preemption field is enabled.</p> <pre> display system-parameters customer-options Page 5 of 10 OPTIONAL FEATURES Multinational Locations? n Station and Trunk MSP? n Multiple Level Precedence & Preemption? y Station as Virtual Extension? y Multiple Locations? n System Management Data Transfer? n Personal Station Access (PSA)? n Tenant Partitioning? n Posted Messages? n Terminal Trans. Init. (TTI)? n PNC Duplication? n Time of Day Routing? n Port Network Support? y Uniform Dialing Plan? y Usage Allocation Enhancements? y Processor and System MSP? n TN2501 VAL Maximum Capacity? y Private Networking? y Processor Ethernet? y Wideband Switching? n Wireless? n Remote Office? n Restrict Call Forward Off Net? y Secondary Data Module? y (NOTE: You must logoff & login to effect the permission changes.) </pre>

Step	Description
4.1.4	<p>Proceed to page 6, and verify that the Vectoring (Basic) field is enabled.</p> <div> display system-parameters customer-options <div>Page 6 of 10</div> <div> CALL CENTER OPTIONAL FEATURES <div> Call Center Release: 4.0 <div> <div> ACD? n Reason Codes? n BCMS (Basic)? n Service Level Maximizer? n BCMS/VuStats Service Level? n Service Observing (Basic)? y BSR Local Treatment for IP & ISDN? n Service Observing (Remote/By FAC)? n Business Advocate? n Service Observing (VDNs)? n 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)? n Vectoring (G3V4 Enhanced)? n EAS-PHD? n Vectoring (3.0 Enhanced)? n Forced ACD Calls? n Vectoring (ANI/II-Digits Routing)? n Least Occupied Agent? n Vectoring (G3V4 Advanced Routing)? n Lookahead Interflow (LAI)? n Vectoring (CINFO)? n Multiple Call Handling (On Request)? n Vectoring (Best Service Routing)? n Multiple Call Handling (Forced)? n Vectoring (Holidays)? n PASTE (Display PBX Data on Phone)? n Vectoring (Variables)? n (NOTE: You must logoff & login to effect the permission changes.) </div> </div> </div> </div> </div>

4.2. Configure a Dial Plan

Step	Description																																																																																																																					
4.2.1	<p>Issue the command “change dialplan analysis”, and administer settings as displayed. Refer to [5] for definitions regarding fields in this form.</p> <ul style="list-style-type: none">• Add an entry in the table for AAR.• Add entries in the table for ARS.• Add an entry in the table for a DAC.• Add an entry in the table for a FAC.• Note the entries for extensions in the dial plan analysis table, as they are referenced in subsequent steps.																																																																																																																					
	<div>change dialplan analysis<div>Page1 of 12</div><div>DIAL PLAN ANALYSIS TABLE</div><div>Percent Full:1</div><table><thead><tr><th>Dialed String</th><th>Total Length</th><th>Call Type</th><th>Dialed String</th><th>Total Length</th><th>Call Type</th><th>Dialed String</th><th>Total Length</th><th>Call Type</th></tr></thead><tbody><tr><td>0</td><td>1</td><td>fac</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>1</td><td>3</td><td>dac</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>2</td><td>3</td><td>ars</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>3</td><td>5</td><td>ext</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>4</td><td>3</td><td>ars</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>5</td><td>3</td><td>aar</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>6</td><td>3</td><td>ext</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>7</td><td>5</td><td>ext</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>8</td><td>2</td><td>fac</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>9</td><td>2</td><td>dac</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>*</td><td>1</td><td>fac</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>#</td><td>3</td><td>fac</td><td></td><td></td><td></td><td></td><td></td><td></td></tr></tbody></table></div>	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	0	1	fac							1	3	dac							2	3	ars							3	5	ext							4	3	ars							5	3	aar							6	3	ext							7	5	ext							8	2	fac							9	2	dac							*	1	fac							#	3	fac						
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type																																																																																																														
0	1	fac																																																																																																																				
1	3	dac																																																																																																																				
2	3	ars																																																																																																																				
3	5	ext																																																																																																																				
4	3	ars																																																																																																																				
5	3	aar																																																																																																																				
6	3	ext																																																																																																																				
7	5	ext																																																																																																																				
8	2	fac																																																																																																																				
9	2	dac																																																																																																																				
*	1	fac																																																																																																																				
#	3	fac																																																																																																																				

4.3. Configure Call Routing

The following steps show procedures to enable call routing from Avaya Communication Manager to Avaya Meeting Exchange. For this sample configuration, ARS/AAR dialing without FAC is utilized to route calls to Avaya Meeting Exchange. Note that other forms of call routing may be utilized. Refer to [5] for definitions regarding fields in the forms displayed in this section.

Step	Description
4.3.1	<p>Issue the command “change route-pattern <n>”, where n is the number of the route pattern to be administered. Add an entry in the table to utilize a SIP trunk group between Avaya Communication Manager and Avaya Meeting Exchange.</p> <ul style="list-style-type: none"> Enter the number of a SIP trunk group that has been configured and is operational in the Grp No field. Refer to [1] for details on configuring secure SIP connectivity utilizing Transport Layer Security (TLS) between Avaya Communication Manager and Avaya Meeting Exchange (S6200). Set the FRL field (Facility Restriction Level) to the lowest setting to disable any restrictions for call routing via this route pattern. Enter 0 in the No. Del Dgts field to delete zero digits from any digit strings utilizing this route pattern. <p><i>Note: The Secure SIP field is left at the default value n. This field specifies whether the SIP or SIPS prefix in SIP URI from Avaya Communication Manager will be used. For this sample configuration, the SIP URI used the SIP prefix.</i></p> <pre> change route-pattern 3 Page 1 of 3 Pattern Number: 3 Pattern Name: 002s6200 SIP SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC No Mrk Lmt List Del Digits Intw 1: 3 0 0 n user 2: n user 3: n user 4: n user 5: n user 6: n user BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR 0 1 2 3 4 W Request Dgts Format Subaddress 1: Y Y Y Y Y n n rest none 2: Y Y Y Y Y n n rest none 3: Y Y Y Y Y n n rest none 4: Y Y Y Y Y n n rest none 5: Y Y Y Y Y n n rest none 6: Y Y Y Y Y n n rest none </pre>

Step	Description
4.3.2	<p>Issue the command “change aar analysis <n>”, where n is the leading digit of a digit string to be administered, and add an entry in the table to account for a standing conference that is utilized for meetings and a role call.</p> <ul style="list-style-type: none">Enter a number in the Dialed String field that will be utilized by the call branding table on Avaya Meeting Exchange (see Step 5.2.2). <i>Note: This number is in agreement with the corresponding AAR entry in the dial plan provisioned in Step 4.2.1.</i>Enter the number of the route pattern provisioned in Step 4.3.1 in the Route Pattern field.
change aar analysis 4	
Page 1 of 2	
AAR DIGIT ANALYSIS TABLE	
Percent Full: 2	
Dialed String	Total Min Max Route Pattern Call Type Node Num ANI Req'd
555	3 3 3 aar n

Step	Description
4.3.3	<p>Issue the command “change ars analysis <n>”, where n is the leading digit of a digit string to be administered, and add entries in the table to account for both fire/emergency and off-hook alert scenarios.</p> <p>To account for the fire/emergency scenario:</p> <ul style="list-style-type: none">Enter a number in the Dialed String field that will be utilized by the call branding table on Avaya Meeting Exchange (see Step 5.2.3). <i>Note: This number is in agreement with the corresponding ARS entry in the dial plan provisioned in Step 4.2.1.</i>Enter the number of the route pattern provisioned in Step 4.3.1 in the Route Pattern field.Set the Call Type field to emer. <p>To account for the off-hook alert scenario:</p> <ul style="list-style-type: none">Enter a number in the Dialed String field that will be utilized by the call branding table on Avaya Meeting Exchange (see Step 5.2.4). <i>Note: This number is in agreement with the corresponding ARS entry in the dial plan provisioned in Step 4.2.1.</i>Enter the number of the route pattern provisioned in Step 4.3.1 in the Route Pattern field.Set the Call Type field to alrt to enable an audible alert for calls routed via this entry.
change ars analysis 4	
Page 1 of 2	
ARS DIGIT ANALYSIS TABLE	
Location: all	
Percent Full: 1	

4.4. Configure Multiple Level Precedence and Preemption

The following steps show procedures to administer MLPP on Avaya Communication Manager. The MLPP features allow users to request priority processing, or precedence of their calls during critical situations. Precedence calling allows users, on a call-by-call basis, to select a level of priority for each call based on their need and importance. Users may access five levels of precedence when placing calls:

- Flash Override (the highest precedence level)
- Flash
- Immediate
- Priority
- Routine (the default, and lowest precedence level)

Each station is administered with a maximum precedence level (the more important the user, the higher the precedence level). Users cannot originate calls at precedence levels higher than their maximum administered level. Note that non-MLPP calls are treated as routine level precedence calls.

Step	Description
4.4.1	<p>Issue the command “change system-parameters mlpp”, and administer settings to utilize the Worldwide Numbering Dial Plan (WNDP).</p> <pre>change system-parameters mlpp Page 1 of 1 MULTIPLE LEVEL PRECEDENCE & PREEMPTION PARAMETERS ANNOUNCEMENTS Blocked Precedence Level: Unauthorized Precedence Level: Vacant Code: Service Interruption: Busy, Not Equipped: PRECEDENCE CALLING-DIALED DIGIT ASSIGNMENT Flash Override: 0 Flash: 1 Immediate: 2 Priority: 3 Routine: 4 Attendant Diversion Timing (sec): Remote Attendant Route String: Worldwide Numbering Dial Plan Active? y Default Route Digit: 0 Precedence Call Timeout (sec): 30 Line Load Control Restriction Level: 0 Limited Line Load Control Origination: n WNDP Emergency 911 Route String: Preempt Emergency Call? y Default Service Domain: 0 ISDN Precedence Call Timeout (sec): 30</pre>

Step	Description														
4.4.2	<p>Issue the command “change feature-access-codes”, and proceed to page 8. Administer settings to access the MLPP feature via FAC.</p> <p><i>Note: The W NDP PRECEDENCE ACCESS CODES are in agreement with the corresponding DAC entry in the dial plan provisioned in Step 4.2.1.</i></p> <div><div>change feature-access-codes</div><div>Page8 of8</div><div>FEATURE ACCESS CODE (FAC) MLPP Features</div><div>Authorization Access code: Precedence Calling Access Code:</div><div>W NDP PRECEDENCE ACCESS CODES: Flash Override Access Code:90 Flash Access Code:91 Immediate Access Code:92 Priority Access Code:93 Routine Access Code:94</div></div>														
4.4.3	<p>Issue the command “change precedence-routing digit-conversion <n>”, where n is a qualifier for any digit or valid wildcard character. Add an entry to facilitate call routing (as provisioned in Section 4.2 and Section 4.3) to extensions on Avaya Communication Manager.</p> <p><i>Note: The rule administered for the Matching Pattern aligns with both the W NDP precedence access code provisioned in Step 4.4.2 and the entry for extensions with a leading 3 in the dial plan provisioned in Step 4.2.1. The wildcard character x in the Matching Pattern will match any single digit. For example, a precedence call to extension 31001 (utilizing any of the W NDP precedence access codes provisioned in Step 4.4.2) is invoked from an extension registered to Avaya Communication Manager by entering 9031001. This 7 digit sequence would match xx3 in the entry below and 2 digits would be deleted, thus allowing a precedence call (with flash override) to be placed to extension 31001.</i></p> <div><div>change precedence-routing digit-conversion x</div><div>Page1 of2</div><div>PRECEDENCE ROUTING DIGIT CONVERSION TABLE Percent Full: 1</div><table><thead><tr><th>Matching Pattern</th><th>Min</th><th>Max</th><th>Del</th><th>Replacement String</th><th>Net</th><th>Conv</th></tr></thead><tbody><tr><td>xx3</td><td>7</td><td>7</td><td>2</td><td></td><td>ext</td><td>n</td></tr></tbody></table></div>	Matching Pattern	Min	Max	Del	Replacement String	Net	Conv	xx3	7	7	2		ext	n
Matching Pattern	Min	Max	Del	Replacement String	Net	Conv									
xx3	7	7	2		ext	n									

