



**Avaya Solution & Interoperability Test Lab**

---

## **Application Notes for Configuring a Sample Video Contact Center Using Avaya Communication Manager, Avaya IP Endpoints, and Polycom Video Endpoints - Issue 1.0**

### **Abstract**

These Application Notes describe a sample video contact center solution comprised of Avaya Communication Manager, Avaya IP endpoints and Polycom VSX 3000 Video endpoints. The sample configuration provided in these Application Notes demonstrates basic functionality for video enabled contact center agents.

# 1. Introduction

These Application Notes describe a sample video contact center solution comprised of Avaya Communication Manager, Avaya IP endpoints and Polycom VSX 3000 Video Endpoints.

The Polycom VSX 3000 (herein referred to as just Polycom) is an executive video control center that features a built-in video camera with a widescreen LCD monitor. In this sample configuration, the Polycom will act as a customer facing video endpoint.

## 1.1. Solution Overview

Avaya Communication Manager provides Automatic Call Distribution (ACD) of calls to contact center agents. A customer will originate a video call from a Polycom. The call will be delivered to a contact center agent who will view incoming audio and video using a web cam enabled PC with Avaya Video IP Softphone installed. The Avaya Video IP Softphone is configured to control an Avaya 4600 series telephone in shared control mode.

The solution was tested for basic contact center functionality including call origination and termination, call hold, and call transfer.

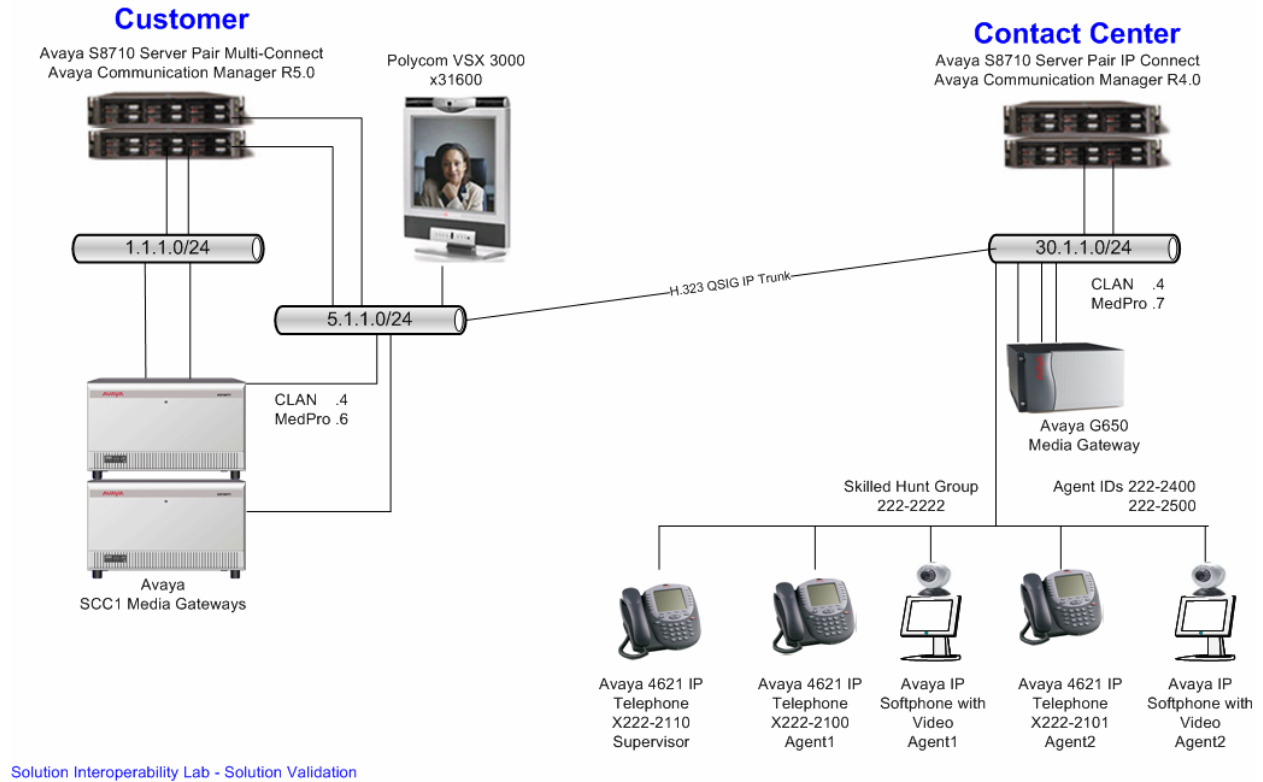
## 1.2. Network Configuration

**Figure 1** illustrates the network configuration used for these Application Notes. The network configuration consists of two locations - the Customer location and the Contact Center location. The Customer location has a pair of Avaya S8710 Servers controlling two SCC1 Cabinets (Multi-Connect). The Contact Center location has a pair of Avaya S8710 Servers controlling a G650 Media Gateway (IP connect). An H.323 QSIG enabled video trunk is established between these two locations. Video calls between the sites will be routed over this trunk.

The Avaya 4600 series telephones will be configured with the appropriate buttons needed for an agent. The Polycom registers with Avaya Communication Manager as an authenticated H.323 endpoint.

An additional Avaya 4621 IP telephone in the Contact Center will be used as a Supervisor to demonstrate basic ACD functionality (i.e. transfer a call).

The solution described herein is also extensible to other Avaya Servers and Media Gateways, as well as similar Polycom video endpoints that run the same software versions used for these Application Notes (see Section 2).



**Figure 1: Network Configuration**

## 2. Equipment and Software Validated

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

Equipment and Software	Location(s)	Version
S8710 Servers	Customer	Avaya Communication Manager R5.0 (R015x.00.0.825.4)
S8710 Servers	Contact Center	Avaya Communication Manager R4.0 (R014x.00.1.731.2)
Avaya SCC1 Media Gateway IPSI (TN2312BP) C-LAN (TN799DP) MEDPRO (TN2302AP)	Customer	HW12 FW065 HW01 FW024 HW20 FW116
Avaya G650 Media Gateway IPSI (TN2312BP) C-LAN (TN799DP) MEDPRO (TN2602AP)	Contact Center	HW12 FW040 HW01 FW024 HW02 FW032
Avaya 4621SW IP Telephones	Contact Center	R2.8 (H.323)
Avaya IP Softphone with Polycom Video Integrator	Contact Center	R6.0.0.25
Windows XP Professional PC Logitech USB Camera	Contact Center	Service Pack 2 10.0.0.1438
Polycom VSX 3000	Customer	Release 8.5.3

**Table 1: Equipment List**

## 3. Configure Avaya Communication Manager

This section provides the procedures for configuring Avaya Communication Manager in both the Customer location and the Contact Center location. The Avaya System Access Terminal (SAT) is used to issue the commands.

### 3.1. Customer Location

This section reviews the features that are required in the Customer location for the solution described in these Application Notes.

#### 3.1.1. System Parameters

For licensed features that are not enabled in this section, contact an authorized Avaya account representative to obtain the licenses.

If any of the **system-parameters customer-options** parameters are changed, it is necessary to logout of Avaya Communication Manager, and login to effect the permission changes.

