Avaya Video Conferencing Solutions Quick Setup

Release 6.0
16-300310
Issue 1
August 2010

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the Avaya Support Web site:

http://www.avaya.com/support

License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License type(s)

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (For example,., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Product that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated by Avaya provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site:

http://support.avaya.com/ThirdPartyLicense/

Preventing toll fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site:

http://www.avaya.com/support

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that can be accessed by this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who might be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions might be either to/through synchronous (time-multiplexed and/or circuit-based), or asynchronous (character-, message-, or packet-based) equipment, or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there might be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it might result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you — Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers must carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers might experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Standards Compliance

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment is the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. might void the user's authority to operate this equipment.

Federal Communications Commission Statement

Part 15:

Canadian Department of Communications (DOC) Interference Information

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

European Union Declarations of Conformity

CE

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (*Conformity Europeénne*) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (89/336/EEC) and Low Voltage Directive (73/23/EEC).

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the Avaya Support Web site:

http://www.avaya.com/support

Trademarks

Avaya, the Avaya logo, DEFINITY, MultiVantage, and COMPAS are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site:

http://www.avaya.com/support

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Support Web site:

http://www.avaya.com/support

Overview

This Quick setup guide covers the basic administration tasks to set up SIP and H.323 video endpoints. For detailed information, see *Avaya video conferencing Solutions Networking Guide 6.0*. This guide is intended for technicians installing the following video endpoints:

SIP endpoints

- Avaya Series 1000 Video Conferencing Endpoints
- Avaya one-X® Communicator

H.323 endpoints

- Polycom HDX video calling systems
- Polycom RMX video conferencing bridge platforms
- Polycom PathNavigator/CMA Gatekeeper
- Avaya one-X® Communicator

Prerequisites

- Avaya Aura™ Communication Manager Release 6.0 is installed and functional.
- Avaya Aura™ System Manager 6.0 is installed and functional.
- Avaya Aura™ Session Manager is installed and functional.
- The SIP or H.323 endpoint is installed installed and functional.

Note:
Installation of video features on the endpoints requires Session Manager to be configured. For instructions, see *Administering Avaya Aura™ Session Manager* on http://support.avaya.com.

Note:
All Avaya Aura™ components and endpoints must be connected to the network and able to communicate with each other.

- Familiarity with System Manager domains, SIP entities, entity links, locations,routing, and dial patterns.
- Familiarity with administering Communication Manager, Domains on Signaling Group and IP Network Regions, AAR/ARS routing, and endpoint interfaces.

- Perform a network readiness test or network assessment to ensure your network is capable of supporting bandwidth demands of video over IP. Avaya recommends implementing quality of service (QoS) across your network

Configuration of SIP video endpoints on Communication Manager 6.0

This section provides the procedure to configure video calling facility on SIP endpoints with Communication Manager 6.0.

Enabling video on Communication Manager

The following steps describe administration on both interfaces, SAT and System Manager. Only the fields that require change are mentioned, the rest may be left as default.

Table 1: Enabling video on Communication Manager

1	**Enabling Multimedia IP SIP Trunking feature on Communication Manager System Management Interface** 1. Log in to the Communication Manager System Management Interface. 2. Click **Licensing** > **Administration** and navigate to the **Feature Administration** page. 3. Verify that the **Multimedia IP SIP Trunking** feature is set to yes.
2	**Enabling Multimedia IP SIP Trunking feature** 1. On the System Manager interface, click **Elements** > **Feature Management** > **Parameters** > **System Parameters** - **Customer Options**. 2. Click the arrow icon next to the **Select Device(s) from Communication Manager List**. 3. Select the appropriate Communication Manager, and click **Show List**. 4. Select the radio button in the first column and click **View**. 5. Click **Next Page** and ensure the feature **Multimedia IP SIP Trunking** is set to y. Alternatively: ● On the Communication Manager SAT screen, enter **`display system-parameters customer-options`** and ensure the feature **Multimedia IP SIP Trunking** is set to y.