Step	Description
4.4.4	<p data-bbox="293 268 1507 342">Issue the command “change cor <n>”, where n is the number of a class of restriction. Proceed to page 2, and administer settings as displayed.</p> <ul data-bbox="342 342 1490 678" style="list-style-type: none"> • Set the Maximum Precedence Level field to the highest level in this sample configuration. For this sample configuration, Flash Override (fo) was selected. Note that for this sample configuration, the only other precedence level utilized is Routine (the default, and lowest precedence level). Therefore, any value higher than Routine could have been selected. • Set the Preemptable field to n. This prohibits preemption to any station assigned to this class of restriction. Note that since Flash Override is the highest precedence level, setting the Preemptable field to n has the effect of not allowing a preemptive call to any station mapped to this class of restriction. <div data-bbox="293 709 1507 1266"> <div>change cor 2Page 2 of 22</div> <div> <div>CLASS OF RESTRICTION</div> <div> 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 </div> <div> Station Lock COR: 2 Outgoing Trunk Disconnect Timer (minutes): Line Load Control: 1 Maximum Precedence Level: foPreemptable? n MLPP Service Domain: </div> <div> Station-Button Display of UI IE Data? n Service Observing by Recording Device? n 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 </div> </div> </div>

4.5. Configure Malicious Call Trace

The following steps show procedures to administer MCT on Avaya Communication Manager. The MCT feature is used to track malicious calls. Both users (either calling or called party) and attendants can track malicious calls, and display information that identifies the source of the call. For this sample configuration, the MCT feature applied to users only.

Step	Description																																																																							
4.5.1	Issue the command “ change mct-group-extensions ”, and administer settings to enable MCT controllers by adding an entry for each MCT controller in the enterprise network. For this sample configuration, the station administered in Step 4.7.1 was the only station designated as an MCT controller.																																																																							
	change mct-group-extensions Page 1 of 2																																																																							
	<div>Extensions Administered to have an MCT-Control Button:</div> <table><tr><td>1: 33001</td><td>19:</td><td>37:</td><td>55:</td></tr><tr><td>2:</td><td>20:</td><td>38:</td><td>56:</td></tr><tr><td>3:</td><td>21:</td><td>39:</td><td>57:</td></tr><tr><td>4:</td><td>22:</td><td>40:</td><td>58:</td></tr><tr><td>5:</td><td>23:</td><td>41:</td><td>59:</td></tr><tr><td>6:</td><td>24:</td><td>42:</td><td>60:</td></tr><tr><td>7:</td><td>25:</td><td>43:</td><td>61:</td></tr><tr><td>8:</td><td>26:</td><td>44:</td><td>62:</td></tr><tr><td>9:</td><td>27:</td><td>45:</td><td>63:</td></tr><tr><td>10:</td><td>28:</td><td>46:</td><td>64:</td></tr><tr><td>11:</td><td>29:</td><td>47:</td><td>65:</td></tr><tr><td>12:</td><td>30:</td><td>48:</td><td>66:</td></tr><tr><td>13:</td><td>31:</td><td>49:</td><td>67:</td></tr><tr><td>14:</td><td>32:</td><td>50:</td><td>68:</td></tr><tr><td>15:</td><td>33:</td><td>51:</td><td>69:</td></tr><tr><td>16:</td><td>34:</td><td>52:</td><td>70:</td></tr><tr><td>17:</td><td>35:</td><td>53:</td><td>71:</td></tr><tr><td>18:</td><td>36:</td><td>54:</td><td>72:</td></tr></table>	1: 33001	19:	37:	55:	2:	20:	38:	56:	3:	21:	39:	57:	4:	22:	40:	58:	5:	23:	41:	59:	6:	24:	42:	60:	7:	25:	43:	61:	8:	26:	44:	62:	9:	27:	45:	63:	10:	28:	46:	64:	11:	29:	47:	65:	12:	30:	48:	66:	13:	31:	49:	67:	14:	32:	50:	68:	15:	33:	51:	69:	16:	34:	52:	70:	17:	35:	53:	71:	18:	36:	54:
1: 33001	19:	37:	55:																																																																					
2:	20:	38:	56:																																																																					
3:	21:	39:	57:																																																																					
4:	22:	40:	58:																																																																					
5:	23:	41:	59:																																																																					
6:	24:	42:	60:																																																																					
7:	25:	43:	61:																																																																					
8:	26:	44:	62:																																																																					
9:	27:	45:	63:																																																																					
10:	28:	46:	64:																																																																					
11:	29:	47:	65:																																																																					
12:	30:	48:	66:																																																																					
13:	31:	49:	67:																																																																					
14:	32:	50:	68:																																																																					
15:	33:	51:	69:																																																																					
16:	34:	52:	70:																																																																					
17:	35:	53:	71:																																																																					
18:	36:	54:	72:																																																																					

Step	Description
4.5.2	<p>Issue the command “change feature-access-codes”, and proceed to page 3. Administer settings to activate and deactivate the MCT feature.</p> <p><i>Note: The FACs entered for Malicious Call Trace Activation and Deactivation are in agreement with the corresponding FAC entry in the dial plan provisioned in Step 4.2.1.</i></p>
	<div>change feature-access-codes Page 3 of 8</div> <div> <div>FEATURE ACCESS CODE (FAC)</div> <div> <div>Leave Word Calling Send A Message:</div> <div>Leave Word Calling Cancel A Message:</div> <div>Limit Number of Concurrent Calls Activation: Malicious Call Trace Activation: 81 Deactivation: Deactivation: 82</div> <div>Meet-me Conference Access Code Change:</div> </div> <div> <div>PASTE (Display PBX data on Phone) Access Code:</div> <div>Personal Station Access (PSA) Associate Code: Dissociate Code:</div> <div>Per Call CPN Blocking Code Access Code:</div> <div>Per Call CPN Unblocking Code Access Code:</div> </div> <div> <div>Priority Calling Access Code:</div> <div>Program Access Code:</div> </div> <div> <div>Refresh Terminal Parameters Access Code:</div> <div>Remote Send All Calls Activation: Deactivation:</div> <div>Self Station Display Activation: Deactivation:</div> <div>Send All Calls Activation: Deactivation:</div> <div>Station Firmware Download Access Code:</div> </div> </div>

Step	Description
4.5.3	<p>Issue the command “change cor <n>”, where n is the number of a class of restriction, and administer settings as displayed.</p> <ul style="list-style-type: none"> Set the Calling Party Restriction field to none to eliminate any restrictions regarding outbound calling for stations utilizing this class of restriction. Verify that the Access to MCT field is set to y to enable activation of the MCT feature (via FAC, provisioned in Step 4.5.2) by stations mapped to this class of restriction. For this sample configuration, this includes all stations in the Facility and on the Response Team. <p><i>Note: This COR will be utilized by all stations in this sample configuration other than the MCT controller. The MCT Controller will use the COR provisioned in Step 4.4.4 and Step 4.5.4.</i></p>
	<div>display cor 1</div> <div>Page 1 of 22</div> <div> <div>CLASS OF RESTRICTION</div> <div> <div>COR Number: 1</div> <div>COR Description:</div> <div> <div>FRL: 0</div> <div>Can Be Service Observed? n</div> <div>Can Be A Service Observer? n</div> <div>Partitioned Group Number: 1</div> <div>Priority Queuing? n</div> <div>Restriction Override: none</div> <div>Restricted Call List? n</div> <div> <div>APLT? y</div> <div>Calling Party Restriction: none</div> <div>Called Party Restriction: none</div> <div>Forced Entry of Account Codes? n</div> <div>Direct Agent Calling? n</div> <div>Facility Access Trunk Test? n</div> <div>Can Change Coverage? n</div> <div> <div>Access to MCT? y</div> <div>Fully Restricted Service? n</div> <div>Group II Category For MFC: 7</div> <div>Send ANI for MFE? n</div> <div>MF ANI Prefix:</div> <div>Automatic Charge Display? n</div> <div>Hear System Music on Hold? y</div> <div>PASTE (Display PBX Data on Phone)? n</div> <div>Can Be Picked Up By Directed Call Pickup? n</div> <div>Can Use Directed Call Pickup? n</div> <div>Group Controlled Restriction: inactive</div> </div> </div> </div> </div> </div>

Step	Description
4.5.4	<p>Issue the command “change cor <n>”, where n is the number of the class of restriction provisioned in Step 4.4.4, and administer settings for use by MCT controllers.</p> <ul style="list-style-type: none"> Set the Calling Party Restriction field to none to eliminate any restrictions regarding outbound calling for stations utilizing this class of restriction. Verify that the Access to MCT field is set to y to enable the display of MCT information on any station designated as an MCT controller. For this sample configuration, this class of restriction will be utilized by the station in the Control Room.
	<div>change cor 2</div> <div>Page 1 of 22</div> <div> <div>CLASS OF RESTRICTION</div> <div> <div>COR Number: 2</div> <div>COR Description: Preemptable FlashOverride</div> <div> <div>FRL: 0</div> <div>Can Be Service Observed? n</div> <div>Can Be A Service Observer? n</div> <div>Partitioned Group Number: 1</div> <div>Priority Queuing? n</div> <div>Restriction Override: none</div> <div>Restricted Call List? n</div> </div> <div> <div>APLT? y</div> <div>Calling Party Restriction: none</div> <div>Called Party Restriction: none</div> <div>Forced Entry of Account Codes? n</div> <div>Direct Agent Calling? n</div> <div>Facility Access Trunk Test? n</div> <div>Can Change Coverage? n</div> </div> <div> <div>Access to MCT? y</div> <div>Group II Category For MFC: 7</div> <div>Send ANI for MFE? n</div> <div>MF ANI Prefix:</div> <div>Hear System Music on Hold? y</div> </div> <div> <div>Fully Restricted Service? n</div> <div>Automatic Charge Display? n</div> <div>PASTE (Display PBX Data on Phone)? n</div> <div>Can Be Picked Up By Directed Call Pickup? n</div> <div>Can Use Directed Call Pickup? n</div> <div>Group Controlled Restriction: inactive</div> </div> </div> </div>

4.6. Configure Off-Hook Alert

The following steps show procedures to enable the off-hook alert feature on Avaya Communication Manager. This will enable an alerting/emergency call to be routed from Avaya Communication Manager to Avaya Meeting Exchange if an invalid call is attempted from a station registered to Avaya Communication Manager. For this sample configuration, the definition of an invalid call is if a station registered to Avaya Communication Manager goes off-hook and does not enter a valid destination phone number within a prescribed time limit.