Step	Description
1.	<p data-bbox="285 268 1437 380">Log into Avaya Communication Manager with the proper credentials, and enter the <b>display system-parameters special-applications</b> command. Go to Page 5 and verify that <b>(SA8697) – 3<sup>rd</sup> Party H.323 Endpoint Support</b> is set to ‘y’.</p> <div data-bbox="285 401 1437 974" style="border: 1px solid black; padding: 10px;"> <pre data-bbox="302 411 1421 953"> display system-parameters special-applications                                Page    5 of    8                                 SPECIAL APPLICATIONS                                  (SA8622) - Enhanced Call Pickup Alerting? n                                 (SA8623) - Chained Call Forwarding? n                                 (SA8652) - No Hold Consult? n (SA8654) - Crisis Alert Call Monitoring and Recording? n                                 (SA8661) - Increased Automatic Wakeup Calls? n                                 (SA8662) - Expanded PMS Name &amp; Number? n                                 (SA8684) - PMS Wakeup Message? n (SA8693) - Connectivity Check for Direct IP Shuffling? n                                 (SA8694) - Enhanced Redirection Notification? n                                 (SA8697) - 3rd Party H.323 Endpoint Support? y (SA8701) - Net Region Support H.323 Endpoints Behind ALG? n                                 (SA8702) - CDR Enhancements for Network? n                                 (SA8731) - Block Outgoing Bridged Call Display? n                                 (SA8734) - Enhanced Extension Display? n                                 (SA8741) - CDR Identifier for IP Station Calls? n                                 (SA8744) - Block Name for Room to Room Calls? n                                 (SA8747) - Softphone Indication on DCP Terminals? n </pre> </div>

Step	Description
2.	<p>Enter the <b>display system parameters customer-options</b> command. On Page 2, verify that there are sufficient licenses for the following:</p> <ul style="list-style-type: none"> <li>• <b>Maximum Video Capable Stations</b> – must be equal to or greater than the number of H.323 video stations. In this sample configuration, the Polycom is administered as four H.323 video stations.</li> <li>• <b>Maximum Video Capable IP Softphones</b> - must be equal to or greater than the number of Avaya IP Softphones enabled with video capabilities.</li> </ul> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <pre> display system-parameters customer-options OPTIONAL FEATURES  IP PORT CAPACITIES Maximum Administered H.323 Trunks: 100 82 Maximum Concurrently Registered IP Stations: 2000 22 Maximum Administered Remote Office Trunks: 8000 0 Maximum Concurrently Registered Remote Office Stations: 12000 0 Maximum Concurrently Registered IP eCons: 20 0 Max Concur Registered Unauthenticated H.323 Stations: 100 0 <b>Maximum Video Capable Stations: 100 22</b> <b>Maximum Video Capable IP Softphones: 100 10</b> Maximum Administered SIP Trunks: 400 262 Maximum Administered Ad-hoc Video Conferencing Ports: 0 0 Maximum Number of DS1 Boards with Echo Cancellation: 12 0 Maximum TN2501 VAL Boards: 10 1 Maximum Media Gateway VAL Sources: 10 2 Maximum TN2602 Boards with 80 VoIP Channels: 128 0 Maximum TN2602 Boards with 320 VoIP Channels: 128 1 Maximum Number of Expanded Meet-me Conference Ports: 300 0  (NOTE: You must logoff &amp; login to effect the permission changes.) </pre> </div>

Step	Description																																		
3.	<p data-bbox="284 235 1421 304">On Page 4 of the <b>system parameters customer-options</b> form, verify that <b>IP Trunks</b>, <b>IP Stations</b>, and <b>ISDN-PRI</b> are set to 'y'.</p> <div data-bbox="284 331 1432 953" style="border: 1px solid black; padding: 10px;"> <p data-bbox="305 344 1411 367">display system-parameters customer-options <span style="float: right;">Page 4 of 11</span></p> <p data-bbox="764 373 1008 394" style="text-align: center;">OPTIONAL FEATURES</p> <table border="0" data-bbox="316 424 1414 884"> <tr> <td data-bbox="349 424 812 447">Emergency Access to Attendant? y</td><td data-bbox="1208 424 1414 447" style="text-align: right;"><b>IP Stations? y</b></td></tr> <tr> <td data-bbox="462 453 812 476">Enable 'dadmin' Login? y</td><td></td></tr> <tr> <td data-bbox="462 480 812 504">Enhanced Conferencing? y</td><td data-bbox="1122 480 1414 504" style="text-align: right;">ISDN Feature Plus? y</td></tr> <tr> <td data-bbox="560 508 812 531">Enhanced EC500? y</td><td data-bbox="894 508 1414 531" style="text-align: right;">ISDN/SIP Network Call Redirection? y</td></tr> <tr> <td data-bbox="362 535 812 558">Enterprise Survivable Server? n</td><td data-bbox="1149 535 1414 558" style="text-align: right;">ISDN-BRI Trunks? y</td></tr> <tr> <td data-bbox="404 562 812 585">Enterprise Wide Licensing? n</td><td data-bbox="1252 562 1414 585" style="text-align: right;"><b>ISDN-PRI? y</b></td></tr> <tr> <td data-bbox="506 590 812 613">ESS Administration? y</td><td data-bbox="992 590 1414 613" style="text-align: right;">Local Survivable Processor? n</td></tr> <tr> <td data-bbox="448 617 812 640">Extended Cvg/Fwd Admin? y</td><td data-bbox="1078 617 1414 640" style="text-align: right;">Malicious Call Trace? y</td></tr> <tr> <td data-bbox="376 644 812 667">External Device Alarm Admin? n</td><td data-bbox="1019 644 1414 667" style="text-align: right;">Media Encryption Over IP? y</td></tr> <tr> <td data-bbox="334 672 812 695">Five Port Networks Max Per MCC? n</td><td data-bbox="849 672 1414 695" style="text-align: right;">Mode Code for Centralized Voice Mail? n</td></tr> <tr> <td data-bbox="534 699 812 722">Flexible Billing? n</td><td></td></tr> <tr> <td data-bbox="349 726 812 749">Forced Entry of Account Codes? n</td><td data-bbox="1019 726 1414 749" style="text-align: right;">Multifrequency Signaling? y</td></tr> <tr> <td data-bbox="391 753 812 777">Global Call Classification? n</td><td data-bbox="906 753 1414 777" style="text-align: right;">Multimedia Call Handling (Basic)? y</td></tr> <tr> <td data-bbox="493 781 812 804">Hospitality (Basic)? y</td><td data-bbox="863 781 1414 804" style="text-align: right;">Multimedia Call Handling (Enhanced)? y</td></tr> <tr> <td data-bbox="318 808 812 831">Hospitality (G3V3 Enhancements)? n</td><td data-bbox="992 808 1414 831" style="text-align: right;">Multimedia IP SIP Trunking? y</td></tr> <tr> <td data-bbox="634 835 812 858" style="text-align: center;"><b>IP Trunks? y</b></td><td></td></tr> <tr> <td data-bbox="464 863 812 886">IP Attendant Consoles? Y</td><td></td></tr> </table> <p data-bbox="380 911 1305 934" style="text-align: center;">(NOTE: You must logoff &amp; login to effect the permission changes.)</p> </div>	Emergency Access to Attendant? y	<b>IP Stations? y</b>	Enable 'dadmin' Login? y		Enhanced Conferencing? y	ISDN Feature Plus? y	Enhanced EC500? y	ISDN/SIP Network Call Redirection? y	Enterprise Survivable Server? n	ISDN-BRI Trunks? y	Enterprise Wide Licensing? n	<b>ISDN-PRI? y</b>	ESS Administration? y	Local Survivable Processor? n	Extended Cvg/Fwd Admin? y	Malicious Call Trace? y	External Device Alarm Admin? n	Media Encryption Over IP? y	Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n	Flexible Billing? n		Forced Entry of Account Codes? n	Multifrequency Signaling? y	Global Call Classification? n	Multimedia Call Handling (Basic)? y	Hospitality (Basic)? y	Multimedia Call Handling (Enhanced)? y	Hospitality (G3V3 Enhancements)? n	Multimedia IP SIP Trunking? y	<b>IP Trunks? y</b>		IP Attendant Consoles? Y	
Emergency Access to Attendant? y	<b>IP Stations? y</b>																																		
Enable 'dadmin' Login? y																																			
Enhanced Conferencing? y	ISDN Feature Plus? y																																		
Enhanced EC500? y	ISDN/SIP Network Call Redirection? y																																		
Enterprise Survivable Server? n	ISDN-BRI Trunks? y																																		
Enterprise Wide Licensing? n	<b>ISDN-PRI? y</b>																																		
ESS Administration? y	Local Survivable Processor? n																																		
Extended Cvg/Fwd Admin? y	Malicious Call Trace? y																																		
External Device Alarm Admin? n	Media Encryption Over IP? y																																		
Five Port Networks Max Per MCC? n	Mode Code for Centralized Voice Mail? n																																		
Flexible Billing? n																																			
Forced Entry of Account Codes? n	Multifrequency Signaling? y																																		
Global Call Classification? n	Multimedia Call Handling (Basic)? y																																		
Hospitality (Basic)? y	Multimedia Call Handling (Enhanced)? y																																		
Hospitality (G3V3 Enhancements)? n	Multimedia IP SIP Trunking? y																																		
<b>IP Trunks? y</b>																																			
IP Attendant Consoles? Y																																			

### 3.1.2. IP Codec Set

This section describes the configuration steps for creating an ip-codec set with multimedia capabilities to support video.