Table 1: Enabling video on Communication Manager

3	**Enabling video for the SIP signaling group** 1. On System Manager, click **Elements** > **Feature Management** > **Network** - **Signaling Groups.** 2. On the Signaling Groups page, click the arrow icon next to the Select Device(s) from Communication Manager List. 3. From the Communication Manager list, select the appropriate Communication Manager, and click Show List. 4. Select the appropriate **Signaling Group Number** and click edit to set parameters as mentioned below: • **IP Video** : y • **Direct IP-IP Audio connections** : y • **Initial IP-IP Direct Media** : y Alternatively: On the Communication Manager SAT screen, enter **`change signaling-group n`** and set parameters as mentioned below: • **IP Video** : y • **Direct IP-IP Audio connections** : y • **Initial IP-IP Direct Media** : y **Note:** Modifying the default Priority video option is not necessary. See *Avaya video conferencing Solutions Networking Guide 6.0* for further details.

Table 1: Enabling video on Communication Manager

4	**Identifying the IP-codec-set** 1. Note the values of the **Near-end Node Name** and **Far-end Network Region** fields. 2. If the **Near-end Node Name** field is set to **PROCR,** the listed value is used. If the **Near-end Node Name** field is set to **CLAN,** enter **`list ip-interface clan`** to find the correct **CLAN** and make a note of the slot value. These values are used to determine the IP-Codec-set. 3. On the Communication Manager SAT screen, enter **`display ip-interface procr/slot`**. 4. Note the value of the **Network Region** field. 5. On the Communication Manager SAT screen, enter **`display-ip-network-region`** and move to the Inter Network Region Connection Management page. 6. Ensure the dst rgn number aligns with the **Far-end Network Region** . Make note of the **codec set** number.
5	**Adding video to ip-codec-set** 1. On the SAT screen enter **`change ip-codec-set n`** , where **n** is the codec set number used by the SIP signalling group. 2. Add or change the appropriate audio codecs as required. Set the following Multimedia parameters: • **Allow Direct-IP Multimedia** : y • **Maximum Call Rate for Direct-IP Multimedia** : 1024 Kbits **Note:** These values are examples only. 1024 allows for 720p High Definition. Higher resolutions require more bandwidth. See *Avaya video Conferencing Solutions Networking Guide* for further details. • Maximum Call Rate for Priority Direct-IP Multimedia: **2048 Kbits** **Note:** This applies to priority video users and is not required for minimal administration. See *Avaya video Conferencing Solutions Networking Guide* for further details. **Note:** Verify that the list of audio codecs on the first page includes at least one of the audio codecs supported by the video endpoint, such as G.722 or G.711

Administration of Avaya Series 1000 Video Conferencing and Avaya one-X® Communicator video endpoints and users using System Manager

Perform the following steps to configure all Avaya Series 1000 Video Conferencing Endpoints and Avaya one-X® Communicator with SIP video. This section describes how to use System Manager to create an endpoint template and how to add users using these templates.

Creating a template

Table 2: Creating a template

1	**Creating a custom template for any SIP endpoint on System Manager** 1. Click **Elements** > **Templates** > **Endpoint**, select Communication Manager 6.0 on the **Endpoint Templates** page and click New. Set the following parameters: • **Set Type** : 9630SIP, an alias for the 1000 series endpoints • **Template Name** : Avaya recommends naming the template according to its AV10x0 type and Communication Manager release, such as **AV1010_CM_6_0**. • **COR** : 1 • **COS** : 1 or an appropriate cos group for priority video calling and bit-rate management **Note:** This applies to priority video users and is not required for minimal administration. See *Avaya video Conferencing Solutions Networking Guide 6.0* for further details. • **SIP trunk** : AAR or specific SIP trunk used between System Manager and Communication Manager 2. Select the **IP video** check box.

Table 3: Creating a template

1	**Enabling Call Appearace feature** 1. To enable the **Call Appearance** feature, click **Button Assignment**, and set the main buttons to **call appr** as follows : • **Avaya 1010** : 1 • **Avaya 1020** : 1 • **Avaya 1030** : 1 • **Avaya 1040** : 3 • **Avaya one-X® Communicator** : 3 • **Avaya 1050** : 7 **Note:** The call appearances must be set to the maximum limit permitted for each endpoint. 2. Select the **IP SoftPhone** check box for Avaya one-X® Communicator. When you select this check box, the title of the check box changes to IP Video SoftPhone. 3. Click Commit, and repeat this step for each endpoint.