Step	Description																																																																																																																																																																																																																																																																																																																	
4.6.1	<p>Issue the command “change cos”, and administer settings to enable off-hook alerting for stations utilizing this class of service. Set the Off-hook Alert field to y under the class of service 1.</p> <p><i>Note: All stations in this sample configuration were mapped to this class of service, thus enabling the off-hook alert feature for all stations.</i></p>																																																																																																																																																																																																																																																																																																																	
	<table><tr><td>change cos</td><td colspan="15">Page 1 of 2</td></tr><tr><td></td><td colspan="16">CLASS OF SERVICE</td></tr><tr><td></td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td></tr><tr><td>Auto Callback</td><td>n</td><td>y</td><td>y</td><td>n</td><td>y</td><td>n</td><td>y</td><td>n</td><td>y</td><td>n</td><td>y</td><td>n</td><td>y</td><td>n</td><td>y</td><td>n</td></tr><tr><td>Call Fwd-All Calls</td><td>n</td><td>y</td><td>n</td><td>y</td><td>y</td><td>n</td><td>n</td><td>y</td><td>y</td><td>n</td><td>n</td><td>y</td><td>y</td><td>n</td><td>n</td><td>y</td></tr><tr><td>Data Privacy</td><td>n</td><td>y</td><td>n</td><td>n</td><td>n</td><td>y</td><td>y</td><td>y</td><td>y</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>y</td><td>y</td></tr><tr><td>Priority Calling</td><td>n</td><td>y</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>y</td><td>y</td><td>y</td><td>y</td><td>y</td><td>y</td><td>y</td></tr><tr><td>Console Permissions</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td></tr><tr><td>Off-hook Alert</td><td>n</td><td>y</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td></tr><tr><td>Client Room</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td></tr><tr><td>Restrict Call Fwd-Off Net</td><td>y</td><td>n</td><td>y</td><td>n</td><td>y</td><td>y</td><td>y</td><td>y</td><td>y</td><td>y</td><td>y</td><td>y</td><td>y</td><td>y</td><td>y</td><td>y</td></tr><tr><td>Call Forwarding Busy/DA</td><td>n</td><td>n</td><td>n</td><td>y</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td></tr><tr><td>Personal Station Access (PSA)</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td></tr><tr><td>Extended Forwarding All</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td></tr><tr><td>Extended Forwarding B/DA</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td></tr><tr><td>Trk-to-Trk Transfer Override</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td></tr><tr><td>QSIG Call Offer Originations</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td></tr><tr><td>Contact Closure Activation</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td><td>n</td></tr></table>	change cos	Page 1 of 2																CLASS OF SERVICE																	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Auto Callback	n	y	y	n	y	n	y	n	y	n	y	n	y	n	y	n	Call Fwd-All Calls	n	y	n	y	y	n	n	y	y	n	n	y	y	n	n	y	Data Privacy	n	y	n	n	n	y	y	y	y	n	n	n	n	n	y	y	Priority Calling	n	y	n	n	n	n	n	n	n	y	y	y	y	y	y	y	Console Permissions	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	Off-hook Alert	n	y	n	n	n	n	n	n	n	n	n	n	n	n	n	n	Client Room	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	Restrict Call Fwd-Off Net	y	n	y	n	y	y	y	y	y	y	y	y	y	y	y	y	Call Forwarding Busy/DA	n	n	n	y	n	n	n	n	n	n	n	n	n	n	n	n	Personal Station Access (PSA)	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	Extended Forwarding All	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	Extended Forwarding B/DA	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	Trk-to-Trk Transfer Override	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	QSIG Call Offer Originations	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	Contact Closure Activation	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n
change cos	Page 1 of 2																																																																																																																																																																																																																																																																																																																	
	CLASS OF SERVICE																																																																																																																																																																																																																																																																																																																	
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15																																																																																																																																																																																																																																																																																																		
Auto Callback	n	y	y	n	y	n	y	n	y	n	y	n	y	n	y	n																																																																																																																																																																																																																																																																																																		
Call Fwd-All Calls	n	y	n	y	y	n	n	y	y	n	n	y	y	n	n	y																																																																																																																																																																																																																																																																																																		
Data Privacy	n	y	n	n	n	y	y	y	y	n	n	n	n	n	y	y																																																																																																																																																																																																																																																																																																		
Priority Calling	n	y	n	n	n	n	n	n	n	y	y	y	y	y	y	y																																																																																																																																																																																																																																																																																																		
Console Permissions	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n																																																																																																																																																																																																																																																																																																		
Off-hook Alert	n	y	n	n	n	n	n	n	n	n	n	n	n	n	n	n																																																																																																																																																																																																																																																																																																		
Client Room	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n																																																																																																																																																																																																																																																																																																		
Restrict Call Fwd-Off Net	y	n	y	n	y	y	y	y	y	y	y	y	y	y	y	y																																																																																																																																																																																																																																																																																																		
Call Forwarding Busy/DA	n	n	n	y	n	n	n	n	n	n	n	n	n	n	n	n																																																																																																																																																																																																																																																																																																		
Personal Station Access (PSA)	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n																																																																																																																																																																																																																																																																																																		
Extended Forwarding All	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n																																																																																																																																																																																																																																																																																																		
Extended Forwarding B/DA	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n																																																																																																																																																																																																																																																																																																		
Trk-to-Trk Transfer Override	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n																																																																																																																																																																																																																																																																																																		
QSIG Call Offer Originations	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n																																																																																																																																																																																																																																																																																																		
Contact Closure Activation	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n	n																																																																																																																																																																																																																																																																																																		

Step	Description
4.6.2	<p>Issue the command “change system-parameters features”, and proceed to page 4. Administer settings for the off-hook alert feature.</p> <ul style="list-style-type: none"> Set the Time before Off-hook Alert field to an appropriate value. <i>Note: This setting is not a one-to-one mapping in seconds. For this sample configuration, the value 4 was selected, which correlated with generating an off-hook alert in approximately fourteen seconds.</i> Enter a number that corresponds to an available and valid extension in the Emergency Access Redirection Extension field.
	<div>change system-parameters features Page 4 of 17</div> <pre> FEATURE-RELATED SYSTEM PARAMETERS Reserved Slots for Attendant Priority Queue: 5 Time before Off-hook Alert: 4 Emergency Access Redirection Extension: 77444 Number of Emergency Calls Allowed in Attendant Queue: 15 Maximum Number of Digits for Directed Group Call Pickup:4 Call Pickup on Intercom Calls? y Call Pickup Alerting? n Temporary Bridged Appearance on Call Pickup? y Directed Call Pickup? n 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 Controlled Toll Restriction Replaces: none </pre>

Step	Description
4.6.3	<p>Issue the command “change vector <n>”, where n is the number of an available vector, and administer a vector to utilize the dial plan and call routing provisioned in Section 4.2 and Section 4.3 respectively.</p> <pre> change vector 2 Page 1 of 6 CALL VECTOR Number: 2 Name: Off-Hook-Alert Multimedia? n Meet-me Conf? n Lock? n Basic? y EAS? n G3V4 Enhanced? n ANI/II-Digits? n ASAI Routing? n Prompting? y LAI? n G3V4 Adv Route? n CINFO? n BSR? n Holidays? n Variables? n 3.0 Enhanced? n 01 route-to number 444 with cov n if unconditionally 02 03 04 05 Press 'Esc f 6' for Vector Editing </pre>
4.6.4	<p>Issue the command “change vdn <n>”, where n is the number of an available extension, and administer a vector directory number to direct incoming calls from the emergency access redirection extension provisioned in Step 4.6.2 to the vector provisioned in Step 4.6.3.</p> <ul style="list-style-type: none"> Enter the emergency access redirection extension provisioned in Step 4.6.2 in the Extension field. Enter the number of the vector provisioned in Step 4.6.3 in the Vector Number field. <pre> change vdn 77444 Page 1 of 2 VECTOR DIRECTORY NUMBER Extension: 77444 Name*: Off-Hook-Alert Vector Number: 2 Meet-me Conferencing? n Allow VDN Override? n COR: 1 TN*: 1 Measured: none * Follows VDN Override Rules </pre>

4.7. Administer a Station

The following steps show procedures to administer a station on Avaya Communication Manager to utilize the MLPP, MCT and off-hook alert features provisioned in **Section 4.4**, **Section 4.5** and **Section 4.6** respectively.

Step	Description
4.7.1	<p>Issue the command “add station <n>”, where n is the number of an available and valid extension, and add a station as displayed.</p> <ul style="list-style-type: none"> Enter a descriptive label for this station in the Name field. <i>Note: The entry in the name field is utilized for Automatic Number Identification (ANI) and may be used for identifying this station. For this sample configuration, the ANI is utilized to identify the physical location of a station.</i> Enter the number of the class of restriction provisioned in Step 4.4.4 and Step 4.5.4 in the COR field. Enter the number of the class of service provisioned in Step 4.6.1 in the COS field. <p><i>Note: For this sample configuration, an IP station was added for utilization in the Control Room as displayed in Figure 1. Any station type that supports feature button assignments could have been selected for this location.</i></p> <pre> add station 33001 Page 1 of 5 STATION Extension: 33001 Lock Messages? n BCC: 0 Type: 4620 Security Code: 123456 TN: 1 Port: IP Coverage Path 1: COR: 2 Name: H.323 33001 Control Room Coverage Path 2: COS: 1 Hunt-to Station: STATION OPTIONS Loss Group: 19 Time of Day Lock Table: Speakerphone: 2-way Personalized Ringing Pattern: 1 Display Language: english Message Lamp Ext: 33001 Survivable GK Node Name: Mute Button Enabled? y Expansion Module? n Survivable COR: internal Media Complex Ext: Survivable Trunk Dest? y IP SoftPhone? n Customizable Labels? y </pre>

Step	Description
4.7.2	<p>Proceed to page 4, and administer settings as displayed.</p> <ul style="list-style-type: none"> Add a feature button assignment for mct-contr to designate this station as an MCT controller. An MCT controller can view real time MCT activity in the enterprise network by pressing the mct-contr button when the MCT feature is activated. <p><i>Note: Stations designated as MCT controllers receive a special ring-tone to alert them when the MCT feature is activated.</i></p> Add a feature button assignment for crss-alert to enable this station to receive, and clear off-hook alerts. <p><i>Note: Feature button assignments may be added in any location. For this sample configuration, feature button assignments 5 and 8 were chosen to align horizontally on opposite sides of the display screen on this 4620 station.</i></p>
	<pre> add station 33001 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: mct-contr 2: call-appr 6: 3: call-appr 7: 4: 8: crss-alert </pre>

Step	Description
4.7.3	<p>Issue the command “change system-parameters features”, and proceed to page 6. Set the Auto Hold field to y.</p> <p><i>Note: This is an optional step to simplify the management of receiving multiple calls on a station. This is accomplished by enabling incoming calls to a station that is provisioned with multiple call appearances to automatically connect to each call when the appropriate call appearance is selected. For this sample configuration, the operator of the station in the Control Room is able to respond to multiple incoming calls from Avaya Meeting Exchange by simply selecting the appropriate call appearance. If this feature were not enabled, the operator would have to first select the hold button to place the current call on hold, and then select the appropriate call appearance.</i></p> <pre> display system-parameters features Page 6 of 17 FEATURE-RELATED SYSTEM PARAMETERS Public Network Trunks on Conference Call: 5 Auto Start? n Conference Parties with Public Network Trunks: 6 Auto Hold? y Conference Parties without Public Network Trunks: 6 Attendant Tone? y Night Service Disconnect Timer (seconds): 180 Bridging Tone? n Short Interdigit Timer (seconds): 3 Conference Tone? n Unanswered DID Call Timer (seconds): Intrusion Tone? n Line Intercept Tone Timer (seconds): 30 Mode Code Interface? n Long Hold Recall Timer (seconds): 0 Reset Shift Timer (seconds): 0 Station Call Transfer Recall Timer (seconds): 0 Recall from VDN? n DID Busy Treatment: tone Allow AAR/ARS Access from DID/DIOD? n Allow ANI Restriction on AAR/ARS? n Use Trunk COR for Outgoing Trunk Disconnect? n 7405ND Numeric Terminal Display? n 7434ND? n DISTINCTIVE AUDIBLE ALERTING Internal: 1 External: 2 Priority: 3 Attendant Originated Calls: external </pre>

5. Avaya Meeting Exchange Configuration

This section describes the steps for configuring Avaya Meeting Exchange to interoperate with Avaya Communication Manager and to provide security applications for an enterprise network.