Step	Description																																
1.	<p>Enter the <b>change ip-codec-set X</b> command, where <b>X</b> is an available IP codec set number. On Page 1 of the <b>ip-codec-set</b> form, enter the codecs listed below. Set <b>Media Encryption</b> to ‘<b>none</b>’ as Avaya Communication Manager does not support the encryption of video. Of the codecs listed below, the Polycom supports <b>G.722.1-32K</b> and <b>G.711</b>, and Avaya IP Softphone at the Contact Center supports <b>G.729A</b> and <b>G.711</b>.</p> <div><div>change ip-codec-set 1<div>Page1 of 2</div></div><div><div>IP Codec Set</div><div>Codec Set: 1</div><table><tr><th>Audio Codec</th><th>Silence Suppression</th><th>Frames Per Pkt</th><th>Packet Size(ms)</th></tr><tr><td>1: G.722.1-32K</td><td></td><td>1</td><td>20</td></tr><tr><td>2: G.729A</td><td>n</td><td>2</td><td>20</td></tr><tr><td>3: G.711MU</td><td>n</td><td>2</td><td>20</td></tr><tr><td>4:</td><td></td><td></td><td></td></tr><tr><td>5:</td><td></td><td></td><td></td></tr><tr><td>6:</td><td></td><td></td><td></td></tr><tr><td>7:</td><td></td><td></td><td></td></tr></table><div>Media Encryption</div><div>1: none</div><div>2:</div><div>3:</div></div></div>	Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)	1: G.722.1-32K		1	20	2: G.729A	n	2	20	3: G.711MU	n	2	20	4:				5:				6:				7:			
Audio Codec	Silence Suppression	Frames Per Pkt	Packet Size(ms)																														
1: G.722.1-32K		1	20																														
2: G.729A	n	2	20																														
3: G.711MU	n	2	20																														
4:																																	
5:																																	
6:																																	
7:																																	
2.	<p>On Page 2 of the ip-codec-set form, set <b>Allow Direct-IP Multimedia</b> to ‘<b>y</b>’. Set <b>Maximum Call Rate for Direct-IP-Multimedia</b> and <b>Maximum Call Rate for Priority Direct-IP Multimedia</b> appropriately based on network requirements.</p> <div><div>change ip-codec-set 1<div>Page2 of 2</div></div><div><div>IP Codec Set</div><div>Allow Direct-IP Multimedia? y</div><div>Maximum Call Rate for Direct-IP Multimedia: 1920:Kbits</div><div>Maximum Call Rate for Priority Direct-IP Multimedia: 1920:Kbits</div><table><tr><th></th><th>Mode</th><th>Redundancy</th></tr><tr><td>FAX</td><td>t.38-standard</td><td>0</td></tr><tr><td>Modem</td><td>off</td><td>0</td></tr><tr><td>TDD/TTY</td><td>US</td><td>3</td></tr><tr><td>Clear-channel</td><td>n</td><td>0</td></tr></table></div></div>		Mode	Redundancy	FAX	t.38-standard	0	Modem	off	0	TDD/TTY	US	3	Clear-channel	n	0																	
	Mode	Redundancy																															
FAX	t.38-standard	0																															
Modem	off	0																															
TDD/TTY	US	3																															
Clear-channel	n	0																															



### 3.1.3. IP Network Region

This section describes the configuration steps for creating an ip-network region that supports multimedia capabilities using the ip-codecs created in Section 3.1.2.

Step	Description
1.	<p>Enter the <b>change ip-network-region X</b> command, where ‘X’ is an unused network region. On Page 1, of the <b>IP NETWORK REGION</b> form, enter appropriate values for <b>Location</b> and <b>Name</b>. Set <b>Intra-region IP-IP Direct Audio</b> and <b>Inter-region IP-IP Direct Audio</b> to ‘yes’. Set the <b>Codec Set</b> to ‘1’ to match the codec set configured in step Section 3.1.2.</p> <pre>change ip-network-region 1                                     Page 1 of 19   IP NETWORK REGION Region: 1 Location: 1             Authoritative Domain: Name: To Customer MEDIA PARAMETERS Codec Set: 1            Intra-region IP-IP Direct Audio: yes                         Inter-region IP-IP Direct Audio: yes                         UDP Port Min: 2048                    IP Audio Hairpinning? y                         UDP Port Max: 65535 DIFFSERV/TOS PARAMETERS                                     RTCP Reporting Enabled? y Call Control PHB Value: 46                                   RTCP MONITOR SERVER PARAMETERS Audio PHB Value: 46   Use Default Server Parameters? y Video PHB Value: 26 802.1P/Q PARAMETERS Call Control 802.1p Priority: 6 Audio 802.1p Priority: 6 Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS H.323 IP ENDPOINTS   RSVP Enabled? n H.323 Link Bounce Recovery? y Idle Traffic Interval (sec): 3483 Keep-Alive Interval (sec): 5 Keep-Alive Count: 5</pre>
2.	<p>On Page 2, enter ‘any-auth’ for the first <b>H.323 SECURITY PROFILES</b> entry. The ‘any-auth’ entry ensures that Avaya Communication Manager will use either a challenge or strong (pin-ike) authentication if the endpoint supports it.</p> <pre>change ip-network-region 1                                     Page 2 of 19   IP NETWORK REGION  INTER-GATEWAY ALTERNATE ROUTING / DIAL PLAN TRANSPARENCY Incoming LDN Extension: Conversion To Full Public Number - Delete: 0  Insert: Maximum Number of Trunks to Use for IGAR: 20 Dial Plan Transparency in Survivable Mode? n  BACKUP SERVERS(IN PRIORITY ORDER)    H.323 SECURITY PROFILES 1                                     1  any-auth 2                                     2 3                                     3 4                                     4 5 6</pre>

Step	Description
3.	<p>On Page 3, enter the number of the IP codec set configured in Section 3.1.2 for each pair of IP network regions in which inter-region video and audio communications are expected. Contact Center endpoints are assigned to IP network region <b>2</b>, noted by the <b>dst rgn</b> field. Customer endpoints are assigned to IP network region <b>1</b>.</p> <p>The '<b>NoLimit</b>' entry under <b>WAN-BW-limits Units</b> is an arbitrary value. To calculate the actual available bandwidth between two ip network regions, refer to reference [3] for more details.</p> <div> <pre> change ip-network-region 1 Page 3 of 19  Inter Network Region Connection Management  src dst codec direct WAN-BW-limits Video Dyn rgn rgn set WAN Units Total Norm Prio Shr Intervening-regions CAC IGAR 1 1 1 1 2 1 y NoLimit n 1 3 1 4 1 5 1 6 1 7 1 8 1 9 1 10 1 11 1 12 1 13 1 14 1 15 </pre> </div>

### 3.1.4. H.323 QSIG Trunk

This section describes the configuration steps for creating a signaling group and trunk group from the Customer location to the Contact Center location.