Adding video users

Table 4: Adding video users

1	**Creating a New User Profile** On System Manager, click **Users** > **Manage Users** and click on **New** to open the **New User Profile** page. Fill in the following fields: • **Last Name** • **First Name** • **Login Name** : Example: ext@sip domain • **Authentication Type** : Basic • **SMGR Login Password** : • **Shared Communication Profile Password** : Corresponds to the authorization password for the series Avaya Series 1000 Video Conferencing Endpoints and the password for Avaya one-X® Communicator.
2	**Assigning an address** On the **New User Profile** page, click the **Communication Profile** drop-down arrow and under **Communication Address** click **New**. Set the following parameters: • **Type** : Avaya SIP • **Fully Qualified Address** : **ext@sip domain**, which must match the **Login Name** in step 1.

Table 4: Adding video users

3	**Enabling Session Manager Profile** Select the check box corresponding to **Session Manager profile** and set the following parameters: • **Primary Session Manager** : Appropriate option • **Secondary Session Manager** : None • **Origination Application Sequence** : Appropriate Communication Manager Server • **Terminating Application Sequence** : Appropriate Communication Manager Server • **Survivability Server** : None • **Home Location** : Appropriate option
4	**Creating an Endpoint Profile** 1. On the **New User Profile** page, under **Communication Profile**, check the Box corresponding to **Endpoint Profile**. 2. Select the appropriate Communication Manager system and set the following parameters: • **Extension** : same as **ext** from Assigning an address in step 2 • **Template** : *templatename*, where *templatename* is the name created in Table 2: Creating a template on page 8 • **Port** : IP 3. Click **Commit.**

Configuring the Avaya Series 1000 Video Conferencing Endpoints

Perform the following steps to configure all Avaya Series 1000 Video Conferencing Endpoints using the **IR Remote Control**. You can also configure each endpoint using a Web browser. See the Networking Guide for more information. If configuring the endpoint for the first time, you see the initial configuration wizard. You may set up the endpoint using the wizard or skip this process.

Table 5: Configuring Avaya Series 1000 Video Conferencing Endpoints

1	Click the blue **System Menu** Button on the remote. Select Admin Preferences by using the arrow buttons.Log on to the video endpoint. The default password is 1234.
2	**Setting General Parameters** Select **Network**, click **General**, and set the following parameters: • **DHCP** : If DHCP is in use, ensure the DHCP server is up and then select **Enabled.** If the DHCP is not in use, select **Disabled.** • **IP Address** : The IP address assigned to the actual endpoint • **Subnet Mask** : Appropriate entry • **Default Gateway** : Appropriate entry • **Host Name** : Appropriate entry • **DNS server** : Appropriate entry • **Network Speed** : Auto • **802.1X Authentication** : Disabled

Table 5: Configuring Avaya Series 1000 Video Conferencing Endpoints

3	**Enabling SIP protocol** Select **Communications**, click on **SIP**, and set the following parameters: • **SIP Username** : ext. This parameter is the same as step 1 of Table 4: Adding video users on page 10 • **Authorization Name** : Same as SIP Username • **Authorization Password** : Same as the Shared Communication Profile Password used in step 2 of Table 4: Adding video users on page 10 • **SIP registarion** : Through Proxy • **SIP Proxy** : Enabled • **Proxy Hostname** : Session Manager FQDN or IP address used for registration. This is the Session Manager Security Module / SIP Entity IP address or corresponding FQDN. • **SIP Registrar** : Enabled • **Registrar Hostname** : Same as Proxy Hostname • **TCP Signalling** : Enabled
4	**Confirming Registrar Status** Select **Communication**, click **SIP** and confirm if: • **Registrar Status**: Registered

Configure H.323 video endpoints on Communication Manager 6.0

This section provides a set of guidelines to configure video calling facility on H.323 endpoints with Communication Manager 6.0.

Configure Polycom VSX/HDX Series Video Conferencing Systems and V500/V700 Video Calling Systems

Use the following procedure to configure Polycom VSX/HDX video conferencing systems and V500 and V700 video calling systems. When setting up these systems, you will need to know the following:

- Maximum number of VSX/HDX, V500, and V700 systems on your network.
- PIN for each VSX/HDX/V500/V700 system. The PIN can consist of a maximum of eight numeric characters and is defined by the System Administrator.
- The key code that combines the Avaya option with any other Polycom options.
- If the VSX/HDX system has the multipoint option or IMCU option. If so, you must combine the Polycom Software License for this capability with the Avaya Option Polycom Software License to create a single Key Code to input into the unit.
- IP address of the voice system
- IP codec sets you want to use
- IP network regions you want to use

Configuring Polycom Endpoints

Use this procedure to configure the Video calling facility for all Polycom endpoint users.