The administrative steps in this section have been divided into the following sub-sections:

- Configure call routing to enable the following:
 - Outbound calling from Avaya Meeting Exchange to Avaya Communication Manager.
 - Inbound calling to Avaya Meeting Exchange.
- Configure call branding via the Call Branding Utility (CBUTIL).
- Provision conferences via Avaya Bridge Talk.

5.1. Configure Call Routing

The following steps show procedures to enable call routing for Avaya Meeting Exchange. On Avaya Meeting Exchange, call routing is defined as follows:

- For outbound calls from Avaya Meeting Exchange, telephone number to URI translations are utilized. These translations associate a telephone number pattern with a corresponding SIP URI, thus allowing call origination from Avaya Meeting Exchange.
- For inbound calls to Avaya Meeting Exchange, URI to telephone number translations are utilized. These translations associate calls to Avaya Meeting Exchange with corresponding call flows, based on incoming SIP URIs.

Step	Description
5.1.1	Login to the Avaya Meeting Exchange console to access the Command Line Interface (CLI) with the appropriate credentials.

Step	Description						
5.1.2	<p>To enable outbound calling from Avaya Meeting Exchange to Avaya Communication Manager, configure telephone number to URI translations as follows:</p> <ul style="list-style-type: none">From the /usr/ipcb/config directory, edit the telnumToUri.tab file with a text editor.Add rules, separated by either tabs or single spaces, as a line in the file to route outbound calls from Avaya Meeting Exchange to Avaya Communication Manager. Metacharacters such as * (refers to a character string) or ? (refers to a single character) may be utilized.<ul style="list-style-type: none">The rule entered under the TelnumPattern column matches any five digit pattern with a leading “3”.The rule entered under the TelnumConversion column routes the call to the CLAN on Avaya Communication Manager (192.168.11.10) via SIP/TLS. To enable SIP connectivity utilizing TLS, the rule must syntactically conform to SIP standards regarding URI, and contain 5061 and transport=tls. Avaya Meeting Exchange will replace \$0 with the dialed number in outgoing SIP INVITE messages. For example, if <i>31001</i> is dialed, Avaya Meeting Exchange will send a SIP INVITE message with: sip:<i>31001</i>@192.168.11.10:5061;transport=tls in the SIP URI and “To” header field. <p><i>Note: Alternatively, routing to Avaya Communication Manager could have been enabled with the following entry:</i></p> <p><i>* sip:\$0@192.168.11.10:5061;transport=tls, where * is a wildcard, and routes any dialed digits to Avaya Communication Manager.</i></p>						
	<pre># telnum to uri conversion table # # This file is for dialing out from the Bridge to an external party. The # digits that are dialed are converted into the Request URI in the SIP INVITE. # For example, if the digits dialed were 936543 and one of the patterns was # "93?????" a match would take place. If the conversion for that match was # \$1 then the Request URI for the SIP INVITE would be sip:936543@10.221.11.250 #THE COMMENT COLLUM OR ANY OF THE COLLUMS SHOULD HAVE NO SPACES</pre> <table><tr><th>TelnumPattern</th><th>TelnumConversion</th><th>comment</th></tr><tr><td>3????</td><td>sip:\$0@192.168.11.10:5061;transport=tls</td><td>AvayaCommunicationManager</td></tr></table>	TelnumPattern	TelnumConversion	comment	3????	sip:\$0@192.168.11.10:5061;transport=tls	AvayaCommunicationManager
TelnumPattern	TelnumConversion	comment					
3????	sip:\$0@192.168.11.10:5061;transport=tls	AvayaCommunicationManager					

Step	Description
5.1.3	<p>To associate incoming calls to Avaya Meeting Exchange with corresponding call flows, configure URI to telephone number translations to extract values for both the Direct Inward Dial (DID, also known as DDI in Europe), and the Automatic Number Identification (ANI) as follows:</p> <ul style="list-style-type: none"> From the <code>/usr/ipcb/config</code> directory, edit the UriToTelnum.tab file with a text editor. Add rules, separated by either tabs or single spaces, as a line in the file to match the pattern of the “To” and “From” header fields in SIP INVITE messages from Avaya Communication Manager. The DID is extracted from the “To” header field and the ANI is extracted from the “From” header field. Metacharacters such as * or ? may be utilized. <ul style="list-style-type: none"> The rules under the TelnumPattern and TelnumConversion columns work in conjunction as follows. Assume Avaya Communication Manager sends a SIP INVITE message with the following “To” and “From” header fields. The rule <code>""""*<sip:*"</code> matches the following: <ul style="list-style-type: none"> To: "444" <sip:444@192.168.13.102>, where \$1 utilizes 444 (the variable contained in the first *) as the DID value for the call. From: "Block 08 34002" <sip:34002@avaya.com>, where \$1 utilizes Block 08 34002 as the ANI for the call. Enable an undefined caller to receive a prompt for operator assistance by adding an entry for a wildcard as the last line in this file. This entry accounts for the condition of an unmatched “To” header field. <p><i>Note: Entries in this file are read sequentially, therefore, the entry for the wildcard must be the last line in the file. Otherwise, all calls to Avaya Meeting Exchange would match the wildcard and thus receive a prompt for operator assistance.</i></p> <pre># request URI to telnum conversion table # # This table converts the Request URI in the SIP INVITE request to the # appropriate value specified when a pattern is matched. For example, if the # request Uri was "<sip:3333@10.220.10.4>" and one of the patterns was # "<sip:*@*" a match would take place. If the conversion for that match was # \$1 then 3333 would be passed as the ddi for the call. If the conversion for # that match were "0000" then 0000 would be passed as their ddi for the call. #THE COMMENT COLLUM OR ANY OF THE COLLUMS SHOULD HAVE NO SPACES TelnumPattern TelnumConversion comment """"*<sip:*" \$1 FromAvayaCommunicationManager * \$0 wildcard</pre>
5.1.4	<p>Reboot Avaya Meeting Exchange for changes to take effect.</p> <pre>[S6200]> init 6</pre>

5.2. Configure Call Branding

The following steps provide examples of how to provision a direct call function by utilizing the Call Branding Utility (CBUTIL) on Avaya Meeting Exchange. A command line utility, CBUTIL enables administrators to assign a specific annunciator message, line name, company name, system function, reservation group and prompt sets to a maximum of 30,000 DNIS or DID entries. Avaya Meeting Exchange parses these entries in numerically ascending order, with the wildcard character “?” last in the list. For example, 129? follows 1299. The last entry in the table consists entirely of wildcard characters. The number of characters in this entry corresponds to the number of DNIS/DDI digits specified in the Digit Parameters configuration.

Step	Description
5.2.1	<p>Prior to utilizing the CBUTIL utility, set the UNIX shell environment as follows:</p> <ul style="list-style-type: none">• If not already logged on, login to the Avaya Meeting Exchange console to access the CLI with the appropriate credentials.• At the command prompt, enter “tcsh” to set the UNIX shell environment.• At the command prompt, enter “cbutil” to view a list and description of commands associated with the call branding utility.
	<pre># tcsh .tcshrc on /dev/pts002 You are connected to the root account. Your environment has been set to vt220. This system currently has release 40102h of software installed. S6200->cbutil cbutil Copyright 2004 Avaya, Inc. All rights reserved. Usage: cbutil <command> [command-specific args...] where <command> may be one of: add Add an entry to the Call Branding table remove Remove an entry from the Call Branding table update Update an entry in the Call Branding table lookup Display an entry in the Call Branding table count Display the number of entries in the Call Branding table list List entries in the Call Branding table dnissize Set system configured max dnis length (1-16) Note: This command should only be used when the bridge is not running. Use "cbutil<command> -help" to get help on a specific command</pre>


Step	Description
5.2.2	<p>Add an entry to the call branding table to enable access to conferences provisioned on Avaya Meeting Exchange as moderator, without entering a passcode, as follows:</p> <ul style="list-style-type: none"> Add an entry for a direct call function that maps the DID value obtained from procedures in Step 5.1.3 to a conference (see Step 5.3.6) by entering “cbutil add 555 0 301 1 n direct” at the command prompt. The syntax for this command is defined as follows: cbutil add <dnis> <rg> <msg> <ps> <ucps> <func> [-l <ln> -c <cn>], where: <ul style="list-style-type: none"> <dnis> DNIS <rg> Reservation group <msg> Annunciator message number <ps> Prompt set number (0-20) <ucps> Use conference prompt set (y/n) <func> One of: DIRECT/SCAN/ENTER/HANGUP/AUTOVL/FLEX -l <"ln"> Optional line name to associate with caller -c <"cn"> Optional company name to associate with caller <p>S6200-> cbutil add 555 0 301 1 n direct cbutil Copyright 2004 Avaya, Inc. All rights reserved.</p>
5.2.3	<p>Repeat Step 5.2.2 to add an entry to the call branding as follows:</p> <p>S6200->cbutil add 222 0 0 1 n direct cbutil Copyright 2004 Avaya, Inc. All rights reserved.</p>
5.2.4	<p>Repeat Step 5.2.2 to add an entry to the call branding as follows:</p> <p>S6200-> cbutil add 444 0 0 1 n direct cbutil Copyright 2004 Avaya, Inc. All rights reserved.</p>