Step	Description																																								
1.	<p>Enter the <b>list ip-interface all</b> command and verify that there is at least one C-LAN and MedPro board in the same IP network region as configured in Section 3.1.3. Note the <b>Node Name</b> of the C-LAN board.</p> <div><pre>list ip-interface all</pre><div>Page1</div><table><thead><tr><th colspan="10">IP INTERFACES</th></tr><tr><th>ON</th><th>Type</th><th>Slot</th><th>Code</th><th>Sfx</th><th>Node Name/ IP-Address</th><th>Subnet Mask</th><th>Gateway Address</th><th>Net Rgn</th><th>VLAN</th></tr></thead><tbody><tr><td>y</td><td>C-LAN</td><td>01A03</td><td>TN799</td><td>D</td><td>C-LAN-A 5.1.1.4</td><td>255.255.255.0</td><td>5.1.1.254</td><td>1</td><td>n</td></tr><tr><td>y</td><td>MEDPRO</td><td>01A04</td><td>TN2302</td><td></td><td>MedPro-A 5.1.1.6</td><td>255.255.255.0</td><td>5.1.1.254</td><td>1</td><td>n</td></tr></tbody></table></div>	IP INTERFACES										ON	Type	Slot	Code	Sfx	Node Name/ IP-Address	Subnet Mask	Gateway Address	Net Rgn	VLAN	y	C-LAN	01A03	TN799	D	C-LAN-A 5.1.1.4	255.255.255.0	5.1.1.254	1	n	y	MEDPRO	01A04	TN2302		MedPro-A 5.1.1.6	255.255.255.0	5.1.1.254	1	n
IP INTERFACES																																									
ON	Type	Slot	Code	Sfx	Node Name/ IP-Address	Subnet Mask	Gateway Address	Net Rgn	VLAN																																
y	C-LAN	01A03	TN799	D	C-LAN-A 5.1.1.4	255.255.255.0	5.1.1.254	1	n																																
y	MEDPRO	01A04	TN2302		MedPro-A 5.1.1.6	255.255.255.0	5.1.1.254	1	n																																
2.	<p>Enter the <b>change node-names ip</b> command. Specify a node name for the Contact Center C-LAN and enter its IP address.</p> <div><pre>change node-names ip</pre><div>Page1 of2</div><table><thead><tr><th colspan="2">IP NODE NAMES</th></tr><tr><th>Name</th><th>IP Address</th></tr></thead><tbody><tr><td>C-LAN-1B09</td><td>5.1.1.8</td></tr><tr><td>C-LAN-2A</td><td>6.1.1.4</td></tr><tr><td>C-LAN-A</td><td>5.1.1.4</td></tr><tr><td>C-LAN-B</td><td>5.1.1.5</td></tr><tr><td>clan-cc</td><td>30.1.1.4</td></tr></tbody></table></div>	IP NODE NAMES		Name	IP Address	C-LAN-1B09	5.1.1.8	C-LAN-2A	6.1.1.4	C-LAN-A	5.1.1.4	C-LAN-B	5.1.1.5	clan-cc	30.1.1.4																										
IP NODE NAMES																																									
Name	IP Address																																								
C-LAN-1B09	5.1.1.8																																								
C-LAN-2A	6.1.1.4																																								
C-LAN-A	5.1.1.4																																								
C-LAN-B	5.1.1.5																																								
clan-cc	30.1.1.4																																								

Step	Description
3.	<p>Enter the <b>add signaling-group X</b> command, where 'X' is an unused signaling group number. Set <b>Near-end Node Name</b> to the Node Name of the C-LAN board identified in Step 1, and set <b>Far-end Node Name</b> to the Node Name of the C-LAN identified in Step 2. Set the other bolded fields below to the values indicated. The <b>Far-end Network Region</b> is set to the IP network region selected for the Contact Center.</p> <pre> add signaling-group 50                                      Page 1 of 1                                       SIGNALING GROUP  Group Number: 50                    Group Type: h.323                                      Remote Office? n      Max number of NCA TSC: 0                                      SBS? n                Max number of CA TSC: 0 IP Video? y      Priority Video? n    Trunk Group for NCA TSC: Trunk Group for Channel Selection: TSC Supplementary Service Protocol: b Network Call Transfer? y                                      T303 Timer(sec): 10  Near-end Node Name: C-LAN-A          Far-end Node Name: clan-cc Near-end Listen Port: 1720           Far-end Listen Port: 1720                                      Far-end Network Region: 2 LRQ Required? n                      Calls Share IP Signaling Connection? n RRQ Required? n Media Encryption? n                  Bypass If IP Threshold Exceeded? n                                      H.235 Annex H Required? n DTMF over IP: in-band                Direct IP-IP Audio Connections? y Link Loss Delay Timer(sec): 90        IP Audio Hairpinning? y Enable Layer 3 Test? y                Interworking Message: PROgress H.323 Outgoing Direct Media? y        DCP/Analog Bearer Capability: 3.1kHz </pre>
4.	<p>Enter the <b>add trunk-group X</b> command, where 'X' is an unused trunk group number. On Page 1 of the <b>trunk-group</b> form, set <b>Group Type</b> to 'isdn'. Enter a descriptive <b>Group Name</b> and an available Trunk Access Code (TAC) that is valid under the provisioned dial plan. Set <b>Carrier Medium</b> as 'H.323' to designate this as an IP trunk. The <b>Service Type</b> should be set to 'tie'. Enter 'auto' for <b>Member Assignment Method</b>, and enter the signaling group number added in Step 3 in <b>Signaling Group</b> and the appropriate value in <b>Number of Members</b>.</p> <pre> add trunk-group 50                                      Page 1 of 21                                       TRUNK GROUP  Group Number: 50                    Group Type: isdn          CDR Reports: y Group Name: To ContactCtr           COR: 1                   TN: 1                TAC: 150 Direction: two-way                 Outgoing Display? n      Carrier Medium: H.323 Dial Access? y                     Busy Threshold: 255      Night Service: Queue Length: 0 Service Type: tie                   Auth Code? n                                      Member Assignment Method: auto                                      Signaling Group: 50                                      Number of Members: 23 </pre>

Step	Description
5.	<p>On Page 2, set <b>Supplementary Services Protocol</b> to '<b>b</b>' to enable QSIG features. <b>Digit Handling (in/out)</b> should be set to '<b>enbloc/enbloc</b>' and <b>Format</b> as '<b>unk-unk</b>'.</p> <pre> add trunk-group 50 Group Type: isdn  TRUNK PARAMETERS Codeset to Send Display: 6      Codeset to Send National IEs: 6 Charge Advice: none Supplementary Service Protocol: b  Digit Handling (in/out): enbloc/enbloc  Incoming Calling Number - Delete:      Insert:      Digital Loss Group: 18 Format: unk-unk  Disconnect Supervision - In? y  Out? n Answer Supervision Timeout: 0 </pre>
6.	<p>On Page 3, set <b>Send Name</b> and <b>Send Calling Number</b> to '<b>y</b>' and <b>Format</b> to '<b>public</b>'. Default values may be used in the remaining fields.</p> <pre> add trunk-group 50 TRUNK FEATURES ACA Assignment? n      Measured: none Internal Alert? n      Maintenance Tests? y Data Restriction? n    NCA-TSC Trunk Member: Send Name: y          Send Calling Number: y Used for DCS? n        Hop Dgt? n      Send EMU Visitor CPN? n Suppress # Outpulsing? n  Format: public UII IE Treatment: service-provider  Replace Restricted Numbers? n Replace Unavailable Numbers? n Send Called/Busy/Connected Number: y Hold/Unhold Notifications? y Modify Tandem Calling Number? n  Send UII IE? y Send UCID? n Send Codeset 6/7 LAI IE? y </pre>