Table 6: Configuring Polycom Endpoints

1	Enter **`display system-parameters customer-options`** to verify the Maximum Video Capable Stations (page 2 of screen). This number is provided by the RFA license file. The Maximum Video Capable Stations was determined using the following criteria: • Each V500/700 system is considered to be one station • Each single-point VSX/HDX system is considered to be one station • Each VSX multpoint system can be three to six stations Each HDX system can be three stations for multipoint plus four and seven for multipoint plus eight multipoint licensed options for the HDX9004. The HDX9002 only has multipoint plus 4 as an option.
2	Enter **`change cos`** to set Priority Video Calling (page 2 of screen) for the appropriate COS levels.
3	Enter **`add station`** to add a station for the Polycom system. Set the following parameters: • **Type** :H.323 • **Security Code** : the “pin” you will administer for the VSX, HDX, V500 or V700 system • **IP Video** : y • If you want this station to be able to make priority video calls, make sure you select a COS level that has Priority Video Calling enabled. (See Step 2) • On page 2 of the screen, set **Direct IP-IP Audio** Connections to y **Note:** You can create an alias for VSX/HDX stations.

Add Users/stations to Polycom endpoints

Use this procedure to add users/stations to the Polycom endpoints.

Table 7: Add users/stations to Polycom endpoints

1	Install the Polycom system and connect it to your network.
2	Upgrade the Polycom system software (if necessary).
3	Using a web browser, access the Polycom home page for the unit, and select **Admin Settings** > **Network** > **IP Network**.
4	Check the Enable IP H.323 check box.
5	Check the Display H.323 Extension check box.
6	In the H.323 Extension (E.164) box, enter the station number you specified for this system on the Avaya Communication Manager system.
7	From the Use Gatekeeper box, select Specify with PIN.
8	In the Gatekeeper IP Address box, enter the IP address of the CLAN or PCLAN followed by: 1719 (to specify the correct port to use).
9	In the Authentication PIN box, enter the security code you entered in Step 5.
10	In the Number box in the Gateway area, enter the extension you specified in Step 8.
11	Select the Enabled PVEC check box.
12	In the Type of Service box in the Quality of Service area, select the appropriate setting. Both IP Precedence and Diffserve are supported. Contact your Network Administrator for this information.
13	In the Type of Service Value boxes (Video, Audio, and Far End Camera Control), enter the QoS values for the IP Network Region settings in which the VSX/HDX station belongs.
14	Select the Dynamic Bandwidth check box.
15	From the Maximum Transmit Bandwidth box, select the setting that matches the Maximum Call Rate for Direct-IP Multimedia setting you specified for the Avaya Communication Manager system.
16	From the Maximum Receive Bandwidth box, select the setting that matches the Maximum Call Rate for Direct-IP Multimedia setting you specified for the Avaya Communication Manager system.
17	Complete the Firewall and Streaming sections as necessary.
18	When finished, click the Update button.
19	Repeat Steps 1 through 18 for each Polycom system.

Configuring Polycom RMX Series Video Conferencing Bridge Platform

Use this procedure to configure the Polycom RMX series video conferencing Bridge platform.

Table 8: Configuring Polycom RMX Series Video conferencing on Bridge Platform

1.	Enter **`change node-names ip`** to add an entry for the RMX system. Be sure to enter the IP address of the IP board for the RMX system.
2	Enter **`add trunk-group`** to add a two-way trunk group for the RMX system. Set the following parameters: • Group Type: **ISDN** • Direction: **Two-way** • Carrier Medium: **H.323** • Service Type: **Tie**
3	Enter **`add signaling-group`** to add a signaling group for the RMX system. Set the following parameters: • Group Type: **H.323** • IP Video: **y** • Priority Video. If you want all incoming calls to receive priority video transmissions: **y** • Trunk Group for Channel Selection to the two-way trunk group you added. • Near-end Node Name. **PROCR** may be used for all systems and **CLAN** may be used for systems with port networks. • Near-end Listen Port: **1720** • LRQ Required: **n** • RRQ Required: **y** • Enable Layer 3 Test: **n** • Far-end Node Name to the name you entered for the RMX system • Far-end Listen Port: **1720** • Far-end Network Region • Calls Share IP Signaling Connection: **n** • Direct IP-IP Audio Connections: **y** • IP Audio Hairpinning: **n**