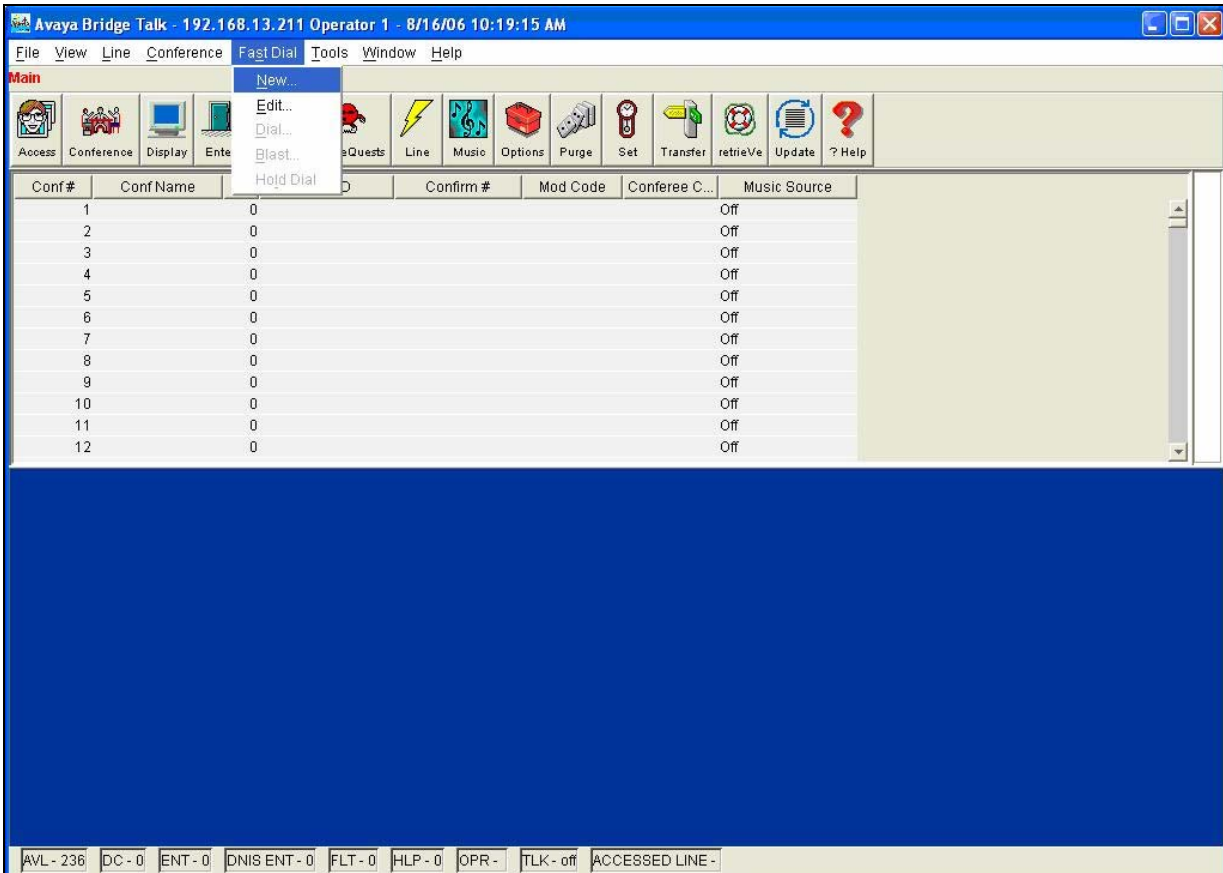
Step	Description																																																
5.2.5	<p>At the command prompt, enter “cbutil list” to verify the entries provisioned in Steps 5.2.2 - 5.2.4.</p> <p><i>Note: The last entry in the call branding table, with a DNIS value ???, was added previously, and is a wild card entry. This entry captures any wrong number (e.g., unmatched DID values) and places the call into the enter queue for operator assistance.</i></p>																																																
	<pre>S6200-> cbutil list cbutil Copyright 2004 Avaya, Inc. All rights reserved.</pre> <table><thead><tr><th>DNIS</th><th>Grp</th><th>Msg</th><th>PS</th><th>CP</th><th>Function</th><th>Line Name</th><th>Company Name</th></tr><tr><th>-----</th><th>---</th><th>---</th><th>---</th><th>--</th><th>-----</th><th>-----</th><th>-----</th></tr></thead><tbody><tr><td>222</td><td>0</td><td>0</td><td>1</td><td>N</td><td>DIRECT</td><td></td><td></td></tr><tr><td>444</td><td>0</td><td>0</td><td>1</td><td>N</td><td>DIRECT</td><td></td><td></td></tr><tr><td>555</td><td>0</td><td>301</td><td>1</td><td>N</td><td>DIRECT</td><td></td><td></td></tr><tr><td>???</td><td>0</td><td>208</td><td>1</td><td>N</td><td>ENTER</td><td></td><td></td></tr></tbody></table>	DNIS	Grp	Msg	PS	CP	Function	Line Name	Company Name	-----	---	---	---	--	-----	-----	-----	222	0	0	1	N	DIRECT			444	0	0	1	N	DIRECT			555	0	301	1	N	DIRECT			???	0	208	1	N	ENTER		
DNIS	Grp	Msg	PS	CP	Function	Line Name	Company Name																																										
-----	---	---	---	--	-----	-----	-----																																										
222	0	0	1	N	DIRECT																																												
444	0	0	1	N	DIRECT																																												
555	0	301	1	N	DIRECT																																												
???	0	208	1	N	ENTER																																												

5.3. Administer Conferences

The following steps utilize Avaya Bridge Talk to provision conferences on Avaya Meeting Exchange. Avaya Bridge Talk is an application that runs on a standard Windows based PC, and is utilized for provisioning, and managing conferencing applications on Avaya Meeting Exchange. Refer to [4] for information regarding the PC requirements.

***Note:** If any of the features displayed in the Avaya Bridge Talk screen captures are not present, contact an authorized Avaya sales representative to make the appropriate changes.*

Step	Description
5.3.1	<p>From the PC that has the Avaya Bridge Talk application installed (and that also has network connectivity to Avaya Meeting Exchange), login to Avaya Bridge Talk as follows:</p> <ul style="list-style-type: none">• [Not Shown] Open the Avaya Bridge Talk application via start → Programs from the PC.• Enter the IP address of Avaya Meeting Exchange in the Bridge field.• Enter the appropriate credentials in the Sign-In and Password fields. <div data-bbox="621 863 1169 1222"></div>

Step	Description
5.3.2	<p>Provision a new dial list for outbound calling (e.g., blast dial and fast dial) from Avaya Meeting Exchange. From the Avaya Bridge Talk Menu Bar, click Fast Dial → New.</p> 

Step	Description
5.3.3	<p>From the New Dial List window that is displayed, add participants to the dial list that are members of the Response Team as well as the Control Room operator.</p> <ul style="list-style-type: none"> • Enter a descriptive label for this dial list in the Name field. • Add entries to the dial list by clicking on the Add button for each participant. <ul style="list-style-type: none"> ○ Enter a descriptive label for each participant in the Name field. ○ Enter a number in the Telephone field that corresponds to stations registered to either Avaya Communication Manager or Avaya SIP Enablement Services. • Enable conference participants on the dial list to enter the conference without a passcode by checking the Directly to Conf box. • Refer to [4] for provisioning the remaining fields in this screen. • When finished, click on the Save button on the bottom of the screen.

New Dial List

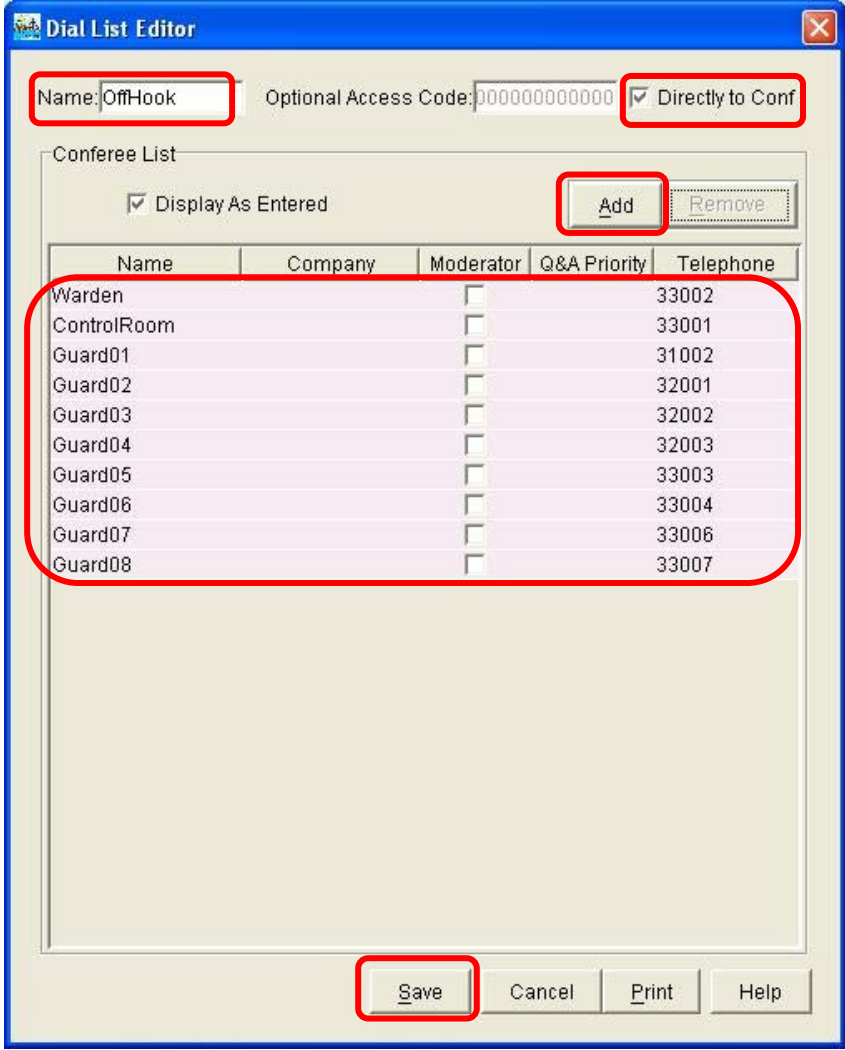
Name: ManDown Optional Access Code: 000000000000 ☒ Directly to Conf

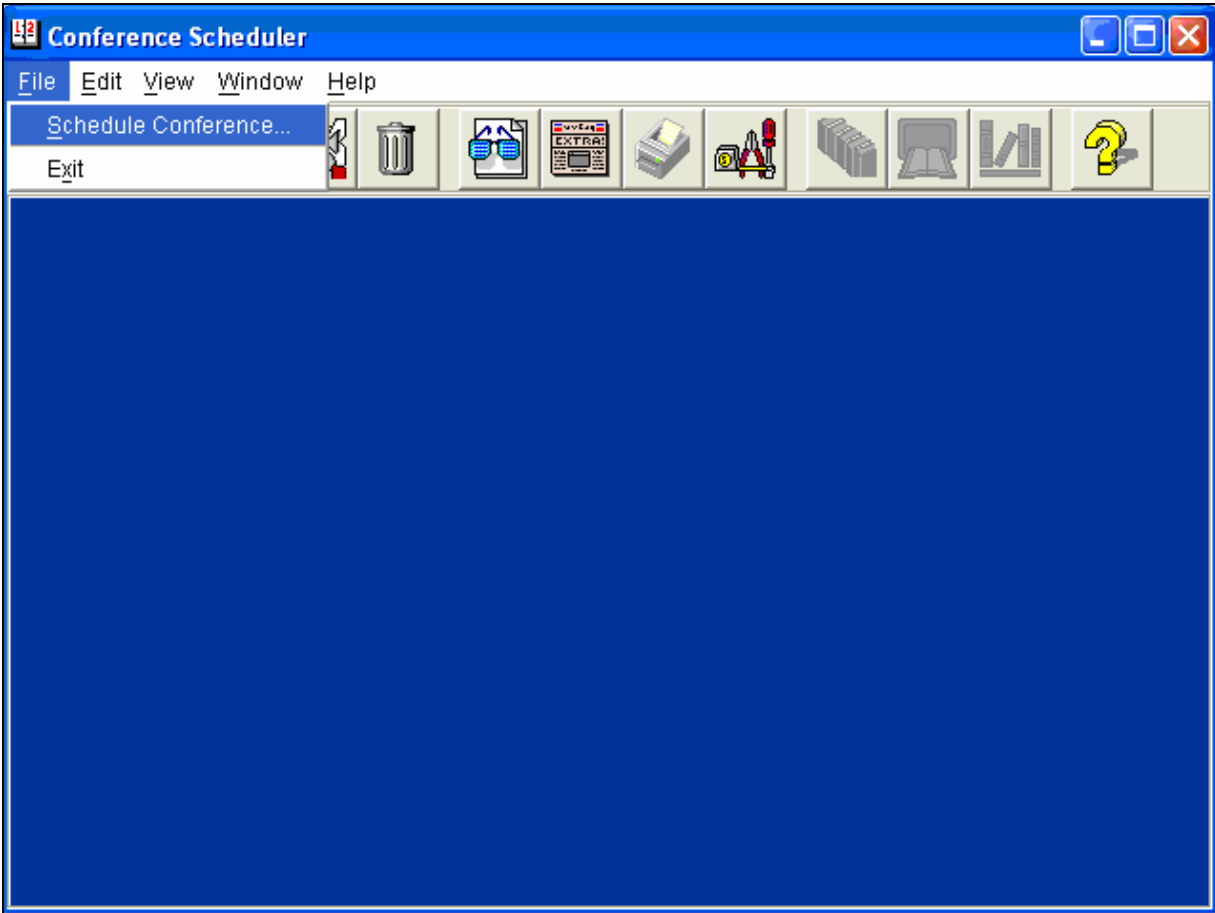
Conferee List

☒ Display As Entered **Add** Remove

Name	Company	Moderator	Q&A Priority	Telephone
Warden		<input type="checkbox"/>		33002
ControlRoom		<input type="checkbox"/>		33001
Guard01		<input type="checkbox"/>		31002
Guard02		<input type="checkbox"/>		32001
Guard03		<input type="checkbox"/>		32002
Guard04		<input type="checkbox"/>		32003
Guard05		<input type="checkbox"/>		33003
Guard06		<input type="checkbox"/>		33004
Guard07		<input type="checkbox"/>		33006
Guard08		<input type="checkbox"/>		33007