Step	Description
7.	<p>On Page 4, set <b>QSIG Value-Added</b> to 'y'. When this field is enabled, the <b>QSIG-Value Coverage Encoding</b> field is displayed. Leave the default value as 'proprietary'.</p> <div> <pre> add trunk-group 50                                 QSIG TRUNK GROUP OPTIONS                                 Page    4 of 21  TSC Method for Auto Callback: drop-if-possible   Diversion by Reroute? y     Path Replacement? y Path Replacement with Retention? y                                  SBS? n Display Forwarding Party Name? y   Character Set for QSIG Name: eurofont                                 QSIG Value-Added? y                                 QSIG-Value Coverage Encoding: proprietary </pre> </div>
8.	<p>Enter <b>change signaling-group 50</b> to add the trunk group created in Steps 4-8 to the signaling group. Set <b>Trunk Group for Channel Selection</b> to '50', which is the trunk group number configured in the previous steps.</p> <div> <pre> change signaling-group 50                                 SIGNALING GROUP                                 Page    1 of 1  Group Number: 50                Group Type: h.323                                 Remote Office? N      Max number of NCA TSC: 0                                 SBS? n                Max number of CA TSC: 0                                 IP Video? y          Priority Video? n    Trunk Group for NCA TSC:                                 <b>Trunk Group for Channel Selection: 50</b>                                 TSC Supplementary Service Protocol: b      Network Call Transfer? y                                 T303 Timer(sec): 10  Near-end Node Name: C-LAN-A      Far-end Node Name: clan-retail Near-end Listen Port: 1720      Far-end Listen Port: 1720                                 Far-end Network Region: 1                                 LRQ Required? n        Calls Share IP Signaling Connection? y                                 RRQ Required? n                                 Media Encryption? n      Bypass If IP Threshold Exceeded? n   H.235 Annex H Required? n                                 DTMF over IP: in-band    Direct IP-IP Audio Connections? y                                 Link Loss Delay Timer(sec): 90      IP Audio Hairpinning? y                                 Enable Layer 3 Test? y      Interworking Message: PROGress                                 H.323 Outgoing Direct Media? y      DCP/Analog Bearer Capability: 3.1kHz </pre> </div>

### 3.1.5. Call Routing

This section describes the configuration steps for routing calls using Automatic Alternate Routing (AAR).

Step	Description
1.	<p>Enter the <b>change feature-access-codes</b> command. For <b>Auto Alternate Routing (AAR) Access Code</b>, enter a FAC that is valid under the provisioned dial plan. In the example below, '8' is used to invoke AAR.</p> <pre> change feature-access-codes                                     Page 1 of 9                                 FEATURE ACCESS CODE (FAC) Abbreviated Dialing List1 Access Code: *01 Abbreviated Dialing List2 Access Code: *02 Abbreviated Dialing List3 Access Code: *03 Abbreviated Dial - Prgm Group List Access Code: Announcement Access Code: *20 Answer Back Access Code: *42 Attendant Access Code: <b>Auto Alternate Routing (AAR) Access Code: 8</b> Auto Route Selection (ARS) - Access Code 1: 9      Access Code 2: Automatic Callback Activation: *10      Deactivation: *11 Call Forwarding Activation Busy/DA: *33      All: *34      Deactivation: *35 Call Forwarding Enhanced Status: *36      Act: *37      Deactivation: *38 Call Park Access Code: *41 Call Pickup Access Code: *72 CAS Remote Hold/Answer Hold-Unhold Access Code: CDR Account Code Access Code: Change COR Access Code: Change Coverage Access Code: Contact Closure      Open Code:      Close Code: </pre>
2.	<p>Enter the <b>change aar analysis X</b> command, where 'X' is any digit. Add an entry as follows:</p> <ul style="list-style-type: none"> <li>• <b>Dialed String, Total Min and Max</b> - Enter a number string with minimum and maximum length specifications that matches the range of Contact Center location telephone numbers.</li> <li>• <b>Route Pattern</b> – Enter the number of an unused route pattern. The route pattern will be defined in the next step.</li> <li>• <b>Call Type</b> – Set to 'aar'.</li> <li>• <b>ANI Req'd</b> – Set to 'n'.</li> </ul> <pre> change aar analysis 222                                     Page 1 of 2                                 AAR DIGIT ANALYSIS TABLE                                 Location: all      Percent Full: 1 Dialed      Total      Route      Call      Node      ANI String      Min  Max    Pattern    Type      Num      Req'd 222         7    7     80      aar      n </pre>

Step	Description
3.	<p>Enter the <b>change route-pattern X</b> command where '<b>X</b>' is the number of the route pattern specified in Step 2. Add a routing entry as follows:</p> <ul style="list-style-type: none"> <li>• <b>Grp No</b> – Enter the number of the trunk group configured in Section 3.1.4.</li> <li>• <b>FRL</b> – Assign a Facility Restriction Level to this routing preference. '0' is the least restrictive.</li> </ul> <p>Thus, in this example, when an internal caller dials 8 (to invoke AAR) followed by a 222-XXXX number, the call will be routed to trunk group 50.</p> <pre> change route-pattern 80                                     Page 1 of 3       Pattern Number: 80  Pattern Name: To Retail       SCCAN? n        Secure SIP? n   Grp FRL NPA Pfx Hop Toll No.  Inserted          DCS/ IXC   No      Mrk Lmt List Del  Digits          QSIG                                      Dgts      Intw 1: 50    0 2: 3: 4: 5: 6:                                      n  user                                      n  user                                      n  user                                      n  user                                      n  user                                      n  user    BCC VALUE  TSC CA-TSC      ITC BCIE Service/Feature PARM  No. Numbering LAR   0 1 2 M 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 </pre>



### 3.1.6. Station Administration

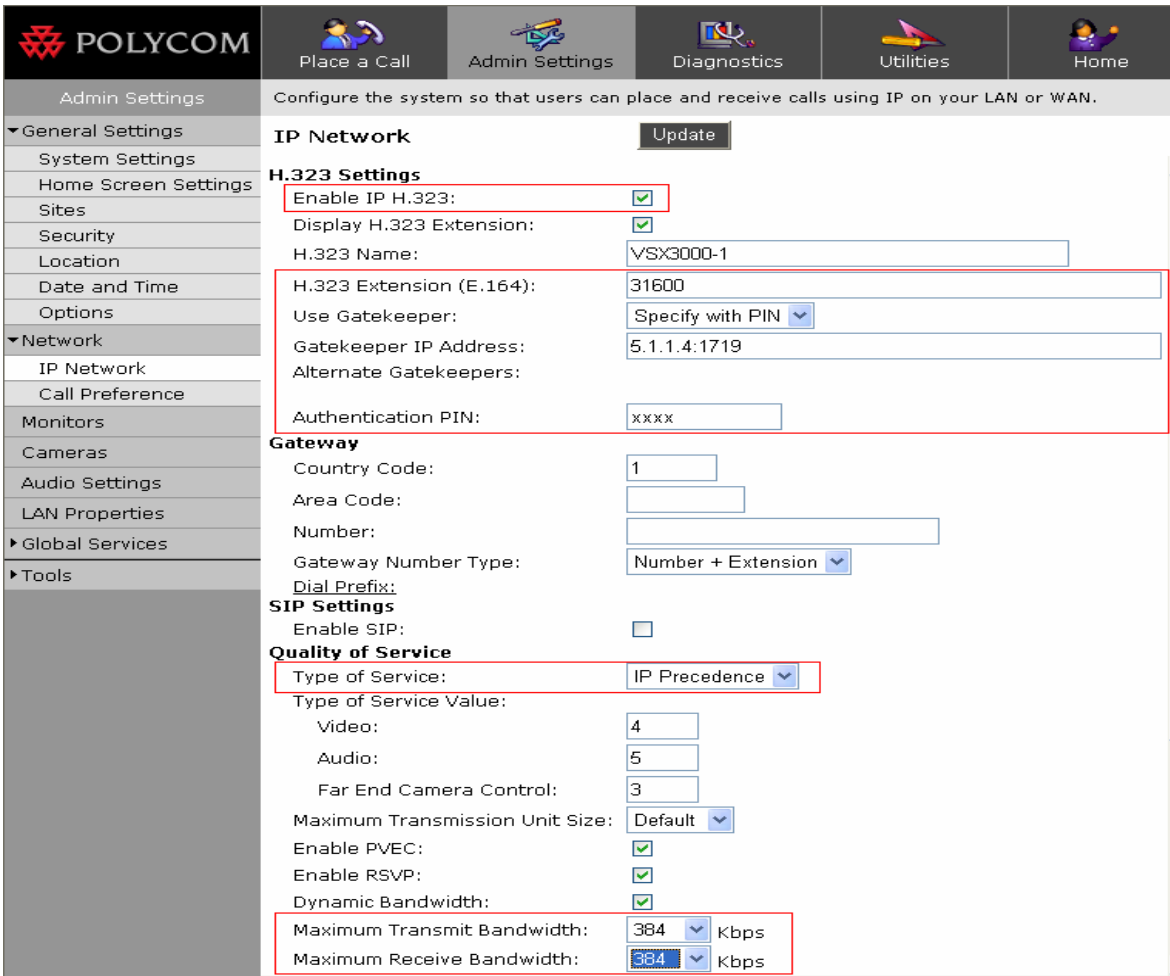
This section describes the steps for administering the Polycom in Avaya Communication Manager.