Table 8: Configuring Polycom RMX Series Video conferencing on Bridge Platform

4	Use the **`change trunk-group n`** command (where n is the trunk group you added in Step 2) to add members to the trunk group. The number of members depends on the maximum simultaneous calls an RMX supports.
5	Use the **`change route-pattern n`** command (where nis the route pattern you want to use) to create a route pattern that points to the two-way trunk group.
6	Install the Polycom system and connect it to your network.
7	Upgrade the Polycom system software (if necessary).
8	Access the Polycom home page for the unit.
9	From the Setup menu, select the System Configuration tab.
10	Under the MCMS_PARAMETERS_USER, configure the following settings: • MCU_DISPLAY_NAME: **POLYCOM RMX-2000** • ENABLE_AUTO_EXTENSION: **YES** • NUMERIC_CONF_ID_LEN: **5** • CP_REGARD_TO_INCOMING_SETUP_RATE: **NO** • NUMERIC_CONF_ID_MAX_LEN: **8** • NUMERIC_CONF_ID_MIN_LEN: **4** • TERMINATE_CONF_AFTER_CHAIR_DROP: **NO** • H323_FREE_VIDEO_RESOURCES: **NO**
11	Under CS_MODULE_PARAMETERS, add:H245_TUNNELING: **YES**
12	Create an H.323 service, and enter the **CLAN** or **PROCR** IP address of the Communication Manager system as the primary gatekeeper. Confirm through a status signaling group that the RMX has registered.
13	Create a meeting room to use a test direct dial conference ID.

Configuring Ad-hoc Video Conferencing for a Polycom RMX Video Conferencing Bridge Platform

To configure Ad-hoc conferencing for a Polycom RMX video conferencing bridge platform, perform the following steps:

Table 9: Configuring Ad-hoc video for Polycom RMX video Conferencing Bridge Platform

1	Perform the procedures in the section Table 8: Configuring Polycom RMX Series Video conferencing on Bridge Platform on page 13 to configure the Polycom RMX system.
2	Enter **`display system-parameters customer-options`** to verify the Maximum Administered Ad-hoc video Conferencing Ports (page 2 of screen). The maximum number of Ad-hoc video conferencing ports allowed is the sum of the ports on your RMX systems. For example, if you have an RMX20 system and an RMX80 system, the maximum number of ports is 100.
3	Enter **`change cos`** to set Ad-hoc video Conferencing (page 2 of screen) for the appropriate COS levels.

Table 9: Configuring Ad-hoc video for Polycom RMX video Conferencing Bridge Platform

4	Use the **`add video-bridge`** command to configure a video bridge for the RMX system. Set the following parameters: • Name to the name for this video bridge (for example, Ad Hoc video Bridge - RMX). • Max Ports to the maximum number of Ad-hoc conferencing ports you want to assign to this bridge. (The minimum you can enter is 3.) This is equivalent to the number of ports for Ad-hoc use on the associated RMX. You can use Max Ports to limit the extent of Ad-hoc usage of an RMX and thereby reserve ports for scheduled usage • Trunk Groups to the administered two-way ISDN H.323 trunk groups you added . All entries must be of the same carrier type (that is, all H.323 trunks) • Far End Resource Info :**y** • ID Range to the range of ports. The IDs you specify on this form must NOT be configured on the RMX. You must leave these IDs free for the factory to create its own conferences there. Note that AAR and UDP are not used to connect to these meeting room numbers. Conference IDs (and factory numbers) are completely independent of the dial plan • Priority Factory Number. This number represents the Entry Queue created on the RMX and corresponds to a priority conference service level (for example, 784 Kbps). The Priority Factory Number must NEVER be in the conference ID range. If this field is left blank, all conferences can use the bridge. However, priority conferences will try to find a video bridge that has a priority factory (if there is one) • Standard Factory Number. This number represents the Entry Queue created on the RMX and corresponds to a standard conference service level (for example, 384 Kbps). The Standard Factory Number must NEVER be in the conference ID range. If this field is left blank, non-priority conferences cannot use this video bridge. A conference started by a priority user with non-priority users may be moved to a priority bridge, and the non-priority users will connect to it and receive video **Note:** You must specify either a Priority Factory Number or a Standard Factory Number. Do not leave both fields blank.
5	Create conference profiles for Ad-hoc (and Meeting Room) style conferences. **Note:** Ensure to choose Auto Layout under the video settings.
6	Create the two entry queues (one for Ad-hoc conferences, and one for priority conferences).