Save Cancel Print Help

Step	Description
5.3.4	<p>Repeat Step 5.3.2 to create a new dial list. From the New Dial List window that is displayed, add participants to the dial list that are members of the Response Team as well as the Control Room operator.</p> <ul style="list-style-type: none"> Enter OffHook in the Name field. <ul style="list-style-type: none"> Add the same entries to this dial list as in Step 5.3.3. <p><i>Note: The participants on this dial list and the dial list provisioned in Step 5.3.3 are the same. This is necessary to allow the participants to receive multiple calls associated with both fire/emergency and off-hook alert scenarios originating in this sample configuration.</i></p> Check the Directly to Conf box. 

Step	Description
5.3.5	<p>Schedule conferences that utilize the direct call flows provisioned in Section 5.2 as follows:</p> <ul style="list-style-type: none"> • [Not Shown] From the Avaya Bridge Talk Menu Bar, click View → Conference Scheduler (see <i>Step 5.3.2</i> for a view of the Avaya Bridge Talk Menu Bar). • From the Conference Scheduler window that is displayed, click File → Schedule Conference. 

Step	Description
5.3.6	<p>From the Schedule Conference window that is displayed, administer settings as follows:</p> <ul style="list-style-type: none"> • Enter a unique passcode in the Conferee Code field to allow access to this conference. • Enter a unique passcode in the Moderator Code field to allow access to this conference with moderator (host) privileges. <i>Note: Enable direct access (without entering a passcode) to this conference by ensuring the Moderator Code has an associated direct call function provisioned (see Step 5.2.2).</i> • Enter a descriptive label for this conference in the Conference Name field. • Disable an auto blast dial by setting the Auto Blast field to OFF. • Refer to [4] for provisioning of the remaining fields in this screen. • When finished, click on the OK button on the bottom of the screen.

Schedule Conference [Operator Access]

Conference Information

Status: Mode: Conference Type:

Confirmation No.: Conference ID: Weekend:

Name: Billing Code Prompt:

Telephone: Accounting Code: Start Date (mm/dd/yyyy):

Sign-in Name: Security Passcode: End Date (mm/dd/yyyy):

Change Conf Opt:

Conferee Code: Op Help Available: Name Record/Play:

Moderator Code: Block Dialout: NRP Annunciator:

Conference Name: Auto Blast: PIN Mode:

Dial List: Blast Annunciator: Browse PIN List:

Conference Features

Start Time: End Time: Code Duration:

Entry Tone: Exit Tone: Maximum Lines:

Hang up: Music: Security:

Auto Extend Duration: Auto Extend Ports:

Prompt Set: Conference Viewer:

Step	Description
5.3.7	<p>Repeat Steps 5.3.5 to add another conference. From the Schedule Conference window that is displayed, administer settings as follows:</p> <ul style="list-style-type: none"> • Enter a unique passcode in the Conferee Code field to allow access to this conference. • Enter a unique passcode in the Moderator Code field to allow access to this conference with moderator (host) privileges. <ul style="list-style-type: none"> <i>Note: Enable direct access (without entering a passcode) to this conference by ensuring the Moderator Code has an associated direct call function provisioned (see Step 5.2.3).</i> • Enter a descriptive label for this conference in the Conference Name field. • Administer settings to enable an auto blast dial by setting the Auto Blast field to Auto and selecting the dial list provisioned in Step 5.3.3 in the Dial List field. <ul style="list-style-type: none"> ○ [Not Shown] Select a dial list by clicking on the Dial List button → select a dial list from the Create, Select or Edit Dial List window that is displayed → click on the Select button. • Refer to [4] for provisioning of the remaining fields in this screen. • When finished, click on the OK button on the bottom of the screen.

Schedule Conference [Operator Access]

Conference Information	
Status: <input type="text" value="ENABLED"/>	Mode: <input type="text" value="UNATTENDED"/> Conference Type: <input type="text" value="DAILY"/>
Confirmation No.: <input type="text" value="2"/>	Conference ID: <input type="text"/> Weekend: <input type="text" value="YES"/>
Name: <input type="text"/>	Billing Code Prompt: <input type="text" value="DISABLED"/>
Telephone: <input type="text"/>	Accounting Code: <input type="text" value="OFF"/>
Sign-in Name: <input type="text" value="operator"/>	Security Passcode: <input type="text" value="OFF"/>
	Change Conf Opt: <input type="text" value="ON"/>
Conferee Code: <input type="text" value="1222"/>	Op Help Available: <input type="text" value="OFF"/>
Moderator Code: <input type="text" value="222"/>	Block Dialout: <input type="text" value="OFF"/>
Conference Name: <input type="text" value="ManDown"/>	Auto Blast: <input type="text" value="Auto"/>
Dial List: <input type="text" value="ManDown"/>	Blast Annunciator: 242 <input type="text" value="Browse"/>
	Name Record/Play: <input type="text" value="OFF"/>
	NRP Annunciator: <input type="text" value="Browse"/>
	PIN Mode: <input type="text" value="OFF"/>
	PIN List: <input type="text"/>
Conference Features	
Start Time: <input type="text" value="12:00"/> <input type="text" value="AM"/>	End Time: <input type="text" value="12:00"/> <input type="text" value="AM"/>
Code Duration: <input type="text" value="0"/>	Maximum Lines: <input type="text" value="24"/>
Entry Tone: <input type="text" value="OFF"/>	Exit Tone: <input type="text" value="OFF"/>
Hang up: <input type="text" value="OFF"/>	Music: <input type="text" value="OFF"/>
Security: <input type="text" value="OFF"/>	
Auto Extend Duration: <input type="text" value="ON"/>	Auto Extend Ports: <input type="text" value="ON"/>
Prompt Set: <input type="text" value="English"/>	Conference Viewer: <input type="text" value="NO"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

Step	Description
5.3.8	<p>Repeat Steps 5.3.5 to add another conference. From the Schedule Conference window that is displayed, administer settings as follows:</p> <ul style="list-style-type: none"> Enter a unique passcode in the Conferee Code field to allow access to this conference. Enter a unique passcode in the Moderator Code field to allow access to this conference with moderator (host) privileges. <ul style="list-style-type: none"> <i>Note: Enable direct access (without entering a passcode) to this conference by ensuring the Moderator Code has an associated direct call function provisioned (see Step 5.2.4).</i> Enter a descriptive label for this conference in the Conference Name field. Administer settings to enable an auto blast dial by setting the Auto Blast field to Auto and selecting the dial list provisioned in Step 5.3.4 in the Dial List field. <ul style="list-style-type: none"> [Not Shown] Select a dial list by clicking on the Dial List button → select a dial list from the Create, Select or Edit Dial List window that is displayed → click on the Select button. Refer to [4] for provisioning of the remaining fields in this screen. When finished, click on the OK button on the bottom of the screen.

Schedule Conference [Operator Access]

Conference Information

Status: Mode: Conference Type:

Confirmation No.: Conference ID: Weekend:

Name: Billing Code Prompt:

Telephone: Accounting Code: Start Date (mm/dd/yyyy):

Sign-in Name: Security Passcode: End Date (mm/dd/yyyy):

Change Conf Opt:

Conferee Code: Op Help Available: Name Record/Play:

Moderator Code: Block Dialout: NRP Annunciator:

Conference Name: Auto Blast: PIN Mode:

Dial List: Blast Annunciator: 242 PIN List:

Conference Features

Start Time: End Time: Code Duration:

Entry Tone: Exit Tone: Maximum Lines:

Hang up: Music: Security:

Auto Extend Duration: Auto Extend Ports:

Prompt Set: Conference Viewer:

6. Avaya Alarm Display Terminal Configuration

This section describes the steps for configuring the AADT application to display events generated by Avaya Meeting Exchange via BCAPI. The events displayed by the AADT application are events corresponding to the conferences provisioned in **Section 5.3** on Avaya Meeting Exchange. The AADT application captures and displays information from BCAPI to identify the location and source of an emergency/crisis scenario in an enterprise network.

Step	Description
6.1.1	From a command prompt on the PC running the AADT application: <ul style="list-style-type: none">• Issue the command “java -version”.• Verify that the JRE installed on the PC is 1.5 or greater.
	Microsoft Windows XP [Version 5.1.2600] (C) Copyright 1985-2001 Microsoft Corp. C:\> java -version java version "1.5.0_11" Java(TM) 2 Runtime Environment, Standard Edition (build 1.5.0_11-b03) Java HotSpot(TM) Client VM (build 1.5.0_11-b03, mixed mode)

Step	Description
6.1.2	<p>Administer settings that enable the AADT application to display events that are generated by Avaya Meeting Exchange via BCAP. From the PC running the AADT application:</p> <ul style="list-style-type: none"> • Locate and edit the alarmdisplay.properties file with a text editor, e.g., Notepad. • Assign the IP address of Avaya Meeting Exchange to the BRIDGE_IP variable. • Assign the appropriate login credentials to access Avaya Meeting Exchange for the BRIDGE_USER_NAME and BRIDGE_USER_PASSWORD variables. <i>Note: This login corresponds to an administrator sign-in for an Avaya Bridge Talk user on Avaya Meeting Exchange. Refer to [2] for details on sign-in administration.</i> • Assign ONLY_MODERATORS to the PARTICIPANT_FILTER variable. <i>Note: Setting this variable to ONLY_MODERATORS will only display the station added to a conference as moderator on the AADT. For example, if this variable were set to NO, then all participants in the conference would be displayed. By displaying only the moderator, the operator viewing the AADT can more easily pinpoint the source/location of the emergency/crisis scenario.</i> • Assign a number to the NUMBER_OF_CONFERENCES variable. This number corresponds to the number of emergency/crisis scenarios managed by the AADT application. • Assign the name of each conference as defined by Avaya Bridge Talk administration (see Section 5.3) to the CONF_NAME variable. <ul style="list-style-type: none"> ○ For each conference, assign a unique color as defined by the RGB format to the CONF_COLOR variable. For example, assigning 255, 0, 0 will display events associated with the conference in red on the AADT. • Assign a directory where log files will be written to the LOG_DIRECTORY variable. <pre> BRIDGE_IP=192.168.13.102 BRIDGE_USER_NAME=EnterUserName BRIDGE_USER_PASSWORD=EnterPassword # sets if the participants will be filtered # Possible values: NO, ONLY_MODERATORS, ONLY_INCOMING PARTICIPANT_FILTER=ONLY_MODERATORS # number of conferences that will be listened NUMBER_OF_CONFERENCES=3 # for each conference I add the following keys: # CONF_NAME_I - conference name # CONF_COLOR_I - color that will represent the conference. RGB values CONF_NAME_1=ManDown CONF_COLOR_1=255, 0, 0 CONF_NAME_2=OffHkAlrt CONF_COLOR_2=255, 255, 0 CONF_NAME_3=WatchCall CONF_COLOR_3=0, 191, 205 # directory where the conference logs will be saved LOG_DIRECTORY=C:\\conferences\\ </pre>

7. Interoperability Compliance Testing

7.1. General Test Approach

The general test approach was to place calls between Avaya Communication Manager and Avaya Meeting Exchange utilizing the sample network configuration displayed in **Figure 1**. This approach verified the administration on both Avaya Meeting Exchange and Avaya Communication Manager. There was also specific testing regarding Avaya Communication Manager and the Avaya Alarm Display Terminal.