Step	Description
1.	<p>The Polycom requires the administration of four stations in Avaya Communication Manager which are hunted to one another via the <b>Hunt-to Station</b> field. Four stations are required by Avaya Communication Manager to allow for multiple video streams originating or terminating from a single Polycom station. The Polycom registers to Avaya Communication Manager as authenticated H.323 endpoints.</p> <p>Enter the <b>add station X</b> command where 'X' is an unused extension. Enter a descriptive name in the <b>Name</b> field and select '<b>H.323</b>' as the Type. <b>Authentication Required</b> and <b>IP Video</b> are both set to '<b>y</b>'. Since authentication is required, a <b>Security Code</b> must be defined. At this time, do not enter an extension in the <b>Hunt-to Station</b> field.</p> <div><pre>add station 31600                                     Page 1 of 4                                  STATION  Extension: 31600                                Lock Messages? n                BCC: 0   Type: H.323                                Security Code: XXXX                TN: 1   Port: IP                                Coverage Path 1:                COR: 1   Name: Polycom                            Coverage Path 2:                COS: 1                                 Hunt-to Station:                Tests? y  STATION OPTIONS                                  Time of Day Lock Table:                                 Message Waiting Indicator: none                                  Authentication Required? y                                  Survivable COR: internal                                 Survivable Trunk Dest? y                                 DTMF over IP: in-band                                  IP Video? y</pre></div>
2.	Repeat Step 1 to add the second station, 31601, for the Polycom.
3.	Repeat Step 1 to add the third station, 31602, for the Polycom.
4.	Repeat Step 1 to add the fourth station, 31603, for the Polycom.

Step	Description
5.	<p>Enter the <b>change station 31600</b> command. On Page 1 of the station form, set <b>Hunt-to Station</b> to the extension of the second station '<b>31601</b>' configured for the Polycom.</p> <pre> change station 31600                                     Page 1 of 4                                  STATION  Extension: 31600                                Lock Messages? n                BCC: 0 Type: H.323                                Security Code: XXXX                TN: 1 Port: S01546                                Coverage Path 1:                COR: 1 Name: Polycom                                Coverage Path 2:                COS: 1                                 <b>Hunt-to Station: 31601</b>  Tests? y STATION OPTIONS                                  Time of Day Lock Table:                                 Message Waiting Indicator: none                                  Authentication Required? y                                  Survivable COR: internal Survivable Trunk Dest? y DTMF over IP: in-band                                  IP Video? y </pre>
6.	Repeat Step 5 for station <b>31601</b> . Set <b>Hunt-to Station</b> to the third station ' <b>31602</b> ' configured for the Polycom.
7.	Repeat Step 5 for station <b>31602</b> . Set <b>Hunt-to Station</b> to the fourth station ' <b>31603</b> ' configured for the Polycom.
8.	Repeat Step 5 for station <b>31603</b> . Set <b>Hunt-to Station</b> to the first station ' <b>31600</b> ' configured for the Polycom.

### 3.1.7. Polycom VSX 3000

This section describes the steps for administering the Avaya-specific settings in the Polycom VSX 3000. Other optional settings may be configured directly from the display and keypad of the Polycom. This section assumes an IP address, subnet, and gateway have already been configured. Consult the Polycom documentation [4] for more details on the optional settings, as well as IP configuration.

Step	Description
1.	<p>To access the web interface for the Polycom VSX 3000 videophone, type the IP address for the Polycom into a web browser. From the <b>Admin Settings→Network →IP Network</b> screen, check the <b>Enable IP H.323</b>, set the <b>Use Gatekeeper</b> field as <b>Specify with PIN</b>, and ensure that the <b>Gatekeeper IP Address</b> field has the correct IP address for the call server and the correct port number (1719). The extension and authentication PIN need to match the extension and security code of the station in Avaya Communication Manager. Type of Service should be set to <b>IP Precedence</b>. <b>Maximum Transmit Bandwidth</b> and <b>Maximum Receive Bandwidth</b> should be set based on network requirements. Use defaults for remaining values. Click the <b>Update</b> button when complete.</p> 

## 3.2. Contact Center Location

This section reviews the features that are required in the Contact Center location for the solution described in these Application Notes.

### 3.2.1. System Parameters

For licensed features that are not enabled in this section, contact an authorized Avaya account representative to obtain the licenses.

If any of the **system-parameters customer-options** parameters are changed, it is necessary to logout of Avaya Communication Manager, and login to effect the permission changes.

Step	Description
1.	Repeat Steps 1 and 3 in Section 3.1.1 to verify proper licensing for <b>system-parameters special-applications</b> and <b>system parameters customer-options</b> .
2.	On Page 6 of the <b>system parameters customer-options</b> form, verify that the following Call Center Elite features are set to 'y'. <div><div>change system-parameters customer-options</div><div>Page 6 of 11</div><div>CALL CENTER OPTIONAL FEATURES</div><div>Call Center Release: 5.0</div><div><div>ACD? y</div><div>Reason Codes? n</div><div>BCMS (Basic)? n</div><div>Service Level Maximizer? n</div><div>BCMS/VuStats Service Level? n</div><div>Service Observing (Basic)? n</div><div>BSR Local Treatment for IP &amp; ISDN? n</div><div>Service Observing (Remote/By FAC)? n</div><div>Business Advocate? n</div><div>Service Observing (VDNs)? n</div><div>Call Work Codes? n</div><div>Timed ACW? n</div><div>DTMF Feedback Signals For VRU? n</div><div>Vectoring (Basic)? y</div><div>Dynamic Advocate? n</div><div>Vectoring (Prompting)? y</div><div>Expert Agent Selection (EAS)? y</div><div>Vectoring (G3V4 Enhanced)? y</div><div>EAS-PHD? n</div><div>Vectoring (3.0 Enhanced)? y</div><div>Forced ACD Calls? n</div><div>Vectoring (ANI/II-Digits Routing)? y</div><div>Vectoring (G3V4 Advanced Routing)? y</div><div>Lookahead Interflow (LAI)? n</div><div>Vectoring (CINFO)? y</div><div>Multiple Call Handling (On Request)? n</div><div>Vectoring (Best Service Routing)? n</div><div>Multiple Call Handling (Forced)? n</div><div>Vectoring (Holidays)? n</div><div>PASTE (Display PBX Data on Phone)? n</div><div>Vectoring (Variables)? n</div><div>(NOTE: You must logoff &amp; login to effect the permission changes.)</div></div></div>