Table 9: Configuring Ad-hoc video for Polycom RMX video Conferencing Bridge Platform

7	For the Conference IVR Service, perform the following steps: • Under the Welcome tab, disable the Enable Welcome Messages check box • Under the Conference Chairperson tab, disable the Chairperson messages check box • Under the Conference Password tab, disable the Enable Password Messages check box
8	Under the General tab, perform the following steps: • Deselect any .wav file for the first to Join announcement • Disable roll call • Disable click and view
9	Under the IVR Service tab, click the music icon, and set a silence .wav file as the IVR message. A silence .wav file will disable music from being played to the first party who joins the conference. To create a silence .wav file: • Open the Windows Sound Recorder application. • From the File menu, select Save As • In the Save As dialog box, click Change • In the Name box, enter silence.wav • From the Format box, select PCM • From the Attributes box, select 16.00 kHz, 16 Bit, Mono • Click OK

Display Capacity for Ad-hoc video Conferencing.

To display the capacity for Ad-hoc video conferencing on the Communication Manager system:

Table 10: Display capacity for Ad-hoc video conferencing.

1	Use the display capacity command to access the System Capacity form.
2	Go to page 7. Ad-hoc video Conferencing Ports displays the following Ad-hoc video conferencing information: • Used: **The number of video conferencing ports currently in use** • Available: **The number of video conferencing ports currently available** • System Limit: the total number of video conference ports in your system. (This is the sum of Used ports and available ports)

Administering Polycom PathNavigator/ CMA Gatekeepers

Perform the following steps to configure a Polycom PathNavigator/CMA Gatekeepers:

Table 11: Administering Polycom PathNavigator/ CMA Gatekeepers

1	Use the **`change ip-codec-set 1`** command to set the following parameters: • Allow Direct-IP Multimedia to y (page 2 of screen). • Maximum Call Rate for Direct-IP Multimedia. This setting is the combined audio and video transmit rate or receive rate for non-priority (normal) video calls. You can use this setting to limit the amount of bandwidth used for normal video calls. For example, if you select 384 Kbits, a maximum of 384 Kbits will be used to transmit and to receive audio/video • Maximum Call Rate for Priority Direct-IP Multimedia. This setting is the combined audio and video transmit rate or receive rate for priority video calls. You can use this setting to limit the amount of bandwidth used for priority video calls. For example, if you select 384 Kbits, a maximum of 384 Kbits will be used to transmit and to receive audio/video
2	Use the **`change ip-network-region`** command to put the gatekeeper in its own network region. Set the following parameters: • Intra-region IP-IP Direct Audio: **NO** • Inter-region IP-IP Direct Audio: **NO** • Security Procedures 1 to any-auth (page 2 of screen) • video Norm (page 3 of screen) to the amount of bandwidth that you want to allocate for the normal video pool to each IP network region • video Prio (page 3 of screen) to the amount of bandwidth that you want to allocate for the priority video pool to each IP network region • video Shr (page 3 of screen). Specify whether the normal video pool can be shared for each link between IP network regions
3	Enter **`change node-names ip`** to add an entry for the Polycom PathNavigator gatekeeper. Be sure to enter the IP address of the IP board for the gatekeeper.

Table 11: Administering Polycom PathNavigator/ CMA Gatekeepers

4	Use the **`add signaling-group`** command to add a signaling group for the gatekeeper. Set the following parameters: • Group Type: **H.323** • IP video: **y** • Priority video. If you want all incoming calls to receive priority video transmissions, select **y** • Near-end Listen Port: **1719** • LRQ Required: **y** • Far-end Node Name to the name you entered for the gatekeeper in Step 3. • Far-end Listen Port: **1719** • Far-end Network Region to the IP network region you specified in Step 2. • Direct IP-IP Audio Connections: **y** • IP Audio Hairpinning: **y**
5	Use the add trunk-group command to add a trunk group for the gatekeeper. Set the following parameters: • Group Type: **ISDN** • Carrier Medium: **IP** • Add members to this trunk group
6	Use the **`change signaling-group n`** command (where n is the signaling group you added in Step 4) to set Trunk Group for Channel Selection to the trunk group you added in Step 5.
7	Create a route pattern to the gatekeeper.
8	Configure the gatekeeper.

Configuring Avaya one-X® Communicator

Avaya one-X® Communicator can be configured with either SIP or H.323 protocol. Ensure the check box corresponding to **Enable Video** is selected on the endpoint. To configure one-X Communicator using SIP or H.323 protocol, see *Avaya one-X® Communicator Getting Started Guide*.