7.1.1. Avaya Meeting Exchange

The following was verified on Avaya Meeting Exchange.

- Inbound calling from Avaya Communication Manager to conferences provisioned on Avaya Meeting Exchange via direct call functions, e.g., where conference participants call Avaya Meeting Exchange, and enter a conference as moderator, without entering a passcode.
- Outbound calling from Avaya Meeting Exchange to stations registered to either Avaya Communication Manager or Avaya SIP Enablement Services via an auto blast dial, e.g., where a conference participant enters a conference as moderator via a direct call function and automatically invokes a blast dial to a pre-provisioned dial list of one or more participants.

7.1.2. Avaya Communication Manager

The following was verified on Avaya Communication Manager.

- Multiple Level Precedence and Preemption.
- Malicious Call Trace.
- Off-hook alert.

7.1.3. Avaya Alarm Display Terminal

The following was verified on the AADT application.

- Displaying, clearing and printing of conferences utilized for meetings and a role call.
- Displaying, clearing and printing of alerts associated with fire/emergency scenarios.
- Displaying, clearing and printing of off-hook alert scenarios.
- Displaying, clearing and printing of multiple conferences/alerts of each type.
- Log file generation.

7.2. Test Results


- All test cases, as defined by the general test approach, passed.

8. Verification Steps

The following steps were used to verify the administrative steps presented in these Application Notes and are applicable for similar configurations in the field.

Step	Description
8.1.1	<p>Verify precedence routing corresponding to the MLPP feature.</p> <p>From a SAT session:</p> <ul style="list-style-type: none"> Issue the command “list precedence-routing route-chosen <n>”, where n is a concatenation of the WNDP precedence access code provisioned in Step 4.4.2 plus the extension of the station to call. <p><i>Note: If 9033006 is the number entered, the command returns 33006 for the Dialed String field. Precedence routing will strip off the WNDP precedence access code (90) and route this call with a precedence level of Flash Override to the station 33006.</i></p> <pre>list precedence-routing route-chosen 9033006</pre> <pre> PRECEDENCE ROUTING ROUTE CHOSEN REPORT Partitioned Group Number: 1 Dialed Total Route Preempt String Min Max Pat Method 33006 5 5 group </pre>

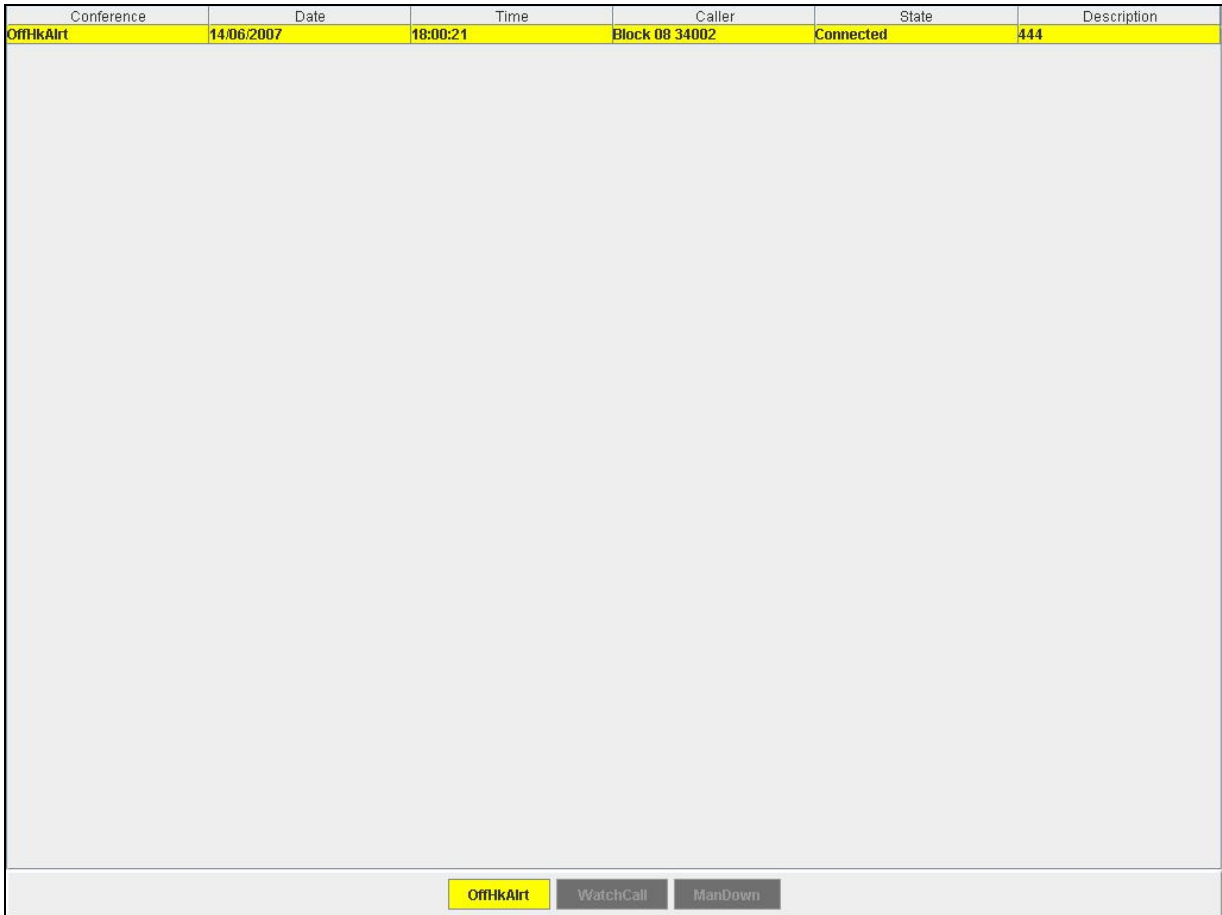
Step	Description																		
8.1.2	<p>Verify the MCT feature can write to translations on Avaya Communication Manager.</p> <p>From a SAT session:</p> <ul style="list-style-type: none">• Issue the command “list mct-history” to display the chronological data associated with the MCT feature in descending order, e.g., most recent data first. The data displayed below indicate the following:<ul style="list-style-type: none">○ The Date and Time fields show the respective date and time the MCT feature was invoked.○ The Contr Ext field shows the associated station designated as a controller for this call. For this call, the station associated with the Control Room (33001), provisioned in Section 4.7 is the only MCT controller.○ The Active Ext field shows the station (33002) that imitated the MCT feature, either by entering the appropriate FAC, or by pressing a feature button assigned to activate the MCT feature.○ The Parties on Call field shows the associated station (33004) on call when the MCT feature was invoked.○ Refer to [5] for definitions regarding the remaining fields in this screen. <p><i>Note: MCT data is saved to translations on Avaya Communication Manager. This verification step validated that the MCT feature was provisioned correctly by verifying the existence of MCT History in the translations, and not showing how the MCT History was populated. For brevity, this step omitted the procedures of how the station designated as the Active Ext invoked the MCT feature.</i></p>																		
<div><div>list mct-history</div><div><div>Page1</div><table><tr><th colspan="6">MALICIOUS CALL TRACE HISTORY</th></tr><tr><th>Date</th><th>Time</th><th>Contr Ext/ Active Ext</th><th>Recorder Port</th><th>Redir From/ Actual Party</th><th>Parties on Call</th></tr><tr><td>6/14</td><td>15:12</td><td>33001 33002</td><td>none</td><td>33004 33002</td><td>33004 no party #3 no party #4 no party #5 no party #6</td></tr></table></div></div> <div>ISDN Notification: not sent</div>		MALICIOUS CALL TRACE HISTORY						Date	Time	Contr Ext/ Active Ext	Recorder Port	Redir From/ Actual Party	Parties on Call	6/14	15:12	33001 33002	none	33004 33002	33004 no party #3 no party #4 no party #5 no party #6
MALICIOUS CALL TRACE HISTORY																			
Date	Time	Contr Ext/ Active Ext	Recorder Port	Redir From/ Actual Party	Parties on Call														
6/14	15:12	33001 33002	none	33004 33002	33004 no party #3 no party #4 no party #5 no party #6														

Step	Description
8.1.3	<p>Verify the AADT application can be opened.</p> <p>From the PC that has the AADT application installed, and that also has network connectivity to Avaya Meeting Exchange, invoke the AADT application as follows:</p> <ul style="list-style-type: none"> • [Not Shown] Open the AADT application via start ➔ Programs from the PC. • The AADT application opens, and is displayed on the monitor of the PC as shown. <p><i>Note: The format of the display presented on the screen capture displayed below was based on customer requirements regarding the AADT application for this Proof of Concept request. The requirements, and hence the format of the display may be subject to change in future releases.</i></p> 

Step	Description
8.1.4	<p>Verify call routing and the off-hook alert feature.</p> <p>Validate signaling and media connectivity for inbound calls to Avaya Meeting Exchange from Avaya Communication Manager. This is accomplished by verifying call origination from a station in the Facility, as displayed in Figure 1, to a conference provisioned on Avaya Meeting Exchange. Since the off-hook alert is provisioned (see Section 4.6) to route to Avaya Meeting Exchange, this feature may be verified in the context of an inbound call to Avaya Meeting Exchange.</p> <p>From a SAT session:</p> <ul style="list-style-type: none"> Issue the command “list trace tac <n>”, where n is the Trunk Access Code (TAC) defined for the trunk group between Avaya Communication Manager and Avaya Meeting Exchange. From a station in the Facility, go off-hook, and do not enter a valid (as defined by the dial plan configured on Avaya Communication Manager) destination phone number within the prescribed time limit. <p><i>Note: The trace below shows a station in the Facility with a Calling Name (e.g., the ANI, 34002 Block 08 3400) and Number (34002) dialing 444 (due to the vector/VDN associated with the off-hook alert feature provisioned in Section 4.6) and routing via ARS to Avaya Meeting Exchange. Recall that “444” is associated with a direct call function (see Step 5.2.4) and the conference provisioned in Step 5.3.8 on Avaya Meeting Exchange. This trace also shows audio connectivity between Avaya Meeting Exchange (192.168.13.102) and the MEDPRO on the Avaya G650 Media Gateway (192.168.11.11) utilizing G.711MU.</i></p> <pre>list trace tac 103</pre> <p style="text-align: right;">Page 1</p> <pre> LIST TRACE time data 18:01:19 dial 444 route:ARS 18:01:19 term trunk-group 3 cid 0x45b 18:01:19 dial 444 route:ARS 18:01:19 route-pattern 3 preference 1 cid 0x45b 18:01:19 seize trunk-group 3 member 50 cid 0x45b 18:01:19 Calling Number & Name 34002 Block 08 3400 18:01:19 Proceed trunk-group 3 member 50 cid 0x45b 18:01:19 active trunk-group 3 member 50 cid 0x45b 18:01:19 G711MU ss:off ps:20 rn:2/1 192.168.13.102:42442 192.168.11.11:2336 18:01:19 xoip: fax:Relay modem:off tty:US 192.168.11.11:2336 uid:0x5010d 18:01:19 VOIP data from: 192.168.11.11:2336 18:05:19 Jitter:0 0 0 0 0 0 0 0 0 0: Buff:8 WC:10 Avg:0 18:05:19 Pkloss:0 0 0 0 0 0 0 0 0 0: Oofo:0 WC:0 Avg:0 </pre>