Step	Description
3.	<p>On Page 10 of the <b>system parameters customer-options</b> form, verify that there are sufficient <b>IP_API_A</b> licenses.</p> <div> <pre> change system-parameters customer-options MAXIMUM IP REGISTRATIONS BY PRODUCT ID Page 10 of 11  Product ID  Rel. Limit      Used AgentSC      : 0           0 <b>IP_API_A</b>    : <b>2400</b>        <b>2</b> IP_API_B      : 2400        0 IP_API_C      : 2400        0 IP_Agent      : 2400        0 IP_IR_A       : 2400        0 IP_Phone      : 12000       22 IP_ROMax      : 12000       0 IP_Soft       : 2400        0 IP_eCons      : 20          0 </pre> </div>
4.	<p>Enter the <b>change system-parameters features</b> command. Navigate to Page 11 and verify <b>Expert Agent Selection (EAS) Enabled</b> is 'y'.</p> <div> <pre> change system-parameters features FEATURE-RELATED SYSTEM PARAMETERS CALL CENTER SYSTEM PARAMETERS EAS     <b>Expert Agent Selection (EAS) Enabled? y</b>     Minimum Agent-LoginID Password Length:     Direct Agent Announcement Extension:      Delay:     Message Waiting Lamp Indicates Status For: station  VECTURING     Converse First Data Delay: 0      Second Data Delay: 2     Converse Signaling Tone (msec): 100    Pause (msec): 70     Prompting Timeout (secs): 10     Interflow-qpos EWT Threshold: 2     Reverse Star/Pound Digit For Collect Step? n     Available Agent Adjustments for BSR? n     BSR Tie Strategy: 1st-found     Store VDN Name in Station's Local Call Log? n SERVICE OBSERVING     Service Observing: Warning Tone? y      or Conference Tone? n     Service Observing Allowed with Exclusion? n     Allow Two Observers in Same Call? y </pre> </div>

Step	Description
5.	<p>On Page 12, verify <b>BCMS/VuStats LoginIDs</b> is set to 'y'.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>change system-parameters features <span style="float: right;">Page 12 of 17</span></p> <p style="text-align: center;">FEATURE-RELATED SYSTEM PARAMETERS</p> <p>AGENT AND CALL SELECTION</p> <p style="padding-left: 40px;">MIA Across Splits or Skills? n</p> <p style="padding-left: 40px;">ACW Agents Considered Idle? y</p> <p style="padding-left: 40px;">Call Selection Measurement: current-wait-time</p> <p style="padding-left: 20px;">Service Level Supervisor Call Selection Override? n</p> <p style="padding-left: 40px;">Auto Reserve Agents: none</p> <p>CALL MANAGEMENT SYSTEM</p> <p style="padding-left: 40px;">REPORTING ADJUNCT RELEASE</p> <p style="padding-left: 60px;">CMS (appl mis):</p> <p style="padding-left: 60px;">IQ (appl ccr):</p> <p style="padding-left: 40px;"><b>BCMS/VuStats LoginIDs? y</b></p> <p style="padding-left: 40px;">BCMS/VuStats Measurement Interval: hour</p> <p style="padding-left: 20px;">BCMS/VuStats Abandon Call Timer (seconds):</p> <p style="padding-left: 40px;">Validate BCMS/VuStats Login IDs? n</p> <p style="padding-left: 40px;">Clear VuStats Shift Data: on-login</p> <p style="padding-left: 20px;">Remove Inactive BCMS/VuStats Agents? n</p> </div>

### 3.2.2. IP Codec Set

Step	Description
1.	Repeat Steps 1 and 2 in Section 3.1.2 to create an IP codec set with multimedia capabilities to support video.

### 3.2.3. IP Network Region

Step	Description
1.	Repeat Steps 1-3 in Section 3.1.3 to create an IP network region that supports multimedia capabilities using the ip codecs created in Section 3.2.2. IP network regions for each set of endpoints do not have to match the IP network regions at the Customer Location.

### 3.2.4. H.323 QSIG Trunk

Step	Description
1.	Repeat Steps 1-8 in Section 3.1.4 to create a signaling group and trunk group from the Contact Center location to the Customer location. Trunk numbers and signaling group numbers do not have to match those in the Customer Location.

### 3.2.5. Call Routing

Step	Description
1.	Repeat Steps 1-3 in Section 3.1.5 if it is desired to have Contact Center agents place outgoing calls to the Customer location.

### 3.2.6. Station Administration

This section describes the steps for configuring Avaya IP Softphone enabled contact center agent telephones. This section assumes successful installation of the Avaya IP Softphone, with the Polycom Adapter as an additional add-on.

Step	Description
1.	<p>To create a new station, with Avaya IP Softphone video capabilities enabled, enter the <b>add station X</b> command where 'X' is an unused station number. Set <b>IP Softphone</b> and <b>IP Video Softphone</b> to 'y' to enable shared control mode of this station with an Avaya IP Softphone with video. Enter the phone type in the <b>Type</b> field, and give a descriptive name for the station in the <b>Name</b> field. The <b>Port</b> field will default to 'IP', as this is an Avaya IP telephone. Enter an appropriate <b>Security Code</b>.</p> <div><pre>add station 222-2100                                     Page 1 of 5                                  STATION  Extension: 222-2100                                Lock Messages? I                BCC: 0   Type: 4621   Security Code: XXXX              TN: 1   Port: IP   Coverage Path 1:                 COR: 1   Name: Agent1                                       Coverage Path 2:                 COS: 1   Hunt-to Station:  STATION OPTIONS                                  Time of Day Lock Table:       Loss Group: 19                                Personalized Ringing Pattern: 1                                 Message Lamp Ext: 222-2100       Speakerphone: 2-way                            Mute Button Enabled? y       Display Language: english                       Expansion Module? n       Survivable GK Node Name:                        Media Complex Ext:       Survivable COR: internal                         IP SoftPhone? y       Survivable Trunk Dest? y                        IP Video Softphone? y                                  Customizable Labels? y</pre></div>

Step	Description
2.	<p>On Page 4 , add the following <b>BUTTON ASSIGNMENTS</b> to the station. The three <b>call-appr</b> buttons are added by default. The <b>aux-work</b>, <b>auto-in</b>, <b>manual-in</b>, and <b>release</b> buttons are added for ACD functionality.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <pre> add station 222-2100                                     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: auto-in                                Grp: 2: call-appr                                6: manual-in                               Grp: 3: call-appr                                7: release 4: aux-work      RC:      Grp:              8: </pre> </div>
3.	Repeat Steps 1-2 to create a station using extension 222-2101.
4.	Repeat Steps 1-2 to create a station using extension 222-2110 which is the Supervisor station.



### 3.2.7. Feature Access Codes

This section describes the steps for configuring Feature Access Codes (FAC) for Automatic Call Distribution (ACD).

Step	Description
1.	<p>Enter the <b>change feature-access-codes</b> command. Navigate to Page 5, and enter FACs that are valid under the provisioned dial plan for the following bolded fields.</p> <div><pre>change feature-access-codes                                     Page   5 of   9                                 FEATURE ACCESS CODE (FAC)                                 Automatic Call Distribution Features                                 After Call Work Access Code:                                 Assist Access Code:                                 <b>Auto-In Access Code: 017</b>                                 <b>Aux Work Access Code: 019</b>                                 <b>Login Access Code: 015</b>                                 <b>Logout Access Code: 016</b>                                 <b>Manual-in Access Code: 018</b>                                 Service Observing Listen Only Access Code:                                 Service Observing Listen/Talk Access Code:                                 Service Observing No Talk Access Code:                                 Add Agent Skill Access Code:                                 Remove Agent Skill Access Code:                                 Remote Logout of Agent Access Code:</pre></div>

### 3.2.8. Administer Skills

This section describes the configuration steps for creating a skill enabled hunt group.