Step	Description																										
8.1.5	<p>Verify call routing via the auto blast dial to the stations associated with Response Team and Control Room operator (with an off-hook alert to the Control Room operator).</p> <p>Validate signaling and media connectivity for outbound calls from Avaya Meeting Exchange to Avaya Communication Manager. This is accomplished by verifying call origination from Avaya Meeting Exchange due to off-hook alert (invoked in Step 8.1.4) and subsequent auto blast dial to stations associated with Response Team and Control Room operator. Also, validate a distinctive audible alert to the station in the Control Room.</p> <p>From a SAT session:</p> <ul style="list-style-type: none"> Issue the command “list trace tac <n>”, where n is the TAC defined for the trunk group between Avaya Communication Manager and Avaya Meeting Exchange. <p><i>Note: The trace below shows a call (originating from Avaya Meeting Exchange via the trunk between Avaya Meeting Exchange and Avaya Communication Manager) to the station in the Control Room (33001). This trace also shows direct IP connectivity between the station (192.168.12.101) and Avaya Meeting Exchange (192.168.13.102) utilizing G.711MU. Although the blast dial invoked in Step 8.1.4 included a total of ten endpoints (see Step 5.3.4), for brevity, this verification step only displays the trace to one endpoint on the dial list.</i></p> <pre>list trace tac 103</pre> <p style="text-align: right;">Page 1</p> <p style="text-align: center;">LIST TRACE</p> <table> <thead> <tr> <th>time</th><th>data</th></tr> </thead> <tbody> <tr> <td>18:01:23</td><td>Calling party trunk-group 3 member 32 cid 0x46d</td></tr> <tr> <td>18:01:23</td><td>Calling Number & Name NO-CPNumber NO-CPName</td></tr> <tr> <td>18:01:23</td><td>active trunk-group 3 member 32 cid 0x46d</td></tr> <tr> <td>18:01:23</td><td>G711MU ss:off ps:20 rn:2/1 192.168.13.102:42472 192.168.11.11:2516</td></tr> <tr> <td>18:01:23</td><td>xoip: fax:Relay modem:off tty:US 192.168.11.11:2516 uid:0x500fb</td></tr> <tr> <td>18:01:23</td><td>dial 33001</td></tr> <tr> <td>18:01:23</td><td>ring station 33001 cid 0x46d</td></tr> <tr> <td>18:01:23</td><td>G711MU ss:off ps:20 rn:1/1 192.168.12.101:2498 192.168.11.11:2520</td></tr> <tr> <td>18:01:23</td><td>xoip: fax:Relay modem:off tty:US 192.168.11.11:2520 uid:0x8ca0</td></tr> <tr> <td>18:01:27</td><td>active station 33001 cid 0x46d</td></tr> <tr> <td>18:01:27</td><td>G711MU ss:off ps:20 rn:2/1 192.168.13.102:42472 192.168.12.101:2498</td></tr> <tr> <td>18:01:27</td><td>G711MU ss:off ps:20 rn:1/2 192.168.12.101:2498 192.168.13.102:42472</td></tr> </tbody> </table>	time	data	18:01:23	Calling party trunk-group 3 member 32 cid 0x46d	18:01:23	Calling Number & Name NO-CPNumber NO-CPName	18:01:23	active trunk-group 3 member 32 cid 0x46d	18:01:23	G711MU ss:off ps:20 rn:2/1 192.168.13.102:42472 192.168.11.11:2516	18:01:23	xoip: fax:Relay modem:off tty:US 192.168.11.11:2516 uid:0x500fb	18:01:23	dial 33001	18:01:23	ring station 33001 cid 0x46d	18:01:23	G711MU ss:off ps:20 rn:1/1 192.168.12.101:2498 192.168.11.11:2520	18:01:23	xoip: fax:Relay modem:off tty:US 192.168.11.11:2520 uid:0x8ca0	18:01:27	active station 33001 cid 0x46d	18:01:27	G711MU ss:off ps:20 rn:2/1 192.168.13.102:42472 192.168.12.101:2498	18:01:27	G711MU ss:off ps:20 rn:1/2 192.168.12.101:2498 192.168.13.102:42472
time	data																										
18:01:23	Calling party trunk-group 3 member 32 cid 0x46d																										
18:01:23	Calling Number & Name NO-CPNumber NO-CPName																										
18:01:23	active trunk-group 3 member 32 cid 0x46d																										
18:01:23	G711MU ss:off ps:20 rn:2/1 192.168.13.102:42472 192.168.11.11:2516																										
18:01:23	xoip: fax:Relay modem:off tty:US 192.168.11.11:2516 uid:0x500fb																										
18:01:23	dial 33001																										
18:01:23	ring station 33001 cid 0x46d																										
18:01:23	G711MU ss:off ps:20 rn:1/1 192.168.12.101:2498 192.168.11.11:2520																										
18:01:23	xoip: fax:Relay modem:off tty:US 192.168.11.11:2520 uid:0x8ca0																										
18:01:27	active station 33001 cid 0x46d																										
18:01:27	G711MU ss:off ps:20 rn:2/1 192.168.13.102:42472 192.168.12.101:2498																										
18:01:27	G711MU ss:off ps:20 rn:1/2 192.168.12.101:2498 192.168.13.102:42472																										

Step	Description
8.1.6	<p>For additional information regarding the active call from Avaya Meeting Exchange initiated in Step 8.1.4, status the trunk group member obtained from the trace in Step 8.1.5.</p> <p>From a SAT session:</p> <ul style="list-style-type: none"> Issue the command “status trunk t/m”, where t is the trunk group and m is the trunk group member. Note the following: <ul style="list-style-type: none"> The signaling connection is between the CLAN (192.168.11.10) on Avaya Communication Manager and Avaya Meeting Exchange (192.168.13.102). The audio connection utilizes G.711MU and is between the station in the Control Room (192.168.12.101) and Avaya Meeting Exchange (192.168.13.102). The Audio Connection Type field returns ip-direct. This indicated a direct audio connection for this trunk group member. <p><i>Note: An Audio Connection Type field returning ip-tdm would indicate that direct IP-to-IP audio connectivity is <u>not</u> enabled.</i></p>
	<pre> status trunk 3/32 Page 1 of 2 TRUNK STATUS Trunk Group/Member: 0003/032 Service State: in-service/active Port: T00251 Maintenance Busy? no Signaling Group ID: IGAR Connection? no Connected Ports: S00006 Port Near-end IP Addr : Port Far-end IP Addr : Port Signaling: 01A0217 192.168. 11. 10 : 5061 192.168. 13.102 : 5061 G.711MU Audio: 192.168. 12.101 : 2498 192.168. 13.102 : 42472 Video: Video Codec: Authentication Type: None Audio Connection Type: ip-direct </pre>

Step	Description
8.1.7	<p>Verify that events associated with emergency/crisis scenarios captured by the AADT application are displayed.</p> <p>Validate the information associated with the off-hook alert scenario that was invoked in Step 8.1.4 is displayed on the monitor of the PC running the AADT application.</p> <p><i>Note: The format of the display presented on the screen capture displayed below was based on customer requirements regarding the AADT application for this Proof of Concept request. The requirements, and hence the format of the display may be subject to change in future releases. The AADT application, as provisioned in Step 6.1.2, displays information in yellow only for the station in the Facility that invoked the off-hook alert scenario.</i></p> 

Step	Description
8.1.8	<p>Verify that events associated with emergency/crisis scenarios captured by the AADT application are written to a log file.</p> <p>Validate the AADT application writes information to a log file that is associated with the off-hook alert scenario invoked in Step 8.1.4.</p> <ul style="list-style-type: none"> • Locate the log file on the PC that has the AADT application installed. • Open the log file with a text editor, e.g., notepad. • Verify information is populated in the log file as displayed. <p><i>Note: The format of the log file displayed below was based on customer requirements regarding the AADT application for this Proof of Concept request. The requirements, and hence the format of the log file may be subject to change in future releases. The log file contains information for all participants involved in this off-hook alert scenario, including the participants on the dial list provisioned in Step 5.3.4.</i></p> <pre> ----- CONFERENCE REPORT ----- Conference :OffHkAlrt Start :14/06/2007 18:00:21 End :14/06/2007 18:01:32 Printed :14/06/2007 18:01:36 ----- PARTICIPANT LIST ----- CALLER DATE TIME STATE DESCRIPTION ----- 31002 14/06/2007 18:00:39 Disconnected Guard01 33007 14/06/2007 18:00:35 Disconnected Guard08 32002 14/06/2007 18:00:30 Disconnected Guard03 33003 14/06/2007 18:00:33 Disconnected Guard05 33001 14/06/2007 18:00:25 Disconnected ControlRoom Block 08 34002 14/06/2007 18:00:21 Disconnected 444 33006 14/06/2007 18:00:40 Disconnected Guard07 32001 14/06/2007 18:00:28 Disconnected Guard02 33004 14/06/2007 18:00:36 Disconnected Guard06 33002 14/06/2007 18:00:42 Disconnected Warden 32003 14/06/2007 18:00:30 Disconnected Guard04 ----- </pre>

9. Conclusion

These Application Notes presented a compliance-tested solution comprised of Avaya Communication Manager and Avaya Meeting Exchange. This solution enables the management of emergency/crisis scenarios originating in an enterprise network. Avaya Communication Manager was configured to provide Multiple Level Precedence and Preemption (MLPP), Malicious Call Trace (MCT) and off-hook alert features to facilitate the management of emergency/crisis scenarios originating in an enterprise network. Avaya Meeting Exchange was administered to generate auto blast dial conferences to a list of participants dedicated to resolving emergency/crisis scenarios. To further assist in the management of emergency/crisis scenarios, the BCAP API on Avaya Meeting Exchange was utilized by a custom software application developed by Avaya to display events corresponding to emergency/crisis scenarios.

10. Additional References

Avaya references are available at <http://support.avaya.com>.

- [1] *Configuring secure SIP connectivity utilizing Transport Layer Security (TLS) between Avaya Communication Manager and Avaya Meeting Exchange (S6200)*, Issue 1.0, August 2006.
- [2] *Meeting Exchange 4.1 Administration and Maintenance S6200/S6800 Media Server*, Issue 1, Doc ID 04-601168, July 2006.
- [3] *Meeting Exchange 4.1 Configuring S6200, S6500, and S6800 Conferencing Servers*, Issue 1, Doc ID 04-601338, July 2006.
- [4] *Avaya Meeting Exchange Groupware Edition Version 4.1 User's Guide for Bridge Talk*, Doc ID 04-600878, Issue 2, July 2006.
- [5] *Administrator Guide for Avaya Communication Manager*, Issue 3.1, Doc ID: 03-300509, February 2007.
- [6] *Administration for Network Connectivity for Avaya Communication Manager*, Issue 12, Doc ID: 555-233-504, February 2007.

©2007 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 Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com