Step	Description
1.	<p>Enter the <b>add hunt group X</b> command., where 'X' is a valid unused hunt group number. Enter a descriptive name for <b>Group Name</b>. Enter an unused valid extension for <b>Group Extension</b>. Enter 'ucd-mia' for <b>Group Type</b>. This allows ACD calls to route to the idlest agent based on when the agent finished the most recent call. Set <b>ACD</b>, <b>Queue</b>, and <b>Vector</b> to 'y'.</p> <div><pre>add hunt-group 100                                     Page 1 of 61                                      HUNT GROUP        Group Number: 100                                ACD? y       Group Name: Video Queue                          Queue? y       Group Extension: 222-2222                        Vector? y       Group Type: ucd-mia       TN: 1       COR: 1   MM Early Answer? n       Security Code:                                Local Agent Preference? n       ISDN/SIP Caller Display:        Queue Limit: unlimited       Calls Warning Threshold:      Port:       Time Warning Threshold:      Port:</pre></div>
2.	<p>On Page 2, set <b>Skill</b> to 'y'.</p> <div><pre>add hunt-group 100                                     Page 2 of 3                                      HUNT GROUP        Skill? y      Expected Call Handling Time (sec): 180       AAS? n       Measured: none      Service Objective (sec): 20       Supervisor Extension:      Service Level Supervisor? n        Controlling Adjunct: none        Timed ACW Interval (sec):      Dynamic Queue Position? n       Multiple Call Handling: none        Redirect on No Answer (rings):       Redirect to VDN:       Forced Entry of Stroke Counts or Call Work Codes? n</pre></div>

### 3.2.9. Administer Agents

This section describes the configuration steps for creating skill-based agents.

Step	Description
1.	<p>Enter the <b>add agent-loginID X</b> command, where '<b>X</b>' is a valid unused extension. Enter a descriptive agent name for <b>Name</b>. Enter and re-enter the agent password in the <b>Password</b> and <b>Password (enter again)</b> fields, respectively.</p> <pre> add agent-loginID 2222400                                     Page 1 of 2                                 AGENT LOGINID        Login ID: 222-2400                                     AAS? n       Name: Agent1   AUDIX? n       TN: 1  LWC Reception: spe       COR: 1  LWC Log External Calls? n       Coverage Path:   AUDIX Name for Messaging:       Security Code:                                  LoginID for ISDN/SIP Display? n                                 Password: XXXX                                 Password (enter again): XXXX                                 Auto Answer: station                                 MIA Across Skills: system                                 ACW Agent Considered Idle: system                                 Aux Work Reason Code Type: system                                 Logout Reason Code Type: system                                 Maximum time agent in ACW before logout (sec): system                                 Forced Agent Logout Time:      :        WARNING: Agent must log in again before changes take effect </pre>
2.	<p>On Page 2, assign the hunt group administered in Section 3.2.8 for <b>SN</b>. Set skill level (<b>SL</b>) to '<b>1</b>', which is the highest priority.</p> <pre> add agent-loginID 2222400                                     Page 2 of 2                                 AGENT LOGINID        Direct Agent Skill:                                     Service Objective? n       Call Handling Preference: skill-level                   Local Call Preference? n        SN  RL SL          SN  RL SL          SN  RL SL          SN  RL SL       1: 100      1      16:          31:          46:       2:          17:          32:          47:       3:          18:          33:          48: </pre>
3.	Repeat Steps 1 and 2 to create an <b>agent-loginID</b> of ' <b>222-2500</b> ' with a <b>Name</b> of ' <b>Agent2</b> '.

## 4. Verification Steps

Perform the following steps to test and verify the sample video solution.

Step	Description
1.	<p>From the Customer location, enter <b>list registered-ip-stations</b> to verify that all four Polycom extensions are registered as H.323 endpoints in Avaya Communication Manager.</p> <pre>list registered-ip-stations</pre> <p style="text-align: right;">Page 1</p> <pre> REGISTERED IP STATIONS  Station Ext/  Set   Product  Prod  Station  Net Gatekeeper  TCP Orig Port    Type   ID       Rel   IP Address Rgn IP Address  Skt 31600        H.323  VSX 2000  0.0   5.1.1.231  1   5.1.1.4      n 31601        H.323  VSX 3000  0.0   5.1.1.231  1   5.1.1.4      n 31602        H.323  VSX 3000  0.0   5.1.1.231  1   5.1.1.4      n 31603        H.323  VSX 3000  0.0   5.1.1.231  1   5.1.1.4      n </pre>
2.	<p>Repeat Step 1 in the Contact Center location to verify that the Avaya 4621 telephones are logged in shared-control mode with an Avaya IP Softphone.</p> <pre>list registered-ip-stations</pre> <p style="text-align: right;">Page 1</p> <pre> REGISTERED IP STATIONS  Station Ext/  Set   Product  Prod  Station  Net Gatekeeper  TCP Orig Port    Type   ID       Rel   IP Address Rgn IP Address  Skt 222-2100     4621  IP_Phone 2.800 30.1.1.185  1   30.1.1.4      y 222-2100     4621  IP_Soft  5.242 30.1.1.194  1   30.1.1.4      y 222-2101     4621  IP_Phone 2.800 30.1.1.185  1   30.1.1.4      y 222-2101     4621  IP_Soft  5.242 30.1.1.194  1   30.1.1.4      y </pre>
3.	Log in agents using FACs (see Section 3.2.7) in the Contact Center location.
4.	<p>From the Contact Center location, enter <b>list agent-loginID</b> to verify agents (<b>Agent1</b> and <b>Agent2</b>) are logged in and display the correct skill level (<b>Skill/Lv</b>).</p> <pre>list agent-loginID</pre> <pre> AGENT LOGINID  Login      Name/      Dir Agt COR Ag SO Skill/Lv  Skill/Lv  Skill/Lv  Skill/Lv ID          Extension  AAS/AUD Pr 222-2400    Agent1      1   1v1 n 100/01  /         /         / 222-2100    222-2100    /         /         /         / 222-2500    Agent2      1   1v1 n 100/01  /         /         / 222-2101    222-2101    /         /         /         / </pre>
5.	Place both agents in the Contact Center location in aux-work mode by pressing the aux-work button that is configured. This removes both agents from ACD call distribution.

Step	Description
6.	Place a call from Polycom in the Customer location to the Contact Center location using the hunt group extension created in Section 3.2.8.
7.	Verify the Polycom in the Customer location is in a ringing state. Verify neither of the agent's telephones should be ringing, as they are not available to answer a call.
8.	Place Agent1 in auto-in mode, by pressing that button on the Avaya 4621 telephone. This allows the agent to become available for new ACD calls.
9.	Verify that the incoming call is routed to Agent1. Both the telephone and Avaya IP Softphone should be in a ringing state.
10.	Answer the call using either the telephone or the Avaya IP Softphone. Verify incoming video is seen on the Avaya IP Softphone. Two-way talk path should exist via the Avaya 4621 telephone.
11.	From the Polycom in the Customer location, verify both incoming video and two-way talk path exists.
12.	Transfer the call to the Supervisor at station 222-2110. Verify two-way talk path between the Supervisor and the Polycom exists. Video should be suspended on the Polycom.
13.	Transfer the call back to Agent1. Verify both video and two-way talk path is present when Agent1 is active on the call.
14.	Agent1 places the call on hold. Verify both video and two-way talk is suspended.
15.	Agent1 activates the held call. Verify both video and two-way talk path is resumed.

## 5. References

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

- [1] *Administrator Guide for Avaya Communication Manager*, Issue 4, January 2008.
- [2] *Avaya IP Softphone Release 6.0 User Reference*, Issue 1, March 2007.
- [3] *Avaya Video Telephony Solution Release 4.0 Networking Guide*, Issue 3, January 2008.

Product documentation for Polycom products may be found at <http://www.polycom.com>

- [4] *Administrators Guide for the VSX Series*, Version 8.7, July 2007.

---

**© 2008 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 and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at [interoplabnotes@list.avaya.com](mailto:interoplabnotes@list.avaya.com)